MATHEMATICA, Tome 54 (77), N° 2, 2012, pp. 181–194

IDEMPOTENTS IN GROUP ALGEBRAS

GABRIELA OLTEANU

Abstract. In this survey we collect and present the classical and some recent methods to compute the primitive (central) idempotents in semisimple group algebras.

MSC 2000. 20C05, 20C15, 16S34, 16U60.

Key words. Idempotents, group algebras, group rings, Wedderburn decomposition, group codes.

1. INTRODUCTION

The knowledge of the idempotents in a group algebra represents a useful information for various problems like the study of the group of units in orders of the group algebra as was done by Ritter and Sehgal [RS91], by Jespers and Leal [JL93], by Jespers and del Río [JdR00], by Jespers, Olteanu, del Río and Van Gelder [JOdRVG]), the computation of the Wedderburn decomposition of a semisimple group algebra done by Olteanu [Olt07], or the description of the automorphism group of o group algebra done by Herman [Her97], by Olivieri, del Río and Simón [OdRS06]. A good description of the primitive central idempotents was proved to be also useful for proving results like the one of Perlis–Walker [PW50] which states that the rational group algebra of a finite abelian group A determines, up to isomorphism, the group A.

Finding explicit expressions of the primitive central idempotents in a rational group algebra $\mathbb{Q}G$ using alternative methods of the classical one, character-free methods or methods which do not involve computation in extensions of the rationals was a problem studied by several authors, for example by Ayoub and Ayoub[AA69], Jespers, Leal and Paques [JLP03], Olivieri, del Río and Simón [OdRS04], Jespers, Olteanu and del Río [JOdR12], Janssens [Jan12], Bakshi and Passi [BP12], Bakshi, Kulkarni and Passi [BKP12]. The case of a finite semisimple group algebra was also studied by Broche and del Río [BdR07], Bakshi, Gupta and Passi [BGP12], Bakshi and Raka [BR03], Ferraz and Polcino Milies [FP07] with the possibility to apply some of these results in coding theory. Some of these methods were also implemented in a package called `wedderga` [Wedderga09] of the computer algebra system GAP [GAP].

The primitive idempotents in a simple component of a semisimple group algebra were also studied by Jespers, Olteanu and del Río [JOdR12], Olteanu

The research has been partially supported by the grant PN-II-RU-TE-2009-1 project ID_303.

and Van Gelder [VGO11] with a special interest for the applications in units of integral group rings.

We shall collect and present the classical and some recent methods to compute the primitive (central) idempotents in a semisimple group algebra over a finite field or over the rationals.

2. PRELIMINARIES

We introduce some useful notation and results, mainly from [JLP03] and [OdRS04]. 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 $N_G(K)/K$.

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 [Sho33] or [CR62, 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 [Hup98, Theorem 24.3]) and in [OdRS04] it is proved that it is even strongly monomial. We will use these results in order to study the primitive (central) idempotents of group algebras for some abelian-by-supersolvable groups, including finite nilpotent groups.

Now we focus on finite fields. First, we introduce some notations and results from [BdR07]. Let $\mathbb{F} = \mathbb{F}_{q^m}$ denote a finite field of characteristic q with q^m elements, for q a prime and m a positive integer, and G a finite group of order n such that $\mathbb{F}G$ is semisimple, that is $(q, n) = 1$. We fix an algebraic closure of $\mathbb{F}$, denoted by $\overline{\mathbb{F}}$. For every positive integer k coprime with q, ξ_k denotes a primitive kth root of unity in $\overline{\mathbb{F}}$ and o_k denotes the multiplicative order of q^m modulo k. Recall that $\mathbb{F}(\xi_k) \simeq \mathbb{F}_{q^{mo_k}}$, the field of order q^{mo_k}.

Let $\mathcal{Q}$ denote the subgroup of $\mathbb{Z}_n^*$, the group of units of the ring $\mathbb{Z}_n$, generated by the class of q^m and consider $\mathcal{Q}$ acting on G by $s \cdot g = g^s$. The q^m-cyclotomic classes of G are the orbits of G under the action of $\mathcal{Q}$ on G. Let G^* be the group of irreducible characters in $\overline{\mathbb{F}}$ of G. Now let $\mathcal{C}(G)$ denote the set of q^m-cyclotomic classes of G^*, which consist of linear faithful characters of G.

Let $K \trianglelefteq H \leq G$ be such that H/K is cyclic of order k and $C \in \mathcal{C}(H/K)$. If $\chi \in C$ and $\mathrm{tr} = \mathrm{tr}_{\mathbb{F}(\xi_k)/\mathbb{F}}$ denotes the field trace of the Galois extension $\mathbb{F}(\xi_k)/\mathbb{F}$, then we set

$$\varepsilon_C(H, K) = |H|^{-1} \sum_{h \in H} \mathrm{tr}(\chi(hK))h^{-1} = [H : K]^{-1}\widetilde{K} \sum_{X \in H/K} \mathrm{tr}(\chi(X))h_X^{-1},$$

where h_X denotes a representative of $X \in H/K$. Note that $\varepsilon_C(H, K)$ does not depend on the choice of $\chi \in C$. Furthermore, $e_C(G, H, K)$ denotes the sum of the different G-conjugates of $\varepsilon_C(H, K)$. Note that the elements $\varepsilon_C(H, K)$ will occur later as the building blocks for the primitive central idempotents of finite group algebras.

