International Electronic Journal of Algebra
Published Online: December 4, 2024
DOI: 10.24330/ieja.1596075

GROUP STRUCTURES OF TWISTULANT MATRICES OVER RINGS

Horacio Tapia-Recillas and J. Armando Velazco-Velazco

Received: 20 April 2024; Revised: 29 July 2024; Accepted 15 September 2024
Communicated by Abdullah Harmancı

Abstract. In this work the algebraic structures of twistulant matrices defined over a ring are studied, with particular attention on their multiplicative structure. It is determined these matrices over a ring are an abelian group and when they are defined over a field the diagonalization of such matrices is considered.

Mathematics Subject Classification (2020): 15B33, 15A20, 15A30
Keywords: Twistulant matrix, discrete Fourier transform, finite field

1. Introduction

Circulant matrices ([4]) have received considerable attention of several research groups for their own right and for their potential applications including image processing, communications, network systems, signal processing, coding theory and cryptography ([8],[9]).

Twistulant matrices were introduced as a generalization of circulant matrices, and algebraic structures of these matrices over the complex numbers have been determined ([6]).

In this note, following [6] right (left) β-twistulant matrices over a ring are introduced and focus on given group structures of these matrices. The manuscript is organized as follows: in Section 2 the definition of right (left) β-twistulant matrices and basic results are given. Section 3 is devoted to the group structure of subsets of the introduced matrices. In [6] the mentioned matrices are defined over the complex numbers, $\mathbb{C}$, but in our case the results are presented over any commutative ring $\mathcal{R}$. Later, in Section 4, the ring $\mathcal{R}$ will be taken to be a field with particular properties,

The first author was partially supported by Sistema Nacional de Investigadoras e Investigadores (SNII), México, Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT) and the second author was partially supported by the fellowship number 764803 from Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT), México.

placing special emphasis on the case of a finite field. In Section 5 several examples are presented illustrating the main results. Final comments are given in Section 6.

2. Twistulant matrices

Let $\mathcal{R}$ be a commutative ring and $\mathcal{R}^n$ be the cartesian product for $n > 1$. Let $\sigma : \mathcal{R}^n \longrightarrow \mathcal{R}^n$ be the permutation $\sigma(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}, a_0, \ldots, a_{n-2})$. Observe that $\sigma^n = I$, where σ is applied n times and I is the identity permutation, from which it follows that $\tau := \sigma^{-1} = \sigma^{n-1}$ is the permutation on $\mathcal{R}^n$ given by $\tau(a_0, a_1, \ldots, a_{n-1}) = (a_1, a_2, \ldots, a_0)$. For an element $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n$ consider the matrix

$$\mathrm{circ}_\sigma(\mathbf{a}) = (\mathbf{a}, \sigma(\mathbf{a}), \ldots, \sigma^{n-1}(\mathbf{a}))^t,$$

where $(X)^t$ denotes the transpose matrix of X. This matrix is called the *right-circulant* matrix. Similarly the matrix

$$\mathrm{circ}_\tau(\mathbf{a}) = (\mathbf{a}, \tau(\mathbf{a}), \ldots, \tau^{n-1}(\mathbf{a}))^t,$$

is called the *left-circulant* matrix.

Now we introduce the β-twistulant matrices. Let $\beta \in \mathcal{R} \setminus \{0\}$ and consider the following map on $\mathcal{R}^n$, $\sigma_\beta : \mathcal{R}^n \longrightarrow \mathcal{R}^n$ defined by $\sigma_\beta(a_0, a_1, \ldots, a_{n-1}) = (\beta a_{n-1}, a_0, \ldots, a_{n-2})$. It is readily seen that this map is a permutation on $\mathcal{R}^n$.

