

An algorithm to compute the primitive central idempotents and the Wedderburn decomposition of a rational group algebra

Aurora Olivieri and Ángel del Río *

January 8, 2003

Abstract

We present an algorithm to compute the primitive central idempotents and the Wedderburn decomposition of a rational group algebra. This algorithm has been implemented for System GAP, version 4.

Let G be a finite group and $\mathbb{Q}G$ the rational group algebra over G . A good understanding of the Wedderburn decomposition of $\mathbb{Q}G$, that is the decomposition of $\mathbb{Q}G$ as a direct sum of simple algebras, is a good tool to deal with several problems. For example, it is useful to study the group of automorphisms of $\mathbb{Q}G$ [4] or the group of units of the integral group ring $\mathbb{Z}G$ [5, 7, 11, 12, 13].

The problem of describing the Wedderburn decomposition of $\mathbb{Q}G$ leads naturally to the problem of computing the primitive central idempotents of $\mathbb{Q}G$. The classical method to do that is first computing the primitive central idempotents $e(\chi)$ of $\mathbb{C}G$ associated to the irreducible characters χ of G and then adding the primitive central idempotents of the form $e(\sigma \circ \chi)$, with $\sigma \in \text{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$ [14]. In theory the Wedderburn decomposition of $\mathbb{Q}G$ can be computed using powerful but rather complicated methods, including the use of the Brauer-Witt Theorem.

Recently Jespers, Leal and Paques [6] have given an alternative method to compute the primitive central idempotents of $\mathbb{Q}G$ for G nilpotent that avoids calculating the irreducible characters of G and also avoids computations on extensions of the rationals. The results of [6] have been extended and simplified in [9]. The approach of [9] allows to obtain a description of the simple factors of $\mathbb{Q}G$ using only elementary methods and therefore describing the Wedderburn decomposition of $\mathbb{Q}G$ for many finite groups G , including abelian-by-supersolvable groups.

In this paper we explain an algorithm that following the approach of [9] computes the primitive central idempotents and the Wedderburn decomposition of $\mathbb{Q}G$ for many groups, including abelian-by-supersolvable groups. We have implemented this algorithm in a package of programs [8] for System GAP, version 4 [3]. We present also an experimental comparison of the speed of our algorithm with the classical method to compute the primitive central idempotents which shows that our algorithm is usually faster than the classical method.

In Section 1 we establish the basic notation and collect several results from [9]. In Section 2, we explain several algorithms to compute primitive central idempotents of $\mathbb{Q}G$, the irreducible characters of G and the basic data to describe the Wedderburn decomposition of $\mathbb{Q}G$. In Section 3 we explain the interpretation of the data that describe the Wedderburn decomposition of $\mathbb{Q}G$. Finally in Section 4 we show an experimental comparison of the running time of our algorithms with the classical algorithms to compute the primitive central idempotents of $\mathbb{Q}G$ and the irreducible characters of G .

1 Preliminaries

We start fixing some notation. Throughout G is a finite group. The order of G is denoted by $|G|$, its derived subgroup by G' and the rational group algebra over G by $\mathbb{Q}G$. By $H \leq G$ we mean that H is a subgroup of G and by $H \trianglelefteq G$ that H is a normal subgroup of G . If X is a subset of G then $\langle X \rangle$ denotes the subgroup

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

generated by G and we simplify the notation to $\langle Y, Z \rangle$ if either $X = Y \cup Z$ or $X = Y \cup \{Z\}$ or $X = \{Y, Z\}$. If $H \leq G$ then $N_G(H)$ denotes the normalizer of H in G . For $g \in G$ and $x \in \mathbb{Q}G$ set $x^g = g^{-1}xg$ and let us denote by $\text{Cen}_G(x)$ the centralizer of x in G . If $H \leq G$ then we also set $H^g = g^{-1}Hg$. We use exponential notation too for the action of an automorphism of a group or an algebra.

For every positive integer n , let ξ_n denote a complex primitive n -th root of unity.

All the characters of a group are assumed to be complex characters. If χ is a character of a subgroup K of G then χ^G denotes the character of G induced by χ . If χ is an irreducible character of G then the primitive central idempotent of $\mathbb{Q}G$ associated to χ is denoted by $e_{\mathbb{Q}}(\chi)$, that is $e_{\mathbb{Q}}(\chi)$ is the only primitive central idempotent e of $\mathbb{Q}G$ such that $\chi(e) \neq 0$.

If $H \leq G$ then set $\widehat{H} = \frac{1}{|H|} \sum_{x \in H} x \in \mathbb{Q}G$. If $g \in G$, then let $\widehat{g} = \langle \widehat{g} \rangle$. Note that \widehat{H} is an idempotent of $\mathbb{Q}G$ which is central in $\mathbb{Q}G$ if and only if $H \trianglelefteq G$.

If $N \trianglelefteq G$ then let

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

where $\mathcal{M}(G, N)$ denotes the set of minimal normal subgroups of G containing N properly. Let $\omega_N : \mathbb{Q}G \rightarrow \mathbb{Q}(G/N)$ denote the augmentation map associated to N . Note that $\text{Ker } \omega_N = \mathbb{Q}G(1 - \widehat{N})$ and so ω_N induces an isomorphism $\mathbb{Q}G\widehat{N} \simeq \mathbb{Q}(G/N)$ (see [13]). Moreover if $N \leq H \leq K \leq G$ then

$$\omega_N(\varepsilon(K, H)) = \varepsilon(K/N, H/N). \quad (1.1)$$

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

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

The notation $S * G$ stands for a crossed product over G with coefficient ring S [10]. If $B = \{u_g : g \in G\}$ is an S -basis of $S * G$ such that for each $g \in G$, u_g is an invertible homogeneous element of $S * G$ of degree g then B is said to be a homogeneous basis of $S * G$. A homogeneous basis B gives rise to the following action σ and twisting τ of G over S

$$s^{\sigma(g)} = u_g^{-1} s u_g, \quad \tau(g, h) = u_{gh}^{-1} u_g u_h, \quad (s \in S, g, h \in G)$$

and the product in $S * G$ is determined by σ and τ .