If H is a subgroup of G, ψ a linear character of H and $g \in G$, then ψ^g denotes the character of H^g given by $\psi^g(h^g) = \psi(h)$. This defines an action of G on the set of linear characters of subgroups of G. Note that if $K = \mathrm{Ker}\,\psi$, then $\mathrm{Ker}\,\psi^g = K^g$ and therefore the rule $\psi \mapsto \psi^g$ defines a bijection between the set of linear characters of H with kernel K and the set of linear characters of H^g with kernel K^g. This bijection maps q^m-cyclotomic classes to q^m-cyclotomic classes and hence induces a bijection $\mathcal{C}(H/K) \to \mathcal{C}(H^g/K^g)$. The image of $C \in \mathcal{C}(H/K)$ under this map is denoted as C^g. The following equality is obvious

$$\varepsilon_C(H, K)^g \quad = \quad \varepsilon_{C^g}(H^g, K^g).$$

Let $K \trianglelefteq H \leq G$ be such that H/K is cyclic. Then the action from the previous paragraph induces an action of $N = N_G(H) \cap N_G(K)$ on $\mathcal{C}(H/K)$ and it is easy to see that the stabilizer of a cyclotomic class in $\mathcal{C}(H/K)$ is independent of the cyclotomic class. We denote by $E_G(H/K)$ the stabilizer of such (and thus of any) cyclotomic class in $\mathcal{C}(H/K)$ under this action.

Remark 2.1. The set $E_G(H/K)$ can be determined without the need to use characters. Let $K \trianglelefteq H \leq G$ be such that H/K is cyclic. Then $N =$

$N_G(H) \cap N_G(K)$ acts on H/K by conjugation and this induces an action of N on the set of q^m-cyclotomic classes of H/K. It is easy to verify that the stabilizers of all the q^m-cyclotomic classes of H/K containing generators of H/K are equal and coincide with $E_G(H/K)$.

There is a strong connection between the elements $\varepsilon(H,K)$ and $\varepsilon_C(H,K)$ given in the following Lemma from [BdR07].

Lemma 2.2. *Let $\mathbb{Z}_{(q)}$ denote the localization of $\mathbb{Z}$ at q. We identify $\mathbb{F}_q$ with the residue field of $\mathbb{Z}_{(q)}$, denote with $\overline{x}$ the projection of $x \in \mathbb{Z}_{(q)}$ in $\mathbb{F}_q \subseteq \mathbb{F}$ and extend this notation to the projection of $\mathbb{Z}_{(q)}G$ onto $\mathbb{F}_qG \subseteq \mathbb{F}G$.*

1. *Let $K \trianglelefteq H \leq G$ be such that H/K is cyclic. Then*
$$\overline{\varepsilon(H,K)} = \sum_{C \in \mathcal{C}(H/K)} \varepsilon_C(H,K).$$
2. *Let $K \leq H \trianglelefteq N_G(K)$ be such that H/K is cyclic and R a set of representatives of the action of $N_G(K)$ on $\mathcal{C}(H/K)$. Then*
$$\overline{e(G,H,K)} = \sum_{C \in R} e_C(G,H,K).$$

Remark 2.3. From [BdR07, Theorem 7], we know that there is a strong relation between the primitive central idempotents in a rational group algebra $\mathbb{Q}G$ and the primitive central idempotents in a finite group algebra $\mathbb{F}G$ that makes use of the strong Shoda pairs of G. Hence, if X is a set of strong Shoda pairs of G and every primitive central idempotent of $\mathbb{Q}G$ is of the form $e(G,H,K)$ for $(H,K) \in X$, then every primitive central idempotent of $\mathbb{F}G$ is of the form $e_C(G,H,K)$ for $(H,K) \in X$ and $C \in \mathcal{C}(H/K)$, as one can see in Section 4.

3. PRIMITIVE CENTRAL IDEMPOTENTS IN RATIONAL GROUP ALGEBRAS

The classical method used for the computation of the primitive central idempotents of $\mathbb{Q}G$ starts by calculating the primitive central idempotents $e(\chi)$ of $\mathbb{C}G$ associated to the irreducible (complex) characters χ of G, for which there is a well known formula given by
$$e(\chi) = \frac{\chi(1)}{|G|} \sum_{g \in G} \chi(g^{-1})g$$
and continues by summing up all the primitive central idempotents of the form $e(\sigma \circ \chi)$ with $\sigma \in \mathrm{Gal}(F(\chi)/F)$.