Observe that the map $\sigma_\beta : \mathcal{R}^n \longrightarrow \mathcal{R}^n$ can also be defined, by

$$\sigma_\beta(\mathbf{a}) = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ \beta & 0 & 0 & \ldots & 0 \end{pmatrix} = \mathbf{a}J_\beta.$$

Let $\mathcal{M}_n(\mathcal{R})$ be the set of square matrices over $\mathcal{R}$. We define the map $\mathrm{rcirc}_\beta : \mathcal{R}^n \longrightarrow \mathcal{M}_n(\mathcal{R})$ by

$$\mathrm{rcirc}_\beta(\mathbf{a}) = \begin{pmatrix} \mathbf{a} & \mathbf{a}J_\beta & \ldots & \mathbf{a}J_\beta^{n-1} \end{pmatrix}^t,$$

where $(*)^t$ indicates the matrix operation transpose and $\mathbf{a}J_\beta^j = (\mathbf{a}J_\beta^{j-1})J_\beta$ for $j = 1, \ldots, n-1$ with the convention $\mathbf{a}J_\beta^0 = \mathbf{a}$. By definition rcirc_β is $\mathcal{R}$-linear. Notice $\ker(\mathrm{rcirc}_\beta) = \{\mathbf{0}\}$ for all $\beta \in \mathcal{R} \setminus \{0\}$. The set of right β-twistulant matrices of order n is defined as $\mathrm{RC}_{n,\beta}(\mathcal{R}) = \{\mathrm{rcirc}_\beta(\mathbf{a}) \mid \mathbf{a} \in \mathcal{R}^n\}$.

The set of left β-twistulant matrices is defined in a similar way.

Example 2.1. Let $\mathcal{R}$ be a commutative ring, $\mathbf{a} = (a_0, a_1, a_2, a_3) \in \mathcal{R}^4$ and $\beta \in \mathcal{R} \setminus \{0\}$. Then

$$\mathrm{rcirc}_\beta(\mathbf{a}) = \begin{pmatrix} \mathbf{a} \\ \mathbf{a}J_\beta \\ \mathbf{a}J_\beta^2 \\ \mathbf{a}J_\beta^3 \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ \beta a_3 & a_0 & a_1 & a_2 \\ \beta a_2 & \beta a_3 & a_0 & a_1 \\ \beta a_1 & \beta a_2 & \beta a_3 & a_0 \end{pmatrix}.$$

An example of a left β-twistulant matrix can be given likewise.

Notice that a circulant (and negacirculant) matrix is a special case of a β-twistulant matrix when $\beta \in \{1, -1\}$. Furthermore, the β-twistulant matrices are a subclass of the so-called vector-circulant matrices ([7]).

Let

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \dots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix} \in \mathcal{M}_n(\mathcal{R}).$$

Recall that the anti-diagonal of A is given by the elements $a_{1,n}, a_{2,n-1}, \dots, a_{n-1,2}, a_{n,1}$. The transpose of A with respect to its anti-diagonal, denoted by A^τ, is defined as,

$$A^\tau = \begin{pmatrix} a_{n,n} & a_{n-1,n} & \dots & a_{1,n} \\ a_{n,n-1} & a_{n-1,n-1} & \dots & a_{1,n-1} \\ \vdots & \vdots & \dots & \vdots \\ a_{n,1} & a_{n-1,1} & \dots & a_{1,1} \end{pmatrix}.$$

Example 2.2. Let $\mathcal{R} = \mathbb{Z}_9$ and $A \in \mathcal{M}_3(\mathcal{R})$ given by

$$A = \begin{pmatrix} 1 & 0 & 8 \\ 2 & 3 & 5 \\ 0 & 6 & 4 \end{pmatrix} \text{ then } A^\tau = \begin{pmatrix} 4 & 5 & 8 \\ 6 & 3 & 0 \\ 0 & 2 & 1 \end{pmatrix}.$$

We have the usual properties $(A^\tau)^\tau = A$ and $(A+B)^\tau = A^\tau + B^\tau$ for $A, B \in \mathcal{M}_n(\mathcal{R})$. The definition can be extended to $\begin{pmatrix} r_0 & r_1 & \dots & r_{n-1} \end{pmatrix} \in \mathcal{M}_{1\times n}(\mathcal{R})$ by

$$\begin{pmatrix} r_0 & r_1 & \dots & r_{n-1} \end{pmatrix}^\tau = \begin{pmatrix} r_{n-1} \\ \vdots \\ r_1 \\ r_0 \end{pmatrix} \in \mathcal{M}_{n\times 1}(\mathcal{R}).$$

Remark 2.3. We observe, by construction that, $J_\beta^\tau = J_\beta$, in other words J_β is symmetric with respect to this transpose operation.

