Finite Fields and Their Applications 95 (2024) 102386

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Twisted group algebras of Abelian groups[☆]

André Duarte[*], Raul Antonio Ferraz, César Polcino Milies

Instituto de Matemática e Estatística, Universidade de São Paulo,
Caixa Postal 66.281, CEP 05314-970, Brazil

ARTICLE INFO

Article history:
Received 10 August 2023
Received in revised form 15 December 2023
Accepted 2 February 2024
Available online 15 February 2024
Communicated by Gary L. Mullen

MSC:
11Txx
16Bxx
16Dxx
16Kxx
16Uxx
12Fxx

Keywords:
Twisted group algebra
Finite fields
Idempotent
Simple component

ABSTRACT

We study twistings for finite Abelian groups over fields and then show how to extend the notion of idempotent determined by a subgroup, so useful in the case of group algebras, to the case of twisted group algebras, at least when the subgroup is cyclic. In doing so, we obtain a method to compute in a direct way the primitive central idempotents of these algebras over a finite field and fully describe their simple components.

© 2024 Elsevier Inc. All rights reserved.

[☆] Supported by FAPESP, Proc. No 2020/16594-0.

[*] Corresponding author.
E-mail addresses: anddutu@yahoo.com.br (A. Duarte), raul@ime.usp.br (R.A. Ferraz), polcino@ime.usp.br (C. Polcino Milies).

https://doi.org/10.1016/j.ffa.2024.102386
1071-5797/© 2024 Elsevier Inc. All rights reserved.

1. Introduction

Twisted group algebras were introduced by I. Schur in the period 1904 - 1907 [15–17] to study projective representations of finite groups and have been extremely useful ever since.

Maschke's Theorem asserts that, when $char(\mathbb{F}) \nmid |G|$, the twisted group algebra is semisimple [9] and actually this result holds in the more general context of crossed products (see [11, Section 1.4]). In this case, every ideal is generated by an idempotent element and $\mathbb{F}^tG$ can be written as a (unique) direct sum of a finite number of two-sided ideals $\{A_i\}_{1\leq i\leq r}$, called the *simple components* of $\mathbb{F}^tG$, which are simple algebras, and also a direct sum (in more than one way) of minimal left ideals. We shall assume, throughout the paper that we are always in this case; i.e. that $char(\mathbb{F}) \nmid |G|$.

The number of simple components of a twisted group algebra, in the semisimple case, was computed by W.R. Reynolds [13], [14]. Results on radicals of twisted group algebras were given by D.S. Passman [10].

Explicit descriptions of idempotents in special cases were given by G. Karpilovsky [7, Chapter 1], P. Grover and A.K. Bhandari [4], T.Zh. Mollov [8] and A.J. van Zanten [20].

In particular, research in the area is presently quite active due to their connection to coding theory (see, for example, [1], [2], [3], [6], [18], [19]).

In Section §2 we show how to compute the primitive idempotents of $\mathbb{F}^tA$ when A is a finite Abelian group and, in Section §3 we characterize the simple components of this algebra. We conclude with an example illustrating how to obtain all these elements in a particular case.

2. Background

Twisted group algebras can be defined as follows.

Definition 2.1. Let G be a group and R a commutative ring whose set of invertible elements we denote by $\mathcal{U}(R)$. A map $t : G \times G \to \mathcal{U}(R)$ is called a **twisting** or a **factor set** if, for $g, h, \ell \in G$ we have that

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

If also

$$t(g,1) = t(1,g) = 1 \quad \text{for all } g \in G,$$

the twisting is called **normalized**. We shall always assume that the twistings are normalized.

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

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

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

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

extended linearly.

An element $g \in G$ is called **t-regular** if $t(g,h) = t(h,g)$ whenever $h \in C_G(g)$, the centralizer of g in G. We shall denote by G_0 the set of all regular elements of G, i.e.

$$G_0 \;=\; \{g \in G \mid t(g,h) = t(h,g),\ \forall h \in C_G(g)\}. \tag{1}$$

In particular, we shall need the following result.

Theorem 2.2. *[7, Theorem 8.2.8] Let A be a finite abelian group, $\mathbb{F}$ an arbitrary field and let t be a twisting of A over $\mathbb{F}$. Then the following conditions are equivalent:*

(1) $\mathbb{F}^{\,t}A$ is a central simple $\mathbb{F}$-algebra.
(2) $A_0 = \{1\}$.

There is a close connection between factor sets and 2-cocycles as used in cohomology (see, for example [5, p. 83]). Several results in this area can be proved via cohomological concepts and also using projective representation theory, but in the present paper we use only ring-theoretical techniques via straightforward computations.

In the special case of group algebras, there is a standard method to construct idempotents of $\mathbb{F}G$ from subgroups of G. If H is a subgroup, then the element

$$\widehat{H} = \sum_{h\in H} h, \tag{2}$$

is an idempotent of $\mathbb{F}G$ and it is central if and only if H is normal in G.

As shown in [12, Proposition 3.6.7] we have that $(\mathbb{F}G)(1-\widehat{H}) = \Delta(G,H)$, the kernel of the natural projection $\pi : \mathbb{F}G \to \mathbb{F}[G/H]$ and it is easy to see that $(FG)\widehat{H} \cong \mathbb{F}[G/H]$.

In the case of twisted group algebras this construction no longer gives idempotent elements. The necessary correction will be the key step to our approach.

We shall need some well-known facts.

