G-equivalence in group algebras and minimal abelian codes

Marinês Guerreiro

marines@ufv.br

C. Polcino Milies
Raul Ferraz

Departamento de Matemática
Universidade Federal de Viçosa

Instituto de Matemática e Estatística
Universidade de São Paulo

Universidad de León

Research supported by CAPES, PROCAD 915/2010, CNPq, Proc. 300243/79-0(RN), FAPESP, Proc. 09/52665-0, FAPEMIG,

APQ CEX 00438-08 and PCE-00151-12 (Brazil).

This work was published in IEEE Transactions of Information Theory, Vol 60 (1) (2014), 252-260.

Origins of Coding Theory

The origins of Information Theory and Coding Theory

C. Shannon, *A Mathematical Theory of Communication*. The Bell System Technical Journal, **27** (1948) 379-423 July and 623-656 October.

Error-Correcting Codes (Códigos Correctores de Errores)

A **alphabet** - non empty set.

A **code** C is a proper subset of A^n, where n is the **length** of the code.

$(a_0, a_1, \ldots, a_{n-1}) \in C$ is a **word** of the code.

Hamming distance

$u, v \in C$, $d_H(u, v) = |\{i : u_i \neq v_i, i = 0, \ldots, n-1\}|$

Group Algebra

Let $\mathbb{F}$ be a field and G be a group (finite or infinite). The group algebra $\mathbb{F}G$ is the set of formal sums

$$\mathbb{F}G = \left\{ \sum_{g \in G} a_g \, g \, / \, a_g \in \mathbb{F}, \text{ finite sums} \right\}.$$

$$\left(\sum_{g \in G} a_g \, g \right) + \left(\sum_{g \in G} b_g \, g \right) = \left(\sum_{g \in G} (a_g + b_g) \, g \right).$$

$$\left(\sum_{g \in G} a_g \, g \right) \cdot \left(\sum_{h \in G} b_h \, h \right) = \left(\sum_{g, h \in G} (a_g \, b_h) \, gh \right).$$

Cyclic Codes as Ideals in Group Algebras

Let $\mathbb{F}_q$ be a finite field with q elements.

A linear **cyclic code** is a linear code $C \subset \mathbb{F}_q^n$ such that, for each word $(a_0, a_1, \ldots, a_{n-1})$ in C, the word $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is also in C.

Linear cyclic codes are ideals in the quotient ring $R_n = \dfrac{\mathbb{F}_q[x]}{< x^n - 1 >}$ and the *cyclic shift* is equivalent to multiplication by the class of x in R_n.

Let $G =< a >$ be a finite cyclic group of order n generated by a.
A linear cyclic code is also a proper ideal of the group algebra $\mathbb{F}_q G$.

The **minimal cyclic codes** are the ones generated by the primitive idempotents of $\mathbb{F}_q G$.

Cyclic Codes as Ideals in Group Algebras

$$\begin{array}{lccccc}
 & C \subset \mathbb{F}_q^n & \xrightarrow{\cong} & R_n = \frac{\mathbb{F}_q[x]}{<x^n-1>} & \xrightarrow{\cong} & \mathbb{F}_q G = \mathbb{F}_q < a > \\
\text{cyclic} & & & & & \\
 & \downarrow & & \bar{x} \downarrow & & a \downarrow \\
\text{shift} & & & & & \\
 & C \subset \mathbb{F}_q^n & \xrightarrow{\cong} & R_n = \frac{\mathbb{F}_q[x]}{<x^n-1>} & \xrightarrow{\cong} & \mathbb{F}_q G = \mathbb{F}_q < a >
\end{array}$$

Group Codes

Let G be a finite abelian group and $\mathbb{F}_q$ be a finite field with q elements.

Definition (Berman (1967) and MacWilliams (1970))

An **abelian code** is a proper ideal of the group algebra $\mathbb{F}_q G$.

The **minimal abelian codes** are the ones generated by the primitive idempotents of $\mathbb{F}_q G$.

Definition (Miller (1979))

Two abelian codes $\mathcal{I}_1$ and $\mathcal{I}_2$ are *G-equivalent* if there exists an automorphism θ of G whose linear extension to $\mathbb{F}_q G$ maps $\mathcal{I}_1$ on $\mathcal{I}_2$.

This Work

OBJECTIVES:

1) Determine G-equivalence of minimal ideals (codes) in semisimple abelian group algebras.

2) Prove that the G-equivalence classes of minimal codes depend on the structure of the lattice of the subgroups of G.