Proposition 3.1. [Yam73, Proposition 1.1] *For G a finite group and χ an irreducible complex character of G, $e_F(\chi)$ is given by the formula*
$$e_F(\chi) = \sum_{\sigma \in \mathrm{Gal}(F(\chi)/F)} e(\chi^\sigma) \tag{1}$$
where χ^σ is the character of G given by $\chi^\sigma(g) = \sigma(\chi(g))$, for $g \in G$.

The primitive (central) idempotents of $\mathbb{Q}A$ for A abelian are well known (see [AA69], [GJP96] or [PW50]). A description in terms of the idempotents of the form $\varepsilon(A,H)$ has been given by Jespers, Leal and Paques.

PROPOSITION 3.2. [JLP03, Corollary 2.1] *If A is an abelian group, then the primitive central idempotents of $\mathbb{Q}A$ are the elements of the form $\varepsilon(A,H)$ where H is a subgroup of A such that A/H is cyclic.*

An alternative method to compute the primitive central idempotents of $\mathbb{Q}G$, for G a finite nilpotent group, that does not use the character table of G has been introduced by Jespers, Leal and Paques [JLP03].

THEOREM 3.3. [JLP03, Theorem 2.1] *Let G be a finite nilpotent group. The primitive central idempotents of $\mathbb{Q}G$ are precisely all elements of the form*

$$\sum_g (\varepsilon(G_m, H_m))^g$$

(the sum of all G-conjugates of $\varepsilon(G_m,H_m)$), where H_m and G_m are subgroups of G that satisfy all of the following properties:

(1) *$H_0 \subseteq H_1 \subseteq \cdots \subseteq H_m \subseteq G_m \subseteq \cdots \subseteq G_1 \subseteq G_0 = G$;*
(2) *for $0 \leq i \leq m$, H_i is a normal subgroup of G_i and $Z(G_i/H_i)$ is cyclic;*
(3) *for $0 \leq i < m$, G_i/H_i is not abelian, and G_m/H_m is abelian;*
(4) *for $0 \leq i < m$, $G_{i+1}/H_i = C_{G_i/H_i}(Z_2(G_i/H_i))$, where $Z_2(G_i/H_i)$ is the second center of G_i/H_i and $C_{G_i/H_i}(Z_2(G_i/H_i))$ is the centralizer of $Z_2(G_i/H_i)$;*
(5) *for $1 \leq i \leq m$, $\bigcap_{x \in G_{i-1}/H_{i-1}} H_i^x = H_{i-1}$.*

Olivieri, del Río and Simón pointed out that this method relies on the fact that nilpotent groups are monomial and, using a theorem of Shoda [Sho33], they gave an alternative presentation. This method was generalized and improved in [OdRS04] and it was given 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 Shoda pairs of the group G, that are 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. This method is applicable to all abelian-by-supersolvable finite groups, in particular to finite nilpotent groups.

THEOREM 3.4. [OdRS04, Theorem 2.1] *Let G be a finite group, H a subgroup of G, ψ a linear character of H and ψ^G the induced character of ψ on G. If ψ^G is irreducible, then the primitive central idempotent of $\mathbb{Q}G$ associated to ψ^G is*

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

where K is the kernel of ψ.

Moreover, if the character ψ from the previous theorem is a linear character of H with kernel K and (H,K) is a strong Shoda pair, then $e_{\mathbb{Q}}(\psi^G) = e(G,H,K)$, that is, if we denote the coefficient $\alpha = \frac{[\mathrm{Cen}_G(\varepsilon(H,K)):H]}{[\mathbb{Q}(\psi):\mathbb{Q}(\psi^G)]}$ and (H,K) is a strong Shoda pair then $\alpha = 1$ (see [OdRS04, Theorem 4.4]).

This method was implemented in a computer GAP package called `wedderga` [Wedderga09]. This package includes a function for the computation of the primitive central idempotents in semisimple group algebras using characters, named `PrimitiveCentralIdempotentsByCharacterTable`. The function using strong Shoda pairs is called `PrimitiveCentralIdempotentsByStrongSP`.

For groups that are not monomial, only for very few has been obtained a character-free description of the primitive central idempotents of the corresponding rational group algebra. In [GJ98] this is done for alternating groups. In [BP12] is provided an explicit description of the primitive central idempotents of a group algebra $\mathbb{Q}G$ associated to complex irreducible characters of G having a property called $\mathcal{P}$. A complex irreducible character χ of a finite group G , with affording representation ρ, said to have property $\mathcal{P}$ if, for every $g \in G$, either $\chi(g) = 0$ or all eigenvalues of $\rho(g)$ have the same order. The following result gives equivalent conditions for a character χ to have the property $\mathcal{P}$.