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

$$t_\lambda(g^i, g^j) = \begin{cases} 1 & \text{if } i + j < n, \\ \lambda & \text{if } i + j \geq n, \end{cases} \tag{3}$$

is a twisting. The proof is straightforward (see [5, p. 80]).

The following result is usually proved using ideas from cohomology. For the sake of completeness we offer a very simple proof.

Theorem 2.3. *Let $C = \langle g \rangle$ be a cyclic group of order n and let R^tC be its twisted group algebra over a commutative ring R. Set*

$$\lambda = \prod_{\ell=1}^{n-1} t(g, g^\ell). \tag{4}$$

Then $R^tC \cong R^{t_\lambda}C$ where t_λ is as in equation (3).

Proof. Let $\overline{C} = \{\overline{g^i} \mid 0 \leq i \leq n-1\}$ be the set of symbols used to define R^tC. Then $\overline{g^i}\,\overline{g^j} = t(g^i, g^j)\overline{g^{i+j}}$ and thus

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

So

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

Set $\widetilde{g^i} = \prod_{\ell=1}^{i-1} t(g, g^\ell)\overline{g^i} = \overline{g}^i$. Then, the set $\{\widetilde{g^i} \mid 0 \leq i \leq n-1\}$ is an R-basis of R^tC.

If $0 \leq i + j < n$ we readily get that $\widetilde{g^i}\widetilde{g^j} = \widetilde{g^i + g^j}$.

If $i + j \geq n$, writing $i + j = n + r$ we have that $r \leq n$ and

$$\widetilde{g^i}\widetilde{g^i} = \overline{g}^{i+j} = \overline{g}^n\overline{g}^r = \lambda\overline{g}^r = \lambda\widetilde{g^r} = \lambda\widetilde{g^{i+j}}.$$

So the map $\overline{g^i} \mapsto \widetilde{g^i}$, extended linearly, gives the desired isomorphism. □

Notice that the proof above shows that R^tC and $R^{t_\lambda}C$ are actually the same as sets, with the same operations, though they are constructed from different bases. In what follows, when dealing with twisted group algebras of cyclic groups, we shall always assume that they are endowed with a twisting as in formula (3).

It is easily seen that $R^{t_\lambda}C$ is commutative. Hence, in view of Theorem 2.3 we have the following.

Corollary 2.4. *The twisted group algebra of a cyclic group over a commutative ring is commutative.*

3. Twisted group algebras of Abelian groups

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:

$$t_\Lambda(a, b) = t_\Lambda(g_1^{i_1} \cdots g_s^{i_s}, g_1^{j_1} \cdots g_s^{j_s}) = \prod_{k=1}^{s} t_{\lambda_k}(g_k^{i_k}, g_k^{j_k}), \tag{5}$$

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

Proposition 3.1. *Let t be a twisting of A over $\mathbb{F}$ such that R^tA is commutative. Then, there exists a twisting t_Λ as defined in (5) such that $R^tA = R^{t_\Lambda}A$.*

Conversely, a twisted group algebra of the form $R^{t_\Lambda}A$ is commutative.

Proof. For a fixed integer k, $1 \leq k \leq s$, and for all positive integer j, we have

$$\overline{g}_k{}^j = c_{kj}\, \overline{g_k^j},$$

where $c_{kj} = \prod_{\ell=1}^{j-1} t(g_k, g_k^\ell)$.

If i and j are arbitrary positive integers, then

$$c_{k(i+j)}\overline{g_k^{i+j}} = \overline{g}_k^{i+j} = \overline{g}_k^i \overline{g}_k^j = (c_{ki}\overline{g_k^i})(c_{kj}\overline{g_k^j}).$$

We compute

$$\overline{g}_1{}^i\ \overline{g}_2{}^j = c_{1i}\, c_{2j}\, \overline{g_1^i}\ \overline{g_2^j} = c_{1i}\, c_{2j}\, t(g_1^i, g_2^j)\, \overline{g_1^i g_2^j}.$$

If we set $c(i, j) = c_{1i}\, c_{2j}\, t(g_1^i, g_2^j)$, then $\overline{g}_1{}^i\ \overline{g}_2{}^j = c(i, j)\overline{g_1^i g_2^j}$. Given a set of integers $i_1, \ldots, i_s$, we have inductively that

$$\overline{g}_1{}^{i_1} \cdots \overline{g}_s{}^{i_s} = c_{\ell_s}\, \overline{g_1^{i_1} \cdots g_s^{i_s}},$$

where $c_{\ell_1} = c_{1i_1}$ and $c_{\ell_s} = c_{\ell_{s-1}}\, c_{1i_s}\, t(g_1^{i_1} \cdots g_{s-1}^{i_{s-1}}, g_s^{i_s})$.

For $g = g_1^{i_1} \cdots g_s^{i_s} \in A$, with $0 \leq i_k < m_k$ for $1 \leq k \leq s$, we denote $c(g) = c_{\ell_s}$.

If we set $\widetilde{g} = c(g)\overline{g}$, for all $g \in A$, then $\widetilde{A} = \{\widetilde{g} \mid g \in A\}$ is another copy of A in R^tA.

Let $\lambda_k = c_{km_k}$, $1 \leq k \leq s$. For a fixed k and for any $\ell \geq m_k$, we have $c_{k\ell} = \lambda_k\, c_{kr}$, where r is the remainder of dividing ℓ by m_k. So, if $i, j = 1, \ldots, m_k$, we get $c_{k(i+j)} = t_{\lambda_k}(g_k^i, g_k^j)c_{kr}$, where r, $0 \leq r < m_k$, is an integer.

