Finite Fields and Their Applications 51 (2018) 62–70

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Idempotents and codes in some non semi-simple metacyclic group algebras

Mostafa Alaoui Abdallaoui, Mohammed El Badry, Abdelfattah Haily *

Department of Mathematics, Chouaib Doukkali University, BP 20, El jadida, Morocco

ARTICLE INFO

Article history:
Received 29 April 2017
Received in revised form 8 January 2018
Accepted 9 January 2018
Available online xxxx
Communicated by Dieter Jungnickel

MSC:
primary 11T30
secondary 11T71, 94B60

Keywords:
Group algebra
Primary decomposition
Metacyclic code

ABSTRACT

We consider group algebra of a metacyclic group of order $p^n q$ over a field of characteristic p, where p and q are distinct prime numbers. We determine the terms of the primary decomposition of this algebra. The central primitive idempotents are also calculated. In the end we give the characteristics (dimension and minimal weight) of codes generated by these idempotents.

1. Introduction and notations

Throughout this paper, $\mathbb{F}$ denotes a finite field of characteristic p. If G is a finite group, then the group algebra $\mathbb{F}[G]$ is defined as the $\mathbb{F}$-linear space with basis the elements of G,

* Corresponding author.
E-mail address: haily.a@ucd.ac.ma (A. Haily).

https://doi.org/10.1016/j.ffa.2018.01.004

where the addition and multiplication by scalars are defined componentwise and the ring multiplication is given by

$$(\sum_{g\in G} x_g g)(\sum_{h\in G} y_h h) = \sum_{g,\, h\in G} x_g y_h gh$$

Maschke's theorem says that $\mathbb{F}[G]$ is semisimple (and then decomposes into finite product of matrix rings over division algebras), if and only if, p does not divide the order $|G|$ of G. When p divides $|G|$, the structure of $\mathbb{F}[G]$ is more complicated and no general decomposition theorem is known. However, in some cases, considered in this work, there exists another type of decomposition, given by the following theorem:

Theorem 1. *[6, Chapter 6, Lemma 1.10] Let G be a finite group and $\mathbb{F}$ a perfect field of characteristic p dividing the order of G. Assume that $\mathbb{F}$ is a splitting field of G and $G = HP$, where P is a Sylow-p-subgroup, and H a normal p'-subgroup of G. Then the following decomposition holds:*

$$\mathbb{F}[G] \cong \prod_{i=0}^{k} \mathcal{M}_{n_i}(\mathbb{F}[P_i])$$

where, for every $i = 0, 1, \ldots, k$, $n_i = m_i|\Omega_i|$, Ω_i is the orbit of conjugation action of G on the set of central primitive idempotents of $\mathbb{F}[H]$, m_i is such that $\mathbb{F}[H]e_i \cong \mathcal{M}_{m_i}(\mathbb{F})$ and $P_i = Cent(e_i) \cap P$ for every $e_i \in \Omega_i$, where $Cent(e_i)$ is the centralizer of e_i.

By splitting field of G we mean that $\mathbb{F}$ contains a primitive n-th root of unity, where n is the order of G or, equivalently, if $\mathbb{F}$ is finite, that n divides $|\mathbb{F}| - 1$. Notice that $e_0 = \dfrac{\sum_{h\in H} h}{|H|}$ is the principal idempotent of $\mathbb{F}[H]$, and is central in $\mathbb{F}[G]$, so that $n_0 = 1$ and $P_0 = P$.

From the preceding theorem, it follows that the number $k + 1$ of components in the decomposition is equal to the number of conjugacy classes of central primitive idempotents of $\mathbb{F}[H]$, which in turn is equal, by the Brauer theorem [5, Theorem 8.9], to the number of the conjugacy classes of the p'-elements, that is the elements of H in our case.

Moreover, since $p \nmid |H|$, then by Maschke's and Wedderburn–Artin Theorems, and also the splitting condition, we have $\mathbb{F}[H] \cong \prod_{i=1}^{s} \mathcal{M}_{m_i}(\mathbb{F})$. If moreover H is abelian, then $\mathbb{F}[H]$ is isomorphic to the product of $|H|$ copies of $\mathbb{F}$ and has $|H|$ primitive (central) idempotents.

In general the determination of idempotents in a group algebra in terms of elements of G and $\mathbb{F}$ is a difficult problem even in the semisimple case. This problem has been treated by some authors, for example [4] in the abelian case and [3] in the case of semisimple case and when the group is dihedral. When the group is cyclic we have the following result