Definition 1.1 Let (K, H) be a pair of subgroups of G . We say that (K, H) is a Shoda pair of G if the following conditions hold:

- (S1) $H \trianglelefteq K$,
- (S2) K/H is cyclic and
- (S3) If $g \in G$ and $[K, g] \cap K \subseteq H$ then $g \in K$.

We also say that (K, H) is a strongly Shoda pair of G if the following conditions hold:

- (SS1) $H \leq K \trianglelefteq N_G(H)$;
- (SS2) K/H is cyclic and maximal abelian subgroup of $N_G(H)/H$ and
- (SS3) for every $g \in G \setminus N_G(H)$, $\varepsilon(K, H)\varepsilon(K, H)^g = 0$.

The following proposition collects several results of [9].

Proposition 1.2 [9] Let G be a finite group and $H \leq K \leq G$.

(1) If H is the kernel of a linear character χ of K then the induced character χ^G is irreducible if and only if (K, H) is a Shoda pair.

Conversely, if (K, H) is a Shoda pair of G then there is a linear character χ of K with kernel H such that χ^G is irreducible. In that case there is a (necessarily unique) $\alpha \in \mathbb{Q}$ such that

$$e_{\mathbb{Q}}(\chi^G) = \alpha e(G, K, H)$$

and we say that the primitive central idempotent $e_{\mathbb{Q}}(\chi^G)$ is realizable by the Shoda pair (K, H) .

(2) If (K, H) is a strongly Shoda pair of G then it is also a Shoda pair of G and $e(G, K, H)$ is a primitive central idempotent of $\mathbb{Q}G$ (that is, the α of (1) is 1).

(3) If G is abelian-by-supersolvable then every primitive central idempotent of $\mathbb{Q}G$ is realizable by a strongly Shoda pair.

(4) Let (K, H) be a strongly Shoda pair of G and let $N = N_G(H)$, $n = [G : N]$ and $\varepsilon = \varepsilon(K, H)$. Then the simple algebra $\mathbb{Q}Ge(G, K, H)$ can be described as follows:

- $\mathbb{Q}Ge(G, K, H) \simeq M_n(\mathbb{Q}N\varepsilon)$.
- $\mathbb{Q}N\varepsilon = \mathbb{Q}K\varepsilon * N/K$, that is $\mathbb{Q}N\varepsilon$ is a crossed product of N/K with coefficient ring $\mathbb{Q}K\varepsilon$.
- If $\phi : N/K \rightarrow N/H$ is a left inverse of the canonical projection $N/H \rightarrow N/K$ then $\phi(N/K)$ is a homogeneous basis of $\mathbb{Q}K\varepsilon * N/K$.
- If $k = [K : H]$, x is a generator of K/H and $y \in K$ is representative of x then $\mathbb{Q}K\varepsilon = \mathbb{Q}(y\varepsilon)$ and there is an isomorphism $\psi : \mathbb{Q}K\varepsilon \rightarrow \mathbb{Q}(\xi_k)$ given by $\psi(y\varepsilon) = \xi_k$.
- If $\mathbb{Q}K\varepsilon$ and $\mathbb{Q}(\xi_k)$ are identified via ψ , and thus $\mathbb{Q}K\varepsilon * N/K$ is considered as a crossed product of N/K with coefficient ring $\mathbb{Q}(\xi_k)$, then the action σ and twisting τ of this crossed product associated to the homogeneous basis $\phi(N/K)$ are given by:

$$\begin{aligned} \xi_k^{\sigma(a)} &= \xi_k^i, & \text{if } x^a = x^i; \\ \tau(a, b) &= \xi_k^j, & \text{if } \phi(ab)^{-1}\phi(a)\phi(b) = x^j, \end{aligned} \quad (a, b \in N/K, i, j \in \mathbb{Z})$$

In the remainder of this section all the numbers in brackets refer to the statements of Proposition 1.2. By (2) the rule $(K, H) \mapsto e(G, K, H)$ defines a map e_G from the set SSP of strongly Shoda pairs of G to the set E of primitive central idempotents of G . The image of e_G is the set E_{SSP} of primitive central idempotents of $\mathbb{Q}G$ realizable by strongly Shoda pairs of $\mathbb{Q}G$. We say that a subset S of SSP is complete and not redundant if e_G restricts to a bijection between S and E_{SSP} .

We have written a package of programs [8] for System GAP version 4 [3] that includes the following functions:

PCIsFromShodaPairs($\mathbb{Q}G$): computes the primitive central idempotents of $\mathbb{Q}G$ realizable by Shoda pairs of G ;

PCIsFromSSP($\mathbb{Q}G$): computes the primitive central idempotents of $\mathbb{Q}G$ realizable by strongly Shoda pairs of G ;

StronglyShodaPairs($\mathbb{Q}G$): computes a complete and not redundant set of strongly Shoda pairs of G .

SimpleAlgebraFromSSP(G, K, H): computes a list of data describing the simple algebra $\mathbb{Q}Ge(G, K, H)$ for a strongly Shoda pair (K, H) of G .

SimpleFactorsFromListOfSSP(G, L): computes a list formed by the output of **SimpleAlgebraFromSSP**(G, K, H) for (K, H) running through the entries of L , where L is a list of strongly Shoda pairs of G .

By (1), **PCIsFromShodaPairs**($\mathbb{Q}G$) computes all the primitive central idempotents of $\mathbb{Q}G$ if and only if G is monomial. By (3), if G is abelian-by-supersolvable then $E = E_{SSP}$, that is **PCIsFromSSP**($\mathbb{Q}G$) computes all the primitive central idempotents of $\mathbb{Q}G$. By (4), if $E = E_{SSP}$ for a group G , then the Wedderburn decomposition of $\mathbb{Q}G$ can be easily described from a complete and not redundant set of strongly Shoda pairs of G . This will be explained in Section 3.

2 Algorithms to compute primitive central idempotents

The algorithms implemented by `PCIsFromShodaPairs`, `PCIsFromSSP` and `StronglyShodaPairs` are quite similar. We are going to explain the one implemented by `PCIsFromSSP` and then we explain the small differences with the other algorithms. Remember that `PCIsFromSSP(QG)` computes the primitive central idempotents realizable by strongly Shoda pairs. The obvious method to do that by brute force consists in computing the lattice \mathcal{L} of subgroups of G and checking the axioms (SS1)-(SS3) for all the pairs $(K, H) \in \mathcal{L}^2$. The disadvantage of this blind search is that the number of pairs to check can be too large. Instead `PCIsFromSSP` implements the algorithm of Figure 1.

