International Journal of Statistika and Mathematika, ISSN: 2277- 2790 E-ISSN: 2249-8605, Volume 10, Issue 2, 2014 pp 36-41

Some Idempotents in Abelian Group Algebra

Dalip Singh[1*], Jagbir Singh[2*], Pankaj Arora[3*]

[1,2,3] Department of Mathematics,M.D. University, Rohtak – 124001, INDIA.

[*]Corresponding Address:

[1]dsmdur@gmail.com, [2]ahlawatjagbir@gmail.com, [3]pankajarora1242@yahoo.com

Research Article

Abstract: Expressions for pairwise orthogonal idempotents in FG, the semi simple group algebra of the abelian group G oforder p^n and $p^n q$ over the finite field F of prime power order $p^n\lambda+1$ and $p^n q\lambda+1$ respectively, are obtained.

Keywords : Group algebra, finite field, orthogonal idempotents.

Introduction

Let $F=GF(q)$ be a finite field of prime power order q and let n be a positive integer which is relatively prime to q. The cyclic codes of length n over F can be viewed as ideals in either $\frac{F[x]}{<x^n-1>}$ or as ideals in the group algebra FC_n, where C_n denotes a cyclic group of order n. If G is an abelian group of order n, then the ideals of the group algebra FG are called abelian codes. Milies and Ferraz [6] have found some minimal abelian codes of length p^n and $2p^n$ extending the results of Arora and Pruthi ([1],[8]). In this paper,we describe method to find pair wise orthogonali dempotents in group algebra FG, where G is an abelian group of order p^n and $p^n q$. In Section 2, we give expression for these idempotents in FG, where G is an abelian group of order p^n, where p is an odd prime and F is a field of prime power order q with $q=p^n\lambda+1$. In section 3,we discuss the case when G is an abelian group of order $p^n q$, p and q are odd primes, and F is a field of prime power order q with $q=p^n q\lambda+1$. .In section 4, we give an example for an abelian group of order 9.

G is Abelian group of order p^n, p is an odd prime

If $G=<g>=C_n$ is a finite cyclic group of order n, F is a field of order q with $(q,n)=1$ and $q=n\lambda+1$ for some $\lambda\geq 0$.

Then, FC_n has n primitive idempotents given by

$$e_i=\frac{1}{n}\sum_{j=0}^{n-1}\alpha^{ij}g^j, \qquad 0\leq i\leq n\text{-}1,$$

where α is n^{th} root of unity in F [8].

Theorem

Let G is an abelian group of order p^n, where p is an odd prime and H is a subgroup of G of order p^m such that G/H is cyclic, say $<\mathrm{a}H>$. F Is a field of order $p^n\lambda+1$ for some $\lambda>0$ .Then,

$$S_i=\left(\frac{1}{p^n}\sum_{h\in H}h\right)\left(\sum_{j=0}^{p^{n-m}-1}\alpha^{ij}\mathrm{a}^j\right),$$

$0\leq \mathrm{i}\leq p^{n-m}-1$, Where α is $\left(p^{n-m}\right)^{th}$ root of unity in F, are orthogonal idempotents in FG,.

Proof Let G be an abelian group of order p^n and H be a subgroup of G of order p^m such that G/H is cyclic, say $<\mathrm{a}H>$.
Here, $\left|G/H\right| = p^{n-m} = t$ (say).
Also, $\mathrm{a}^t \in H$. Consider a cyclic group G_1 of order t and let $G_1 = <b>$. Then, $G_1 \cong G/H$. The orthogonalidempotents of FG_1 are

$$e_i = \frac{1}{t}\sum_{j=0}^{t-1} \alpha^{ij} b^j, \qquad 0 \le i \le t\text{-}1,$$

where α is t^{th} root of unity in F, that is, α is a solution of $\mathrm{x}^t = 1$.
Now consider the elements of FG given by

$$\xi_i = \frac{1}{t}\sum_{j=0}^{t-1} \alpha^{ij} \mathrm{a}^j, \qquad 0 \le \mathrm{i} \le \mathrm{t}\text{-}1.$$

