Essential Idempotents in Algebras and Coding Theory

César Polcino Milies

Instituto de Matemática e Estatística
Universidade de São Paulo

.

Encontro de Códigos, Reticulados e Informação
IMECC - UNICAMP
2023

Linear Codes

- We shall take, as an alphabet A, a finite field $\mathbb{F}$.

Linear Codes

- We shall take, as an alphabet A, a finite field $\mathbb{F}$.
- In this case, $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$.

Linear Codes

- We shall take, as an alphabet A, a finite field $\mathbb{F}$.
- In this case, $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$.
- We shall take, as codes, subespaces of $\mathbb{F}^n$ of dimensión $m < n$.

Linear Codes

- We shall take, as an alphabet A, a finite field $\mathbb{F}$.
- In this case, $\mathbb{F}^n$ is an n-dimensional vector space over $\mathbb{F}$.
- We shall take, as codes, subespaces of $\mathbb{F}^n$ of dimensión $m < n$.

Definition

A code $\mathcal{C}$ as above is called a **linear code** over $\mathbb{F}$.

If d the minimum distance of $\mathcal{C}$, we shall call it a **(n,m,d)-code.**

Definition

A linear code $\mathcal{C} \subset \mathbb{F}^n$ is called a **cyclic code** if for every vector $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ in the code, we have that also the vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is in the code.

Definition

A linear code $\mathcal{C} \subset \mathbb{F}^n$ is called a **cyclic code** if for every vector $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ in the code, we have that also the vector $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ is in the code.

Notice that the definition implies that if $(a_0, a_1, \ldots, a_{n-2}, a_{n-1})$ is in the code, then all the vectors obtained from this one by a cyclic permutation of its coordinates are also in the code.

Let

$$\mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle};$$

We shall denote by $[f]$ the class of the polynomial $f \in \mathbb{F}[X]$ in $\mathcal{R}_n$.

Let

$$\mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle};$$

We shall denote by $[f]$ the class of the polynomial $f \in \mathbb{F}[X]$ in $\mathcal{R}_n$. The mapping:

$$\varphi : \mathbb{F}^n \to \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle}$$

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in \mathbb{F}[X] \quad \mapsto \quad [a_0 + a_1 X + \ldots + a_{n-2}X^{n-2} + a_{n-1}X^{n-1}].$$

Let

$$\mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1\rangle};$$

We shall denote by $[f]$ the class of the polynomial $f \in \mathbb{F}[X]$ in $\mathcal{R}_n$. The mapping:

$$\varphi : \mathbb{F}^n \rightarrow \frac{\mathbb{F}[X]}{\langle X^n - 1\rangle}$$

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in \mathbb{F}[X] \qquad \mapsto \qquad [a_0 + a_1 X + \ldots + a_{n-2}X^{n-2} + a_{n-1}X^{n-1}].$$

φ is an isomorphism of $\mathbb{F}$-vector spaces. Hence *A code $\mathcal{C} \subset \mathbb{F}^n$ is cyclic if and only if $\varphi(\mathcal{C})$ is an ideal of $\mathcal{R}_n$.*

In the case when $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \dots, a^{n-1}\}$ is a cyclic group of order n, and $\mathbb{F}$ is a field, the elements of $\mathbb{F}C_n$ are of the form:

$$\alpha = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1} a^{n-1}.$$

In the case when $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic group of order n, and $\mathbb{F}$ is a field, the elements of $\mathbb{F}C_n$ are of the form:

$$\alpha = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1} a^{n-1}.$$

It is easy to show that

$$\mathbb{F}C_n \;\cong\; \mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle};$$

In the case when $C_n = \langle a \mid a^n = 1 \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ is a cyclic group of order n, and $\mathbb{F}$ is a field, the elements of $\mathbb{F}C_n$ are of the form:

$$\alpha = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_{n-1} a^{n-1}.$$

It is easy to show that

$$\mathbb{F}C_n \;\cong\; \mathcal{R}_n = \frac{\mathbb{F}[X]}{\langle X^n - 1 \rangle};$$

Hence, to study cyclic codes is equivalent to study ideals of a group algebra of the form $\mathbb{F}C_n$.