Now we are going to explain the logic of the algorithm in Figure 1. The numbers in brackets refer to the labels included in the algorithm. The main loop of the algorithm selects one representative H of each conjugacy class C of subgroups of G (3) and searches for a subgroup K such that (K, H) is a strongly Shoda pair of G . The reason for considering only one representative in each conjugacy class is that if $g \in G$ and (K, H) is a strongly Shoda pair of G then so is (K^g, H^g) and $e(G, K^g, H^g) = e(G, K, H)$.

At a certain stage of the computations, the list Id , which is initialized as the empty list, contains the primitive central idempotents found so far and $SumId$ is the sum of the elements of Id . When a new strongly Shoda pair (K, H) is discovered the algorithm computes $e = e(G, K, H)$ and if e is not in the list Id then Id is enlarged with e and the value of $SumId$ is actualized (6,6'). The algorithm stops when either the sum $SumId$ of the primitive central idempotents discovered is 1 (the identity of $\mathbb{Q}G$) or when all the conjugacy classes C have been considered (2). It would be desirable to avoid as many conjugacy classes as possible and therefore it would be desirable to obtain $SumId = 1$ before all the conjugacy classes were considered. Notice that the conjugacy classes are selected in decreasing order, that is if the class C_1 is taken before the class C_2 then the order of a representative of C_2 is at most the order of a representative of C_1 . The reason for this is that some of the primitive central idempotents can only be realized by strongly Shoda pairs (K, H) for which H is at the upper part of the lattice of subgroups, namely some of the “unavoidable” strongly Shoda pairs are those of the form (G, H) with $G' \leq H$. This is justified by the following proposition.

- Proposition 2.1** 1. *If $G' \leq H \leq G$, then (K, H) is a Shoda pair of G if and only if $K = G$ and G/H is cyclic. In that case (G, H) is a strongly Shoda pair and $e(G, G, H) = \varepsilon(G, H)$.*
2. *Conversely, if e is a primitive central idempotent of $\mathbb{Q}G\widehat{G}'$ then there is a unique strongly Shoda pair that realizes e and this strongly Shoda pair is of the form (G, H) with $G' \leq H$.*

To prove Proposition 2.1 we need next lemma that we take from [9].

Lemma 2.2 [9] *Let $H \trianglelefteq K \leq G$ such that K/H is cyclic and set $e = \varepsilon(K, H)$. Then H is determined by $\varepsilon(K, H)$, namely*

$$H = \{g \in G : g\varepsilon(K, H) = \varepsilon(K, H)\}.$$

Proof of Proposition 2.1. 1 is trivial.

2. Let e be a primitive central idempotent of $\mathbb{Q}G\widehat{G}'$. Using the isomorphism $\omega_{G'} : \mathbb{Q}G\widehat{G}' \simeq \mathbb{Q}(G/G')$, Proposition 1.2 and the formula (1.1) one deduces that $e = e(G, K, H)$ for (K, H) a strongly Shoda pair of G with $G' \leq H$. By 1, $K = G$ and $e = \varepsilon(G, H)$.

Let (K_1, H_1) be a strongly Shoda pair of G such that $e = e(G, K_1, H_1)$. By (SS3) one has $\widehat{G}'\varepsilon(K_1, H_1) = \widehat{G}'e\varepsilon(K_1, H_1) = e\varepsilon(K_1, H_1) = \varepsilon(K_1, H_1)$. Then for every $g \in G'$ one has $g\varepsilon(K_1, H_1) = g\widehat{G}'\varepsilon(K_1, H_1) = \widehat{G}'\varepsilon(K_1, H_1) = \varepsilon(K_1, H_1)$ and we deduce that $G' \leq H_1$ from Lemma 2.2. By 1, $K_1 = G$ and $\varepsilon(G, H) = e = \varepsilon(G, H_1)$. Using again Lemma 2.2 one deduces that $H = H_1$. ■

Thus, if $G' \leq H \leq G$ then the search for a K making (K, H) a strongly Shoda pair reduces to check with $K = G$. However, if $G' \not\leq H \leq G$ then the search for a strongly Shoda pair of G of the form (K, H) is more complicated because there might be more than one candidate for K as the following example shows.

Example 2.3 *If $Q_8 = \langle x, y | x^4 = x^2y^2 = 1, x^y = x^{-1} \rangle$ is the quaternion group of order 8, then both $(\langle x \rangle, 1)$ and $(\langle y \rangle, 1)$ are strongly Shoda pairs of Q_8 .*

Input: A finite group G .

$\mathcal{C} :=$ Conjugacy classes of subgroups of G ; (in decreasing order) (1)

$Id := \emptyset$;

$SumId := 0$;

for $C \in \mathcal{C}$ and while $SumId \neq 1$ do (2)

$H :=$ Representative of C ; (3)

$N := N_G(H)$;

$L := \langle (N/H)', Z(N/H) \rangle$; (4)

 if L is cyclic then (4)

$Cen := Cen_{N/H}(L)$;

 if Cen is abelian then

$K :=$ preimage of Cen in N ; (5)

 if (K, H) satisfies (SS2) and (SS3) then

$e := e(G, K, H)$;

 if $SumId \cdot e = 0$ then

 Add e to the list Id ;

$SumId := SumId + e(G, K, H)$;

 fi;

 fi;

 next C ;

 else

$X := Cen \setminus L$;

 while $X \neq \emptyset$ do

 select $x \in X$;

$KH := \langle L, x \rangle$;

$K :=$ preimage of KH in N ;

 if (K, H) satisfies (SS2) then

 if (K, H) satisfies (SS3) then

$e := e(G, K, H)$;

 if $SumId \cdot e = 0$ then

 Add e to the list Id ;

$SumId := SumId + e(G, K, H)$;

 fi;

 fi;

 next C ;

 fi;

$X := X \setminus KH$;

 od;

fi;

fi;

od;

Output: Id .

