Wedderburn decomposition of finite group algebras

Osnel Broche and Ángel del Río *

Abstract

We show a method to effectively compute the Wedderburn decomposition and the primitive central idempotents of a semisimple finite group algebra of an abelian-by-supersolvable group G from certain pairs of subgroups of G.

In this paper $\mathbb{F} = \mathbb{F}_q$ denotes a finite field with q elements and G is a finite group of order n such that $\mathbb{F}G$ is semisimple, or equivalently $(q, n) = 1$. The group algebra $\mathbb{F}G$ is an algebraic object of major interest in pure and applied algebra. One of the remarkable applications of finite group algebras appears in coding theory because cyclic codes are ideals of group algebras of cyclic groups [10]. More generally, there is a long tradition on the study of abelian codes (ideals in finite abelian group algebras) or group codes (one sided ideals in arbitrary finite group algebras) [1, 2, 3, 5, 6, 11, 13, 14, 15]. One of the major motivations in the study of non cyclic group algebra codes relies on the fact that many important codes can be realized as ideals of a non cyclic group algebras [10, Chapter 9], [2, 15].

This paper focuses on the computation of the Wedderburn decomposition, that is the decomposition of $\mathbb{F}G$ as a direct sum of matrix rings over division rings. With this decomposition at hand it is straightforward to produce all the ideals of $\mathbb{F}G$. If $e_1, \ldots, e_m$ are the primitive central idempotents of $\mathbb{F}G$ then $\mathbb{F}G = FGe_1 \oplus \ldots \oplus FGe_m$ is the Wedderburn decomposition of $\mathbb{F}G$. However the idempotent themselves do not provide information on the structure of $\mathbb{F}Ge_i$'s as matrix rings of division rings. If G is cyclic then the primitive idempotents of $\mathbb{F}G$ are in one-to-one correspondence with the q-cyclotomic classes module $|G|$, the order of G [10] and using this it is not difficult to compute the primitive idempotents and the Wedderburn decomposition of any commutative finite group algebra (see Proposition 2). The primitive central idempotents of non commutative group algebras are more difficult to compute but can be obtained from the character table of the group. Recently Jespers, Leal and Paques [4] have introduced a character free method to compute the primitive central idempotents of a rational group algebra $\mathbb{Q}G$ for G a finite nilpotent. This method has been extended and simplified in [8]. Further the results of [8] provides information on the structure of the simple components of $\mathbb{Q}G$, i.e. information on the Wedderburn decomposition of $\mathbb{Q}G$. The main aim of this paper is showing that this method can be used to compute the primitive central idempotents and the Wedderburn decomposition of $\mathbb{F}G$. For example we show how to compute the Wedderburn decomposition and the primitive central idempotents of $\mathbb{F}G$ if G is abelian-by-supersolvable (see Theorem 7 and Corollary 8).

We start establishing the basic notation. The algebraic closure of $\mathbb{F}$ is denoted by $\widehat{\mathbb{F}}$. For every positive integer k coprime with q, ξ_k denotes a primitive k-th root of unity in $\widehat{\mathbb{F}}$ and $o_k = o_k(q)$ denotes the multiplicative order of q module k. Recall that $\mathbb{F}(\xi_k) = \mathbb{F}_{q^{o_k}}$ the field of order q^{o_k}. If $\alpha \in \mathbb{F}G$ and $g \in G$ then $\alpha^g = g^{-1}\alpha g$ and $\mathrm{Cen}_G(\alpha)$ denotes the centralizer of α in G. The notation

*Partially supported by the MECD of Spain, CAPES of Brazil and Fundación Séneca of Murcia

$H \leq G$ (resp. $H \trianglelefteq G$) means that H is a subgroup (resp. normal subgroup) of G. If $H \leq G$ then $N_G(H)$ denotes the normalizer of H in G and we set $\widehat{H} = |H|^{-1} \sum_{h \in H} h$, an idempotent of $\mathbb{F}G$. If $g \in G$ then $\widehat{x} = \widehat{\langle x \rangle}$.