Let $\mathcal{R}$ be any commutative ring, consider the ring $\mathcal{R}_{n,\beta} = \mathcal{R}[x]/\langle x^n - \beta\rangle$ and define the polynomial representation map of $\mathcal{R}^n$ as follows,

$$\mathcal{P}_\beta : \mathcal{R}^n \longrightarrow \mathcal{R}_{n,\beta},\ \mathcal{P}_\beta(\mathbf{a}) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.$$

It is easily seen that the map $\mathcal{P}_\beta$ is an isomorphism of $\mathcal{R}$-modules. Further, applying the permutation σ_β introduced above to an element of $\mathcal{R}^n$, it has the same effect as multiplying by x the corresponding polynomial. In the study of constacyclic codes this mapping is vital when β is a unit of the ring.

We recall the following ([1],[3]). Let $\mathcal{R}$ be a commutative ring. A linear code of length n over $\mathcal{R}$ is just an $\mathcal{R}$-submodule of $\mathcal{R}^n$. For β a unit of the ring $\mathcal{R}$, a linear code $\mathcal{C}$ over $\mathcal{R}$ is β-constacyclic if for any $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, $\sigma_\beta(\mathbf{c}) = (\beta c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. Thus the concepts of a β-twistulant matrix and β-constacyclic code are related objects.

It is worth mentioning that the concept of β-constacyclic codes is related to the ring $\mathcal{R}_{n,\beta}$, as shown by the following result ([1]).

Proposition 2.4. *Let β be a unit of the ring $\mathcal{R}$. Then a linear code over $\mathcal{R}$ is β-constacyclic if and only if its image under the map $\mathcal{P}_\beta$ is an ideal of the ring $\mathcal{R}_{n,\beta}$.*

Let $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n$, then $\mathbf{a} = \sum_{i=1}^n a_{i-1}\mathbf{e}_i$. It is clear that $\mathrm{rcirc}_\beta(\mathbf{a}) = \sum_{i=1}^n a_{i-1}\,\mathrm{rcirc}_\beta(\mathbf{e}_i)$, where $\{\mathbf{e}_i \mid i = 1, 2, \ldots, n\}$ is the set of canonical generators of $\mathcal{R}^n$.

Proposition 2.5. *Let $\mathcal{R}$ be any commutative ring and $\beta \in \mathcal{R}$.*

- *Let $A \in \mathcal{M}_n(\mathcal{R})$ with rows $A_1, A_2, \ldots, A_n$. Then*

$$AJ_\beta = \begin{pmatrix} A_1 J_\beta & A_2 J_\beta & \ldots & A_n J_\beta \end{pmatrix}^t.$$

- $\mathrm{rcirc}_\beta(\mathbf{e}_1) = I_n$, *where I_n is the identity matrix of order n in $\mathcal{M}_n(\mathcal{R})$.*
- $\mathrm{rcirc}_\beta(\mathbf{e}_{j+1}) = J_\beta^j$, *$j = 1, \ldots, n-1$.*
- $\mathbf{e_j} = \mathbf{e}_1 J_\beta^{j-1}$.

Proof. The first claim follows from the definitions. For the second and third claims, it is enough to notice $\mathbf{e}_j J_\beta = \mathbf{e}_{j+1}$ for $i = 1, \ldots, n-1$ while $e_n J_\beta = \beta\mathbf{e}_1$. As a consequence, $\mathbf{e}_{i+1} = \mathbf{e}_1 J_\beta^i$, $i = 1, \ldots, n-1$ and hence $\mathbf{e}_j J_\beta = \mathbf{e}_1 J_\beta^j$, $j = 1, \ldots, n-1$.

With these facts,

$$J_\beta = \begin{pmatrix} \mathbf{e}_2 \\ \mathbf{e}_3 \\ \vdots \\ \mathbf{e}_n \\ \beta\mathbf{e}_1 \end{pmatrix} = \mathrm{rcirc}_\beta(\mathbf{e}_2) = \begin{pmatrix} \mathbf{e}_1 J_\beta \\ \mathbf{e}_2 J_\beta \\ \vdots \\ \mathbf{e}_{n-1} J_\beta \\ \mathbf{e}_n J_\beta \end{pmatrix}.$$