Figure 1: Algorithm of PCIsFromSSP.

The next proposition shows some properties of strongly Shoda pairs that will help to eliminate subgroups H which cannot appear as the second component of a strongly Shoda pair and to reduce the number of subgroups to consider in the first component.

Proposition 2.4 *If (K, H) is a strongly Shoda pair and $N = N_G(H)$ then the following conditions hold:*

1. N/K is isomorphic to a subgroup of the group of units of $\mathbb{Z}/[K : H]\mathbb{Z}$ and in particular N/K is abelian.

2. $\langle\langle(N/H)', Z(N/H)\rangle\rangle \leq K/H$ and therefore $\langle\langle(N/H)', Z(N/H)\rangle\rangle$ is cyclic.

Proof. 1. Consider N/H acting by conjugation on K/H . By (SS2), the kernel of this action is K/H and hence N/K is isomorphic to a subgroup of the group $\text{Aut}(K/H)$ of automorphisms of K/H . Since K/H is cyclic, $\text{Aut}(K/H)$ is isomorphic to the group of units of $\mathbb{Z}/[K : H]\mathbb{Z}$.

2. By 1, $N' \leq K$ and therefore $(N/H)' = N'H/H \subseteq K/H$. Moreover $Z(N/H)K/H$ is abelian and hence $Z(N/H) \subseteq K/H$, by the maximality of K/H . Thus $\langle\langle(N/H)', Z(N/H)\rangle\rangle \leq K/H$ and since K/H is cyclic, so is $\langle\langle(N/H)', Z(N/H)\rangle\rangle$. ■

Let H be the subgroup selected at (3). Set $N = N_G(H)$ and $L = \langle\langle(N/H)', Z(N/H)\rangle\rangle$. By Proposition 2.4, if L is not cyclic then H cannot appear as the second component of a strongly Shoda pair and so, in that case the algorithm passes to the next conjugacy class (4). Assume now that L is cyclic, that is the question at (4) has positive answer, and we are in the position to look for a subgroup K of G for which (K, H) is a strongly Shoda pair of G . Let $\text{Cen} = \text{Cen}_{N/H}(L)$. By Proposition 2.4, if (K, H) is a strongly Shoda pair of G then $L \leq K/H$, and since K/H is cyclic one has that $K/H \subseteq \text{Cen}$. Thus we look for K among the subgroups such that K/H is a cyclic subgroup of Cen containing L . Note that this condition ensures that (K, H) satisfies condition (SS1) and K/H is abelian.

Assume first that Cen is abelian. In this case if (K, H) is a strongly Shoda pair of G then $K/H = \text{Cen}$, by the maximality of K/H . That is why the algorithm only considers the preimage of Cen in N as a candidate for K (5) and passes to the next conjugacy class (7).

Assume now that Cen is not abelian. Then L is properly contained in K/H . This is a consequence of the maximality of K/H . Thus we look for cyclic subgroups of Cen containing L properly. More specifically, what the algorithm does is considering, as candidate for K , the preimage in N of $\langle L, x \rangle$ for $x \in X$, where X is initially $\text{Cen} \setminus L$. Since K/H is abelian, if (K, H) does not satisfy condition (SS2) then K does not contain any other group K_1 such that (K_1, H) satisfies (SS2). That is why in that case X is resettled as $X \setminus K/H$ and the algorithm continues looking for K until a pair (K, H) satisfying condition (SS2) (and (SS1)) is founded or $X = \emptyset$ (8,8'). Assume that the algorithm has found such a pair (K, H) at (9). Notice, that at this stage, the algorithm checks if (K, H) satisfies condition (SS3) and if it does then the algorithm considers $e(G, K, H)$ as a candidate to enlarge the list Id (6'). Then whether (K, H) satisfies (SS3) or not, then the algorithm passes to the next conjugacy class (10). One could argue that whether or not (K, H) satisfies (SS3) and whether or not $e(G, K, H)$ is added to the list Id maybe there is a different possibility for K to consider. In fact this new K may exist as Example 2.3 shows. However we do not want to find all the strongly Shoda pairs but the primitive central idempotents realizable by strongly Shoda pairs. The next proposition shows that if a pair (K, H) of subgroups of G satisfies conditions (SS1) and (SS2) then $e(G, K, H)$ is determined by H . This justifies why passing to the next conjugacy class in (10) if the question at (9) has a positive answer.

Proposition 2.5 *If (K_1, H) and (K_2, H) are two pairs of subgroups of G satisfying conditions (SS1) and (SS2) then*

1. $\varepsilon(K_1, H) = \varepsilon(K_2, H)$,
2. $e(G, K_1, H) = e(G, K_2, H)$ and
3. (K_1, H) is a strongly Shoda pair if and only if (K_2, H) is a strongly Shoda pair.

Proof. 2 and 3 are obvious consequences of 1, so we only prove 1.

Since $\varepsilon(K_i, H)$ belongs to $\mathbb{Q}N_G(H)$ for $i = 1, 2$, we may assume that $N_G(H) = G$, that is $H \trianglelefteq G$. Note also that $\varepsilon(K_i, H) \in \mathbb{Q}G\widehat{H}$. Using the isomorphism $\omega_H : \mathbb{Q}G\widehat{H} \simeq \mathbb{Q}(G/H)$ and factoring out by H , one may assume that $H = \{1\}$. In other words one may assume that K_1 and K_2 are cyclic, normal and maximal abelian subgroups of G . We prove that every minimal subgroup of K_2 is embedded in K_1 . By symmetry $\mathcal{M}(K_1, 1) = \mathcal{M}(K_2, 1)$ and then the proposition follows.