By assumption all the characters of any finite group are considered as characters in $\widehat{\mathbb{F}}$. For an irreducible character χ of G, let $\mathbb{F}(\chi)$ denote the character field of χ, $e(\chi) = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})g$ the primitive central idempotent of $\widehat{\mathbb{F}}G$ associated to χ and $e_{\mathbb{F}}(\chi)$ the only primitive central idempotent e of $\mathbb{F}G$ such that $e(\chi)e \neq 0$. The Galois group $\mathrm{Gal}(\mathbb{F}(\chi)/\mathbb{F})$ of the field extension $\mathbb{F}(\chi)/\mathbb{F}$ acts on $\mathbb{F}(\chi)G$ by acting on the coefficients, that is

$$\sigma \cdot \sum_{g \in G} a_g g = \sum_{g \in G} \sigma(a_g) g.$$

We recall the following formula [16]

$$e_{\mathbb{F}}(\chi) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}(\chi)/\mathbb{F})} \sigma \cdot e(\chi).$$

The group $\mathbb{Z}_n^*$ of units of the ring $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ acts on G by $m \cdot g = g^m$. Let Q denote the subgroup of $\mathbb{Z}_n^*$ generated by the class of q and consider Q acting on G by restriction of the previous action. The q-cyclotomic classes of G are the orbits of G under the action of Q on G. Notice that if $g \in G$ then the cardinality of the cyclotomic class $C_q(g)$ containing g is the multiplicative order o of q module the order of g and $C_q(g) = \{g, g^q, g^{q^2}, \ldots, g^{q^{o-1}}\}$. Notice that the q-cyclotomic classes of the cyclic group $(\mathbb{Z}_n, +)$ are the so called q-cyclotomic classes module n (see e.g. [10]).

Assume for a while that G is cyclic. Then the set G^* of irreducible characters of G is a group with the natural product: $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$, for $\chi_1, \chi_2 \in G^*$ and $g \in G$. Furthermore G and G^* are isomorphic and in particular G^* is cyclic and the generators of G^* are precisely the faithful representations of G.

Notation 1 *If G is cyclic then let $\mathcal{C}(G) = \mathcal{C}_q(G)$ denote the set of q-cyclotomic classes of G^* that contains generators of G^*.*

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

$$\varepsilon_C(G, N) = |G|^{-1} \sum_{g \in G} \mathrm{tr}(\chi(\overline{g}))g^{-1} = [G : N]^{-1} \widehat{N} \sum_{X \in G/N} \mathrm{tr}(\chi(X))g_X^{-1},$$

where $\overline{g}$ denotes the image of g in G/N and g_X denotes a representative of $X \in G/N$.

Let $H \trianglelefteq K \leq G$ such that K/H is cyclic and $C \in \mathcal{C}(K/H)$. Then $e_C(G, K, H)$ denotes the sum of the different G conjugates of $\varepsilon_C(K, H)$.

Notice that if g is a generator of G then the map $\phi : \mathbb{Z}_n \to G^*$ given by $\phi(m)(g) = \xi_n^m$ is a group homomorphism and ϕ induces a one to one correspondence between the q-cyclotomic classes of q module n contained in $\mathbb{Z}_n^*$ and $\mathcal{C}(G)$. On the other hand if $N \trianglelefteq G$ is such that G/N is cyclic then $\varepsilon_C(G, N)$ does not depend on the choice of $\chi \in C$. Indeed if ψ is another element of C then $\psi = \chi^{q^i}$ for some i and hence $\mathrm{tr}(\psi(g)) = \mathrm{tr}(\chi(g)^{q^i}) = \mathrm{tr}(\chi(g))$ because the Frobenius automorphism, $x \to x^q$ belongs to $\mathrm{Gal}(\mathbb{F}_{q^o}/\mathbb{F})$.

It is well known that if G is cyclic then the primitive central idempotents of $\mathbb{F}G$ are in one to one correspondence with the q-cyclotomic classes module n which in turn are in one to one correspondence with the q-cyclotomic classes of G or G^*. From this it follows in a basically straightforward

way that the primitive central idempotents of $\mathbb{F}G$ for G abelian are in one to one correspondence with the q-cyclotomic classes of the cyclic quotients of G or equivalently with the elements of the different $\mathcal{C}(G/N)$ for G/N cyclic. Although this is well known we states and proves this result using Notation 1.