HOW TO DO IT?

Establish a correspondence between the G-equivalence classes of minimal abelian ideals in $\mathbb{F}G$ and certain classes of isomorphism of subgroups of the abelian group G.

This Work

OBJECTIVES:
1) Determine G-equivalence of minimal ideals (codes) in semisimple abelian group algebras.
2) Prove that the G-equivalence classes of minimal codes depend on the structure of the lattice of the subgroups of G.

HOW TO DO IT?
Establish a correspondence between the G-equivalence classes of minimal abelian ideals in $\mathbb{F}G$ and certain classes of isomorphism of subgroups of the abelian group G.

Subgroups and Idempotents

Definition

Let G be a group. A subgroup H of G is said a **co-cyclic subgroup** if the quotient $G/H \neq 1$ is a cyclic group.

We use the notation

$$\mathcal{S}_{cc}(G) = \{H \,|\, H \text{ is a co-cyclic subgroup of } G\}.$$

We shall repeatedly use the following rather obvious fact.

Lemma

Let G be a finite abelian p-group and $H \leq G$. Then G/H is a cyclic group if and only if there exists a unique subgroup L such that $H < L \leq G$ and $[L : H] = p$.

Subgroups and Idempotents

Let G be an abelian p-group and $\mathbb{F}$ be a finite field whose characteristic does not divide the order of G.

For a subgroup H of G, denote

$$\widehat{H} = \frac{1}{|H|} \sum_{h \in H} h$$

and, for an element $x \in G$, set $\widehat{x} = \widehat{\langle x \rangle}$.

For each co-cyclic subgroup H of G, we define the idempotent

$$e_H = \widehat{H} - \widehat{H^*}$$

of $\mathbb{F}G$, where H^* is the unique subgroup of G containing H such that $|H^*/H| = p$, since G/H is a cyclic p-group.

Subgroups and Idempotents

Consider the set

$$\{\widehat{G}\} \cup \{e_H = \widehat{H} - \widehat{H^\sharp} \mid H \in \mathcal{S}_{cc}(G)\}. \tag{1}$$

For a rational abelian group algebra $\mathbb{Q}G$, the set above is the set of primitive central idempotents [4, Theorem 1.4].

Theorem

[FM, Lemma 5] *Let p be a prime number and G a finite abelian group of exponent p^n and $\mathbb{F}_q$ a finite field such that $p \not| q$. Then* (1) *is a set of pairwise orthogonal idempotents of $\mathbb{F}_qG$ whose sum is equal to* 1*.*

Theorem

[FM, Theorem 4.1] *Under the hypotheses above, the set* (1) *is the set of primitive idempotents of $\mathbb{F}_qG$ if and only if $o(\bar{q}) = \phi(p^n)$ in $U(\mathbb{Z}_{p^n})$, where ϕ denotes Euler´s totient function.*

Subgroups and Idempotents

For a finite abelian group G, write $G = G_{p_1} \times \cdots \times G_{p_t}$, where G_{p_i} denotes the p_i-Sylow subgroup of G, for the distinct positive prime numbers $p_1, \ldots, p_t$.

Lemma

Let $G = G_{p_1} \times \cdots \times G_{p_t}$ be a finite abelian group and $H \in \mathcal{S}_{cc}(G)$. Write $H = H_{p_1} \times \cdots \times H_{p_t}$, where H_{p_i} is the p_i-Sylow subgroup of H. Then each subgroup H_{p_i} is co-cyclic in G_{p_i}, $1 \leq i \leq t$.

Demonstração.

For $H \in \mathcal{S}_{cc}(G)$, the quotient $G/H \cong G_{p_1}/H_{p_1} \times \cdots \times G_{p_t}/H_{p_t}$ is cyclic, hence each factor G_{p_i}/H_{p_i} must be cyclic. Therefore, $H_{p_i} \in \mathcal{S}_{cc}(G_{p_i})$, $1 \leq i \leq t$. □