For arbitrary integers $i, j = 1, \ldots, m_k$, if r is the remainder of dividing $i + j$ by m_k, we have

$$\begin{aligned}\widetilde{g_k^i}\,\widetilde{g_k^j} &= c_{ki}\,c_{kj}\,\overline{g_k^i}\,\overline{g_k^j} = c_{k(i+j)}\,\overline{g_k^{i+j}} \\ &= t_{\lambda_k}(g_k^i, g_k^j)c_{kr}\,\overline{g_k^{i+j}} = t_{\lambda_k}(g_k^i, g_k^j)\,\widetilde{g_k^{i+j}}.\end{aligned}$$

For $g = g_1^{i_1} \cdots g_s^{i_s}$ and $h = g_1^{j_1} \cdots g_s^{j_s}$ in A, the product of $\widetilde{g}$ and $\widetilde{h}$ is

$$\begin{aligned}\widetilde{g}\,\widetilde{h} &= \left(\widetilde{g_1^{i_1}} \cdots \widetilde{g_s^{i_s}}\right)\left(\widetilde{g_1^{j_1}} \cdots \widetilde{g_s^{j_s}}\right) \\ &= t_{\lambda_1}(g_1^{i_1}, g_1^{j_1})\widetilde{g_1^{i_1+j_1}} \cdots t_{\lambda_s}(g_s^{i_s}, g_1^{j_s})\widetilde{g_s^{i_s+j_s}} = t_\Lambda(g, h)\widetilde{gh}.\end{aligned}$$

So $R^t A = R^{t_\Lambda} A$, as claimed.

The converse follows from a straightforward computation. □

We first introduce subgroup idempotents in the special case of cyclic subgroups.

Proposition 3.2. *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 α of $X^n - \lambda$ in a field $\mathbb{K}$ containing $\mathbb{F}$, 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 $\mathbb{K}^{t_\lambda}C$.

Moreover, if $\beta \neq \alpha$ is another root of $X^n - \lambda$, then $\widehat{C}_\alpha \widehat{C}_\beta = 0$.

Proof. Since $\alpha^{i+j} = \lambda\alpha^r$ and $\bar{g}^{i+j} = \lambda\bar{g}^r$, whenever $i + j = n + r$ and $0 \leq r < m$, we obtain

$$\begin{aligned}\bar{g}^i\widehat{C}_\alpha &= \frac{1}{n}\sum_{j=0}^{n-1} \alpha^{-j}\bar{g}^{\ i+j} \\ &= \frac{\alpha^i}{n}\sum_{j=0}^{n-1} \alpha^{-i-j}\bar{g}^{\ i+j} = \alpha^i\widehat{C}_\alpha,\end{aligned}$$

implying that $\alpha^{-i}\bar{g}^{\ i}\widehat{C}_\alpha = \widehat{C}_\alpha$. Then,

$$\widehat{C}_\alpha^2 = \frac{1}{n}\sum_{j=0}^{n-1} \alpha^{-j}\bar{g}^{\ j}\widehat{C}_\alpha = \frac{1}{n}\sum_{j=0}^{n-1} \alpha^{-j}\alpha^j\widehat{C}_\alpha = \widehat{C}_\alpha.$$

If $\beta \neq \alpha$ is another root of $X^n - \lambda$, we compute

$$\begin{aligned}\widehat{C}_\alpha \widehat{C}_\beta &= \frac{1}{n}\sum_{i=0}^{n-1} \alpha^{-i}\bar{g}^{\;i}\widehat{C}_\beta \\ &= \frac{1}{n}\sum_{j=0}^{n-1} \alpha^{-i}\beta^{i}\widehat{C}_\beta = \left(\frac{1}{n}\sum_{j=0}^{n-1}(\alpha^{-1}\beta)^i\right)\widehat{C}_\beta.\end{aligned}$$

Since $\alpha^{-1}\beta \neq 1$ is a root of $X^n - 1$, it is also a root of $X^{n-1} + X^{n-2} + \cdots + X + 1$ and thus $\sum_{j=0}^{n-1}(\alpha^{-1}\beta)^i = 0$. Hence $\widehat{C}_\alpha \widehat{C}_\beta = 0$. □

Let $\mathbb{K}$ be a splitting field of the polynomial $X^n - \lambda$ over $\mathbb{F}$. In the case when G is an Abelian group, formulas giving the primitive idempotents of the group algebra $\mathbb{K}G$ in terms of irreducible characters are well-known (see [12, p. 185]). Grover and Bhadari [4] extended this result to twisted group algebras using projective characters and assuming that the twisting is as in formula (5). We shall show how these idempotents can be obtained, even without this assumption, in terms of subgroup idempotents. As before, we study first the case when G is cyclic.

Lemma 3.3. *Let $\mathbb{F}$ be a finite field and $\mathbb{K}$ the splitting field of $X^n - \lambda$ over $\mathbb{F}$. Let $\mathbb{K}^tC$ be the twisted group algebra of a cyclic group $C = \langle g \rangle$, of order n, and $\mathbb{K}$ a splitting field of the polynomial $X^n - \lambda$ over $\mathbb{F}$ such that $char(\mathbb{K}) \nmid |G|$ where λ is as given in formula (4). Let $\{\alpha_i\}_{1 \leq i \leq n}$ be the set of all roots of the polynomial $X^n - \lambda$ in $\mathbb{K}$. Then*

$$\{\widehat{C}_{\alpha_i} \mid 1 \leq i \leq n\}, \tag{6}$$

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

Proof. Our previous result shows that $\{\widehat{C}_{\alpha_i}\}$ is a set of orthogonal idempotents. Since they are n in number, which is precisely the dimension of $\mathbb{K}^tC$ over $\mathbb{K}$, it follows that it is the complete set of primitive idempotents of this algebra. □

This result extends in a natural way to finite Abelian groups.