Proposition 3.5. [BP12, Theorem 1] *Let χ be an irreducible complex character of the finite group G with ρ a representation of G affording χ. For $g \in G$, the following are equivalent:*

(i) *All the eigenvalues of $\rho(g)$ have the same order;*
(ii) *$\overline{\chi}|_{\langle \mathrm{Ker}(\chi)g\rangle}$ is a sum of faithful irreducible characters of $\langle \mathrm{Ker}(\chi)g\rangle$, where $\overline{\chi}$ is the character of the representation $\overline{\rho}$ of $G/\mathrm{Ker}(\chi)$;*
(iii) *$\overline{\rho}$ maps all primitive central idempotents of the rational group algebra $\mathbb{Q}\langle \mathrm{Ker}(\chi)g\rangle$ to zero, except the idempotent $\varepsilon(\langle \mathrm{Ker}(\chi)g\rangle, 1)$, which gets mapped to the identity matrix.*

An explicit description of the primitive central idempotents of a group algebra $\mathbb{Q}G$ associated to complex irreducible characters of G having the property $\mathcal{P}$ is given in the following result.

Theorem 3.6. [BP12, Theorem 1] *Let χ be a complex irreducible character of a finite group G with affording representation ρ such that for every $g \in G$, either $\chi(g) = 0$ or all eigenvalues of $\rho(g)$ have the same order. Then the primitive central idempotent $e_{\mathbb{Q}}(\chi)$ of $\mathbb{Q}G$ associated with χ is given by*

$$e_{\mathbb{Q}}(\chi) = \frac{1}{\sum_{g\in G,\chi(g)\neq 0}\left(\frac{\mu(d(g))}{\varphi(d(g))}\right)^2} \sum_{g\in G,\chi(g)\neq 0} \frac{\mu(d(g))}{\varphi(d(g))} g,$$

where, for $g \in G$, $d(g)$ denotes the order of g modulo $\mathrm{Ker}(\chi)$, and μ and φ are the Möbius and the Euler's function respectively.

Remember that for any integer $n \geq 1$, $\varphi(n)$ denotes the number of integers i, $1 \leq i \leq n$ such that $\gcd(i, n) = 1$, and

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^r, & \text{if } n \text{ is square-free and is a product of } r \text{ distinct primes;} \\ 0, & \text{if } n \text{ is not square-free.} \end{cases}$$

The previous theorem is applied in [BP12] in order to explicitly write the primitive central idempotents in the rational group algebra of an extra-special p-group, a CM_{p-1}-group, a nilpotent group of class ≤ 2 and those associated with some monomial characters.

For arbitrary finite groups G, it has remained an open problem to give a character-free description of the primitive central idempotents of $\mathbb{Q}G$. In [JOdR12] it is proved 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.

Proposition 3.7. [JOdR12, 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.

Notice that the formula from Proposition 3.7 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 from Theorem 3.4 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. The previous formula does not give a bound for the integers a_i used in the previous proposition and on the pairs of groups (H_i, K_i) that one has to consider in the description of $e_{\mathbb{Q}}(\chi)$.

In [Jan12] a similar description of the primitive central idempotents e of $\mathbb{Q}G$ is given for arbitrary finite groups G with a better control of the coefficients done by the use of the Artin Induction Theorem.

Theorem 3.8. [Jan12, Theorem 2] *Let G be a finite group, χ an irreducible complex character of G and $C_i = \langle c_i \rangle$. Then*

$$e_{\mathbb{Q}}(\chi) = \sum_{i=1}^{r} \frac{b_{C_i}\chi(1)}{[G : \mathrm{Cen_G(\varepsilon(C_i, C_i))}]} e(G, C_i, C_i) = \sum_{i=1}^{r} \frac{b_{C_i}\chi(1)}{[G : C_i]} \left(\sum_{k=1}^{m_i} \varepsilon(C_i, C_i)^{g_{ik}} \right),$$

where the sum runs through a set $\{C_1, \ldots, C_r\}$ of representatives of conjugacy classes of cyclic subgroups of G and

$$b_{C_i} = \frac{[G : \mathrm{Cen_G(c_i)}]}{[G : C_i]} \sum_{C_i^* \geq C_i} \mu\left([C_i^* : C_i]\right) \left(\sum_{\sigma \in G_\chi} \sigma(\chi) \right) (z^*),$$

where the sum runs through all the cyclic subgroups C_i^* of G which contain C_i and z^* is a generator of C_i^*.

An alternative approach is used in [BKP12] for the computation of an explicit expression for the primitive central idempotents of the rational group algebra of a finite group G associated with an irreducible complex character of G. For any integer $d \geq 1$, $g \in G$ and an irreducible complex character χ of a finite group G afforded by a representation ρ, denote by $\nu_d^\chi(g)$ the number of eigenvalues of $\rho(g)$ of order d.

Theorem 3.9. [BKP12, Theorem 1] *Let χ an irreducible complex character of a finite group G. The primitive central idempotent $e_{\mathbb{Q}}(\chi)$ of $\mathbb{Q}G$ associated to χ is given by*

$$e_{\mathbb{Q}}(\chi) = \frac{\chi(1)}{\sum_{g \in G, \chi(g) \neq 0} \sum_{d|n} \left(\frac{\nu_d^\chi(g)\mu(d)}{\varphi(d)} \right)^2} \sum_{g \in G, \chi(g) \neq 0} \sum_{d|n} \frac{\nu_d^\chi(g)\mu(d)}{\varphi(d)} g.$$

4. PRIMITIVE CENTRAL IDEMPOTENTS IN FINITE GROUP ALGEBRAS

The computation of the primitive (central) idempotents in finite semisimple group algebras provides useful information for the computation of the Wedderburn decomposition of the group algebras and can have applications in coding theory (see for example [PA96], [KS01], [BR03], [FP07]).