We assert that

$$S_i = \left(\frac{1}{|H|}\sum_{h\in H} h\right)\xi_i$$

for $0 \le i \le t-1$, are orthogonalidempotents in FG.
For $0 \le i \le t-1$, we have

$$\begin{aligned}
S_i^2 &= S_i S_i \\
&= \left(\left(\frac{1}{p^n}\sum_{h\in H} h\right)\left(\sum_{j=0}^{t-1}\alpha^{ij}\mathrm{a}^j\right)\right)\left(\left(\frac{1}{p^n}\sum_{h\in H} h\right)\left(\sum_{j=0}^{t-1}\alpha^{ij}\mathrm{a}^j\right)\right) \\
&= \frac{1}{p^{2n-m}}\left\{t\left(\sum_{h\in H} h + \alpha^i \mathrm{a}\sum_{h\in H} h + \alpha^{2i}\mathrm{a}^2\sum_{h\in H} h + \ldots\right.\right. \\
&\left.\left. + \alpha^{(t-2)i}\mathrm{a}^{t-2}\sum_{h\in H} h + \alpha^{(t-1)i}\mathrm{a}^{t-1}\sum_{h\in H} h\right)\right\} \\
&= \left(\frac{1}{p^n}\sum_{h\in H} h\right)\left(\sum_{j=0}^{t-1}\alpha^{ij}\mathrm{a}^j\right) \\
&= S_i
\end{aligned}$$

Also for i, j such that $i \ne j, i > j$, we have

$$\begin{aligned}
S_i S_j &= \left(\left(\frac{1}{p^n}\sum_{h\in H} h\right)\left(\sum_{k=0}^{t-1}\alpha^{ik}\mathrm{a}^k\right)\right)\left(\left(\frac{1}{p^n}\sum_{h\in H} h\right)\left(\sum_{l=0}^{t-1}\alpha^{jl}\mathrm{a}^l\right)\right) \\
&= \frac{1}{p^{2n-m}}\left\{\sum_{h\in H} h + \alpha^i\sum_{h\in H} h\mathrm{a} + \alpha^{2i}\sum_{h\in H} h\mathrm{a}^2 + \ldots + \alpha^{(t-1)i}\sum_{h\in H} h\,\mathrm{a}^{t-1}\right. \\
&+ \alpha^j\sum_{h\in H} h\mathrm{a} + \alpha^{i+j}\sum_{h\in H} h\mathrm{a}^2 + \ldots + \alpha^{(t-1)i+j}\sum_{h\in H} h\mathrm{a}^t \\
&+ \alpha^{2j}\sum_{h\in H} h\mathrm{a}^2 + \alpha^{i+2j}\sum_{h\in H} h\mathrm{a}^3 \ldots + \alpha^{(t-1)i+2j}\sum_{h\in H} h\mathrm{a}^{t+1} + \ldots \\
&\left. + \alpha^{(t-1)j}\sum_{h\in H} h\mathrm{a}^{t-1} + \alpha^{i+(t-1)j}\sum_{h\in H} h\mathrm{a}^t \ldots + \alpha^{(t-1)i+(t-1)j}\sum_{h\in H} h\,\mathrm{a}^{2t-2}\right\}
\end{aligned}$$

Since $\mathrm{a}^t \in H$, so we have

$$\sum_{g\in H} g\mathrm{a}^t = \sum_{g\in H} g \quad \text{and} \quad \sum_{g\in H} g\mathrm{a}^{t+i} = \sum_{g\in H} g\mathrm{a}^i \qquad \text{for all } i \ge 0.$$

Using this coefficient of $\frac{1}{p^{2n-m}}\sum_{g\in H} g\mathrm{a}^k$ in the above expression is

$$\begin{matrix}\left\{\alpha^{kj}+\alpha^{(k-1)j+i}+\alpha^{(k-2)j+2i}+...+\alpha^{ki}\right\} \\ +\left\{\alpha^{(k+1)i+(t-1)j}+\alpha^{(k+2)i+(t-2)j}+...+\alpha^{(t-1)i+(k+1)j}\right\}\end{matrix} = \alpha^{kj}\left\{\frac{\alpha^{(k+1)(i-j)}-1}{\alpha^{(i-j)}-1}\right\}+\alpha^{(k+1)i+(t-1)j}\left\{\frac{\alpha^{(t-k-1)(i-j)}-1}{\alpha^{(i-j)}-1}\right\}=0.$$ Thus, $\{S_i\}$ $0 \le i \le t\text{-}1,$ are orthogonalidempotentsin $FG.$