Theorem 3.4. *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 $\mathbb{F}^{t_\Lambda}A$ is endowed with a twisting t_Λ as defined in (5), with $\lambda_i \in \mathbb{F},\ 1 \leq i \leq s$.*

Let $\mathbb{K}$ be the splitting field of the polynomial $f = \prod_{i=1}^{t}(X^{m_i} - \lambda_i)$; let $\mathcal{R}_i = \{\alpha_{ij} \mid 1 \leq j \leq m_i\}$ be the set of all roots of the polynomial $X^{m_i} - \lambda_i$, in $\mathbb{K},\ 1 \leq i \leq m_i$, and set $\mathcal{R} = \prod_{i=1}^{s}\mathcal{R}_i$. 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 $\mathbb{K}^{t_\Lambda}A$.

Proof. As seen in the previous Lemma, for each fixed index i, the set of all elements of the form $\widehat{(C_{m_i})}_{\alpha_{ij_i}}$ is a set of orthogonal idempotents, and as the algebra $\mathbb{K}^{t_\Lambda}A$ is commutative by Proposition 3.1, it follows that the full set of elements given in our statement is also a set of orthogonal idempotents. Since their number is equal to the dimension of $\mathbb{K}^{t_\Lambda}A$ over $\mathbb{K}$, the result follows. □

The case of a finite Abelian group can be reduced to the previous one due to a simple remark.

Lemma 3.5. *Let A be a finite Abelian group, R a commutative ring, R^tA the corresponding twisted group algebra and $A_0 = \{a \in A \mid t(a,h) = t(h,a),\ \forall h \in A\}$ the set of regular elements of A. Let t_0 be the twisting of A_0 obtained by restriction of t. Then, the center of $\mathbb{F}^{\,t}A$ is the twisted group algebra*

$$\mathcal{Z}(\mathbb{F}^{\,t}A) \;=\; \mathbb{F}^{\,t_0}A_0.$$

Proof. It is easy to see that $\mathbb{F}^{\,t_0}A_0 \subseteq \mathcal{Z}(\mathbb{F}^{\,t}A)$. Conversely, if $\gamma = \sum_{a\in A} x_a\overline{a} \in \mathcal{Z}(\mathbb{F}^{\,t}A)$ and $x_b \neq 0$ for some $b \in A$, then $t(b,a) = t(a,b)$ for all $a \in A$, which implies that $\mathcal{Z}(\mathbb{F}^{\,t}A) \subseteq \mathbb{F}^{\,t_0}A_0$, as required. □

Since the central primitive idempotents of a semisimple algebra are also the primitive idempotents of its center, to find the primitive idempotents of a twisted group algebra of the form $\mathbb{K}^tA$, using the lemma above, all we need is to determine A_0, its set of regular elements and then use Theorem 3.4.

Finally, we see how to obtain the idempotents of the original twisted group algebra $\mathbb{F}^{\,t}A$ via the process known as Galois descent.

With the notations above, let $\mathcal{G} = Gal(\mathbb{K},\mathbb{F})$ be the Galois group of $\mathbb{K}$ over $\mathbb{F}$. For $\sigma \in \mathcal{G}$ and $\alpha = (\alpha_{1i_1},\ldots,\alpha_{si_s}) \in \mathcal{R}$, we set

$$\sigma\cdot\alpha = (\alpha_{1i_1}^{\sigma},\ldots,\alpha_{si_s}^{\sigma}).$$

Thus, $\mathcal{G}$ acts on $\mathcal{R}$.

We also define an action of $\mathcal{G}$ on $\mathbb{K}^{\,t_\Lambda}A$ setting:

$$\sigma\Big(\sum_{a\in A} b_a\overline{a}\Big) = \sum_{a\in A} b_a^{\sigma}\overline{a} \quad \sigma \in \mathcal{G}.$$

If $\sigma \in \mathcal{G}$, then

$$\begin{aligned}\sigma(e_\alpha) &= \sigma\cdot\left(\widehat{(C_{m_1})}_{\alpha_{1i_1}}\cdots\widehat{(C_{m_s})}_{\alpha_{si_s}}\right)\\ &= \sigma\widehat{(C_{m_1})}_{\alpha_{1i_1}}\cdots\sigma\widehat{(C_{m_s})}_{\alpha_{si_s}}\\ &= \widehat{(C_{m_1})}_{\alpha^\sigma_{1i_1}}\cdots\widehat{(C_{m_s})}_{\alpha^\sigma_{si_s}}\\ &= e_{\sigma\cdot\alpha}.\end{aligned}$$

Hence, for $\alpha\in\mathcal{R}$ and $\sigma\in\mathcal{G}$, we get $\sigma(e_\alpha)=e_{\sigma\cdot\alpha}$. Since $e_{\sigma\cdot\alpha}$ is also a primitive central idempotent, we have $\mathcal{G}$ acting on $\{e_\alpha\,|\,\alpha\in\mathcal{R}\}$. We denote

$$S_\alpha=\{\sigma\cdot\alpha\,|\,\sigma\in\mathcal{G}\}.$$

Proposition 3.6. *If $\alpha\in\mathcal{R}$, then $\widetilde{e_\alpha}=\sum_{\beta\in S_\alpha}e_\beta$ is a primitive idempotent of $\mathbb{F}^{\,t_\Lambda}A$. In addition, every primitive idempotent of $\mathbb{F}^{\,t_\Lambda}A$ is of form $\widetilde{e_\alpha}$ for some $\alpha\in\mathcal{R}$.*

