Vol.09 Issue-01, (January - June, 2017) ISSN: 2394-9309 (E) / 0975-7139 (P)
Aryabhatta Journal of Mathematics and Informatics (Impact Factor- 5.856)

ON A CLASS OF GROUP ALGEBRAS AND THEIR PRIMITIVE IDEMPOTENTS

[1]Dr.M.Mary Jansi Rani ,[2]V.Sangeetha,[3]K.Jamshida

[1]Head and Assistant Professor, Department of Mathematics, Thanthai Hans Roever College

Perambalur, Tamilnadu, India.[2,3]Research scholar, Department of Mathematics, Kadhirmohideen College,Adirampattinam,Pattukottai, Tamilnadu, India.

ABSTRACT

Let F denotes a finite field having q = t (t is a prime,s ≥ 1) elements .We Consider the group algebra F_qG where G is a finite group of order n. When F contains a primitive n^{th} root of unity (implying that characteristic of $F_q$does not divide n) there is a known formula for obtaining the fall system of primitive idempotent of F_qG which is also an orthogonal $F_q$basis for the group algebra F_qG. The approach is via group character which are homeomorphisms from G into the cyclic group F_q^* of non zero elements of F_q.Earlier, ManjuPruthi ,S.K .Aroraetal have obtained expressions for primitive idempotent of the group algebra F_qC_m where C_m is a cyclic group of order m . They used techniques from the notation of q-cyclotomiccosets modulo m. The method presented here explains the role of “semi simplicity”of the ring $F_q[x]/(x^m-1)$ and its connection with the group algebra F_qC_m. Inparticular examples are given when the group G is cyclic of order n or the dihedral group D_n of order 2n .

KEYWORDSCharacter group, group algebra, semi–simple, primitive idempotents,cyclic group of order n, dihedral group D_n.

INTRODUCTION

Let R be a commutative ring with unity 1_R. Suppose that we are given a group G. By a group algebra RG of G over R .We mean an algebraic structure consisting of all formal linear combinations

$$X = \sum_{g\in G} X_g.g, \qquad X_g \in R \text{ with finitely many } X_g \neq O_R$$

$$Y = \sum_{g\in G} y_g.g \qquad Y_g \neq O_R$$ is a second element of RG, then by definition X=Y if and only if,$X_g = Y_g$ for all $g\in G$. As an illustration, we take the case when G is a cyclic group of order n. Let g be a generator for G so that g^n= e. The mapping

$f : G \rightarrow R[X] / (X^n - 1)$ is given by $f(g) = X + (X^n - 1)$…………………(1) That is f(g) is the cosets $X + (X^n - 1)$ in the quotient ring $R[X] / (X^n - 1)$. (1) is an injective homomorphism whose image is an R– basis for $R[X] / (X^n - 1)$. Then$R[X] / (X^n - 1)$ is isomorphic to the group algebra RG in [4] This takes us to the study of cyclic codes of length n over a finite field F_q .

1.1 DEFINITION An element $r \in R$ is called an idempotent if $r^2 = r$.

1.2 DEFINITION Two idempotent $u, v \in R$ are said to be orthogonal if $u v = O_R$

1.3 DEFINITIONA non zero idempotent u is called ‘primitive ‘if it cannot written as a sum of two non zero orthogonal idempotent.The motivation for this note is from the interesting papers of [5] on primitive idempotent of a group algebra, cyclic codes of length 2^m [7] minimal codes of prime power of length [8] and minimal cyclic codes of length $2p^n$ [6].Their approach is via the notion of q-cyclotomiccosets modulo n. But it appears that a fall system of primitive idempotent of a group algebra FG could be obtained via the notion of group characters. We are attempting a study of primitive idempotent of the group algebra F_qC_m where C_m is a cyclic group of order m. We also consider the group algebra F_qD_n where D_n is dihedral group of order 2n.

2. PRELIMINARIES

We consider only commutative rings with identity 1_R

2.1 DEFINITION An ideal I of R is called a minimal ideal if $I \neq (O_R)$ and for every ideal J such that $(O_R) \subset J \subset I$ either $J = (O_R)$ or $J = I$.

2.2 DEFINITIONA ring R is said to satisfy the descending chain condition on ideals if for every chain $I_1 \supset I_2 \supset I_3 \supset$ ………of ideals of R,there is an integer m such that $I_j = I_m$ for all $j \geq m$.

2.3 DEFINITIONA ring R is called an Artinian ring if R satisfies the descending chain condition on ideals.

2.4 DEFINITION Let R be a ring .An element $X \in R$ is called a nilpotent element if $X^n = O_R$ for some $n \geq 1$.

2.5 DEFINITION The ideal N (R) is called the nil radical of R it is known that the nil radical of R is the intersection of all prime ideals of R.