Group Codes

Definition

A **group code** is an ideal of a finite group algebra.

Definition

A **group code** is an ideal of a finite group algebra.

In what follows, we shall always assume that $char(K) \not| \, |G|$ so all group algebras considered here will be semisimple and thus, all ideals of $\mathbb{F}G$ are of the form $I = \mathbb{F}Ge$, where $e \in \mathbb{F}G$ is an idempotent element.

Idempotents from subgroups

Let H be a subgroup of a finite group G and let $\mathbb{F}$ be a field such that $car(\mathbb{F}) \nmid |G|$. The element

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

is an idempotent of the group algebra $\mathbb{F}G$, called the **idempotent determined by** H.

Idempotents from subgroups

Let H be a subgroup of a finite group G and let $\mathbb{F}$ be a field such that $car(\mathbb{F}) \nmid |G|$. The element

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

is an idempotent of the group algebra $\mathbb{F}G$, called the **idempotent determined by** H.

$\widehat{H}$ is central if and only if H is normal in G.

Essential idempotents

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

Let e be a primitive central idempotent of $\mathbb{F}G$. Then:

- If e is not a constituent of $\widehat{H}$ we have that $e\widehat{H} = 0$.

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

Let e be a primitive central idempotent of $\mathbb{F}G$. Then:

- If e is not a constituent of $\widehat{H}$ we have that $e\widehat{H} = 0$.
- If e is a constituent of $\widehat{H}$ we have that $e\widehat{H} = e$.

Let H be a normal subgroup of G. Then, $\widehat{H}$ is a central idempotent and, as such, a sum of primitive central idempotents called its **constituents**.

Let e be a primitive central idempotent of $\mathbb{F}G$. Then:

- If e is not a constituent of $\widehat{H}$ we have that $e\widehat{H} = 0$.
- If e is a constituent of $\widehat{H}$ we have that $e\widehat{H} = e$.

In this last case, we have that $\mathbb{F}G \cdot e \subset \mathbb{F}G \cdot \widehat{H}$.

Denote by T a transversal of H in G. Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

$$\alpha = \sum_{\nu \in T} \alpha_\nu \nu \hat{H}.$$

Denote by T a transversal of H in G. Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

$$\alpha = \sum_{\nu \in T} \alpha_\nu \nu \hat{H}.$$

If we denote $T = \{t_1, t_2, \ldots, t_d\}$ and $H = \{h_1, h_2, \ldots, h_m\}$, the explicit expression of α is

$$\alpha = \alpha_1 t_1 h_1 + \alpha_2 t_2 h_1 + \cdots + \alpha_d t_d h_1 + \cdots + \alpha_1 t_1 h_m + \alpha_2 t_2 h_m + \cdots + \alpha_d t_d h_m.$$

Denote by T a transversal of H in G. Then, an element $\alpha \in \mathbb{F}G \cdot e$ can be written in the form

$$\alpha = \sum_{\nu \in T} \alpha_\nu \nu \hat{H}.$$

If we denote $T = \{t_1, t_2, \ldots, t_d\}$ and $H = \{h_1, h_2, \ldots, h_m\}$, the explicit expression of α is

$$\alpha = \alpha_1 t_1 h_1 + \alpha_2 t_2 h_1 + \cdots + \alpha_d t_d h_1 + \cdots + \alpha_1 t_1 h_m + \alpha_2 t_2 h_m + \cdots + \alpha_d t_d h_m.$$

The sequence of coefficients of α, when written in this order, is formed by d repetitions of the subsequence $\alpha_1, \alpha_2, \cdots \alpha_d$. In terms of coding theory, this means that the code given by the minimal ideal $\mathbb{F}Ge$ is a **repetition code**. We shall be interested in idempotents that are not of this type.

Definition

A primitive idempotent e in the group algebra $\mathbb{F}G$, is an **essential idempotent** if $e \cdot \widehat{H} = 0$, for every subgroup $H \neq (1)$ in G.

A minimal ideal of $\mathbb{F}G$ will be called **essential ideal** if it is generated by an essential idempotent.