Subgroups and Idempotents

For each $H \in \mathcal{S}_{cc}(G)$, define an idempotent $e_H \in \mathbb{F}G$ as follows. For each $1 \leq i \leq t$, either $H_{p_i} = G_{p_i}$ or there exists a unique subgroup $H_{p_i}^{\sharp}$ such that $[H_{p_i}^{\sharp} : H_{p_i}] = p_i$. Thus, let $e_{H_{p_i}} = \widehat{G_{p_i}}$ or $e_{H_{p_i}} = \widehat{H_{p_i}} - \widehat{H_{p_i}^{\sharp}}$, respectively, and define

$$e_H = e_{H_{p_1}} e_{H_{p_2}} \cdots e_{H_{p_t}}. \tag{2}$$

For any other $K \in \mathcal{S}_{cc}(G)$, with $K \neq H$, we have $K_{p_i} \neq H_{p_i}$, for some $1 \leq i \leq t$, hence $e_{H_{p_i}} e_{K_{p_i}} = 0$ and so $e_H e_K = 0$. Thus:

Proposition

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| \, |G|$. Then

$$\mathcal{B} = \{e_H \,|\, H \in \mathcal{S}_{cc}(G)\}$$

is a set of orthogonal idempotents of $\mathbb{F}G$. For $\mathbb{Q}G$, these idempotents are primitive while for finite fields this is usually not true.

Subgroups, Idempotents and Automorphisms

G-equivalence of ideals $\longmapsto$ action of $\mathrm{Aut}(G)$ on the lattice of the subgroups of G $\longmapsto$ action of $\mathrm{Aut}(\mathbb{F}G)$ on the idempotents of $\mathcal{B}$

Note: same notation for $\psi \in \mathrm{Aut}(G)$ and its linear extension to $\mathbb{F}G$.

Lemma

Let G be a finite abelian group, $H \in \mathcal{S}_{cc}(G)$ and e_H its corresponding idempotent defined as in (2). Then, for any $\psi \in \mathrm{Aut}(G)$, we have $\psi(e_H) = e_{\psi(H)}$.

Lemma

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| \, |G|$. Then, in the group algebra $\mathbb{F}G$, we have:

$$1 = \widehat{G} + \sum_{H \in \mathcal{S}_{cc}(G)} e_H. \tag{3}$$

Subgroups, Idempotents and Automorphisms

What about primitive idempotents and corresponding subgroups?

Lemma

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| \, |G|$. For each primitive idempotent $e \in \mathbb{F}G$, there exists a unique $H \in \mathcal{S}_{cc}(G)$ such that $e \cdot e_H = e$ and $e \cdot e_K = 0$, for any other $K \in \mathcal{S}_{cc}(G)$.

Demonstração.

By Lemma 7, $1 = \widehat{G} + \sum_{H \in \mathcal{S}_{cc}(G)} e_H$. Multiplying by e, we have:

$$e = e\left(\widehat{G} + \sum_{H \in \mathcal{S}_{cc}(G)} e_H\right) = e \cdot \widehat{G} + \sum_{H \in \mathcal{S}_{cc}(G)} e \cdot e_H. \tag{4}$$

As $e_H \cdot e_K = 0$, for $H \neq K \in \mathcal{S}_{cc}(G)$, the right hand side of (4) is a sum of orthogonal idempotents. Therefore, as e is a primitive idempotent, only one summand is non-zero. □

Subgroups, Idempotents and Automorphisms

Set $\mathcal{P}(\mathbb{F}G) = \{e \in \mathbb{F}G \mid e$ **is a primitive idempotent in** $\mathbb{F}G\}$. Under the same hypotheses of Lemma 8, the following map is well-defined:

$$\begin{array}{cccc} \Phi & : & \mathcal{P}(\mathbb{F}G) & \longrightarrow & \mathcal{S}_{cc}(G) \\ & & e & \longmapsto & \Phi(e) = H_e, \end{array} \tag{5}$$

where H_e is the unique co-cyclic subgroup of G such that $e \cdot e_{H_e} = e$.

Theorem

Let G be a finite abelian group, $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| \, |G|$ and $H \in \mathcal{S}_{cc}(G)$. Then e_H is the sum of all primitive idempotents $e \in \mathcal{P}(\mathbb{F}G)$ such that $\Phi(e) = H$.

Demonstração.

Write $1 = \sum_{e \in \mathcal{P}(\mathbb{F}G)} e$. Then

$$e_H = \sum_{e \in \mathcal{P}(\mathbb{F}G)} e_H e = \sum_{\Phi(e) \neq H} e_H e + \sum_{\Phi(e) = H} e_H e = \sum_{\Phi(e) = H} e.$$

G-isomorphisms and G-equivalence

Definition

Two subgroups H and K of a group G are *G-isomorphic* if there exists an automorphism $\varphi \in Aut(G)$ such that $\varphi(H) = K$.

Isomorphic subgroups are not necessarily G-isomorphic.