In [BdR07, Theorem 7] is given a description of the primitive central idempotents of a finite group algebra and the Wedderburn decomposition of the corresponding simple components for those idempotents coming from Shoda pairs of the finite group G. This is implemented in the package `wedderga`.

Theorem 4.1. [BdR07, Theorem 7] *Let G be a finite group and F a finite field such that FG is semisimple.*

1. *Let (H, K) be a strongly Shoda pair of G and $C \in \mathcal{C}(H/K)$. Then $e_C(G, H, K)$ is a primitive central idempotent of FG and*

$$FGe_C(G, H, K) \simeq M_{[G:H]}(F_{q^{o/[E:H]}}),$$

   where $E = E_G(H/K)$ and o is the multiplicative order of q module $[H : K]$.
2. *Let X be a set of strongly Shoda pairs of G. If every primitive central idempotent of $\mathbb{Q}G$ is of the form $e(G, H, K)$ for $(H, K) \in X$ then every primitive central idempotent of FG is of the form $e_C(G, H, K)$ for $(H, K) \in X$ and $C \in \mathcal{C}(H/K)$.*

For abelian-by-supersolvable groups which have all primitive central idempotents of this kind we have the following result as consequence.

Theorem 4.2. [BdR07, Corollary 8] *If G is an abelian-by-supersolvable group and $\mathbb{F}$ is a finite field of order q^m such that $\mathbb{F}G$ is semisimple, then every primitive central idempotent of $\mathbb{F}G$ is of the form $e_C(G,H,K)$ for (H,K) a strong Shoda pair of G and $C \in \mathcal{C}(H/K)$. Furthermore, for every strong Shoda pair (H,K) of G and every $C \in \mathcal{C}(H/K)$,*

$$\mathbb{F}Ge_C(G,H,K) \simeq M_{[G:H]}(\mathbb{F}_{q^{mo/[E:K]}}),$$

where $E = E_G(H/K)$ and o is the multiplicative order of q^m modulo $[H:K]$.

In [BGP12, Theorem 1] is explicitly computed a complete set of primitive central idempotents of a semisimple group algebra F_qG, where G is a group of order p_1p_2 with p_1, p_2 primes and F_q denotes a finite field of order q coprime to p_1p_2. This result may be compared with the particular case provided by [BdR07, Corollary 9].

5. PRIMITIVE IDEMPOTENTS IN SIMPLE COMPONENTS OF SEMISIMPLE RATIONAL GROUP ALGEBRAS

Now we show an effective method to calculate a complete set of orthogonal primitive idempotents of $\mathbb{Q}G$ for G a finite nilpotent group given in [JOdR12]. Since G is abelian-by-supersolvable and hence strongly monomial, it follows from [OdRS04, 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.

Theorem 5.1. [JOdR12, 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

$$T_{2'} = \{1, a_{2'}, a_{2'}^2, \dots, a_{2'}^{[N_{2'}:H_{2'}]-1}\},$$

$T_{G/N}$ 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*

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

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

$$\begin{aligned}\langle \overline{a_2}, \overline{b_2}, \overline{c_2} \quad | \quad & \overline{a_2}^{2^n} = \overline{b_2}^{2^k} = 1,\ \overline{c_2}^2 = 1,\ \overline{a_2}^{\overline{b_2}} = \overline{a_2}^r, \\ & \overline{a_2}^{\overline{c_2}} = \overline{a_2}^{-1},\ [\overline{b_2}, \overline{c_2}] = 1\rangle,\end{aligned}$$

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*

$$\begin{aligned}\langle \overline{a_2}, \overline{b_2}, \overline{c_2} \quad | \quad & \overline{a_2}^{2^n} = \overline{b_2}^{2^k} = 1,\ \overline{c_2}^2 = \overline{a_2}^{2^{n-1}},\ \overline{a_2}^{\overline{b_2}} = \overline{a_2}^r, \\ & \overline{a_2}^{\overline{c_2}} = \overline{a_2}^{-1},\ [\overline{b_2}, \overline{c_2}] = 1\rangle,\end{aligned}$$

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) $\beta_2 = \widehat{b_2}\frac{1 + x a_2^{2^{n-2}} + y a_2^{2^{n-2}} c_2}{2}$ *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 $n-k > 2$.