Definition

A primitive idempotent e in the group algebra $\mathbb{F}G$, is an **essential idempotent** if $e \cdot \widehat{H} = 0$, for every subgroup $H \neq (1)$ in G.

A minimal ideal of $\mathbb{F}G$ will be called **essential ideal** if it is generated by an essential idempotent.

Lemma

Let $e \in \mathbb{F}G$ be a primitive central idempotent. Then e is essential if and only if the map $\pi : G \to Ge$, is a group isomorphism.

Definition

A primitive idempotent e in the group algebra $\mathbb{F}G$, is an **essential idempotent** if $e \cdot \widehat{H} = 0$, for every subgroup $H \neq (1)$ in G.

A minimal ideal of $\mathbb{F}G$ will be called **essential ideal** if it is generated by an essential idempotent.

Lemma

Let $e \in \mathbb{F}G$ be a primitive central idempotent. Then e is essential if and only if the map $\pi : G \to Ge$, is a group isomorphism.

Corollary

If G is abelian and $\mathbb{F}G$ contains an essential idempotent, then G is cyclic.

Assume that G is cyclic of order $n = p_1^{n_1} \cdots p_t^{n_t}$. Then, G can be written as a direct product $G = C_1 \times \cdots \times C_t$, where C_i is cyclic, of order $p_i^{n_i}$, $1 \leq i \leq t$.

Assume that G is cyclic of order $n = p_1^{n_1} \cdots p_t^{n_t}$. Then, G can be written as a direct product $G = C_1 \times \cdots \times C_t$, where C_i is cyclic, of order $p_i^{n_i}$, $1 \leq i \leq t$.
Let K_i be the minimal subgroup of C_i; i.e. the unique subgroup of order p_i in C_i and denote by a_i a generator of this subgroup, $1 \leq i \leq t$. Set

$$e_0 = (1 - \widehat{K_1}) \cdots (1 - \widehat{K_t})$$

Then e_0 is a non-zero central idempotent.

Assume that G is cyclic of order $n = p_1^{n_1} \cdots p_t^{n_t}$. Then, G can be written as a direct product $G = C_1 \times \cdots \times C_t$, where C_i is cyclic, of order $p_i^{n_i}$, $1 \leq i \leq t$.
Let K_i be the minimal subgroup of C_i; i.e. the unique subgroup of order p_i in C_i and denote by a_i a generator of this subgroup, $1 \leq i \leq t$. Set

$$e_0 = (1 - \widehat{K_1}) \cdots (1 - \widehat{K_t})$$

Then e_0 is a non-zero central idempotent.

Proposition

Let G be a cyclic group. Then, a primitive idempotent $e \in \mathbb{F}G$ is essential if and only if $e \cdot e_0 = e$.
Moreover, e_0 is the sum of all essential idempotents of $\mathbb{F}G$.

Proposition

Let $\mathbb{F}_q$ denote a finite field with q elements, $C = C_n$ the cyclic of order n, with generator g such that $(q, n) = 1$. Let m be the multiplicative order of $\overline{q}$ in the unit group $U(\mathbb{Z}_n)$. Then

Proposition

Let $\mathbb{F}_q$ denote a finite field with q elements, $C = C_n$ the cyclic of order n, with generator g such that $(q, n) = 1$. Let m be the multiplicative order of $\overline{q}$ in the unit group $U(\mathbb{Z}_n)$. Then

(i) If e is an essential idempotent, then the dimension of $\mathbb{F}_q C \cdot e$ is precisely m.

Proposition

Let $\mathbb{F}_q$ denote a finite field with q elements, $C = C_n$ the cyclic of order n, with generator g such that $(q, n) = 1$. Let m be the multiplicative order of $\overline{q}$ in the unit group $U(\mathbb{Z}_n)$. Then

(i) If e is an essential idempotent, then the dimension of $\mathbb{F}_q C \cdot e$ is precisely m.

(ii) $dim(\mathbb{F}_q C_n)e_0 = \varphi(n)$ where φ denotes Euler's Totient function.