Proposition 2 *If G is a finite abelian group of order n and $\mathbb{F}$ is a finite field of order q such that $\gcd(q,n)=1$ then the map $(N,C)\to\varepsilon_C(G,N)$ is a bijection from the set of pairs (N,C) with $N\trianglelefteq G$, such that G/N is cyclic and $C\in\mathcal{C}_q(G/N)$ to the set of primitive central idempotents of $\mathbb{F}G$. Further for every $N\trianglelefteq G$ and $C\in\mathcal{C}(G/N)$, $\mathbb{F}G\epsilon_C(G,N)\simeq\mathbb{F}(\xi_k)$ where $k=[G:N]$.*

Proof. If e is a primitive central idempotent of $\mathbb{F}G$ then there is an irreducible character ψ of G such that $e=e(\psi)$. Since G is abelian ψ is linear. Let $N=\ker\psi$ and let χ be the faithful character of G/N given by $\chi(\overline{g})=\psi(g)$. Then G/N is cyclic, the cyclotomic class C of G/N containing χ belongs to $\mathcal{C}(G/N)$ and

$$\begin{array}{rcl} e_{\mathbb{F}}(\psi) & = & \sum_{\sigma\in\mathrm{Gal}(\mathbb{F}(\psi),\mathbb{F})}\sigma\cdot e(\chi)=\frac{1}{|G|}\sum_{\sigma\in\mathrm{Gal}(\mathbb{F}(\psi),\mathbb{F})}\sum_{g\in G}\sigma(\psi(g))g^{-1}\\ & = & \frac{1}{|G|}\sum_{g\in G}\mathrm{tr}(\chi(\overline{g}))g^{-1}=\varepsilon_C(G,N). \end{array} \tag{1}$$

This shows that the map is surjective and that $\mathbb{F}G\varepsilon_C(G,N)=\mathbb{F}Ge_{\mathbb{F}}(\psi)\simeq\mathbb{F}(\xi_k)$.

To show that the map is injective assume that $e_{C_1}(G,N_1)=e_{C_2}(G,N_2)$ with $N_i\trianglelefteq G$, G/N_i cyclic and $\chi_i\in C_i\in\mathcal{C}(G/N_i)$. Let $\pi_i:G\to G/N_i$ be the canonical projection and $\psi_i=\chi_i\circ\pi_i$. By (1), $e_{\mathbb{F}}(\psi_1)=e_{C_1}(G,N_i)=e_{C_2}(G,N_2)=e_{\mathbb{F}}(\psi_2)$ and hence $\mathbb{F}(\psi_1)=\mathbb{F}(\psi_2)$. Further if $K=\mathbb{F}(\psi_i)$ then there is $\sigma\in\mathrm{Gal}(K/\mathbb{F})$ such that $\psi_2=\sigma\circ\psi_1$ and hence $N_1=\ker\psi_1=\ker\psi_2=N_2$. Finally, since $\mathrm{Gal}(K/\mathbb{F})$ is generated by the Frobenius automorphism, there is i such that $\sigma(x)=x^{q^i}$ for every $x\in K$ and hence $\chi_2=\chi_1^{q^i}$. Thus $C_2=C_1$. ∎

Corollary 3 *If $N\trianglelefteq G$ is such that G/N is cyclic and $C\in\mathcal{C}(G/N)$ then $\varepsilon_C(G,N)$ is a primitive central idempotent of $\mathbb{F}G$ and $\mathbb{F}G\varepsilon_C(G,N)\simeq\mathbb{F}(\xi_k)$ where $k=[G:N]$. Furthermore if D is another element of $\mathcal{C}(G/N)$ then $\varepsilon_C(G,N)=\varepsilon_D(G,N)$ if and only if $C=D$.*

Proof. The natural projection $G\to G/N$ induces an isomorphism $\phi:\mathbb{F}G\widehat{N}\simeq\mathbb{F}(G/N)$. Since $\varepsilon_C(G,N)\in\mathbb{F}G\widehat{N}$ and $\phi(\varepsilon_C(G,N))=\varepsilon_C(G/N,1)$ is primitive idempotent of $\mathbb{F}G/N$, by Proposition 2, $\varepsilon_C(G,N)$ is a primitive central idempotent of $\mathbb{F}G$ and $\varepsilon_C(G,N)=\varepsilon_D(G,N)$ if and only if $C=D$. ∎