The given explicit and character-free construction of a complete set of orthogonal primitive idempotents of a rational group algebra of a finite nilpotent group allows 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 of [JOdR12, Theorem 4.5] one obtains 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 [JOdRVG] it is shown an explicit construction of a complete set of orthogonal primitive idempotents of $\mathbb{Q}G$, for a class of groups inside the finite strongly monomial groups, namely groups G for which the simple components $\mathbb{Q}G$ are determined by a strong Shoda pair (H, K) such that $\tau(nH, n'H) = 1$ for all $n, n' \in N_G(K)$. The construction is based on the isomorphism of Theorem 5.2 on classical crossed products with trivial twisting. Hence, when the twisting τ is cohomologicaly trivial, the classical crossed product is isomorphic to a matrix algebra over its center. Moreover, when $\tau = 1$ we get an explicit isomorphism. More precisely, denoting the matrix associated to an endomorphism f in a basis B as $[f]_B$, we have

THEOREM 5.2. [Rei75, Corollary. 29.8] *Let L/F be a finite Galois extension and $n = [L : F]$. The classical crossed product $(L/F, 1)$ is isomorphic to $M_n(F)$ as F-algebra. Moreover, an isomorphism is given by*

$$\begin{array}{rcccc} \psi : (L/F,1) & \to & \mathrm{End}_F(L) & \to & M_n(F) \\ xu_\sigma & \mapsto & x' \circ \sigma & \mapsto & [x' \circ \sigma]_B, \end{array}$$

for $x \in L$, $\sigma \in \mathrm{Gal}(L/F)$, B an F-basis of L and where x' denotes multiplication by x on L.

A basis of $\mathbb{Q}(\zeta_{[H:K]})/\mathbb{Q}(\zeta_{[H:K]})^{N_G(K)/H}$ is of the form $\{w^x \mid x \in N_G(K)/H\}$ with $w \in \mathbb{Q}(\zeta_{[H:K]})$. By a general theory we know that this exists. If E/F is a finite Galois extension, then by the Normal Basis Theorem, there exists an element $w \in E$ such that $\{\sigma(w) \mid \sigma \in \mathrm{Gal}(E/F)\}$ is an F-basis of E, a so-called normal basis, whence w is called normal in E/F.

THEOREM 5.3. [JOdRVG, Theorem 4.1] *Let (H, K) be a strong Shoda pair of a finite group G such that $\tau(nH, n'H) = 1$ for all $n, n' \in N_G(K)$. Let $\varepsilon = \varepsilon(H, K)$ and $e = e(G, H, K)$. Let F denote the fixed field of $\mathbb{Q}H\varepsilon$ under the natural action of $N_G(K)/H$ and $[N_G(K) : H] = n$. Let w be a normal element of $\mathbb{Q}H\varepsilon/F$ and B the normal basis determined by w. Let ψ be the isomorphism between $\mathbb{Q}N_G(K)\varepsilon$ and the matrix algebra $M_n(F)$ with respect to the basis B as stated in Theorem 5.2. Let $P, A \in M_n(F)$ be the matrices*

$$P = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & -1 & 0 \\ 1 & 0 & 0 & \cdots & 0 & -1 \end{pmatrix} \quad \textit{and} \quad A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}.$$

A complete set of orthogonal primitive idempotents of $\mathbb{Q}Ge$ is formed by the set

$$\{x\widehat{T_1}\varepsilon x^{-1} \mid x \in T_2 \langle x_e \rangle\},$$

where $x_e = \psi^{-1}(PAP^{-1})$, T_1 is a transversal of H in $N_G(K)$ and T_2 is a right transversal of $N_G(K)$ in G. By $\widehat{T_1}$ we denote the element $\frac{1}{|T_1|}\sum_{t \in T_1} t$ in $\mathbb{Q}G$.

The previous result allows a description of a complete set of matrix units in a simple component $\mathbb{Q}Ge(G, H, K)$ for a strong Shoda pair (H, K) of a finite group G such that $\tau(nH, n'H) = 1$ for all $n, n' \in N$.

6. PRIMITIVE IDEMPOTENTS IN SIMPLE COMPONENTS OF SEMISIMPLE FINITE GROUP ALGEBRAS

Finite group algebras and their Wedderburn decomposition are not only of interest in pure algebra, they also have applications in coding theory. Cyclic codes can be realized as ideals of group algebras over cyclic groups [HP98] and many other important codes appear as ideals of noncyclic group algebras [HP98, ESL95]. In particular, the Wedderburn decomposition is used to compute idempotent generators of minimal abelian codes [FP07]. Using a complete set of orthogonal primitive idempotents, one would be able to construct all left G-codes, i.e. left ideals of the finite group algebra FG, which is a much richer class then the (two-sided) G-codes [OVG13].

In [VGO11] is provided a complete set of orthogonal primitive idempotents in a simple algebra of type FGe for e a primitive central idempotent of the semisimple finite group algebra FG for G a finite nilpotent group. It is used the description of the primitive central idempotents and the simple components for abelian-by-supersolvable groups, given in [BdR07].