Proof. Let σ be an automorphism in $\mathcal{G}$. Since $\beta\mapsto\sigma\cdot\beta$ is a bijective map on S_α, it follows that

$$\sigma\cdot\widetilde{e_\alpha}=\sigma\cdot\sum_{\beta\in S_\alpha}e_\beta=\sum_{\beta\in S_\alpha}e_{\sigma\cdot\beta}=\widetilde{e_\alpha}.$$

Thus, $\widetilde{e_\alpha}\in\mathbb{F}^{\,t_\Lambda}A$. The set $\{e_\beta\,|\,\beta\in S_\alpha\}$ is a set of orthogonal idempotents in $\mathbb{K}^{\,t_\Lambda}A$, which implies that $\widetilde{e_\alpha}$ is an idempotent. Assume that $\widetilde{e_\alpha}=e+f$ with e and f orthogonal idempotents in $\mathbb{F}^{\,t_\Lambda}A$. Since $\widetilde{e_\alpha}$ is also an idempotent in $\mathbb{K}^{\,t_\Lambda}A$, we have $\widetilde{e_\alpha}e_\alpha=e_\alpha$ implying that $e_\alpha=ee_\alpha+fe_\alpha$. As e_α is a primitive idempotent in $\mathbb{K}^{\,t_\Lambda}A$ and ee_α, fe_α are orthogonal idempotents, we get $ee_\alpha=0$ or $fe_\alpha=0$. Suppose that $fe_\alpha=0$. Then $\sigma\cdot e_\alpha=\sigma\cdot ee_\alpha=ee_{\sigma\cdot\alpha}$, which implies that $\widetilde{e_\alpha}=e\widetilde{e_\alpha}$ and thus $e=\widetilde{e_\alpha}$.

Assume that e is a primitive idempotent in $\mathbb{F}^{\,t_\Lambda}A$. Since e is also an idempotent of $\mathbb{K}^{\,t_\Lambda}A$, it follows that $ee_\alpha=e_\alpha$ for some $\alpha\in\mathcal{R}$. Thus $e_{\sigma\cdot\alpha}=ee_{\sigma\cdot\alpha}$, for all $\sigma\in\mathcal{G}$, which implies that $\widetilde{e_\alpha}=e\widetilde{e_\alpha}$. As both e and $\widetilde{e_\alpha}$ are primitive idempotents in $\mathbb{F}^{\,t_\Lambda}A$, we conclude that $e=\widetilde{e_\alpha}$. □

Let

$$St(\alpha)=\{\sigma\in\mathcal{G}\mid\sigma\cdot\alpha=\alpha\},$$

denote the *stabilizer* of α in $\mathcal{G}$.

For an idempotent $e_\alpha=\sum_{a\in A}k_aa$ we can obtain the expression of the corresponding $\widetilde{e_\alpha}$ in $\mathbb{F}^tA$ computing:

$$\widetilde{e_\alpha}=\frac{1}{|St(\alpha)|}\sum_{\sigma\in\mathcal{G}}\Big(\sum_{a\in A}k_a^\sigma\overline{a}\Big)$$

$$\begin{aligned}&= \frac{1}{|St(\alpha)|}\sum_{a\in A}\Big(\sum_{\sigma\in\mathcal{G}} k_a^{\sigma}\Big)\overline{a}\\ &= \frac{1}{|St(\alpha)|}\sum_{a\in A} tr_{\mathbb{K}|\mathbb{F}}(k_a)\overline{a}.\end{aligned}$$

4. The simple components over finite fields

If a group G contains a central subgroup N of regular elements, then its twisted group algebra R^tG over a commutative ring R can also be realized as a twisted group algebra $R^tN^{\gamma}[G/N]$ of the factor group G/N over the ring R^tN. We develop the necessary computations since we shall need the explicit expression of the twisting γ.

Let T denote a transversal of N in G. Given two elements $x, y \in T$ there exists $z \in T$ and an element $\tau(x, y) \in N$ such that

$$xy \;=\; \tau(x,y)z. \tag{7}$$

An element $\theta = \sum_{g\in G} r_g\overline{g} \in R^tG$ can also be written in the form

$$\begin{aligned}\theta &= \sum_{x\in T}\sum_{h\in N} r_{hx}\overline{hx} = \sum_{x\in T}\sum_{h\in N} r_{hx}t(h,x)^{-1}\overline{h}\overline{x}\\ &= \sum_{x\in T}\Big(\sum_{h\in N} r_{hx}t(h,x)^{-1}\overline{h}\Big)\overline{x},\end{aligned}$$

with $\Big(\sum_{h\in N} r_{hx}t(h,x)^{-1}\overline{h}\Big) \in R^tN$. Since the set $\{\overline{x} \mid x \in T\}$ is clearly linearly independent over $R\ ^tN$, this shows that it is a basis over R^tN.