Example: For p prime, if $G = \langle a \rangle \times \langle b \rangle$ with $o(a) = p^2$ and $o(b) = p$, then $\langle a^p \rangle$ and $\langle b \rangle$ are isomorphic but not G-isomorphic, since $\langle b \rangle$ is contained properly only in $\langle a^p \rangle \times \langle b \rangle$ and $\langle a^p \rangle$ is contained in $\langle a \rangle$ and in $\langle a^i b \rangle$, for $1 \leq i \leq p-1$.

Proposition

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| \, |G|$. If $e, e_1 \in \mathcal{P}(\mathbb{F}G)$ are such that $\psi(e) = e_1$, for some automorphism $\psi \in \mathrm{Aut}(G)$ linearly extended to $\mathbb{F}G$, then

$$\psi(H_e) = H_{\psi(e)} = H_{e_1},$$

i.e., H_e and H_{e_1} are G-isomorphic.

G-isomorphisms and G-equivalence

Definition

Two subgroups H and K of a group G are *G-isomorphic* if there exists an automorphism $\varphi \in Aut(G)$ such that $\varphi(H) = K$.

Isomorphic subgroups are not necessarily G-isomorphic.

Example: For p prime, if $G = \langle a \rangle \times \langle b \rangle$ with $o(a) = p^2$ and $o(b) = p$, then $\langle a^p \rangle$ and $\langle b \rangle$ are isomorphic but not G-isomorphic, since $\langle b \rangle$ is contained properly only in $\langle a^p \rangle \times \langle b \rangle$ and $\langle a^p \rangle$ is contained in $\langle a \rangle$ and in $\langle a^i b \rangle$, for $1 \leq i \leq p - 1$.

Proposition

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| \, |G|$. If $e, e_1 \in \mathcal{P}(\mathbb{F}G)$ are such that $\psi(e) = e_1$, for some automorphism $\psi \in \mathrm{Aut}(G)$ linearly extended to $\mathbb{F}G$, then

$$\psi(H_e) = H_{\psi(e)} = H_{e_1},$$

i.e., H_e and H_{e_1} are G-isomorphic.

G-isomorphisms and G-equivalence

Definition

Two subgroups H and K of a group G are *G-isomorphic* if there exists an automorphism $\varphi \in Aut(G)$ such that $\varphi(H) = K$.

Isomorphic subgroups are not necessarily G-isomorphic.

Example: For p prime, if $G = \langle a \rangle \times \langle b \rangle$ with $o(a) = p^2$ and $o(b) = p$, then $\langle a^p \rangle$ and $\langle b \rangle$ are isomorphic but not G-isomorphic, since $\langle b \rangle$ is contained properly only in $\langle a^p \rangle \times \langle b \rangle$ and $\langle a^p \rangle$ is contained in $\langle a \rangle$ and in $\langle a^i b \rangle$, for $1 \leq i \leq p-1$.

Proposition

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| \, |G|$. If $e, e_1 \in \mathcal{P}(\mathbb{F}G)$ are such that $\psi(e) = e_1$, for some automorphism $\psi \in \mathrm{Aut}(G)$ linearly extended to $\mathbb{F}G$, then

$$\psi(H_e) = H_{\psi(e)} = H_{e_1},$$

i.e., H_e and H_{e_1} are G-isomorphic.

G-isomorphisms and G-equivalence

The converse of the Proposition 5 is also true. For this, set

$$\mathcal{L}\mathrm{Aut}(G) = \{\psi \in \mathrm{Aut}(G) \,|\, \psi(H) = H, \text{ for all } H \leq G\}.$$

Lemma

Let G be a finite abelian group, $g \in G$ and $r \in \mathbb{N}$ with $\gcd(r, o(g)) = 1$. Then there exists $\psi \in \mathcal{L}\mathrm{Aut}(G)$ such that $\psi(g) = g^r$.

Lemma

Let G be a finite abelian group and $\psi \in \mathrm{Aut}(G)$. Then $\psi \in \mathcal{L}\mathrm{Aut}(G)$ if and only if there exists $r \in \mathbb{N}$ such that $\gcd(r, |G|) = 1$ and $\psi(g) = g^r$, for all $g \in G$.

G-isomorphisms and G-equivalence

Lemma

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| |G|$. *Then $\mathcal{B} = \{e_H \mid H \in \mathcal{S}_{cc}(G)\}$ is both a basis for the algebra*

$$\mathcal{A} = \{\alpha \in \mathbb{F}G \mid \psi(\alpha) = \alpha, \text{ for all } \psi \in \mathcal{L}\mathrm{Aut}(G)\}$$

and the set of primitive idempotents of $\mathcal{A}$.