Theorem 6.1. [VGO11, Theorem 3.3] *Let $\mathbb{F}$ be a finite field of order q^m and G a finite nilpotent group such that $\mathbb{F}G$ is semisimple. Let (H,K) be a strong Shoda pair of G, $C \in \mathcal{C}(H/K)$ and set $e_C = e_C(G,H,K)$, $\varepsilon_C = \varepsilon_C(H,K)$, $H/K = \langle \overline{a} \rangle$, $E = E_G(H/K)$. Let E_2/K and $H_2/K = \langle \overline{a_2} \rangle$ (respectively $E_{2'}/K$ and $H_{2'}/K = \langle \overline{a_{2'}} \rangle$) denote the 2-parts (respectively $2'$-parts) of E/K and H/K respectively. Then $\langle \overline{a_{2'}} \rangle$ has a cyclic complement $\langle \overline{b_{2'}} \rangle$ in $E_{2'}/K$.*

A complete set of orthogonal primitive idempotents of $\mathbb{F}Ge_C$ consists of the conjugates of $\beta_{e_C} = \widetilde{b_{2'}}\beta_2\varepsilon_C$ by the elements of $T_{e_C} = T_{2'}T_2T_E$, where $T_{2'} = \{1, a_{2'}, a_{2'}^2, \dots, a_{2'}^{[E_{2'}:H_{2'}]-1}\}$, T_E denotes a right transversal of E 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 E_2/K then $\beta_2 = \widetilde{M_2}$. Moreover, if M_2/K is cyclic, then there exists $b_2 \in E_2$ such that E_2/K is given by the following presentation*

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

and if M_2/K is not cyclic, then there exist $b_2, c_2 \in E_2$ such that E_2/K is given by the following presentation

$$\begin{aligned} \langle \overline{a_2}, \overline{b_2}, \overline{c_2} \quad \mid \quad & \overline{a_2}^{2^n} = \overline{b_2}^{2^k} = \overline{c_2}^2 = 1, \overline{a_2}^{\overline{b_2}} = \overline{a_2}^r, \\ & \overline{a_2}^{\overline{c_2}} = \overline{a_2}^{-1}, [\overline{b_2}, \overline{c_2}] = 1 \rangle, \end{aligned}$$

with $r \equiv 1 \mod 4$ (or equivalently $\overline{a_2}^{2^{n-2}}$ is central in E_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 E_2/K (unless $n \leq 1$) and M_2/K is cyclic; and*

(ii) *$T_2 = \{1, a_2, a_2^2, \dots, a_2^{d/2-1}, a_2^{2^{n-2}}, a_2^{2^{n-2}+1}, \dots, a_2^{2^{n-2}+d/2-1}\}$, where $d = [E_2 : H_2]$, otherwise.*

(2) *If H_2/K has no complement in E_2/K, then there exist $b_2, c_2 \in E_2$ such that E_2/K is given by the following presentation*

$$\begin{aligned} \langle \overline{a_2}, \overline{b_2}, \overline{c_2} \quad \mid \quad & \overline{a_2}^{2^n} = \overline{b_2}^{2^k} = 1, \overline{c_2}^2 = \overline{a_2}^{2^{n-1}}, \overline{a_2}^{\overline{b_2}} = \overline{a_2}^r, \\ & \overline{a_2}^{\overline{c_2}} = \overline{a_2}^{-1}, [\overline{b_2}, \overline{c_2}] = 1 \rangle, \end{aligned}$$

with $r \equiv 1 \mod 4$. *In this case,* $\beta_2 = \widetilde{b_2}\frac{1+xa_2^{2^{n-2}}+ya_2^{2^{n-2}}c_2}{2}$ *and*

$$T_2 = \{1, a_2, a_2^2, \dots, a_2^{2^k-1}, c_2, c_2a_2, c_2a_2^2, \dots, c_2a_2^{2^k-1}\},$$

with $x, y \in \mathbb{F}$ *and* $y \neq 0$, *satisfying* $x^2 + y^2 = -1$.

Theorem 6.1 provides a straightforward implementation in a programming language, for example in GAP [GAP]. Computations involving strong Shoda pairs and primitive central idempotents are already provided in the GAP package Wedderga [Wedderga09].

REFERENCES

[AA69] Ayoub, R.G. and Ayoub, C., *On the group ring of a finite abelian group*, Bull. Aust. Math. Soc., **1** (1969), 245–261.

[BdR07] Broche, O. and del Río, Á., *Wedderburn decomposition of finite group algebras*, Finite Fields Appl., **13** (2007), 71–79.

[BGP12] Bakshi, G.K., Gupta, S. and Passi, I.B.S., *Semisimple metacyclic group algebras*, Proc. Indian Acad. Sci. Math. Sci., **121** (2012), 379–396.

[Wedderga09] Broche, O., Konovalov, A., Olteanu, G., Olivieri, A. and del Río, Á., *Wedderga–Wedderburn Decomposition of Group Algebras*, Version 4.3.3 (2009). `http://www.gap-system.org/Packages/wedderga.html`

[BKP12] Bakshi, G.K., Kulkarni, R.S. and Passi, I.B.S., *The rational group algebra of a finite group*, J. Algebra Appl., **12** (2013) 1250168 (17 pages).

[BP12] Bakshi, G.K. and Passi, I.B.S., *Primitive central idempotents in rational group algebras*, Comm. Algebra, **40** (2012), 1413–1426.