Theorem

The complete set of orthogonalidempotents in $FG,$ where F is a field of order q with $q = p^n\lambda+1$ for some $\lambda > 0$ and G is an abelian group of order p^n having a sequence of subgroups $G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_{n-1} \supset G_n =< e >$ such that $|G_i/G_{i+1}| = p\,(0 \le i \le n-1),$ is given by $\left\{e_{0,i_0}e_{1,i_1}...e_{n-1,i_{n-1}}\right\},$ $(0 \le i_j \le p)(0 \le j \le n-1)$ where $G_j/G_{j+1} =< \mathrm{a}_j G_{j+1} >$ and

$$e_{j,i_j} = \frac{1}{p^{n-j}}\left(\sum_{g_{j+1}\in G_{j+1}} g_{j+1}\right)\left(\sum_{k=0}^{p-1}\alpha_j^{i_jk}\mathrm{a}_j^{\,k}\right),$$ α_j is p^{th} root of unity in $F,$ are orthogonalidempotents in FG_j for $0 \le j \le n-1.$

Proof

Let G be an abelian group of order p^n and G_1 be the subgroup of order $p^{n-1}.$ Then, $|G/G_1| = p$ and so G/G_1 is cyclic. Let $G/G_1 =< \mathrm{a}_0G_1 >.$ Then,

$$e_{0,i_0} = \frac{1}{p^{n-1}}\left(\sum_{g_1\in G_1} g_1\right)\left(\frac{1}{p}\sum_{j=0}^{p-1}\alpha_0^{i_0j}\mathrm{a}_0^{\,j}\right)$$
$$= \frac{1}{p^{n}}\left(\sum_{g_1\in G_1} g_1\right)\left(\sum_{j=0}^{p-1}\alpha_0^{i_0j}\mathrm{a}_0^{\,j}\right),$$

for $0 \le i_0 \le p-1,$ are orthogonalidempotents in $FG,$ α_0 is p^{th} root of unity in $F.$

Now, let G_2 be the subgroup of G_1 of order $p^{n-2}.$ Then, $|G_1/G_2| = p$ and so G_1/G_2 is cyclic. Let $G_1/G_2 =< \mathrm{a}_1G_2 >.$ Then,

$$e_{1,i_1} = \frac{1}{p^{n-2}}\left(\sum_{g_2\in G_2} g_2\right)\left(\frac{1}{p}\sum_{j=0}^{p-1}\alpha_1^{i_1j}\mathrm{a}_1^{\,j}\right)$$
$$= \frac{1}{p^{n-1}}\left(\sum_{g_2\in G_2} g_2\right)\left(\sum_{j=0}^{p-1}\alpha_1^{i_1j}\mathrm{a}_1^{\,j}\right),$$

for $0 \le i_1 \le p-1,$ are orthogonalidempotents in $FG_1,$ α_1 is p^{th} root of unity in $F.$

Continuing in this way, we will obtain a subgroup G_{n-2} of order p^2 and its subgroup G_{n-1} of order $p.$ Then, $|G_{n-1}/G_{n-2}| = p$ and so G_{n-2}/G_{n-1} is cyclic. Let $G_{n-2}/G_{n-1} =< \mathrm{a}_{n-2}G_{n-1} >.$ Then,

$$e_{n-2,i_{n-2}} = \frac{1}{p}\left(\sum_{g_{n-1}\in G_{n-1}} g_{n-1}\right)\left(\frac{1}{p}\sum_{j=0}^{p-1}\alpha_{n-2}^{i_{n-2}j}\mathrm{a}_{n-2}^{\,j}\right)$$
$$= \frac{1}{p^2}\left(\sum_{g_{n-1}\in G_{n-1}} g_{n-1}\right)\left(\sum_{j=0}^{p-1}\alpha_{n-2}^{i_{n-2}j}\mathrm{a}_{n-2}^{\,j}\right),$$

for $0 \le i_{n-2} \le p-1$, are orthogonalidempotents in FG_{n-2}, α_{n-2} is p^{th} root of unity in F.

Also, $|G_{n-1}/G_n| = p$, so G_{n-1} is cyclic. Let $G_{n-1} =< \mathrm{a}_{n-1} >$. Then,

$$e_{n-1,i_{n-1}} = \frac{1}{p}\left(\sum_{j=0}^{p-1} \alpha_{n-1}^{i_{n-2}j} \mathrm{a}_{n-1}{}^{j}\right),$$

for $0 \le i_{n-1} \le p-1$, are orthogonalidempotents in FG_{n-1}, α_{n-1} is p^{th} root of unity in F.

