Finite Fields and Their Applications 35 (2015) 204–214

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Structure of finite dihedral group algebra

F.E. Brochero Martínez

Departamento de Matemática, Universidade Federal de Minas Gerais, UFMG, Belo Horizonte, MG 30123-970, Brazil

ARTICLE INFO

Article history:
Received 30 July 2014
Received in revised form 27 February 2015
Accepted 1 May 2015
Available online 17 May 2015
Communicated by Dieter Jungnickel

MSC:
primary 20C05
secondary 16S34

Keywords:
Central idempotent
Dihedral group

ABSTRACT

In this article, we show explicitly all central irreducible idempotents and their Wedderburn decomposition of the dihedral group algebra $\mathbb{F}_q D_{2n}$, in the case when every divisor of n divides $q-1$.

This characterization depends to the relation of the irreducible idempotents of the cyclic group algebra $\mathbb{F}_q C_n$ and the central irreducible idempotents of the group algebras $\mathbb{F}_q D_{2n}$.

1. Introduction

Let K be a field and G be a group with n elements. It is known that, if $char(K) \nmid n$, then the group algebra KG is semisimple and as a consequence of the Wedderburn Theorem, we have that KG is isomorphic to a direct sum of matrix algebras over division rings, such that each division algebra is a finite algebra over the field K, i.e., there exists an isomorphism

$$\rho : KG \to M_{l_1}(D_1) \oplus M_{l_2}(D_2) \oplus \cdots \oplus M_{l_t}(D_t),$$

E-mail address: fbrocher@mat.ufmg.br.

http://dx.doi.org/10.1016/j.ffa.2015.05.002
1071-5797/

where D_j are division rings such that $|G| = \sum_{j=1}^{t} l_j^2 [D_j : K]$. Observe that KG has t central irreducible idempotents, each one of the form

$$e_i = \rho^{-1}(0 \oplus \cdots \oplus 0 \oplus I_i \oplus 0 \oplus \cdots \oplus 0),$$

where I_i is the identity matrix of the component $M_{l_i}(D_j)$. Then, the isomorphism ρ determines explicitly each central irreducible idempotent.

In the case $K = \mathbb{Q}$, the calculus of central idempotents and Wedderburn decomposition is widely studied; the classical method to calculate the primitive central idempotents of group algebras depends on computing the character group table. Another method is shown in [8], where Jespers, Leal and Paques describe the central irreducible idempotents when G is a nilpotent group, using the structure of its subgroups, without employing the characters of the group. Generalizations and improvements of this method can be found in [11], where the authors provide information about the Wedderburn decomposition of $\mathbb{Q}G$. This computational method is also used in [2] to compute the Wedderburn decomposition and the primitive central idempotents of a semisimple finite group algebra KG, where G is an abelian-by-supersolvable group G and K is a finite field.

The structure of KG when $G = D_{2n}$ is the dihedral group with $2n$ elements is well known for $K = \mathbb{Q}$ (see [7]). In [5], Dutra, Ferraz and Polcino Milies impose conditions over q and n in order for $\mathbb{F}_q D_{2n}$ to have the same number of irreducible components as that of $\mathbb{Q}D_{2n}$. This result is generalized in [6], where Ferraz, Goodaire and Polcino Milies find, for some families of groups, conditions on q and G in order for $\mathbb{F}_q G$ to have the minimum number of simple components.

In this article, assuming that every prime factor of n divides $q-1$, we show explicitly the central irreducible idempotents of $\mathbb{F}_q D_{2n}$ and an isomorphism between the group algebra $\mathbb{F}_q D_{2n}$ and its Wedderburn decomposition. Observe that this isomorphism also shows the structure of $\mathcal{U}(\mathbb{F}_q D_{2n})$, the unit group of $\mathbb{F}_q D_{2n}$.

2. Idempotents of cyclic group algebra

Throughout this article, $\mathbb{F}_q$ denotes a finite field of order q, where q is a power of a prime and n is a positive integer such that $\gcd(n, q) = 1$. For every polynomial $g(x)$ with $g(0) \neq 0$, g^* denotes the *reciprocal polynomial* of g, i.e., $g^*(x) = x^{\deg(g)} g(\frac{1}{x})$. We say that a polynomial g is an auto-reciprocal polynomial if g and g^* have the same roots in its splitting field. The polynomial $x^n - 1 \in \mathbb{F}_q[x]$ splits into monic irreducible factors as

$$x^n - 1 = f_1 f_2 \cdots f_r f_{r+1} f_{r+1}^* f_{r+2} f_{r+2}^* \cdots f_{r+s} f_{r+s}^*,$$

where $f_1 = x - 1$, $f_2 = x + 1$ if n is even, and $f_j^* = f_j$ for $2 \le j \le r$, where r is the number of auto-reciprocal factors in the factorization and $2s$ the number of non-auto-reciprocal factors.