Proposition

Let $\mathbb{F}_q$ denote a finite field with q elements, $C = C_n$ the cyclic of order n, with generator g such that $(q, n) = 1$. Let m be the multiplicative order of $\overline{q}$ in the unit group $U(\mathbb{Z}_n)$. Then

(i) If e is an essential idempotent, then the dimension of $\mathbb{F}_q C \cdot e$ is precisely m.

(ii) $dim(\mathbb{F}_q C_n)e_0 = \varphi(n)$ where φ denotes Euler's Totient function.

(iii) There exist precisely $\varphi(n)/m$ essential idempotents in $\mathbb{F}_q C$.

Applications

Definition (Sabin and Lomonaco (1995))

Let G_1 and G_2 denote two finite groups of the same order and let $\mathbb{F}$ be a field. Two ideals (codes) $I_1 \subset \mathbb{F}G_1$ and $I_2 \subset \mathbb{F}G_2$ are said to be **combinatorially equivalent** if there exists a bijection $\gamma : G_1 \to G_2$ whose linear extension $\overline{\gamma} : \mathbb{F}G_1 \to \mathbb{F}G_2$ is such that $\overline{\gamma}(I_1) = I_2$. The map $\overline{\gamma}$ is called a **combinatorial equivalence** between I_1 and I_2.

Applications

Definition (Sabin and Lomonaco (1995))

Let G_1 and G_2 denote two finite groups of the same order and let $\mathbb{F}$ be a field. Two ideals (codes) $I_1 \subset \mathbb{F}G_1$ and $I_2 \subset \mathbb{F}G_2$ are said to be **combinatorially equivalent** if there exists a bijection $\gamma : G_1 \to G_2$ whose linear extension $\overline{\gamma} : \mathbb{F}G_1 \to \mathbb{F}G_2$ is such that $\overline{\gamma}(I_1) = I_2$. The map $\overline{\gamma}$ is called a **combinatorial equivalence** between I_1 and I_2.

Theorem (Chalom, Ferraz and PM (2017))

Every minimal ideal in the group algebra of a finite abelian group is combinatorially equivalent to a minimal ideal in the group algebra of a cyclic group of the same order.

Recall that a binary linear code of dimension k and length n is called **simplex** if a generating matrix for the code contains all possible non zero columns of length k. Since these are $2^k - 1$ in number, this matrix must be of size $k \times (2^k - 1)$ so, we must have $n = 2^k - 1$.

Applications

Recall that a binary linear code of dimension k and length n is called **simplex** if a generating matrix for the code contains all possible non zero columns of length k. Since these are $2^k - 1$ in number, this matrix must be of size $k \times (2^k - 1)$ so, we must have $n = 2^k - 1$.

Theorem (Chalom, Ferraz and PM (2017))

Let $\mathcal{C}$ be a binary linear code of dimension k and length $n = 2^k - 1$. Then $\mathcal{C}$ is a simplex code if and only if it is essencial.

Applications

Let $\mathcal{C} = \{v_1, \ldots, v_m\}$ be a linear code, whose elements we write as $v_i = (v_{i,1}, v_{i,2}, \ldots v_{i,n})$, $1 \leq i \leq k-1$, $1 \leq i \leq k-1$. We say that $\mathcal{C}$ **contains no zero column** if, for each index j, $1 \leq j \leq n$, there exists at least one vector $v_i \in \mathcal{C}$ such that $v_{i,j} \neq 0$.

Applications

Let $\mathcal{C} = \{v_1, \ldots, v_m\}$ be a linear code, whose elements we write as $v_i = (v_{i,1}, v_{i,2}, \ldots v_{i,n})$, $1 \leq i \leq k-1$, $1 \leq i \leq k-1$. We say that $\mathcal{C}$ **contains no zero column** if, for each index j, $1 \leq j \leq n$, there exists at least one vector $v_i \in \mathcal{C}$ such that $v_{i,j} \neq 0$.

Theorem (Chalom, Ferraz and PM (2018))

Let $\mathcal{C}$ be a binary linear code of constant weight, without zero columns. Then $\mathcal{C}$ is equivalent to a cyclic code which is either essencial or a repetition code of an essencial one.