We consider the set of symbols $\widetilde{G/N} = \{\widetilde{xN} = \overline{x} \mid x \in T\}$ and construct the twisted group algebra of G/N over R^tN using this set as a basis. We wish to see how to multiply elements of this basis so, for $x, y \in T$, we compute using equation (7):

$$\begin{aligned}\widetilde{xN}\widetilde{yN} = \overline{x}\,\overline{y} \;&=\; t(x,y)\overline{xy} \;=\; t(x,y)\overline{\tau(x,y)z}\\ &= t(x,y)t(\tau(x,y),z)^{-1}\overline{\tau(x,y)}\overline{z}\\ &= t(x,y)t(\tau(x,y),\tau(x,y)^{-1}xy)^{-1}\overline{\tau(x,y)}\;\overline{z}\\ &= t(x,y)t(\tau(x,y),\tau(x,y)^{-1}xy)^{-1}\overline{\tau(x,y)}\;\widetilde{zN}\\ &= t(x,y)t(\tau(x,y),\tau(x,y)^{-1}xy)^{-1}\overline{\tau(x,y)}\;\widetilde{xyN}.\end{aligned}$$

Hence, the twisting $\gamma : \frac{G}{N} \times \frac{G}{N} \to \mathcal{U}(R^tN)$ is given by

$$\gamma\Big(\widetilde{xN},\widetilde{yN}\Big) \;=\; t(x,y)t(\tau(x,y),\tau(x,y)^{-1}xy)^{-1}\overline{\tau(x,y)}. \tag{8}$$

Let A be a finite Abelian group, A_0 the subgroup of its regular elements and let t be a twisting of A over a finite field $\mathbb{F}$ such that $char(\mathbb{F}) \nmid |A|$. Let $\{e_1, \ldots, e_r\}$ be a complete set of primitive central idempotents of $\mathbb{F}^{\,t}A_0$ which is also a complete set of central primitive idempotents of $\mathbb{F}^{\,t}A$. Then

$$\mathbb{F}^{\,t}A = \oplus_{i=1}^{r}\mathbb{F}^{\,t}A\,e_i.$$

Let T be a transversal of A_0 in A and $\tau : T \times T \to A_0$, be the map such that $xy = \tau(x,y)z$, for all x, y and z are in T. The map $\gamma : A/A_0 \times A/A_0 \to \mathcal{U}(\mathbb{F}^{\,t}A_0)$ given by

$$\gamma(xA_0, yA_0) = t(x,y)\,t(\tau(x,y), \tau(x,y)^{-1}xy)^{-1}\,\overline{\tau(x,y)} \tag{9}$$

is a twisting of A/A_0 over the commutative ring $\mathbb{F}^{\,t}A_0$ such that $\mathbb{F}^{\,t}A = (\mathbb{F}^{\,t}A_0)^{\gamma}(A/A_0)$. If we set $\widetilde{xA_0} = \overline{x}$, for all $x \in T$, then $\widetilde{xA_0}\,\widetilde{yA_0} = \gamma(xA_0, yA_0)\,\widetilde{xyA_0}$.

We claim that A/A_0 does not contain γ-regular elements. By way of contradiction, assume that $x \in T$ and $0 \neq xA_0 \in A/A_0$ is a regular element. Then, for all $y \in T$, we have $\gamma(xA_0, yA_0) = \gamma(yA_0, xA_0)$. Since A is Abelian, $\tau(x,y) = \tau(y,x)$, for all $y \in T$. By formula (9), we get $t(x,y) = t(y,x)$, implying that $\overline{x}\,\overline{y} = \overline{y}\,\overline{x}$, for every $y \in T$. Now, if $a \in A$, we have $a = a_0 y$ with $a_0 \in A_0$ and $y \in T$. Since $\overline{a_0}$ is central, it follows that

$$\overline{x}\,\overline{a} = \overline{x}\,\left(t(a_0,y)^{-1}\,\overline{a_0}\,\overline{y}\right) = \left(t(a_0,y)^{-1}\,\overline{a_0}\,\overline{y}\right)\overline{x} = \overline{a}\,\overline{x}.$$

However $\overline{x}\,\overline{a} = t(x,a)\overline{xa}$ and $\overline{a}\,\overline{y} = t(a,x)\overline{ax}$, and thus $t(x,a) = t(a,x)$, for any $a \in A$. This implies that $x \in A_0$ and thus $xA_0 = 0$, a contradiction.

The simple component $\mathbb{F}^{\,t}A_0 e_i$ of $\mathbb{F}^{\,t}A_0$ is a field, because $\mathbb{F}^{\,t}A_0 = \mathcal{Z}(\mathbb{F}^{\,t}A)$ is commutative. Then:

$$\mathbb{F}^{\,t}A\,e_i = (\mathbb{F}^{\,t}A_0)^{\gamma}(A/A_0)\,e_i = (\mathbb{F}^{\,t}A_0\,e_i)^{\gamma}(A/A_0).$$

We are ready to prove the following.

Theorem 4.1.

$$\mathbb{F}^{\,t}A\,e_i \cong M_d(\mathbb{F}^{\,t}A_0\,e_i),$$

where $d = \sqrt{[A : A_0]}$.

Proof. Since $\mathbb{F}^{\,t}A\,e_i = (\mathbb{F}^{\,t}A_0\,e_i)^{\gamma}(A/A_0)$ and A/A_0 does not contain γ-regular elements, by Theorem 2.2, we have $\mathbb{F}^{\,t}A\,e_i$ is a central simple $\mathbb{F}^{\,t}A_0\,e_i$-algebra. By Wedderburn's Theorem

$$\mathbb{F}^{\,t}A\,e_i \cong M_d(\mathbb{F}^{\,t}A_0\,e_i).$$

Then $[\mathbb{F}^{\,t}A\,e_i : \mathbb{F}] = d^2[\mathbb{F}^{\,t}A_0\,e_i : \mathbb{F}]$.

