Finite Fields Appl. 28 (2014) 123–131

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Explicit idempotents of finite group algebras

F.E. Brochero Martínez *, C.R. Giraldo Vergara

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

ARTICLE INFO

Article history:
Received 5 August 2013
Received in revised form 20 December 2013
Accepted 7 February 2014
Available online 6 March 2014
Communicated by Dieter Jungnickel

MSC:
primary 16S34
secondary 94B05

Keywords:
Irreducible cyclic codes
Primitive idempotents

ABSTRACT

Let $\mathbb{F}_q$ be a finite field, G a finite cyclic group of order p^k and p an odd prime with $\gcd(q,p)=1$. In this article, we determine an explicit expression for the primitive idempotents of $\mathbb{F}_qG$. This result extends the results in [1,2,8].

1. Introduction

Let G be a finite cyclic group of order n and $\mathbb{F}_q$ a finite field of order q, where q is prime relative to n. The cyclic codes of length n over $\mathbb{F}_q$ can be viewed as an ideal in the group algebra $\mathbb{F}_qG$ and each ideal is generated by an idempotent of $\mathbb{F}_qG$. By the representation theorem of abelian groups we know that

$$G \simeq C_{p_1^{\beta_1}} \times \cdots \times C_{p_r^{\beta_r}}$$

* Corresponding author.
E-mail addresses: fbrocher@mat.ufmg.br (F.E. Brochero Martínez), carmita@mat.ufmg.br (C.R. Giraldo Vergara).

http://dx.doi.org/10.1016/j.ffa.2014.02.002
1071-5797/

where $C_{p_j^{\beta_j}}$ is a cyclic group of order $p_j^{\beta_j}$ and $p_1, \dots, p_r$ are distinct primes. In addition, it is well known that

$$\mathbb{F}_q G \simeq \mathbb{F}_q C_{p_1^{\beta_1}} \otimes \cdots \otimes \mathbb{F}_q C_{p_r^{\beta_r}}.$$

From this fact, in order to construct the idempotents of the cyclic group algebra $\mathbb{F}_q G$, it is enough to consider the case $G = C_n$ where n is a power of a prime. Observe that the condition $\gcd(n, q) = 1$ is necessary by the Maschke theorem (see [4, Theorem 10.8]).

2. Primitive idempotents: General calculation

Let $\Phi_d(x)$ denote the d-th cyclotomic polynomial, i.e., $\Phi_d(x)$ can be defined recursively by $\Phi_1(x) = x - 1$ and $x^k - 1 = \prod_{d|k} \Phi_d(x)$. It is well known (see [5, p. 65, Theorem 2.47]) that if $\gcd(q, d) = 1$ then $\Phi_d(x)$ can be factorized into $r_d = \frac{\varphi(d)}{s_d}$ distinct monic irreducible polynomials of the same degree s_d over $\mathbb{F}_q$ and $s_d = \operatorname{ord}_d q = \min\{k \in \mathbb{N}^* \mid q^k \equiv 1 \pmod{d}\}$, i.e. $\Phi_d(x)$ can be factorized in $\mathbb{F}_q[x]$ as $f_{d,1} \cdot f_{d,2} \cdots f_{d,r_d}$, where each $f_{d,j}$ is an irreducible polynomial of degree s_d, and then

$$x^n - 1 = \prod_{d|n} \prod_{j=1}^{r_d} f_{s,j}.$$

Observe that if K is a decomposition field of the cyclotomic polynomial $\Phi_d(x)$, then for each pair $f_{d,i}$, $f_{d,j}$ there exists $\tau \in Gal(K|\mathbb{F}_q)$ such that $\tau(f_{d,i}) = f_{d,j}$.

By the Chinese remainder theorem, we know that

$$\mathbb{F}_q C_n \simeq \frac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle} \simeq \bigoplus_{d|n} \bigoplus_{j=1}^{r_d} \frac{\mathbb{F}_q[x]}{\langle f_{d,j} \rangle}$$

where the $\mathbb{F}_q$-algebra isomorphisms are naturally defined using a generator g of C_n as $g \mapsto \bar{x} \mapsto (\bar{x}, \dots, \bar{x})$.

Since each direct sum term is a field, then this decomposition is a Weddeburn decomposition of the group algebra and each primitive idempotent is of the form $(\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}, \dots, \bar{0})$. Therefore, if $e_{d,j}$ is a primitive idempotent of $\mathbb{F}_q C_n$, then it can be seen as a polynomial $e_{d,j}(x)$ with the following properties:

(1) $\deg(e_{d,j}(x)) < n$,
(2) $e_{d,j}(x)$ is divisible by f_{d_1,j_1} for all $(d_1, j_1) \neq (d, j)$,
(3) $e_{d,j}(x) - 1$ is divisible by $f_{d,j}$.

From these three properties, we have the following

Theorem 2.1. *Let $\mathbb{F}_q$ be a finite field with q element and $n \in \mathbb{N}^*$ such that* $\gcd(q, n) = 1$, *then each primitive idempotent of $\mathbb{F}_q C_n$ is of the form*