2.6 DEFINITION The Jacobson radical J(R) of R is defined as the intersection of all the maximal ideals of R.

2.7 DEFINITION

A ring R is said to be semi simple if its Jacobson radical J (R) is (O_R).

2.8 DEFINITION

Given a ring R and an element $e \in R$ such that $e^2 = e$ then e is called an idempotent element of R, O_R and 1_R are trivial idempotent.

2.9 DEFINITION

Let G be a group and let F be a field F * = F \{0_F} a linear character X of G over F is a homomorphism $\chi : G \to F^*$.

If G is a finite group the values taken on by a character χ are a roots of the identity 1_F of F since any element $g \in G$ is of finite order say k and so

$\chi(g^k) = \chi(e) = 1_F$ and $\chi(g^k) = \chi(g)$.

THEOREMS ON SPECIAL CASES

As considered earlier, q denotes a prime power say t^s .The nonzero elements of F_q will form a cyclic group of order q-1.The nonzero elements are $(q-1)^{th}$ roots of unity .Suppose that m is an integer > 1.Let m <q , If $F_q^* = F_q \setminus \{0_F\}$ is to contain m^{th} roots of unity, q has to be chosen suitably.

2.10 LEEMA

Let q = t^s where t isa prime and s≥ 1, F_q^* denotes the non zero elements of F_q

Let m< q Then F_q^*contains the m^{th} roots of unity if and only if q ≡ 1(mod m).

Proof If q≡ 1(mod m), m divides q-1 and so let q-1 = mm'.if ζ is an m^{th} root of unity $\zeta^m = 1$ implies that $\zeta^{mm'} = 1$ and so $\zeta^{q-1} = 1$. So an m^{th} root of unity is contained in a $(q-1)^{th}$ root of unity .

Conversely, if ζ is a $(q-1)^{th}$ root of unity and if the set of $(q-1)^{th}$ roots of unity contains m^{th} root of unity, then anm^{th} root of unity ζ is such that $\zeta^{mm'} = 1$and mm'= (q-1) or q-1 ≡ 0 (mod m).

Next we recall that when R is a commutative ring with unity 1_R nd G is a group, the group algebra RG is a free module on the elements of G. When R is a finite field say F_q (q= t^s ,t $is\ a\ prime\ s \geq 1$) and G is a finite group of order n written of the formal sums $\sum_{g\in G} X_g g$ with $x_q \in F_q$ the number of elements in the group algebra F_qG is q^n .That is ,when we form e_x = $1/|G| \sum_{g\epsilon G} \zeta(\, g-1)g, \zeta$ϵ char (G) the collection of $\{e_x | \zeta \epsilon\, Char\ (G)\}$ forms an orthogonal basis for the group algebra F_qG. This collection is a unique set of primitive idempotent of F_qG.

Next , we go to the case of dihedral group D_n is generated by two elements x,y which satisfy x^n = € y^2 = € ,xy =x^{-1}y In particular D_n= { € ,x ,x^2 ,……….x^{n-1}; y, xy, x^2y……………x^{n-1}y} It is clear that $|D_n|$ = 2n in [1]. We apply the theorem on primitive idempotent to the group algebra $F_q D_n$ where F_q contains a primitive $2n^{th}$ root of unity .If q is n odd prime power (q-1) is even and so 2n divids (q-1) if and only if n divides$\frac{(q-1)}{2}$ .If q is odd and 2n < q, 2n divides d if and only if

q ≡ 1(mod 2n).

REFEREENCES

[1] Michael Artin.,ALGEBRA,Prentice Hall of India Private Ltd, New Delhi-110001(1994) Chapter Section 3, 4 pp 162-174.

[2] **Carry Huffman.w.,V.Pless.G.,** Fundamentals of Error- Correcting Codes ,Cambridge

University Press(2004) Chapter 4 pp 121-158.

[3] T.W.Hungerford., ALGEBRA, GTM No: Springer Verlag(1984)Chapter IX pp 414-463.

[4] G.Karpilovsky., Commutative group algebrasMonographs and Textbooks in Pune and Applied Mathematics No:78(1983) Marvel Dekker line Chapters 2,3 pp 27-67.

[5] S.K.Arora., SridhirBatra.,ManjuPreethi., The primitive idempotent of a cyclic group Algebra South East Asian Bulletin of Mathematics (2002) No:26pp 549-557.

[6] S.k.Arora.,ManjuPreethi., Minimal Cyclic codes of length 2p finite fields and their Application Vol III No.4 (2011)pp 177-187.

[7] ManjuPreethi., Cyclic Codes of length 2 Proc.Ind. Acad.Sir(Math.Sci)Vol III No:4(2011) pp 371-379.

[8] ManjuPreethi., S.k.Arora., Minimal Codes of Prime-power length Finite fields and their Applications Vol 3(1997) pp 99-113.