A minimal subgroup of K_2 is of the form $\langle y \rangle$ with y of prime order. Let x be a generator of K_1 . Since $K_1 \trianglelefteq G$, $y^{-1}xy = x^j$, for some j . Then $xyx^{-1} = yx^{j-1}$. Since K_2 is a cyclic normal subgroup of G , so is $\langle y \rangle$ and hence $yx^{j-1} \in \langle y \rangle$. Thus $x^{j-1} \in \langle y \rangle \cap K_1$. If $\langle y \rangle \cap K_1 = \langle y \rangle$, then $y \in K_1$ as desired. Otherwise

$\langle y \rangle \cap K_1 = 1$ and hence $x^{j-1} = 1$. Then $\langle K_1, y \rangle$ is abelian and contains K_1 properly contradicting the maximality of K_1 . ■

The algorithm that implements `StronglyShodaPairs` is basically the same than the one explained above. The only difference is that instead of collecting in `Id` the primitive central idempotents discovered `StronglyShodaPairs` collects the strongly Shoda pairs. Notice that Proposition 2.5 applies here too because `StronglyShodaPairs` does not pretend to find all the strongly Shoda pairs but a complete and not redundant set of strongly Shoda pairs.

The algorithm that implements `PCIsFromShodaPairs` is also very similar to the previous one. The only two differences are based on the fact that Propositions 2.4 and 2.5 may not hold for Shoda pairs. Namely, if (K, H) is a Shoda pair of G and $N = N_G(H)$ then it is easy to see that K/H is a maximal abelian subgroup of N/H and therefore $Z(N/H) \leq K/H$ and $Z(N/H)$ is cyclic. However it is not clear whether or not $N' \subseteq K$. Thus the filter at (4) is changed to asking if $Z(N/H)$ is cyclic. On the other hand, unlike for strongly Shoda pairs (Proposition 2.5), theoretically two Shoda pairs (K_1, H) and (K_2, H) could realize different primitive central idempotents. Thus when a Shoda pair (K_1, H) has been found the algorithm can not pass to the next conjugacy classes. These two reasons makes `PCIsFromShodaPairs` slower than `PCIsFromSSP`.

Notice that if G have a monomial character χ such that $e_{\mathbb{Q}}(\chi)$ is not realizable by a strongly Shoda pair then `PCIsFromShodaPairs` finds this primitive central idempotent while `PCIsFromSSP` does not. Such an example has been given in [9] but this example is a non monomial group. An exhaustive search using `PCIsFromSSP` has shown that every primitive central idempotent of any monomial group of order at most 500 is realizable by a strongly Shoda pair. This suggest the question of whether every primitive central idempotent of $\mathbb{Q}G$ for G monomial is realizable by a strongly Shoda pair.

3 Simple factors

In this section we explain the use of `SimpleAlgebraFromSSP` and `SimpleFactorsFromListOfSSP`. We start considering a general crossed product $R * A$ over a finite abelian group A .

Let $A = C_1 \times \dots \times C_m$, where each C_i is a cyclic group of order o_i , generated by c_i , and let g_i be an invertible homogeneous element of degree c_i of $R * A$. Then $B = \{g_1^{i_1} \dots g_m^{i_m} : 0 \leq i_j < o_j\}$ is a homogeneous basis of $R * A$. For every $i = 1, \dots, m$ let:

- ψ_i be the automorphism of R given by $r^{\psi_i} = g_i^{-1} r g_i$ ($r \in R$);
- $s_i = g_i^{o_i}$ and
- for every $i < j \leq m$ let $t_{ij} = g_j^{-1} g_i^{-1} g_j g_i$.

Then the action and twisting of $R * A$ associated to the homogeneous basis B is determined by the data $(o_i, \psi_i, s_i)_{0 \leq i < m}$ and $(t_{ij})_{0 \leq i < j \leq m}$. This can be expressed alternatively by saying that the crossed product $R * A$ is the R -algebra given by the following presentation:

$$R(g_1, \dots, g_m | r g_i = g_i r^{\psi_i}, g_i^{o_i} = s_i, g_j g_i = g_i g_j t_{ij}, r \in R, 1 \leq i < j \leq m). \quad (3.2)$$

Let (K, H) be a strongly Shoda pair and let $k = [K : H]$, $N = N_G(H)$, $n = [G : N]$, x a generator of K/H and $\phi : N/K \rightarrow N/H$ a left inverse of the canonical projection $N/H \rightarrow N/K$. In Proposition 1.2 we have seen how to describe the simple algebra $\mathbb{Q}Ge(G, K, H)$ from n, k, x and ϕ as $M_n(\mathbb{Q}(\xi_k) * N/K)$. Moreover in Proposition 2.4 we have seen that N/K is abelian. We are going to use this fact to show how to describe the crossed product $\mathbb{Q}(\xi_k) * N/K$ by a list of non negative numbers. Following the general approach explained in the previous paragraph for crossed products of abelian groups we first have to express N/K as a direct product of cyclic groups, say $N/K = C_1 \times \dots \times C_m$. Then we have to find a representative $g_i \in N/H$ of a generator of C_i for each i , that is a the projection of g_i in N/K is a generator of C_i . Next we have to describe the data o_i, ψ_i, s_i and t_{ij} needed to obtain the presentation of (3.2). Since ψ_i is an automorphism of the cyclotomic field $\mathbb{Q}(\xi_k)$, to describe it we only need to know $\psi_i(\xi_k)$. By Proposition 1.2, $\psi_i(\xi_k) = \xi_k^{\alpha_i}$ if and only if $x^{g_i} = x^{\alpha_i}$. Using again Proposition 1.2 one has that $s_i = \xi_k^{\beta_i}$ if $g_i^{o_i} = x^{\beta_i}$, and $t_{ij} = \xi_k^{\gamma_{ij}}$ if $[g_j, g_i] = x^{\gamma_{ij}}$. Therefore $\mathbb{Q}Ge(G, K, H)$ can be described from the following 4-tuple:

$$(n, k, (o_i, \alpha_i, \beta_i)_{1 \leq i \leq m}, (\gamma_{ij})_{1 \leq i < j \leq m}). \quad (3.3)$$

More precisely:

Proposition 3.1 *Let (K, H) be a strongly Shoda pair of G and let $k = [K : H]$, $N = N_G(H)$, $n = [G : N]$, x a generator of K/H and $N/K = C_1 \times \dots \times C_m$ where each C_i is cyclic of order o_i . For every $i = 1, \dots, m$ let $g_i \in N/H$ be a representative of a generator of C_i . Let $(\alpha_i)_{1 \leq i \leq m}$, $(\beta_i)_{1 \leq i \leq m}$ and $(\gamma_{ij})_{1 \leq i < j \leq m}$ be tuples of integers satisfying the following relations:*

$$x^{g_i} = x^{\alpha_i}, \quad g_i^{o_i} = x^{\beta_i}, \quad [g_j, g_i] = x^{\gamma_{ij}}.$$