From the first claim,

$$J_\beta^j = \begin{pmatrix} \mathbf{e}_1 J_\beta^j \\ \mathbf{e}_2 J_\beta^j \\ \vdots \\ \mathbf{e}_{n-1} J_\beta^j \\ \mathbf{e}_n J_\beta^j \end{pmatrix} = \mathrm{rcirc}_\beta(\mathbf{e}_1 J_\beta^j) = \mathrm{rcirc}_\beta(\mathbf{e}_{j+1}),$$

for $j = 1, 2, \ldots, n-1$. □

Corollary 2.6. *With the same hypothesis as in Proposition 2.5,*

$$\mathrm{rcirc}_\beta(\mathbf{e}_n J_\beta) = J_\beta^n = \beta I_n.$$

As consequence, if $\beta \in \mathcal{U}(\mathcal{R})$ is a unit of finite multiplicative order, $o(\beta)$, $J_\beta^{o(\beta)n} = I_n$. A similar consequence arises if the ring $\mathcal{R}$ is such that β is a non-unit with finite nilpotency index.

Proof. Since $J_\beta^n = J_\beta^{n-1} J_\beta = \mathrm{rcirc}_\beta(\mathbf{e}_n) J_\beta = \mathrm{rcirc}_\beta(\mathbf{e}_n J_\beta) = \mathrm{rcirc}_\beta(\beta\mathbf{e}_1) = \beta I_n$, it is clear by Proposition 2.5. □

Now we define the following subsets of the $\mathcal{R}$-algebra $\mathcal{M}_n(\mathcal{R})$ of $n \times n$ matrices over the commutative ring $\mathcal{R}$.

$\mathrm{RC}_{n,\beta}(\mathcal{R}) = \{\mathrm{rcirc}_\beta(\mathbf{a}) : \mathbf{a} \in \mathcal{R}^n\}$, $\overline{\mathrm{RC}}_{n,\beta}(\mathcal{R}) = \{A \in \mathrm{RC}_{n,\beta}(\mathcal{R}) : \det(A) \text{ is a unit}\}$.

3. Structure of β-twistulant matrices

By the $\mathcal{R}$-linearity of the homomorphism rcirc_β, $\mathrm{RC}_{n,\beta}(\mathcal{R})$ is generated as an $\mathcal{R}$ module by the set

$\{\mathrm{rcirc}_\beta(\mathbf{e}_1), \mathrm{rcirc}_\beta(\mathbf{e}_2), \ldots, \mathrm{rcirc}_\beta(\mathbf{e}_n)\}$. Indeed, given $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) = a_0\mathbf{e}_1 + a_1\mathbf{e}_2 + \ldots + a_{n-1}\mathbf{e}_n$, then

$$\mathrm{rcirc}_\beta(\mathbf{a}) = a_0\,\mathrm{rcirc}_\beta(\mathbf{e}_1) + a_1\,\mathrm{rcirc}_\beta(\mathbf{e}_2) + \ldots + a_{n-1}\,\mathrm{rcirc}_\beta(\mathbf{e}_n).$$

From Proposition 2.5 we have,

Proposition 3.1. *Given $\beta \in \mathcal{R}$, the $\mathcal{R}$-module* $\mathrm{RC}_{n,\beta}$ *is generated by*

$$\mathcal{A} = \{I_n, J_\beta, \ldots, J_\beta^{n-1} \;:\; J_\beta^n = \beta I_n\},$$

i.e., given $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n$,

$$\mathrm{rcirc}_\beta(\mathbf{a}) = a_0 I_n + a_1 J_\beta + \cdots + a_{n-1} J_\beta^{n-1}.$$

We know from Remark 2.3 that the matrix J_β is symmetric under the transpose with respect to its antidiagonal. The following is a direct consequence from this fact.

Corollary 3.2. *Let $\mathcal{R}$ be a commutative ring with identity. Given* $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n$, *then* $\mathrm{rcirc}_\beta(\mathbf{a})^\tau = \mathrm{rcirc}_\beta(\mathbf{a})$.