If K is a subgroup of G and ψ is a linear character of K then ψ^g denotes the character of K^g given by $\psi^g(x)=\psi(x^{g^{-1}})$. This defines an action of G on the set of linear characters of subgroups of G. Notice that if $H=\ker\psi$ then $H^g=\ker\psi^g$ and therefore the rule $\psi\mapsto\psi^g$ defines a bijection between the set of linear characters of K with kernel H and the set of linear characters of K^g with kernel H^g. This bijection maps q-cyclotomic classes to q-cyclotomic classes and hence induces a bijection $\mathcal{C}(K/H)\to\mathcal{C}(K^g/H^g)$. The image of $C\in\mathcal{C}(K/H)$ under this map is denoted C^g. The following equality is obvious

$$\varepsilon_C(K,H)^g=\varepsilon_{C^g}(K^g,H^g) \tag{2}$$

Let $H\trianglelefteq K\leq G$ such that K/H is cyclic. Then $N=N_G(H)\cap N_G(K)$ acts on K/H by conjugation and this induces an action of N on the set of q-cyclotomic classes of K/H. It is easy to see that the stabilizers of all the q-cyclotomic class of K/H containing generators of K/H are equal. We denote by $E_G(K/H)$ the stabilizer of any q-cyclotomic class of K/H containing generators of K/H under this action of N. Further the action of the previous paragraph induces an action of N on $\mathcal{C}(K/H)$ and it is easy to see that $E_G(K/H)$ is the stabilizer of any element of $\mathcal{C}(K/H)$.

Lemma 4 *Let $H \trianglelefteq K \leq G$ be such that K/H is cyclic and let $C \in \mathcal{C}(K/H)$.*

1. *The following are equivalent for every $x \in G$:*
   (a) $x \in H$.
   (b) $x\varepsilon_C(K,H) = \varepsilon_C(K,H)$.
   (c) $\widehat{x}\varepsilon_C(K,H) = \varepsilon_C(K,H)$.
2. *If $K \trianglelefteq N_G(H)$, then $\mathrm{Cen}_G(\varepsilon_C(K,H)) = E_G(K/H)$.*

Proof. Let $m = [K:H]$, $o = o_m$, $\varepsilon = \varepsilon_C(K,H)$ and fix $\chi \in C$ and $k \in K$ such that its image $\bar{k}$ in K/H is a generator of K/H. Since χ is a generator of $(K/H)^*$, the image of χ is the set of m-th roots of unity in $\mathbb{F}_{q^o}$ and hence this image generates $\mathbb{F}_{q^o}$ as $\mathbb{F}_q$-vector space.

1. (a) implies (b) and the equivalence between (b) and (c) are obvious. Assume that $x = hk^t$ satisfies (b) with $h \in H$ and $0 \leq t < m$. Then

$$[K:H]^{-1}\widehat{H}\sum_{j=0}^{n-1}\mathrm{tr}(\chi(\bar{k}^{-j}))k^{t+j} = x\varepsilon = \varepsilon = [K:H]^{-1}\widehat{H}\sum_{j=0}^{n-1}\mathrm{tr}(\chi(\bar{k}^{-j}))k^{j}$$

and hence

$$\mathrm{tr}(\chi(\bar{k}^{t+j})) = \mathrm{tr}(\chi(\bar{k}^{j}))$$

for every $0 \leq j < n$. Thus $\mathrm{tr}((\chi(\bar{k}^t)-1)\chi(\bar{k}^{-j})) = 0$ and hence $\chi(\bar{k}^t) = 1$ because the image of χ contains a generating set of $\mathbb{F}_{q^o}$ as $\mathbb{F}_q$-vector space. Thus $\chi(\bar{k})^t = 1$ and hence $m|t$ because $\chi(\bar{k})$ is a primitive m-th root of unity. Therefore $x \in H$.