Then $\mathbb{Q}Ge(G, K, H) \simeq M_n(A)$ where A is the algebra defined by the following presentation:

$$A = \mathbb{Q}(\xi_k)(g_1, \dots, g_m | \xi_k g_i = g_i \xi_k^{\alpha_i}, g_i^{o_i} = \xi_k^{\beta_i}, g_j g_i = g_i g_j \xi_k^{\gamma_{ij}}, 1 \leq i < j \leq m). \quad (3.4)$$

The function `SimpleAlgebraFromSSP`, when applied to (G, K, H) , where (K, H) is a strongly Shoda pair of G computes the 4-tuple of (3.3) which describes $\mathbb{Q}Ge(G, K, H)$ as the $n \times n$ matrix ring of the algebra A of (3.4). Moreover the list $(o_i)_{1 \leq i \leq m}$ computed by `SimpleAlgebraFromSSP` is the list of invariant factors of the abelian group $N_G(H)/K$, that is o_{i+1} divides o_i for every $1 \leq i < m$.

Finally the function `SimpleFactorsFromListOfSSP`, when applied to (G, S) , where S is a list of strongly Shoda pairs of G , applies `SimpleAlgebraFromSSP` to (G, K, H) for (K, H) running through S . In particular, if all the primitive central idempotents of $\mathbb{Q}G$ are realizable by strongly Shoda pairs, then the combination of `StronglyShodaPairs` and `SimpleFactorsFromListOfSSP` describes the Wedderburn decomposition of $\mathbb{Q}G$.

In the remainder of this section we are going to show some examples of computation of the Wedderburn decomposition of some rational group algebras. First we are going to compute the Wedderburn decomposition of $\mathbb{Q}G$ for all the indecomposable groups G of order 54. There are exactly 6 non isomorphic indecomposable groups of order 54, namely the groups given by the following presentations:

$$\begin{aligned} G_1 &= \langle a, b | a^{27} = b^2 = 1, a^b = a^{-1} \rangle, \\ G_2 &= \langle a, b | a^9 = b^6 = 1, a^b = a^5 \rangle, \\ G_3 &= \langle a_1, a_2, b | a_1^9 = a_2^3 = b^2 = 1, [a_1, a_2] = 1, a_i^b = a_i^{-1} \rangle, \\ G_4 &= \langle a_1, a_2, b | a_i^3 = b^6 = 1, [a_1, a_2] = 1, a_1^b = a_1^{-1}, a_2^b = a_1 a_2^{-1} \rangle, \\ G_5 &= \langle a_1, a_2, a_3, b | a_i^3 = b^2 = 1, [a_i, a_j] = 1, a_i^b = a_i^{-1} \rangle, \\ G_6 &= \langle a_1, a_2, a_3, b | a_i^3 = b^2 = 1, [a_1, a_i] = [a_1, b] = 1, a_2^{a_3} = a_1 a_2, a_2^b = a_2^{-1}, a_3^b = a_3^{-1} \rangle. \end{aligned}$$

The table in Figure 2 shows the output of `SimpleFactorsFromListOfSSP(G_i, StronglyShodaPairs(\mathbb{Q}G_i))` for $1 \leq i \leq 6$.

i	Output
1	[[[1, 1, [], []], [1, 2, [], []], [1, 3, [[2, 2, 0]], []], [1, 9, [[2, 8, 0]], []], [1, 27, [[2, 26, 0]], []]]
2	[[[1, 1, [], []], [1, 2, [], []], [1, 3, [], []], [2, 3, [], []], [1, 3, [[2, 2, 0]], []], [1, 6, [], []], [3, 3, [[2, 2, 0]], []]]
3	[[[1, 1, [], []], [1, 2, [], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 9, [[2, 8, 0]], []], [1, 9, [[2, 8, 0]], []], [1, 9, [[2, 8, 0]], []]]
4	[[[1, 1, [], []], [1, 2, [], []], [1, 3, [], []], [2, 3, [], []], [1, 6, [], []], [1, 3, [[2, 2, 0]], []], [3, 3, [[2, 2, 0]], []]]
5	[[[1, 1, [], []], [1, 2, [], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []]]
6	[[[1, 1, [], []], [1, 2, [], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [1, 3, [[2, 2, 0]], []], [3, 3, [], []], [3, 6, [], []]]

Figure 2: Output of `SimpleFactorsFromListOfSSP(G_i, StronglyShodaPairs(\mathbb{Q}G_i))`.

Notice that all 4-tuples in the lists of the table are of one of the following two forms:

$$[n, k, [], []] \quad [n, k, [[2, k-1, 0]], []]$$

for n and k integers. According to Proposition 3.1, the first list correspond to the algebra $M_n(\mathbb{Q}(\xi_k))$ and the second one to $M_n(A_k)$ where $A_k = \mathbb{Q}(\xi_k)(g|\xi_k g = g\xi_k^{-1}, g^2 = 1)$. Thus A_k is a quaternion algebra over its centre and this centre is $\mathbb{Q}(\xi_k + \xi_k^{-1})$. Since $g^2 = 1$, $g + 1$ is a zero divisor of A_k and therefore A_k is not a division ring. We conclude that $A_k \simeq M_2(\mathbb{Q}(\xi_k + \xi_k^{-1}))$ and $M_n(A_k) \simeq M_{2n}(\mathbb{Q}(\xi_k + \xi_k^{-1}))$. Notice that for k a divisor of 4 or 6, $\xi_k + \xi_k^{-1} \in \mathbb{Q}$ and hence the centre of A_k is \mathbb{Q} . Collecting all this information we obtain the Wedderburn decomposition of each $\mathbb{Q}G_i$:

$$\begin{aligned} \mathbb{Q}G_1 &\simeq 2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_9 + \xi_9^{-1})) \oplus M_2(\mathbb{Q}(\xi_{27} + \xi_{27}^{-1})), \\ \mathbb{Q}G_2 &\simeq 2\mathbb{Q} \oplus 2\mathbb{Q}(\xi_3) \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_3)) \oplus M_6(\mathbb{Q}), \\ \mathbb{Q}G_3 &\simeq 2\mathbb{Q} \oplus 4M_2(\mathbb{Q}) \oplus 3M_2(\mathbb{Q}(\xi_9 + \xi_9^{-1})), \\ \mathbb{Q}G_4 &\simeq 2\mathbb{Q} \oplus 2\mathbb{Q}(\xi_3) \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_3)) \oplus M_6(\mathbb{Q}), \\ \mathbb{Q}G_5 &\simeq 2\mathbb{Q} \oplus 13M_2(\mathbb{Q}), \\ \mathbb{Q}G_6 &\simeq 2\mathbb{Q} \oplus 4M_2(\mathbb{Q}) \oplus 2M_3(\mathbb{Q}(\xi_3)). \end{aligned}$$

All the crossed products encountered in the previous examples are cyclic algebras with trivial twisting. Now we present a rational group algebra with a non cyclic simple quotient. Consider the following group of order 48:

$$G = \langle a, b, c | a^{12} = b^2 a^6 = c^2 a^6 = 1, a^b = a^{-1}, a^c = a^7, b^c = ba^9 \rangle.$$

The output of `SimpleFactorsFromListOfSSP(StronglyShodaPairs(QG))` is

$$\begin{aligned} &[[1, 1, [], []], [1, 2, [], []], [1, 2, [], []], \\ &[1, 2, [], []], [2, 2, [], []], [1, 3, [[2, 2, 0]], []], \\ &[2, 6, [], []], [1, 6, [[2, 5, 0]], []], \\ &[1, 8, [[2, 7, 4]], []], \\ &[1, 12, [[2, 11, 6], [2, 7, 6]], [[3]]] \end{aligned}$$

which yields the following Wedderburn decomposition of $\mathbb{Q}G$:

$$\mathbb{Q}G = 4\mathbb{Q} \oplus 3M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\xi_3)) \oplus A \oplus B$$

where

$$\begin{aligned} A &= \mathbb{Q}(\xi_8)(g|\xi_8 g = g\xi_8^{-1}, g^2 = -1), \\ B &= \mathbb{Q}(\xi_{12})(g, h|\xi_{12} g = g\xi_{12}^{-1}, \xi_{12} h = -h\xi_{12}, g^2 = h^2 = -1, hg = ghi). \end{aligned}$$

Notice that the centre of A is $\mathbb{Q}(\xi_8 + \xi_8^{-1}) = \mathbb{Q}(\sqrt{2})$ and A has the following presentation as algebra over its centre:

$$A = \mathbb{Q}(\sqrt{2})(i, g | i^2 = g^2 = -1, ig = -gi) = \mathbb{H}(\mathbb{Q}(\sqrt{2})),$$

that is A is the Hamiltonian quaternion algebra over $\mathbb{Q}(\sqrt{2})$ which is a division ring. However it is more difficult to describe B as a matrix ring over a division ring. This needs more sophisticated methods and this examples shows the limitations of our method.

4 Comparing running time

In this section we present an experimental comparison of running time of the functions `PCIsFromSSP` and `PCIsFromShodaPairs` with the classical algorithm that computes the primitive central idempotents of $\mathbb{Q}G$ using the character table of G [14]. In order to perform this comparison we have included in the package of [8] a function `PCIsUsingCharacterTable` that computes the primitive central idempotents of $\mathbb{Q}G$ using the classical method. Then we have written a program that using the library of GAP [3] of groups of order at most 500 computes the primitive central idempotents of $\mathbb{Q}G$ for a sample S of 1523 monomial groups of orders at most 500 using the three functions and collects the running time of each computation in a file. Then this information is processed to produce Figure 3 where the curves SSP, Sh and Ch represent the

graphic of the functions that associates to each $2 \leq n \leq 500$ the average time, measured in milliseconds, that the algorithms `PCIsFromSSP`, `PCIsFromShodaPairs` and `PCIsUsingCharacterTable` took to compute the primitive central idempotents of a group in S of order $\leq n$ in our computer (AMD Athlon 1.0GHz, 128Mb SDRAM).

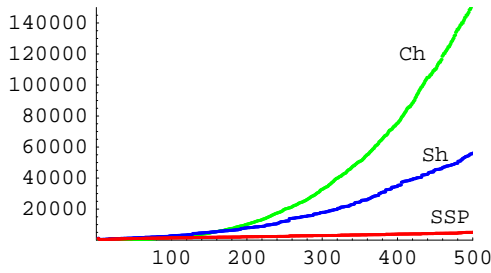


Figure 3: Average time comparison.

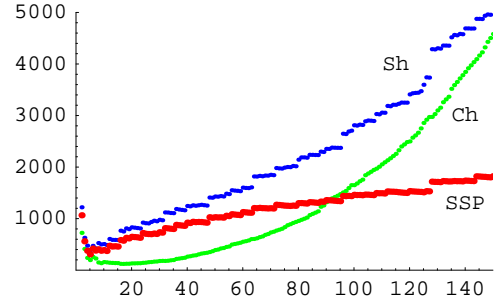


Figure 4: Detail of Figure 3.

Notice that `PCIsFromSSP` computes the primitive central idempotents of $\mathbb{Q}G$ much faster than the other two algorithms. However it should be noticed that for groups of order at most 100, the classical algorithm is faster than the other algorithms as shows Figure 4, which is a portion of Figure 3.

The function used by `PCIsUsingCharacterTable` to compute the irreducible characters is the function `Irr` of GAP (see 69.8.2 of the Manual of [3]). For some classes of groups there exist specific algorithms to compute irreducible characters that are faster than the algorithm implemented by `Irr`. For monomial groups there are two algorithms due to Conlon [2] and Baum and Clausen [1] and GAP has functions that implement these algorithms (see 69.12 of the Manual [3]). We have performed a similar comparison of running time where `PCIsUsingCharacterTable` uses these functions instead of `Irr`. Although the running time of the computation of the irreducible characters are better this is non significant for computing the primitive central idempotents of the rational group algebra.