Now, the complete set of orthogonalidempotents of FG is given by

$$e_i = e_{i_{n-1}p^{n-1}+i_{n-2}p^{n-2}+\ldots+i_1p+i_0} = e_{0,i_0}.e_{1,i_1}\ldots e_{n-1,i_{n-1}},$$

where $i = i_{n-1}p^{n-1} + i_{n-2}p^{n-2} + i_{n-2}p^{n-2} + \ldots + i_1 p + i_0$, as

$$e_i^2 = \left(e_{i_{n-1}p^{n-1}+i_{n-2}p^{n-2}+\ldots+i_1p+i_0}\right)^2$$

$$= \left(e_{0,i_0}.e_{1,i_1}\ldots e_{n-1,i_{n-1}}\right)^2$$

$$= e_{0,i_0}.e_{1,i_1}\ldots e_{n-1,i_{n-1}}$$

$$= e_i$$

For $i \ne j$, the representation of i and j are as follows:

$$i = i_{n-1}p^{n-1} + i_{n-2}p^{n-2} + i_{n-2}p^{n-2} + \ldots + i_1 p + i_0,$$

$$j = j_{n-1}p^{n-1} + j_{n-2}p^{n-2} + j_{n-2}p^{n-2} + \ldots + j_1 p + j_0,$$

and they must differ at at least one indices, say k^{th}, that is, $i_k \ne j_k$, then

$$e_{k,i_k}.e_{k,j_k} = 0$$

Thus $e_i.e_j = 0$.

Theorem

The complete set of orthogonalidempotents in FG where F is a field of order q with $q = p^n\lambda + 1$ for some $\lambda > 0$, G is an abelian group of order p^n having a sequence of subgroups $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_s =< e >$ with the property that G_{i+1} is subgroup of G of smallest order p^{n_i+1} (say), such that G_i / G_{i+1} is cyclic, is given by

$\{e_{0,i_0}.e_{1,i_1}\ldots e_{s-1,i_{s-1}}\}$, $\left(0 \le i_j \le \frac{p^{n_j}}{p^{n_{j+1}}} - 1\right)(0 \le j \le s-1)$ where $G_j / G_{j+1} =< \mathrm{a}_j G_{j+1} >$ and

$$e_{j,i_j} = \left(\frac{1}{p^{n_j}} \sum_{g_{j+1} \in G_{j+1}} g_{j+1}\right)\left(\sum_{k=0}^{p^{n_j - n_{j+1}}-1} \alpha_j^{i_j k} a_j^k\right),$$

α_j is $\left(p^{n_j - n_{j+1}}\right)^{th}$ root of unity in F, are the orthogonalidempotents in FG_j for $0 \le j \le s-1$.

If G is Abeliangroup of order $p^n q$, p and q are distinct odd primes

Theorem

Orthogonalidempotents in group algebra FG, where G is an abelian group of order $p^n q$, (p is an odd prime and q is any prime) and H is a subgroup of G of order $p^m q$ such that $G/H =< \mathrm{a}H >$ and F is a field of order $p^n q\lambda + 1$ for some $\lambda > 0$, are given by

$$S_i = \left(\frac{1}{p^n q} \sum_{h \in H} h \right) \left(\sum_{j=0}^{p^{n-m}-1} \alpha^{ij} a^j \right), \; 0 \le i \le p^{n-m} - 1,$$

where α is $\left(p^{n-m}\right)^{th}$ root of unity in F.

Theorem

If F is a field of order r with $r = p^n q\lambda + 1$ for some λ>0 and G is an abelian group of order $p^n q$ where p is an odd prime and q is any prime and it has a sequence of subgroups

$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_{n-1} \supset G_n =< e >$ Such that $\left| G_i / G_{i+1} \right| = p \left(0 \le i \le n-1\right)$. Then, the complete set of orthogonal idempotents in FG is

$\left\{ e_{0,i_0} e_{1,i_1} ... e_{n-1,i_{n-1}} \right\}$, $\left(0 \le i_j \le p\right)\left(0 \le j \le n-1\right)$

where $G_j / G_{j+1} =< a_j G_{j+1} >$ and

$$e_{j,i_j} = \frac{1}{p^{n-j} q} \left(\sum_{g_{j+1} \in G_{j+1}} g_{j+1} \right) \left(\sum_{k=0}^{p-1} \alpha^{i_j k} a_j^{\,k} \right),$$

α is p^{th} root of unity in F, arethe orthogonalidempotents in FG_j for $0 \le j \le n-1$,

Theorem

Let G be an abelian group of order $p^n q$ where p is an odd prime and q is any prime and F be a field of order r with $r = p^n q \lambda + 1$ for some λ>0. Then, by considering a sequence of subgroups of G