2. Using 1 and (2) it is easy to show that $\mathrm{Cen}_G(\varepsilon) \leq N_G(H)$. Let $g \in N_G(H)$. By Proposition 2, $\varepsilon_C(K,H)$ and $\varepsilon_{C^g}(K,H)$ are two primitive central idempotents of $\mathbb{F}K$ and they are equal if and only if $C = C^g$, i.e. if $g \in E_G(K/H)$. By (2), $\varepsilon_C(K,H)^g = \varepsilon_{C^g}(K,H)$. We conclude that $\varepsilon_C(K,H) = \varepsilon_C(K,H)^g$ if and only if $g \in E_G(K/H)$ as desired. ∎

We now recall some notation from [4] and [8]. If $N \trianglelefteq G$ then let $\varepsilon(G,H)$ be the element of $\mathbb{Q}G$ defined as follows:

$$\varepsilon(G,N) = \begin{cases} \widehat{N}, & \text{if } N = G \\ \prod_{M/N \in \mathcal{M}(G/N)}(\widehat{N} - \widehat{M}), & \text{if } N \neq G. \end{cases} \tag{3}$$

where $\mathcal{M}(G/N)$ denotes the set of minimal subgroups of G/N. Beware that here $\widehat{N}$ and the $\widehat{M}$'s are computed in $\mathbb{Q}G$ rather than in $\mathbb{F}G$ as above.

Given $H \trianglelefteq K \leq G$, let $e(G,K,H)$ denote the sum of all G-conjugates of $\varepsilon(K,H)$, that is if T is a right transversal of $\mathrm{Cen}_G(\varepsilon(K,H))$ in G then

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

Clearly $e(G,K,H)$ is a central element of $\mathbb{Q}G$ and if the G-conjugates of $\varepsilon(K,H)$ are orthogonal, then $e(G,K,H)$ is a central idempotent of $\mathbb{Q}G$.

Definition 5 *A* strongly Shoda pair *of G is a pair (K,H) of subgroups of G satisfying the following conditions:*

(SS1) $H \leq K \trianglelefteq N_G(H)$;

(SS2) K/H is cyclic and a maximal abelian subgroup of $N_G(H)/H$ and

(SS3) for every $g \in G \setminus N_G(H)$, $\varepsilon(K,H)\varepsilon(K,H)^g = 0$.

In [8] it was proved that if (K,H) is a strongly Shoda pair of G then $e(G,K,H)$ is a primitive central idempotent of $\mathbb{Q}G$ and that if G is abelian-by-supersolvable then every primitive central idempotent of $\mathbb{Q}G$ is of the form $e(G,K,H)$ for (K,H) a strongly Shoda pair of G.

Let p be the prime divisor of q and let $\mathbb{Z}_{(p)}$ denote the localization of $\mathbb{Z}$ at p. We identify $\mathbb{F}_p$ with the residue field of $\mathbb{Z}_{(p)}$, denote with $\overline{x}$ the image of $x \in \mathbb{Z}_{(p)}$ in $\mathbb{F}_p$ and extend this notation to the projection of $\mathbb{Z}_{(p)}G$ onto $\mathbb{F}_pG$.

Notice that $\varepsilon(G,N)$ belongs to $\mathbb{Z}_{(p)}$ (for $N \trianglelefteq G$) and hence so does $e(G,K,H)$ (for $H \trianglelefteq K \leq G$). Thus $\overline{\varepsilon(K,H)}$ is an idempotent of $\mathbb{F}_pG$ and if (K,H) is a strongly Shoda pair then $\overline{e(G,K,H)}$ is a central idempotent of $\mathbb{F}_pG$. (Notice that $\overline{\varepsilon(K,H)}$ can be computed as in (3) but interpreting $\widehat{N}$ and the $\widehat{M}$'s as elements in $\mathbb{F}G$.)