On the other hand, we have $[\mathbb{F}^{\,t}A\,e_i : \mathbb{F}] = [(\mathbb{F}^{\,t}A_0\,e_i)^{\gamma}(A/A_0) : \mathbb{F}] = [A : A_0][\mathbb{F}^{\,t}A_0\,e_i : \mathbb{F}]$ and hence $d = \sqrt{[A : A_0]}$. □

Assume that $A_0 = C_{m_1} \times \cdots \times C_{m_s}$, where $C_{m_i} = \langle g_i \rangle$ is cyclic of order m_i. Since $\mathbb{F}\,{}^t A_0$ is commutative, there exist invertible elements $\lambda_i \in \mathbb{F}$, $1 \le i \le s$, such that $\mathbb{F}\,{}^t A_0 = \mathbb{F}\,{}^{t_\Lambda} A_0$, where $\Lambda = (\lambda_1, \ldots, \lambda_s)$. Let $\mathbb{K}$, $\mathcal{R}$ and $\widetilde{e_{\alpha_i}}$, for some $\alpha_i \in \mathcal{R}$, be as constructed in Theorem 3.4.

Theorem 4.2. *$\mathbb{F}\,{}^t A_0\, \widetilde{e_{\alpha_i}} \cong \mathbb{F}(\alpha_i)$ and $[\mathbb{F}\,{}^t A_0\, \widetilde{e_{\alpha_i}} : \mathbb{F}] = |S_\alpha|$.*

Proof. Let $\mathcal{O}(e_{\alpha_i}) = \{\sigma(e_{\alpha_i}) \,|\, \sigma \in \mathcal{G}\}$ be the orbit of e_{α_i} under the action of $\mathcal{G}$. Since $\mathbb{K}$ is a splitting field for the semisimple algebra $\mathbb{K}\,{}^t A_0$ and $\sigma(e_{\alpha_i})$ is a central primitive idempotent of $\mathbb{K}\,{}^t A_0$, for all $\sigma \in \mathcal{G}$, we have

$$\mathbb{K}\,{}^t A_0\, \widetilde{e_{\alpha_i}} = \oplus_{e \in \mathcal{O}(e_{\alpha_i})} \mathbb{K}\,{}^t A_0\, e \cong \oplus_{e \in \mathcal{O}(e_{\alpha_i})} \mathbb{K}.$$

Hence, $[\mathbb{K}\,{}^t A_0\, \widetilde{e_{\alpha_i}} : \mathbb{K}] = |\mathcal{O}(e_{\alpha_i})|$. Since $\mathbb{K}\,{}^t A_0\, \widetilde{e_{\alpha_i}} \cong \mathbb{K} \otimes_{\mathbb{F}} \mathbb{F}\,{}^t A_0\, \widetilde{e_{\alpha_i}}$, we get

$$[\mathbb{F}\,{}^t A_0\, \widetilde{e_{\alpha_i}} : \mathbb{F}] = [\mathbb{K}\,{}^t A_0\, \widetilde{e_{\alpha_i}} : \mathbb{K}] = |\{\sigma \cdot e_{\alpha_i} \,|\, \sigma \in \mathcal{G}\}|.$$

By the Orbit-Stabilizer Theorem we have

$$|\mathcal{O}(e_{\alpha_i})| = \frac{[\mathbb{K} : \mathbb{F}]}{|St(e_{\alpha_i})|} = \frac{[\mathbb{K} : \mathbb{F}]}{|St(\alpha_i)|} = \frac{[\mathbb{K} : \mathbb{F}]}{[\mathbb{K} : \mathbb{F}(\alpha_i)]} = [\mathbb{F}(\alpha_i) : \mathbb{F}].$$

Since $\mathcal{G}$ is cyclic and $[\mathbb{F}\,{}^t A_0 \widetilde{e_{\alpha_i}} : \mathbb{F}] = [\mathbb{F}(\alpha_i) : \mathbb{F}]$, it follows from Galois Correspondence Theorem that $\mathbb{F}\,{}^t A_0 \widetilde{e_{\alpha_i}} \cong \mathbb{F}(\alpha_i)$. □

Remark. It should be noted that the results in this section hold also in the case of infinite fields, when the extension $\mathbb{K} / \mathbb{F}$ is cyclic.

5. An example

Let $\mathbb{F} = \mathbb{F}_5$ be the finite field with 5 elements and set $A = \langle x \rangle \times \langle y \rangle \times \langle z \rangle$ where x and y are of order 2 and z is of order 3.

We define $t : A \times A \to \mathcal{U}(\mathbb{F}_5)$ as follows:

$$t(x^{i_1} y^{j_1} z^{k_1}, x^{i_2} y^{j_2} z^{k_2}) = (-1)^{j_1 i_2}\, t_\lambda(z^{k_1}, z^{k_2}),$$

where t_λ is as in equation (4) and we take $\lambda = -1$.

Since $o(x) = o(y) = 2$ and the multiplicative order of -1 in $\mathcal{U}(\mathbb{F}_5)$ is also equal to 2, it is straightforward to verify that the map t is a twisting of A over $\mathbb{F}$.

Notice that an element $a = x^{i_1} y^{j_1} z^{k_1}$ is in A_0 if and only if $t(a, b) = t(b, a)$ for all $b = x^{i_2} y^{j_2} z^{k_2} \in A$. Using the formula for t we get $(-1)^{j_1 i_2} t_\lambda(z^{k_1}, z^{k_2}) = (-1)^{j_2 i_1} t_\lambda(z^{k_2}, z^{k_1})$ hence $(-1)^{j_1 i_2} = (-1)^{j_2 i_1}$, so we must have $i_1 = j_1 = 0$. Thus $A_0 = \langle z \rangle$.