Twisted Group Algebra

Definition

Let G be a group and R a commutative ring whose set of invertible elements we denote by $U(R)$. Consider a set of symbols $\overline{G} = \{\overline{g} \mid g \in G\}$. The **twisted group algebra** of G over R with twisting t, denoted R^tG, is the set of finite sums

$$R^tG = \left\{ \sum_{g \in G} a_g \overline{g} \mid a_g \in R \right\}$$

where addition is defined componentwise and multiplication is given by the following rules

Definition

Let G be a group and R a commutative ring whose set of invertible elements we denote by $U(R)$. Consider a set of symbols $\overline{G} = \{\overline{g} \mid g \in G\}$. The **twisted group algebra** of G over R with twisting t, denoted R^tG, is the set of finite sums

$$R^tG \;=\; \left\{ \sum_{g\in G} a_g\overline{g} \mid a_g \in R \right\}$$

where addition is defined componentwise and multiplication is given by the following rules

$$\begin{aligned} \bar{x}.\bar{y} = t(x,y)\overline{xy} \qquad & \text{for all } x, y \in G, \\ \bar{x}a = a\bar{x} \qquad & \text{for all } x \in G \text{ and } a \in R, \end{aligned}$$

extended linearly.

Definition

Let G be a group and R a commutative ring whose set of invertible elements we denote by $U(R)$. Consider a set of symbols $\overline{G} = \{\overline{g} \mid g \in G\}$. The **twisted group algebra** of G over R with twisting t, denoted R^tG, is the set of finite sums

$$R^tG = \left\{ \sum_{g \in G} a_g \overline{g} \mid a_g \in R \right\}$$

where addition is defined componentwise and multiplication is given by the following rules

$$\bar{x}.\bar{y} = t(x,y)\overline{xy} \qquad \text{for all } x, y \in G,$$
$$\bar{x}a = a\bar{x} \qquad \text{for all } x \in G \text{ and } a \in R,$$

extended linearly. Here, the map $t : G \times G \to U(R)$ is called a **twisting** or a **factor set** if, for $x, y, z \in G$ we have that

$$t(g,h).t(gh,\ell) = t(h,\ell).t(g,h\ell).$$

There is a close connection between factor sets and 2-cocycles as used in cohomology, actually both concepts coincide (see, for example Lectures in Abstract Algebra - Jacobson).

There is a close connection between factor sets and 2-cocycles as used in cohomology, actually both concepts coincide (see, for example Lectures in Abstract Algebra - Jacobson).
Several results in this area can be proved via cohomological concepts but presently we shall use only classical ring theory.

There is a close connection between factor sets and 2-cocycles as used in cohomology, actually both concepts coincide (see, for example Lectures in Abstract Algebra - Jacobson).
Several results in this area can be proved via cohomological concepts but presently we shall use only classical ring theory.

We begin with a very special example of twisting.

There is a close connection between factor sets and 2-cocycles as used in cohomology, actually both concepts coincide (see, for example Lectures in Abstract Algebra - Jacobson).
Several results in this area can be proved via cohomological concepts but presently we shall use only classical ring theory.

We begin with a very special example of twisting.

Let $C = \langle g \rangle$ be a cyclic group of order n and let λ be an invertible element in R. Then, the map $t_\lambda : C \times C \to U(R)$ given by

$$t_\lambda(g^i, g^j) = \begin{cases} 1 & \text{if } i + j < n, \\ \lambda & \text{if } i + j \geq n. \end{cases}$$

is a twisting.

Theorem

Let $C = \langle g \rangle$ be a cyclic group of order n and let $R^t C$ be its twisted group algebra over a commutative ring R. Set

$$\lambda = \prod_{\ell=1}^{n-1} t(g, g^\ell).$$

Then $R^t C \cong R^{t_\lambda} C$ where t_λ is as above.

Theorem

Let $C = \langle g \rangle$ be a cyclic group of order n and let $R^t C$ be its twisted group algebra over a commutative ring R. Set

$$\lambda = \prod_{\ell=1}^{n-1} t(g, g^{\ell}).$$

Then $R^t C \cong R^{t_\lambda} C$ where t_λ is as above.