Lemma 6 *1. Let $N \trianglelefteq G$ such that G/N is cyclic then*

$$\overline{\varepsilon(G,N)} = \sum_{C \in \mathcal{C}(G/N)} \varepsilon_C(G,N).$$

2. Let $H \trianglelefteq K \leq G$ such that K/H is cyclic and R a set of representatives of the action of $N_G(H)$ on $\mathcal{C}(K/H)$. Then

$$\overline{e(G,K,H)} = \sum_{C \in R} \varepsilon_C(G,K,H).$$

Proof. 1. Since $\varepsilon(G,N)$ and $\varepsilon_C(G,N)$ belong to $\mathbb{F}G\widehat{N}$ for every $C \in \mathcal{C}(G/N)$, by factoring out by N, we may assume without loss of generality that $N = 1$ and hence G is cyclic (see the proof of Corollary 3). By Proposition 2, every primitive idempotent of $\mathbb{F}G$ is of the form $\varepsilon_C(G,H)$ with $H \leq G$ and $C \in \mathcal{C}(G/H)$. Thus to prove 1 it is enough to show that if $H \leq G$ and $C \in \mathcal{C}(G/H)$ then $\overline{\varepsilon(G,1)}\varepsilon_C(G,H) \neq 0$ if and only if $H = 1$. If $C \in \mathcal{C}(G)$ and $1 \neq x \in G$ then $(1-\widehat{x})\varepsilon_C(G,1) \neq 0$, by Lemma 4, and hence $(1-\widehat{x})\varepsilon_C(G,1) = \varepsilon_C(G,1)$ because $\varepsilon_C(G,1)$ is a primitive idempotent. Since $\overline{\varepsilon(G,1)}$ is a product of elements of the form $(1-\widehat{x})$ with $1 \neq x \in G$ we deduce that $\overline{\varepsilon(G,1)}\varepsilon_C(G,1) = \varepsilon_C(G,1) \neq 0$. On the other hand, if $1 \neq H \leq G$ then there is $h \in H$ such that $M = \langle h \rangle$ is a minimal non trivial subgroup of G and hence $\overline{\varepsilon(G,1)}\varepsilon_C(G,H) = \overline{\varepsilon(G,1)}(1-\widehat{x})\varepsilon_C(G,H) = 0$, by Lemma 4. This finish the proof of the claim.

2. Let $N = N_G(H)$, $E = E_G(K/H)$, T_N a right transversal of N in G and T_E a right transversal of E in N. Thus $\{hg : h \in T_E, g \in T_N\}$ is a right transversal of E in G. By [8], $N = \mathrm{Cen}_G(\varepsilon(K,H))$ and hence $e(G,K,H) = \sum_{g \in T_n} \varepsilon(K,H)^g$. On the other hand $\mathcal{C}(K/H)$ is the disjoint union of the sets of the form $\{C^t : t \in T_E\}$ for C running on R and hence using (2) one has

$$\begin{array}{rcl}
\overline{e(G,K,H)} & = & \sum_{g \in T_N} \overline{\varepsilon(K,H)}^g \\
& = & \sum_{g \in T_N} \sum_{C \in \mathcal{C}(K/H)} \varepsilon_C(K,H)^g \\
& = & \sum_{g \in T_N} \sum_{C \in R} \sum_{h \in T_E} \varepsilon_{C^h}(K,H)^g \\
& = & \sum_{C \in R} \sum_{g \in T_N} \sum_{h \in T_E} \varepsilon_C(K,H)^{hg} \\
& = & \sum_{C \in R} e_C(G,K,H). \ \blacksquare
\end{array}$$

We are ready to prove the main result of the paper.

Theorem 7 *Let G be a finite group and $\mathbb{F}$ a finite field such that $\mathbb{F}G$ is semisimple.*

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

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

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

2. *Let X be a set of strongly Shoda pairs of G. If every primitive central idempotent of G is of the form $e(G,K,H)$ for $(K,H) \in X$ then every primitive central idempotent of $\mathbb{F}G$ is of the form $e_C(G,K,H)$ for $(K,H) \in X$ and $C \in \mathcal{C}(K/H)$.*

Proof. 1. Set $\varepsilon = \varepsilon_C(K,H)$, $e = e_C(G,K,H)$ and let T be a right transversal of E in G. By Lemma 4, $E = \mathrm{Cen}_G(\varepsilon)$ and by [8], $N = N_G(H) = \mathrm{Cen}_G(\varepsilon(K,H))$. Thus $e = \sum_{g\in T} \varepsilon^g$.