Let $\mathbb{K}$ be a splitting field for $X^3+1=(X+1)(X^2+4X+1)$ over $\mathbb{F}$. If α is one of the roots of (X^2+4X+1) the other is $\beta=1-\alpha$ and, according to Proposition 3.2 the idempotents of $\mathbb{K}^tA_0$, which are also the idempotents of $\mathbb{K}^tA$, are:

$$\begin{aligned}
e_{-1} &= 2\,(\overline{1}-\overline{z}+\overline{z^2}),\\
e_{\alpha} &= 2\,(\overline{1}+(1+\alpha)\overline{z}-\alpha\overline{z^2}),\\
e_{1-\alpha} &= 2\,(\overline{1}+\alpha\overline{z}+(1-\alpha)\overline{z^2}).
\end{aligned}$$

Computing the stabilizers we get $St(-1)=\mathcal{G}$, $St(\alpha)=\{id\}=St(1+\alpha)$. Then, the central primitive idempotents of $\mathbb{F}^tA$:

$$\widetilde{e_{-1}}=2\,(\overline{1}-\overline{z}+\overline{z^2}),$$

and

$$\begin{aligned}
\widetilde{e_{\alpha}} &= \frac{2}{|St(\alpha)|}\left(Tr_{\mathbb{K}/\mathbb{F}_5}(1)\overline{1}+Tr_{\mathbb{K}/\mathbb{F}_5}(1+\alpha)\overline{z}-Tr_{\mathbb{K}/\mathbb{F}_5}(\alpha)\overline{z^2}\right)\\
&= 2\left(2\overline{1}+(1-\alpha+\alpha)\overline{z}-(\alpha+1-\alpha)\overline{z^2}\right)\\
&= -\overline{1}+2\overline{z}+3\overline{z^2}.
\end{aligned}$$

Finally, the simple components of the center are

$$\mathbb{F}_5^{t_{-1}}\langle z\rangle\widetilde{e_{-1}}\cong\mathbb{F}_5 \quad\text{and}\quad \mathbb{F}_5^{t_{-1}}\langle z\rangle\widetilde{e_{\alpha}}\cong\mathbb{F}_{25}.$$

Since $[A:A_0]=4$, the simple components of $\mathbb{F}_5^tA$ are:

$$\mathbb{F}_5^tA\widetilde{e_{-1}}\cong M_2(\mathbb{F}_5) \quad\text{and}\quad \mathbb{F}_5^tA\widetilde{e_{\alpha}}\cong M_2(\mathbb{F}_{25}).$$

Data availability

No data was used for the research described in the article.

References

[1] J. De La Cruz, R. Villanueva-Polanco, Public key cryptography based on twisted dihedral group algebras, Adv. Math. Commun., https://doi.org/10.3934/amc.2022031.

[2] J. De La Cruz, W. Willems, Twisted group codes, IEEE Trans. Inf. Theory 67 (8) (2021) 5178–5184.

[3] S.T. Dougherty, S. Şahinkaya, B. Yıldız, Skew G-codes, J. Algebra Appl. 22 (02) (2023) 2350056.

[4] P. Grover, A.K. Bhandari, Explicit determination of certain minimal constabelian codes, Finite Fields Appl. 18 (2012) 1037–1060.

[5] N. Jacobson, Lectures in Abstract Algebra, vol. III, Van Nostrand, New York, 1964 (there exists a recent edition by Springer-Verlag, New York, 1975).

[6] Y. Jia, On quasi-twisted codes over finite fields, Finite Fields Appl. 18 (2012) 237–257.

[7] G. Karpilovsky, Group Representations, vol. 3, North-Holland, Amsterdam, 1993.

[8] T.Zh. Mollov, Minimal idempotents of twisted group algebras of cyclic 2-groups, Southeast Asian Bull. Math. 26 (2002) 593–601.

[9] D.S. Passman, On the semisimplicity of twisted group algebras, Proc. Am. Math. Soc. 25 (1970) 161–166.

[10] D.S. Passman, Radicals of twisted group rings, Proc. Lond. Math. Soc. 20 (1970) 409–437.

[11] D.S. Passman, Infinite Crossed Products, Academic Press, Boston, 1989.

[12] C. Polcino Milies, S.K. Sehagal, An Introduction to Group Rings, Kluwer, Dordrecht, 2002.

[13] W.R. Reynolds, Projective representations of finite groups, Proc. Ill. J. Math. 9 (1965) 191–198.

[14] W.R. Reynolds, Twisted group algebras over arbitrary fields, Ill. J. Math. 15 (1971) 91–103.

[15] I. Schur, Uber die Darstellung der endlicher Gruppen durch gebrochene lineare Substitutionen, J. Math. 127 (1904) 20–40.

[16] I. Schur, Untersuchungen uber die Darstellung der endlicher Gruppen durch gebrochene lineare Substitutionen, J. Math. 132 (1907) 85–137.

[17] I. Schur, Uber die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen, J. Math. 139 (1911) 155–250.

[18] M. Shi, Y. Zhang, Quasi-twisted codes with constacyclic constituent codes, Finite Fields Appl. 39 (2016) 159–178.

[19] R. Wu, M. Shi, A modified Gilbert-Varshamov bound for self-dual quasi-twisted codes of index four, Finite Fields Appl. 62 (2020) 101627.

[20] A.J. van Zanten, Primitive idempotent tables and constacyclic codes, Des. Codes Cryptogr. 87 (2019) 1199–1225.