Proposition

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| |G|$. *If $e_1, e_2 \in \mathcal{P}(\mathbb{F}G)$ and $H_{e_1} = H_{e_2}$, then there exists an automorphism $\psi \in \mathcal{L}\mathrm{Aut}(G)$ whose linear extension to $\mathbb{F}G$ maps e_1 to e_2.*

G-isomorphisms and G-equivalence

Proposition

Let G be a finite abelian group and $\mathbb{F}$ a field such that $\mathrm{char}(\mathbb{F}) \not| \, |G|$. If $e_1, e_2 \in \mathcal{P}(\mathbb{F}G)$ are such that $\psi(H_{e_1}) = H_{e_2}$, for some $\psi \in \mathrm{Aut}(G)$, then there exists an automorphism $\theta \in \mathrm{Aut}(G)$ whose linear extension to $\mathbb{F}G$ maps e_1 and e_2, i.e., the ideals of $\mathbb{F}G$ generated by e_1 and e_2 are G-equivalent.

An application to codes

We found the following statements in the paper:

R.L. Miller, *Minimal codes in abelian group algebras*, Journal of Combinatorial Theory, Series A, **26** (1979) 166-178.

Theorem A [M, Theorem 3.6] *"If G is a finite abelian group with exponent n and $\tau(n)$ is the number of divisors of n, then there exist precisely $\tau(n)$ non G-equivalent minimal codes in $\mathbb{F}_2G$.*

Theorem B [M, Theorem 3.9] *"Two minimal abelian codes with the same weight distribution are G-equivalent".*

(Un)fortunately, both statements are not correct!!!!

An application to codes

We found the following statements in the paper:

R.L. Miller, *Minimal codes in abelian group algebras*, Journal of Combinatorial Theory, Series A, **26** (1979) 166-178.

Theorem A [M, Theorem 3.6] *"If G is a finite abelian group with exponent n and $\tau(n)$ is the number of divisors of n, then there exist precisely $\tau(n)$ non G-equivalent minimal codes in $\mathbb{F}_2 G$.*

Theorem B [M, Theorem 3.9] *"Two minimal abelian codes with the same weight distribution are G-equivalent".*

(Un)fortunately, both statements are not correct!!!!

An application to codes

We found the following statements in the paper:

R.L. Miller, *Minimal codes in abelian group algebras*, Journal of Combinatorial Theory, Series A, **26** (1979) 166-178.

Theorem A [M, Theorem 3.6] *"If G is a finite abelian group with exponent n and $\tau(n)$ is the number of divisors of n, then there exist precisely $\tau(n)$ non G-equivalent minimal codes in $\mathbb{F}_2 G$.*

Theorem B [M, Theorem 3.9] *"Two minimal abelian codes with the same weight distribution are G-equivalent".*

(Un)fortunately, both statements are not correct!!!!

Main mistake

In a direct product of two (abelian) groups G_1 and G_2, the product of a primitive idempotent of $\mathbb{F}_2 G_1$ with a primitive idempotent of $\mathbb{F}_2 G_2$ may not be primitive in $\mathbb{F}_2(G_1 \times G_2)$.

In [3] we exhibited counterexamples to both Theorems A and B. However, Theorem A does hold under certain hipotheses, as we show in the sequel.

An application to codes

Lemma

If H is a cyclic subgroup of order p^s in a group $G \cong \underbrace{C_{p^r} \times \cdots \times C_{p^r}}_{m}$, with $s \leq r$, then there exists a cyclic subgroup of G, of order p^r, containing H.

Theorem

Let m and r be positive integers. If $G = \underbrace{C_{p^r} \times \cdots \times C_{p^r}}_{m}$ is a finite abelian p-group, then any co-cyclic subgroup of G contains a subgroup isomorphic to $\underbrace{C_{p^r} \times \cdots \times C_{p^r}}_{(m-1)}$. Hence the subgroups of G isomorphic to $\underbrace{C_{p^r} \times \cdots \times C_{p^r}}_{(m-1)}$ are precisely the minimal co-cyclic subgroups of G.