$G = G_0 \supset G_1 \supset G_2 \supset ... \supset G_s =< e >$

with the property that G_{i+1} is subgroup of G of smallest order $p^{n_i+1} q$ (say), such that G_i / G_{i+1} is cyclic. Then, the complete set of orthogonalidempotentsin FG is given as

$\left\{ e_{0,i_0} . e_{1,i_1} ... e_{s-1,i_{s-1}} \right\}$, $\left(0 \le i_j \le \frac{p^{n_j}}{p^{n_{j+1}}} - 1 \right) \left(0 \le j \le s-1\right)$ where $G_j / G_{j+1} =< a_j G_{j+1} >$ and

$e_{j,i_j} = \left(\frac{1}{p^{n_j} q} \sum_{g_{j+1} \in G_{j+1}} g_{j+1} \right) \left(\sum_{k=0}^{p^{n_j - n_{j+1}} - 1} \alpha_j^{i_j k} a_j^{k} \right)$, α_j is $\left(p^{n_j - n_{j+1}} \right)^{th}$ root of unity in F, arethe orthogonalidempotents in FG_j for $0 \le j \le s-1$.

Example

Example Consider an abelian group G of group 9. Then, G will have a subgroup H of order 3 and $\left| G / H \right| = 3$. Let $G / H =< aH >$. Then,

$$e_{0,0} = \frac{1}{9} \left(\sum_{h \in H} h \right) \left(1 + a + a^2 \right)$$

$$e_{0,1} = \frac{1}{9} \left(\sum_{h \in H} h \right) \left(1 + \alpha a + \alpha^2 a^2 \right)$$

$$e_{0,2} = \frac{1}{9} \left(\sum_{h \in H} h \right) \left(1 + \alpha^2 a + \alpha a^2 \right)$$

are orthogonal idempotents in FG, where α is solution of $x^3 = 1$ in F. Also $\left| H \right| = 3$. Let $H =< b >$. Then, orthogonalidempotents in FH are

$$e_{1,0} = \frac{1}{3}\left(1 + \mathrm{b} + \mathrm{b}^2\right)$$

$$e_{1,1} = \frac{1}{3}\left(1 + \beta\mathrm{b} + \beta^2\mathrm{b}^2\right)$$

$$e_{1,2} = \frac{1}{3}\left(1 + \beta^2\mathrm{b} + \beta\mathrm{b}^2\right)$$

Then, the complete set of orthogonalidempotents of FG is given by

$$\begin{aligned} e_0 &= e_{0,0}e_{1,0} \\ &= \frac{1}{27}\left(\sum_{h\in H} h\right)\left(1 + \mathrm{a} + \mathrm{a}^2 + \mathrm{b} + \mathrm{ab} \right. \\ &\qquad \left. + \mathrm{a}^2\mathrm{b} + \mathrm{b}^2 + \mathrm{ab}^2 + \mathrm{a}^2\mathrm{b}^2\right) \end{aligned}$$

$$e_1 = e_{0,1}e_{1,0}$$

$$e_2 = e_{0,2}e_{1,0}$$

$$e_3 = e_{0,0}e_{1,1}$$

$$e_4 = e_{0,1}e_{1,1}$$

$$e_5 = e_{0,2}e_{1,1}$$

$$e_6 = e_{0,0}e_{1,2}$$

$$e_7 = e_{0,1}e_{1,2}$$

$$e_8 = e_{0,2}e_{1,2}$$

References

1. Arora, S.K., Pruthi, M.: Minimal Cyclic Codes of Length $2p^n$, Finite Fields Appl., 5, 177-187 (1999)
2. Berman, S. D.: On the Theory of Group Codes, Kibernetika, 3, No. 1, 31-39 (1967)
3. Berman, S. D.:Semisimple cyclic and abelian code, II, Cybernatics, 3,17-23 (1967)
4. Blake, I. F., Mullin, R.C.: The Mathematical Theory of Coding, Academic Press, New York (1975)
5. Burrow, M.: Representation Theory of Finite Groups, Academic Press, New York (1965)
6. Ferraz, R. A., Milies, C.P.: Idempotents in group algebras and minimal abelian codes, Finite Fields Appl., 13, 382-393 (2007)
7. Perlis, S., Walker, G.: Abelian group algebras, Trans. Amer. Math. Soc. 68, 420–426 (1950)
8. Pruthi, M., Arora, S.K.: Minimal Codes of Prime-Power Length, Finite Fields Appl., 3, 99-113 (1997)