[BR03] Bakshi, G.K. and Raka, M., *Minimal cyclic codes of length p^nq*, Finite Fields Appl., **9** (2003), 432–448.

[CR62] Curtis, C.W. and Reiner, I., *Representation theory of finite groups and associative algebras*, Pure Appl. Math., Vol. **XI**, Interscience Pub., New York, London, 1962.

[FP07] Ferraz, R. and Polcino Milies, C., *Idempotents in group algebras and minimal abelian codes*, Finite Fields Appl., **13** (2007), 382–393.

[GAP] The GAP Group, *GAP – Groups, Algorithms, and Programming*, Version 4.5.5 (2012). `http://www.gap-system.org`.

[GJ98] Giambruno, A. and Jespers, E., *Central idempotents and units in rational group algebras of alternating groups*, Internat. J. Algebra Comput., **8** (1998), 467–477.

[GJP96] Goodaire, E.G., Jespers, E. and Polcino Milies, C., *Alternative Loop Rings*, North-Holland Mathematics Studies **184**, 1996.

[Her97] Herman, A., *On the automorphism group of rational group algebras of metacyclic groups*, Comm. Algebra, **25** (1997), 2085–2097.

[HP98] Huffman, W. C. and Pless, V.S., *Handbook of Coding Theory*, Elsevier Science Inc., New York, NY, USA, 1998.

[Hup98] Huppert, B., *Character Theory of Finite Groups*, de Gruyer Expositions in Mathematics, **25**, 1998.

[Jan12] Janssens, G., *Primitive central idempotents of rational group algebras*, J. Algebra Appl., **12** (2013) 1250130 (5 pages).

[JdR00] Jespers, E. and del Río, Á, *A structure theorem for the unit group of the integral group ring of some finite groups*, J. Reine Angew. Math., **521** (2000), 99–117.

[JL93] Jespers, E. and Leal, G., *Generators of large subgroups of the unit group of integral group rings*, Manuscripta Math., **78** (1993), 303–315.

[JLP03] Jespers, E., Leal, G. and Paques, A., *Central idempotents in the rational group algebra of a finite nilpotent group*, J. Algebra Appl., **2** (2003), 57–62.

[JOdR12] Jespers, E., Olteanu, G. and del Río, Á., *Rational group algebras of finite groups: from idempotents to units of integral group rings*, Algebr. Represent. Theory, **15** (2012), 359–377.

[JOdRVG] Jespers, E., Olteanu, G., del Río, Á and Van Gelder, I., *Central units of integral group rings*, to appear in Proc. Amer. Math. Soc. http://arxiv.org/abs/1203.5232.

[JOdRVG] Jespers, E., Olteanu, G., del Río, Á and Van Gelder, I., *Group rings of finite strongly monomial groups: central units and primitive idempotents*, submitted. http://arxiv.org/abs/1209.1269.

[KS01] Kelarev, A.V. and Solé, P., *Error correcting codes as ideals in group rings*, Contemp. Math., **273** (2001), 11–18.

[OdRS04] Olivieri, A., del Río, Á. and Simón, J.J., *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra, **32** (2004), 1531–1550.

[OdRS06] Olivieri, A., del Río, Á. and Simón, J.J., *The group of automorphisms of the rational group algebra of a finite metacyclic group*, Comm. Algebra, **34** (2006), 3543–3567.

[Olt07] Olteanu, G., *Computing the Wedderburn decomposition of group algebras by the Brauer–Witt theorem*, Math. Comp., **76** (2007), 1073–1087.

[OVG13] Olteanu, G. and Van Gelder, I., *Construction of minimal non-abelian left group codes*, preprint, 2012.

[PA96] Pruthi, M. and Arora, S.K., *Minimal Codes of Prime-Power Length*, Finite Fields Appl., **3** (1997), 99–113.

[PW50] Perlis, S. and Walker, G.L., *Abelian group algebras of finite order*, Trans. Amer. Math. Soc., **68** (1950), 420–426.

[Rei75] Reiner, I., *Maximal Orders*, Academic Press, London, New York, San Fransisco, 1975.

[RS91] Ritter, J. and Sehgal, S.K., *Construction of units in group rings of monomial and symmetric groups*, J. Algebra, **142** (1991), 511–526.

[ESL95] Evans Sabin, R. and Lomonaco, S.J., *Metacyclic error-correcting codes*, Appl. Algebra Engrg. Comm. Comput., **6** (1995), 191–210.

[Sho33] Shoda, K., *Über die monomialen Darstellungen einer endlichen Gruppe*, Proc. Phys.-math. Soc. Jap., **15** (1933), 249–257.

[VGO11] Van Gelder, I. and Olteanu, G., *Finite group algebras of nilpotent groups: a complete set of orthogonal primitive idempotents*, Finite Fields Appl., **17** (2011), 157–165.

[Yam73] Yamada, T., *The Schur Subgroup of the Brauer Group*, Lect. Notes Math., **397**, Springer-Verlag, 1973.

Received December 10, 2011
Accepted May 2, 2012

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