We claim that the G-conjugates of ε are orthogonal. To prove this it is enough to show that if $g \in G \setminus E$ then $\varepsilon\varepsilon^g = 0$. By Lemma 6, $\varepsilon\varepsilon^g = \varepsilon\overline{e(K,H)}\,e(K,H)^g\varepsilon^g$. By the definition of strongly Shoda pairs, if $g \notin N$ then $e(K,H)e(K,H)^g = 0$ and so $\varepsilon\varepsilon^g = 0$. If $g \in N \setminus E$ then $\varepsilon^g = \varepsilon_{C^g}(K,H)$ (see 2) and thus ε and ε^g are two different primitive central idempotents of $\mathbb{F}K$ (Corollary 3). Thus $\varepsilon\varepsilon^g = 0$.

By Corollary 3, $\mathbb{F}K\varepsilon$ is isomorphic to $\mathbb{F}(\xi_k) = \mathbb{F}_{q^o}$, where $k = [K:H]$. Furthermore $\mathbb{F}\varepsilon = \mathbb{F}K *_\tau^\sigma E/K$ is a crossed product of E/K over the field $\mathbb{F}K$, where the action σ and and twisting τ of the crossed product [9] are the action and twisting associated to the short exact sequence of the group extension $1 \to K/H \to E/H \to E/K \to 1$. The isomorphism $\mathbb{F}K\varepsilon \simeq \mathbb{F}(\xi_k)$ extends to an E/K-graded isomorphism $\mathbb{F}E\varepsilon = \mathbb{F}K\varepsilon *_\tau^\sigma E/K \simeq \mathbb{F}(\xi_k) *_\tau^\sigma E/K$. Since K/H is maximal abelian in E/H, the action σ is faithful and hence $\mathbb{F}E\varepsilon$ is simple ([12, Theorem 29.6]). By Wedderburn Theorem, $\mathbb{F}E\varepsilon \simeq M_{[E:K]}(\mathbb{F}_{q^t})$ where $\mathbb{F}_{q^t}$ is the fix subfield of the action σ on $\mathbb{F}(\xi_k)$. Since σ is faithful $\frac{o}{t} = [\mathbb{F}_{q^o} : \mathbb{F}_{q^t}] = [E:K]$ and hence $t = \frac{o}{[E:K]}$. (A direct proof that $[E:K]$ divides o goes as follows: By the definition of E, $\sigma(E/K)$ is a subgroup of the group of automorphisms of K/H generated by the automorphism α given by $x \to x^q$. Since σ is injective $[E:K]$ divides o, the order of α.)

If $g \in G$ then the map $x \mapsto xg$ is an isomorphism between the $\mathbb{F}G$-modules $\mathbb{F}G\varepsilon$ and $\mathbb{F}G\varepsilon^g$. Therefore ${}_{\mathbb{F}G}\mathbb{F}Ge = \oplus_{g\in T}\mathbb{F}G\varepsilon^g \simeq (\mathbb{F}G\varepsilon)^n$. Moreover $\varepsilon\mathbb{F}G\varepsilon = \oplus_{t\in T}\mathbb{F}E\varepsilon t\varepsilon = \mathbb{F}E\varepsilon$, because ε is central in $\mathbb{F}E$ and $\varepsilon^t\varepsilon = 0$ for every $t \in G \setminus E$. Thus

$$\mathbb{F}Ge \simeq \mathrm{End}_{\mathbb{F}G}(\mathbb{F}Ge) \simeq M_{[G:E]}(\mathrm{End}_{\mathbb{F}G}(\mathbb{F}G\varepsilon)) \simeq M_{[G:E]}(\varepsilon\mathbb{F}G\varepsilon) = M_{[G:E]}(\mathbb{F}E\varepsilon) \simeq M_{[G:K]}(\mathbb{F}_{q^{o/[E:K]}}).$$

2. By assumption there is a subset Y of X such that $\{e(G,K,H) : (K,H) \in Y\}$ is the set primitive central idempotents of $\mathbb{Q}G$. Then $\{\overline{e(G,K,H)} : (K,H) \in Y\}$ is a complete set of non necessarily primitive orthogonal central idempotents of $\mathbb{F}G$. By 1 and Lemma 6, $\{e_C(G,K,H) : (K,H) \in Y, C \in R_{(K,H)}\}$ is the set of primitive central idempotents of $\mathbb{F}G$, where $R_{(K,H)}$ denotes a set of representatives of the orbits of the action of $N_G(H)$ on $\mathcal{C}(K/H)$. ∎

Applying the results of [8] one obtains the following.