Proposition 3.3. *Let $\beta \in \mathcal{R}$. Then* $(\mathrm{RC}_{n,\beta}(\mathcal{R}), +, \times, \cdot)$ *is a finitely generated commutative $\mathcal{R}$-algebra.*

Proof. It is clear that $(\mathrm{RC}_{n,\beta}(\mathcal{R}), +)$ is an $\mathcal{R}$-module. From Proposition 3.1, $(\mathrm{RC}_{n,\beta}(\mathcal{R}), +, \times, \cdot)$ is closed under the operation multiplication of matrices, $\times$, as from Corollary 2.6, given $r, s \in \mathcal{R}$,

$$rJ_\beta^i sJ_\beta^j = rsJ_\beta^{i+j} = rsJ_\beta^{tn+k} = \beta^a J_\beta^k \text{ for some integer } a \text{ and } 0 \le k \le n-1.$$

Next we prove that given $\mathbf{a}, \mathbf{b} \in \mathcal{R}^n$, $\mathrm{rcirc}_\beta(\mathbf{a})\,\mathrm{rcirc}_\beta(\mathbf{b}) = \mathrm{rcirc}_\beta(\mathbf{b})\,\mathrm{rcirc}_\beta(\mathbf{a})$, that is clear by Proposition 2.5: $\mathrm{rcirc}_\beta(\mathbf{e}_{i+1})\,\mathrm{rcirc}_\beta(\mathbf{e}_{j+1}) = J_\beta^i J_\beta^j = J_\beta^{i+j}$. □

Now we establish the following,

Theorem 3.4. *If* $\mathrm{rcirc}_\beta(\mathbf{a}) \in \mathrm{RC}_{n,\beta}(\mathcal{R})$ *is invertible, then* $\mathrm{rcirc}_\beta(\mathbf{a})^{-1} \in \mathrm{RC}_{n,\beta}(\mathcal{R})$. *In other words, the set of invertible elements* $\overline{\mathrm{RC}}_{n,\beta}(\mathcal{R})$ *is an abelian group.*

Proof. Let $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n$ be such that $\mathrm{rcirc}_\beta(\mathbf{a}) \in \mathrm{RC}_{n,\beta}(\mathcal{R})$ is invertible. Let $A = \mathrm{rcirc}_\beta(\mathbf{a})^{-1}$ with rows $A_1, A_2, \ldots, A_n$. From Proposition 3.1, $\mathrm{rcirc}_\beta(\mathbf{a}) = a_0 I_n + a_1 J_\beta + \ldots + a_{n-1} J_\beta^{n-1}$ and

$$A\,\mathrm{rcirc}_\beta(\mathbf{a}) = a_0 A + a_1 A J_\beta + \ldots + a_{n-1} A J_\beta^{n-1} = I_n = \mathrm{rcirc}_\beta(\mathbf{e}_1).$$

From Proposition 2.5,

$$a_0 A_1 + a_1 A_1 J_\beta + \ldots + a_{n-1} A_1 J_\beta^{n-1} = \begin{pmatrix} 1 & 0 & \ldots & 0 \end{pmatrix} = \mathbf{e}_1,$$

hence,

$$a_0 A_1 J_\beta^{j-1} + a_1 (A_1 J_\beta) J_\beta^{j-1} + \cdots + a_{n-1} (A_1 J_\beta^{n-1}) J_\beta^{j-1} = e_j = e_1 J_\beta^{j-1}.$$

Then in matrix notation,

$$a_0 \begin{pmatrix} A_1 \\ A_1 J_\beta \\ \vdots \\ A_1 J_\beta^{n-1} \end{pmatrix} + a_1 \begin{pmatrix} A_1 \\ A_1 J_\beta \\ \vdots \\ A_1 J_\beta^{n-1} \end{pmatrix} J_\beta + \cdots + a_{n-1} \begin{pmatrix} A_1 \\ A_1 J_\beta \\ \vdots \\ A_1 J_\beta^{n-1} \end{pmatrix} J_\beta^{n-1} = I_n,$$

hence,

$$\begin{pmatrix} A_1 \\ A_1 J_\beta \\ \vdots \\ A_1 J_\beta^{n-1} \end{pmatrix} \mathrm{rcirc}_\beta(\mathbf{a}) = I_n,$$

i.e., $A^{-1} = \mathrm{rcirc}_\beta(A_1)$ which implies that $\mathrm{rcirc}_\beta(\mathbf{a})^{-1} \in \mathrm{RC}_{n,\beta}(\mathcal{R})$. □

It is worth mentioning that β could be a non-unit in the ring $\mathcal{R}$ and $\mathrm{rcirc}_\beta(\mathbf{r})$ still be invertible as shown in the following example:

Example 3.5. Let $\mathcal{R} = \mathbb{Z}_4$, $\beta = 2 \in \mathcal{R}$ and let $\mathbf{a} = (1, 1, 0) \in \mathcal{R}^3$. Then

$$J_\beta = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix} \text{ and } \mathrm{rcirc}_\beta(\mathbf{a}) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 2 & 0 & 1 \end{pmatrix},$$

obtaining $\det(\mathrm{rcirc}_\beta(\mathbf{a})) = 3 \in \mathcal{U}(\mathcal{R})$ and therefore $\mathrm{rcirc}_\beta(\mathbf{a})$ is invertible. In fact

$$\mathrm{rcirc}_\beta(\mathbf{a})^{-1} = \begin{pmatrix} 3 & 1 & 3 \\ 2 & 3 & 1 \\ 2 & 2 & 3 \end{pmatrix}.$$

Observe that if the first row of the matrix $\mathrm{rcirc}_\beta(\mathbf{a})^{-1}$ is known, the matrix can be obtained with the method described in the proof of Theorem 3.4.

4. Twistulant matrices over fields

Now assume the ring $\mathcal{R}$ is a field. In the following lines by using a method based on the discrete Fourier transform (DFT) it will be seen that Proposition 3.3 and Theorem 3.4 also hold.

In the case where the field is $\mathbb{C}$, the field of complex numbers, following section 3.2 of [4] we recall the special case in which $\beta = 1$. In this case the circulant matrices are diagonalizable over $\mathbb{C}$ via the discrete Fourier transform matrix F.

Recall (see [5], [2]) that over $\mathbb{C}$, the Discrete Fourier Transform matrix is,

$$F = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{pmatrix}$$

where ω is a primitive n^{th}-root of unity and $\frac{1}{\sqrt{n}}$ is a normalization factor. Notice F is a Vandermonde type of matrix, and therefore, invertible. These considerations can be extended to circulant matrices over a finite field $\mathbb{F}_q$ (see [10] for instance) provided there is an n^{th}-root of unity $\omega \in \mathbb{F}_q$. For our discussion, the constant $\frac{1}{\sqrt{n}}$ is not relevant and it is omitted.

Theorem 4.1. *Let $\mathbb{F}$ be a field containing an n^{th}-root of unity, $\omega \in \mathbb{F}$, and let*

$$J = \begin{pmatrix} \mathbf{e}_2 \\ \mathbf{e}_3 \\ \vdots \\ \mathbf{e}_1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{F}).$$

Then J is diagonalizable by the Discrete Fourier Transform matrix F, indeed

$$F^{-1}JF = \operatorname{diag}(1, \omega, \omega^2, \dots, \omega^{n-1}) = D_\omega.$$

Proof. The claim follows from

$$JF = \begin{pmatrix} 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix} = FD_\omega.$$

□

Corollary 4.2. *Circulant matrices in $\mathcal{M}_n(\mathbb{F})$ are diagonalizable over any field $\mathbb{F}$ that contains an n^{th}-root of unity.*

Proof. Given $F^{-1}JF = \operatorname{diag}(1, \omega, \omega^2, \dots, \omega^{n-1}) = D_\omega$, from Proposition 3.1 with $\beta = 1$, for $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}^n$,

$$F^{-1} \operatorname{rcirc}(\mathbf{a}) F = a_0 I_n + a_1 D_\omega + \ldots + a_{n-1} D_\omega^{n-1}$$

which is a diagonal matrix. □

Example 4.3. Over the field $\mathbb{F}_{19}$, in $\mathcal{M}_6(\mathbb{F}_{19})$ the matrix

$$J = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

is diagonalizable by means of the discrete Fourier transform matrix

$$F = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 8 & 7 & 18 & 11 & 12 \\ 1 & 7 & 11 & 1 & 7 & 11 \\ 1 & 18 & 1 & 18 & 1 & 18 \\ 1 & 11 & 7 & 1 & 11 & 7 \\ 1 & 12 & 11 & 18 & 7 & 8 \end{pmatrix} \text{whose inverse is } F^{-1} = \begin{pmatrix} 16 & 16 & 16 & 16 & 16 & 16 \\ 16 & 2 & 5 & 3 & 17 & 14 \\ 16 & 5 & 17 & 16 & 5 & 17 \\ 16 & 3 & 16 & 3 & 16 & 3 \\ 16 & 17 & 5 & 16 & 17 & 5 \\ 16 & 14 & 17 & 3 & 5 & 2 \end{pmatrix},$$

such that, $F^{-1}JF = \mathrm{diag}(1, 8, 7, 18, 11, 12)$.