The proof actually shows that $R^t C$ and $R^{t_\lambda} C$ are the same as sets, with the same operations, though constructed from different bases.

Theorem

Let $C = \langle g \rangle$ be a cyclic group of order n and let $R^t C$ be its twisted group algebra over a commutative ring R. Set

$$\lambda = \prod_{\ell=1}^{n-1} t(g, g^\ell).$$

Then $R^t C \cong R^{t_\lambda} C$ where t_λ is as above.

The proof actually shows that $R^t C$ and $R^{t_\lambda} C$ are the same as sets, with the same operations, though constructed from different bases.

Corollary

The twisted group algebra of a cyclic group over a commutative ring is commutative.

Twistings for Abelian groups can be studied in a similar way.

Twistings for Abelian groups can be studied in a similar way.

Given a finite Abelian group A, written as a direct product $A = C_{m_1} \times \cdots \times C_{m_s}$, where $C_{m_i} = \langle g_i \rangle$ is cyclic of order m_i, and invertible elements $\lambda_i \in R$, $1 \leq i \leq s$, set

$$t_{\lambda_i}(g_i^j, g_i^k) = \begin{cases} 1, & \text{for } j + k < m_i, \\ \lambda_i, & \text{for } j + k \geq m_i, \end{cases}$$

which is a twisting of $C_{m_i} = \langle g_i \rangle$ over R.

Twistings for Abelian groups can be studied in a similar way.

Given a finite Abelian group A, written as a direct product $A = C_{m_1} \times \cdots \times C_{m_s}$, where $C_{m_i} = \langle g_i \rangle$ is cyclic of order m_i, and invertible elements $\lambda_i \in R$, $1 \leq i \leq s$, set

$$t_{\lambda_i}(g_i^j, g_i^k) = \begin{cases} 1, & \text{for } j + k < m_i, \\ \lambda_i, & \text{for } j + k \geq m_i, \end{cases}$$

which is a twisting of $C_{m_i} = \langle g_i \rangle$ over R.

We denote by t_Λ the twisting of A defined as follows. Given $a = g_1^{i_1} \cdots g_s^{i_s}$, $b = g_1^{j_1} \cdots g_s^{j_s} \in A$ we set:

$$t_\Lambda(a, b) = t_\Lambda(g_1^{i_1} \cdots g_s^{i_s}, g_1^{j_1} \cdots g_s^{j_s}) = \prod_{k=1}^{s} t_{\lambda_k}(g_k^{i_k}, g_k^{j_k}).$$

where $\Lambda = (\lambda_1, \ldots, \lambda_s)$.

Proposition

Let t be a twisting of A over $\mathbb{F}$ such that $R^{t}A$ is commutative. Then, $R^{t}A \cong R^{t_\Lambda}A$ for some twisting t_Λ as defined above. Conversely, a twisted group algebra of the form $R^{t_\Lambda}A$ is commutative.

Proposition

Let t be a twisting of A over $\mathbb{F}$ such that R^tA is commutative. Then, $R^tA \cong R^{t_\Lambda}A$ for some twisting t_Λ as defined above. Conversely, a twisted group algebra of the form $R^{t_\Lambda}A$ is commutative.

The next elementary result is of interest to establish a connection to coding theory.

Proposition

Let t be a twisting of A over $\mathbb{F}$ such that $R^{t}A$ is commutative. Then, $R^{t}A \cong R^{t_\Lambda}A$ for some twisting t_Λ as defined above. Conversely, a twisted group algebra of the form $R^{t_\Lambda}A$ is commutative.

The next elementary result is of interest to establish a connection to coding theory.

Proposition

Let $C = \langle g \rangle$ be a cyclic group of order n, R a commutative ring and λ an invertible element in R. Let $R^{t_\lambda}C$ be the corresponding twisted group algebra. Then

$$R^{t_\lambda}C \cong \frac{R[X]}{(X^n - \lambda)}.$$

We wish to study subgroup idempotents as in group algebras; however their definition needs to be modified to adapt it to products with a twisting.

We wish to study subgroup idempotents as in group algebras; however their definition needs to be modified to adapt it to products with a twisting.