Corollary 8 *If G is an abelian-by-supersolvable group and $\mathbb{F}$ is a finite field such that $\mathbb{F}G$ is semisimple then every primitive central idempotents of $\mathbb{F}G$ is of the form $e_C(G,K,H)$ for (K,H) a strongly Shoda pair of G and $C \in \mathcal{C}(K/H)$. Furthermore for every strongly Shoda pair (K,H) of G and every $C \in \mathcal{C}(K/H)$, $\mathbb{F}Ge_C(G,K,H) \simeq M_{[G:K]}(\mathbb{F}_{q^{o/[E:K]}})$, where $E = E_G(K/H)$ and o is the multiplicative order of q module $[K:H]$.*

Corollary 9 *Let G be a finite metabelian group and $\mathbb{F}$ a finite field such that $\mathbb{F}G$ is semisimple. Then every primitive central idempotent of $\mathbb{F}G$ is of the form $e_C(G,K,H)$ for (K,H) a pair of subgroups of G satisfying the following conditions*

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

and $C \in \mathcal{C}(K/H)$. Furthermore for every pair (K,H) of subgroups of G satisfying 1 and 2 and every $C \in \mathcal{C}(K/H)$, $\mathbb{F}Ge_C(G,K,H) \simeq M_{[G:K]}(\mathbb{F}_{q^o/[E:K]})$, where $E = E_G(K/H)$ and o is the multiplicative order of q module $[K:H]$.

References

[1] S.D. Berman, *On the theory of group codes*, Cybernetics 3 (1967) 25–31.

[2] P. Charpin, *The Reed-Solomon code as ideals in a modular algebra*, C.R. Acad. Sci. Paris, Ser. I. Math. 294 (1982) 597–600.

[3] V. Drensky and P. Lakatos, *Monomial ideals, group algebras and error correcting codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, T. Mora ed., Lect. Notes in Comput. Sci. 257, Springer, Berlin (1989), 181–188.

[4] E. Jespers, G. Leal and A. Paques, *Central idempotents in rational group algebras of finite nilpotent groups*, J. Algebra Appl. 2 (2003), no. 1, 57–62

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

[6] F.J. MacWilliams, *Codes and ideals in group algebras*, Combinatorial Mathematics and its applications, R.C. Bose and T.A. Dowling, eds., Univ. North. Carolina Press, Chapel Hill (1969), 317–328.

[7] A. Olivieri and Á. del Río, *An algorithm to compute the primitive central idempotents and the Wedderburn decomposition of a rational group algebra*, J. of Symb. Comp. 35 (2003) 673–687

[8] A. Olivieri, Á. del Río and J.J. Simón, *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra 32 (2004), no. 4, 1531–1550

[9] D. Passman, Infinite Crossed Products, Academic Press, 1989.

[10] V.S. Pless and W.C. Huffman, Handbook of Coding Theoy, Elsevier, New York, 1998.

[11] A. Poli, *Codes dans les algebras de groups abelienes (codes semisimples, et codes modulaires)*, "Information Theory" (Proc. Internat. CNRS Colloq., Cachan 1977) Colloq. Internat. CNRS 276 (1978) 261–271.

[12] I. Reiner, Maximal orders, Academic Press, 1975.

[13] C. Renteria and H. Tapia Recillas, *Reed-Muller codes: an ideal theory approach*, Comm. Algebra 25 (1997) 401–443.

[14] R.E. Sabin, *On determining all codes in semi-simple group rings*, Lect. Notes in Comp. Sci. 273 (1993) 279-290.

[15] R.E. Evans and S.J. Lomonaco, *Metacyclic error-correcting codes*, AAECC 6 (1995), 191-210.

[16] T. Yamada, The Schur Subgroup of the Brauer Group. Lecture Notes in Math. Vol. 397, Springer-Verlag, 1974.

Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, Brazil. osnelier@ime.usp.br
Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain. adelrio@um.es