Let n be a positive integer, $\mathbb{F}_q$ a finite field with $q = p^m$ elements and $\beta \in \mathbb{F}_q$ be such that an n^{th}-root of this element is in the field $\mathbb{F}_q$. In case this does not happen, the splitting field of the polynomial $x^n - \beta$ is considered. The splitting field is of finite order n over the base field $\mathbb{F}_q$ and it has $|\mathbb{F}_q|^n$ elements. So we can assume the field we are working on contains an n^{th}-root of the element β.

Suppose $\beta \in \mathbb{F}$ is such that there exist $\lambda_1 = \beta^{\frac{1}{n}} \in \mathbb{F}$. Define $\lambda_k = \beta^{\frac{k}{n}}$, $k = 2, \dots, n-1$ and let $\omega \in \mathbb{F}$ be an n$^{\mathrm{th}}$-root of unity. Let $\mathcal{F} \in \mathcal{M}_n(\mathbb{F})$ be defined by

$$\mathcal{F} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_1\omega & \lambda_1\omega^2 & \dots & \lambda_1\omega^{n-1} \\ \lambda_2 & \lambda_2\omega^2 & \lambda_2\omega^4 & \dots & \lambda_2\omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ \lambda_{n-1} & \lambda_{n-1}\omega^{n-1} & \lambda_{n-1}\omega^{2(n-1)} & \dots & \lambda_{n-1}\omega^{(n-1)(n-1)} \end{pmatrix}. \qquad (*)$$

Lemma 4.4. *The matrix $\mathcal{F} \in \mathcal{M}_n(\mathbb{F})$ is non-singular and hence invertible. Furthermore,*

$$\mathcal{F}^{-1} = F^{-1} D_{\lambda^{-1}}$$

where $D_\lambda = \mathrm{diag}(1, \lambda_1, \lambda_2, \ldots, \lambda_{n-1})$ *and, for* ω *an* n^{th}*-root of unity in* $\mathbb{F}$,

$$F = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \ldots & \omega^{(n-1)(n-1)} \end{pmatrix}.$$

Proof. Let $D_\lambda = \mathrm{diag}(1, \lambda_1, \lambda_2, \ldots, \lambda_{n-1})$. The claim follows from the fact that $\mathcal{F} = D_\lambda F$, and then $\det(\mathcal{F}) = \det(D_\lambda F)$. As F is a Vandermonde type of matrix, it is non-singular over any field containing an n-th root of unity, and therefore invertible. Now $\mathcal{F}^{-1} = (D_\lambda F)^{-1} = F^{-1} D_\lambda^{-1} = F^{-1} D_{\lambda^{-1}}$, where $D_{\lambda^{-1}} = \mathrm{diag}(1, \lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_{n-1}^{-1})$. □

Theorem 4.5. *Let* $\beta \in \mathbb{F}$ *and* $\mathcal{F}$ *be as above and assume there is* $\lambda_1 = \beta^{\frac{1}{n}} \in \mathbb{F}$. *Let*

$$J_\beta = \begin{pmatrix} \mathbf{e}_2 \\ \mathbf{e}_3 \\ \vdots \\ \beta \mathbf{e}_1 \end{pmatrix} \in \mathcal{M}_n(\mathbb{F}),$$

and suppose $\omega \in \mathbb{F}$ *is an* n^{th}*-root of unity. Then,* J_β *is diagonalizable by* $\mathcal{F}$ *and*

$$\mathcal{F}^{-1} J_\beta \mathcal{F} = \lambda_1 D_\omega.$$

Proof. It is enough to notice

$$J_\beta \mathcal{F} = \begin{pmatrix} \lambda_1 & \lambda_1\omega & \lambda_1\omega^2 & \ldots & \lambda_1\omega^{n-1} \\ \lambda_2 & \lambda_2\omega^2 & \lambda_2\omega^4 & \ldots & \lambda_2\omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ \lambda_{n-1} & \lambda_{n-1}\omega^{n-1} & \lambda_{n-1}\omega^{2(n-1)} & \ldots & \lambda_{n-1}\omega^{(n-1)(n-1)} \\ \beta & \beta & \beta & \ldots & \beta \end{pmatrix} = \mathcal{F}\lambda_1 D_\omega,$$