Proposition

Let $C = \langle g \rangle$ be a cyclic group of order n and $t = t_\lambda$, with λ in a field $\mathbb{F}$, a twisting of C over $\mathbb{F}$. Given a root $\alpha \in \mathbb{K}$, $X^n - \lambda$ where $\mathbb{K}$ denotes the splitting field of $X^n - \lambda$, we set

$$\widehat{C}_\alpha = \frac{1}{n} \sum_{j=0}^{n-1} \alpha^{-j} \bar{g}^j .$$

Then, $\widehat{C}_\alpha$ is an idempotent of the twisted group algebra $\mathbb{F}^{t_\lambda} C$.

We wish to study subgroup idempotents as in group algebras; however their definition needs to be modified to adapt it to products with a twisting.

Proposition

Let $C = \langle g \rangle$ be a cyclic group of order n and $t = t_\lambda$, with λ in a field $\mathbb{F}$, a twisting of C over $\mathbb{F}$. Given a root $\alpha \in \mathbb{K}$, $X^n - \lambda$ where $\mathbb{K}$ denotes the splitting field of $X^n - \lambda$, we set

$$\widehat{C}_\alpha = \frac{1}{n} \sum_{j=0}^{n-1} \alpha^{-j} \bar{g}^j.$$

Then, $\widehat{C}_\alpha$ is an idempotent of the twisted group algebra $\mathbb{F}^{t_\lambda} C$. Moreover, if $\beta \neq \alpha$ is another root of $X^n - \lambda$, then $\widehat{C}_\alpha \widehat{C}_\beta = 0$.

Lemma

Let $\mathbb{K}^t C$ be the twisted group algebra of a cyclic group $C = \langle g \rangle$, of order n, and $\mathbb{K}$ algebraically closed field such that $char(K) \nmid |G|$. Set λ as needed and let $\{\alpha_i\}_{1 \leq i \leq n}$ be the set of all roots of the polynomial $X^n - \lambda$ in $\mathbb{K}$. Then

$$\{\widehat{C}_{\alpha_i} \mid 1 \leq i \leq n\},$$

is the set of all primitive idempotents of $\mathbb{F}^t C$.

Lemma

Let $\mathbb{K}^t C$ be the twisted group algebra of a cyclic group $C = \langle g \rangle$, of order n, and $\mathbb{K}$ algebraically closed field such that $char(K) \nmid |G|$. Set λ as needed and let $\{\alpha_i\}_{1 \leq i \leq n}$ be the set of all roots of the polynomial $X^n - \lambda$ in $\mathbb{K}$. Then

$$\{\widehat{C}_{\alpha_i} \mid 1 \leq i \leq n\},$$

is the set of all primitive idempotents of $\mathbb{F}^t C$.

As before, this result can be extended to finite Abelian groups.

Theorem

Let A be a finite Abelian group written as a direct product $A = C_{m_1} \times \cdots \times C_{m_s}$, where $C_{m_i} = \langle g_i \rangle$ is cyclic of order m_i, and $\mathbb{F}$ a finite field. Assume that the twisted group algebra $\mathbb{F}^t A$ is endowed with a twisting t_Λ as defined above, with $\lambda_i \in F,\ 1 \leq i \leq s$.

Let $\mathbb{K}$ be the splitting field of the polynomial $f = \prod_{i=1}^{t} (X^{m_i} - \lambda_i)$, and let $\mathcal{R}_i = \{\alpha_{ij} \,|\, 1 \leq j \leq m_i\}$ be the set of all roots of the polynomial $X^{m_i} - \lambda_i,\ 1 \leq i \leq m_i$ in $\mathbb{K}$. For each subset of roots $\alpha = (\alpha_{1j_1}, \ldots, \alpha_{sj_s}) \in \mathcal{R}$, we set:

$$e_\alpha = \widehat{(C_{m_1})}_{\alpha_{1j_1}} \cdots \widehat{(C_{m_s})}_{\alpha_{sj_s}},$$

Then

$$\{e_\alpha \mid \alpha \in \mathcal{R}\}$$

is the set of primitive idempotents of $\mathbb{K}^t A$.