An application to codes

Proposition

Let m and r be positive integers. If $G = \underbrace{C_{p^r} \times \cdots \times C_{p^r}}_{m}$ is a finite abelian p-group and $\mathbb{F}$ is a field with $\mathrm{char}(\mathbb{F}) \neq p$, then a primitive idempotent of $\mathbb{F}G$ is of the form $\widehat{K} \cdot e_h$, where K is a subgroup of G isomorphic to $\underbrace{C_{p^r} \times \cdots \times C_{p^r}}_{(m-1)}$ and e_h is a primitive idempotent of $\mathbb{F}\langle h \rangle$, where $h \in G$ is such that $G = \langle h \rangle \times K$ and $\langle h \rangle \cong C_{p^r}$.

An application to codes

Corollary

Let m and r be positive integers, $G = \underbrace{C_{p^r} \times \cdots \times C_{p^r}}_{m}$ a finite abelian p-group and $\mathbb{F}_q$ a finite field with q elements such that $o(\bar{q}) = \phi(p^r)$ in $U(\mathbb{Z}_{p^r})$. Then the minimal abelian codes (ideals) in $\mathbb{F}_q G$ are as follows:

Primitive Idempotent	Dimension	Minimum Weight
$\widehat{G}$	1	p^{rm}
$\widehat{K}(\widehat{h^p} - \widehat{h})$	$p-1$	$2p^{r(m-1)+(r-1)}$
$\cdots$	$\cdots$	
$\widehat{K}(\widehat{h^{p^i}} - \widehat{h^{p^{i-1}}})$	$p^{i-1}(p-1)$	$2p^{r(m-1)-(r-i)}$
$\cdots$	$\cdots$	
$\widehat{K}(1 - \widehat{h^{p^{r-1}}})$	$p^{r-1}(p-1)$	$2p^{r(m-1)}$

where h is as in Proposition 9. Consequently, the number of non G-equivalent minimal abelian codes (ideals) is $r+1 = \tau(p^r)$.

An application to codes

Corollary

Let $n \geq 2$ be an integer, $G = \underbrace{C_n \times \cdots \times C_n}_{m}$ an abelian group and $\mathbb{F}_q$ a finite field such that $\gcd(q, n) = 1$. Then the primitive idempotents of $\mathbb{F}_q G$ are of the form $\widehat{K} \cdot e_h$, where K is a subgroup of G isomorphic to $\underbrace{C_n \times \cdots \times C_n}_{(m-1)}$, $h \in G$ is such that $G = K \times \langle h \rangle$ and e_h is a primitive idempotent of $\mathbb{F}_q \langle h \rangle$.

Theorem

Let G be a finite abelian group of exponent n and $\mathbb{F}$ a finite field such that $char(\mathbb{F}) \not| |G|$. Then the number of non G-equivalent minimal abelian codes is precisely $\tau(n)$ if and only if G is a direct product of cyclic groups isomorphic to one another.

To know more...

- S.D. Berman, *Semisimple cyclic and abelian codes, II*, Kybernetika **3** (1967) 21-30.
- O. Broche, A. del Río, *Wedderburn decomposition of finite group algebras*, Finite Fields and their Applications **13** (2007) 71-79.
- I.F. Blake, R.C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York, 1975.
- R. Ferraz, M. Guerreiro, C. Polcino Milies, *Minimal codes in binary abelian group algebras*, Proceedings of ITW-IEEE 2011 (to appear).
- R. Ferraz, C. Polcino Milies, *Idempotents in group algebras and minimal abelian codes*, Finite Fields and their Applications, **13**, (2007) 382-393.
- E.G. Goodaire, E. Jespers, C. Polcino Milies, *Alternative Loop Rings*, North-Holland Mathematics Studies **184**, Elsevier, Amsterdam, 1996.

To know more...

- C.J. Hillar, D.L. Rhea, *Automorphisms of finite abelian groups*, American Math. Monthly **114** n. 10 (2007) 917-923.
- E. Jespers, G. Leal, A. Paques, *Central idempotents in the rational group algebra of a finite nilpotent group*, Journal of Algebra and its Applications, **2** No. 1 (2003) 57-62.
- F.J. MacWilliams,*Binary codes which are ideals in the group algebra of an abelian group*, Bell System Tech. Journal, **44**, (1970) 987-1011.
- R.L. Miller, *Minimal codes in abelian group algebras*, Journal of Combinatorial Theory, Series A, **26** (1979) 166-178.
- A. Olivieri, A. del Río, J. J. Simón, *On monomial characters and central idempotents of rational group algebras*, Comm. Algebra **32** (4) (2004) 1531-1550.
- C. Polcino Milies, S.K. Sehgal, *An Introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, 2002.