On the other hand, the graphic of Figure 3 represents average time. In fact the time spent by any of the algorithms vary very much even for groups of the same cardinality and for some concrete group, not necessarily of small cardinality, the classical method is faster than our methods. Figure 5 represents the pairs $\{(|G|, T(G)) : G \in S\}$ where $T(G)$ is the running time that our computer took to compute the primitive central idempotents of $\mathbb{Q}G$ using `PCIsFromSSP`. For most groups G in S , the time $T(G)$ is less than 15000 milliseconds. Figure 6 represents a portion of Figure 5 for a better display of the most relevant part of the graphic.

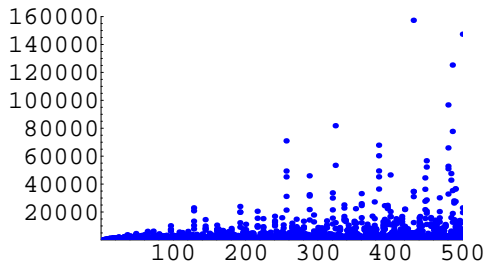


Figure 5: Order versus time comparison.

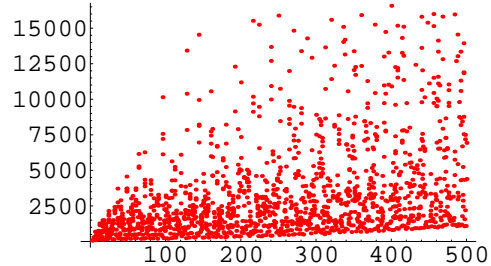


Figure 6: Detail of Figure 5.

Finally, the running time of `PCIsFromSSP` and `PCIsFromShodaPairs` depends very much on the number of conjugacy classes of subgroups of the input group. In fact our computer has not been able to compute the primitive central idempotents of $\mathbb{Q}G$ for the group identified by GAP as `SmallGroup(256,56090)` using `PCIsFromSSP`. This group has 29593 conjugacy classes of subgroups. Just computing these conjugacy classes consumes a lot of time and memory which makes our computer to crash when applying `PCIsFromSSP` or `PCIsFromShodaPairs` to this group. The functions `PCIsFromSSP` and `PCIsFromShodaPairs` use the GAP command `ConjugacyClassesSubgroups` to compute the conjugacy classes of subgroups. It would be useful to have an algorithm which computes the conjugacy classes of subgroups H of G such that

$\langle\langle N_G(H)/H \rangle\rangle', Z(N_G(H)/H)\rangle$ is cyclic (see Proposition 2.4), without computing all the conjugacy classes. This may increase the speed of `PCIsFromSSP`.

We finish explaining how the sample S was selected. To do this we explain how we selected the sample $S(n)$ formed by the groups in S of order n . The idea is taking about 5 groups evenly distributed in the list of non isomorphic groups of order n ordered as in the GAP library of small groups. For every positive number n let $N(n)$ be the number of non isomorphic groups of order n and if $n \leq 500$ and $1 \leq i \leq N(n)$ then let $G_{n,i}$ be the i -th group of order n in the GAP library, that is $G_{n,i}$ is the group that GAP identifies as `SmallGroup(n, i)`. Basically $S(n)$ is formed by groups $G_{n,i}$ for i an integer close to $\frac{N(n)(2k+1)}{10}$, for $k = 1, \dots, 5$. More precisely, let $[x]$ denote the integral part of a real number x and let $inc := \max(1, [N(n)/5])$. Then $S(n)$ is initialized as the empty list and i is initialized as $\max(1, [inc/2])$. If $G = G_{n,i}$ is monomial then the group G is added to the list $S(n)$ and i is resettled as $i + inc$. Otherwise i is resettled as $i + 1$. In both cases the selection continues until $i > N(n)$. The resulting set $S(n)$ has a minimum of 1 and a maximum of 9 groups of order n which are evenly distributed in the GAP library.

References

- [1] U. Baum and M. Clausen, *Computing irreducible representations of supersolvable groups*, Math. Comput., 207, 351-359, 1994.
- [2] S.B. Conlon, Calculating characters of p-groups. J. Symbolic Comput., 9(5 & 6), 535-550, 1990.
- [3] The GAP Group, *GAP — Groups, Algorithms, and Programming, Version 4.3*, 2002 (<http://www.gap-system.org>).
- [4] A. Herman, *On the automorphism group of rational group algebras of metacyclic groups*, Comm. in Algebra, 25(7) (1997) 2085-2097.
- [5] E. Jespers and G. Leal, *Generators of large subgroups of the unit group of integral group rings*, Manuscripta Math. 78 (1993) 303-315.
- [6] E. Jespers, G. Leal and A. Paques, *Central idempotents in rational group algebras of finite nilpotent groups*, to appear in Jour. Alg. and its applications.
- [7] E. Jespers and Á. del Río, *A structure theorem for the unit group of the integral group ring of some finite groups*, Journal für die Reine und Angewandte Mathematik, 521 (2000) 99-117.
- [8] A. Olivieri and Á. del Río, *wedderga, A GAP 4 package for computing central idempotents and simple components of rational group algebras*.
- [9] A. Olivieri, Á. del Río and J.J. Simón, *On monomial characters and central idempotents of rational group algebras*, to appear in Comm. in Algebra.
- [10] D. Passman, *Infinite Crossed Products*, Academic Press, 1989.
- [11] Á. del Río and M. Ruiz, *Computing large direct products of free groups in integral group rings*, Comm. in Algebra 30(4) (2002) 1751-1767.
- [12] J. Ritter and S.K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. 324 (1991) 603-621.
- [13] S.K. Sehgal, *Units of integral group rings*, Longman Scientific and Technical Essex, 1993.
- [14] T. Yamada, *The Schur Subgroup of the Brauer Group*. Lecture Notes in Math. Vol. 397, Springer-Verlag, 1974.

Departamento de Matemáticas, Universidad Simón Bolívar, Apartado Postal 89000, Caracas 1080-A, Venezuela. olivieri@usb.ve

Departamento de Matemáticas, Universidad de Murcia, 30100 Murcia, Spain. adelrio@um.es