computation that follows easily from the fact that multiplying the square matrix $\mathcal{F}$ (see $(*)$) on the right by the diagonal matrix $\lambda_1 D_\omega = (\lambda_1, \lambda_1\omega, \ldots, \lambda_1\omega^{n-1})$ is equivalent to multiplying each column of $\mathcal{F}$ by the i-th element of the diagonal and observing that $\lambda_{n-1}\lambda_1 = \beta^{\frac{n-1}{n}}\beta^{\frac{1}{n}} = \beta$. □

Corollary 4.6. *Let* $\mathbb{F}$ *be a field with an* n^{th}*-root of unity and let* $0 \neq \beta \in \mathbb{F}$. *Assume there is* $\lambda_1 = \beta^{\frac{1}{n}} \in \mathbb{F}$. *Then,*

(1) *The matrix* $\mathrm{rcirc}_\beta(\mathbf{a}) \in \mathcal{M}_n(\mathbb{F})$ *is diagonalizable over the field* $\mathbb{F}$.

(2) *For any* $A, B \in \mathrm{RC}_{n,\beta}(\mathbb{F})$, $AB \in \mathrm{RC}_{n,\beta}(\mathbb{F})$ *and* $AB = BA$.

(3) *If* $\mathrm{rcirc}_\beta(\mathbf{a}) \in \mathrm{RC}_{n,\beta}(\mathbb{F})$, $\mathrm{rcirc}_\beta(\mathbf{a})^{-1} \in \mathrm{RC}_{n,\beta}(\mathbb{F})$. *Further,*

$$\mathrm{rcirc}_\beta(\mathbf{a})^{-1} = \mathcal{F}(a_0 I_n + a_1\lambda_1 D_\omega + \ldots a_{n-1}\lambda_1^{n-1} D_\omega^{n-1})^{-1}\mathcal{F}^{-1}.$$

Note that $a_0 I_n + a_1\lambda_1 D_\omega + \ldots + a_{n-1}\lambda_1^{n-1} D_{\omega^{n-1}}$ is a diagonal matrix and hence easily invertible in a field. It can be seen that each element of the diagonal is the evaluation of $f(X) = a_0 + a_1\lambda_1 X + a_2\lambda_1^2 X^2 + \ldots + a_{n-1}\lambda_1^{n-1}X^{n-1}$ at ω^i for $i = 0, 1, \ldots, n-1$. In other words, the diagonal elements are the values of the discrete Fourier transform of the vector $(a_0, a_1\lambda_1, \ldots, a_{n-1}\lambda_1^{n-1})$.

Corollary 4.7. *With the same hypothesis as in the previous corollary, assume* $J_\beta \in \mathcal{M}_n(\mathbb{F})$ *is diagonalizable. Then given* $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$,

$$\det[\mathrm{rcirc}_\beta(\mathbf{a})] = \det(a_0 I_n + a_1\lambda_1 D_\omega + \ldots + a_{n-1}\lambda_1^{n-1} D_{\omega^{n-1}}).$$

5. Examples

In this section several examples are provided illustrating the main results. The software SageMath ([11]) has been used for computations.

Example 5.1. Let $\beta = 12$ and consider the 3^{th}-root of the unity $\omega = 7 \in \mathbb{F}_{19}$. If $\lambda_1 = \beta^{\frac{1}{3}} = 10$, then

$$\mathcal{F}^{-1} J_\beta \mathcal{F} = \begin{pmatrix} 10 & 0 & 0 \\ 0 & 13 & 0 \\ 0 & 0 & 15 \end{pmatrix},$$

where

$$\mathcal{F} = \begin{pmatrix} 1 & 1 & 1 \\ 10 & 13 & 15 \\ 5 & 17 & 16 \end{pmatrix} \text{ and } \mathcal{F}^{-1} = \begin{pmatrix} 13 & 7 & 14 \\ 13 & 1 & 3 \\ 13 & 11 & 2 \end{pmatrix}.$$

Example 5.2. Consider the finite field $\mathbb{F}_{11}$, let $\beta = 10$ and $\omega = 9$ a 5^{th}-root of unity. Then $J_{10} \in \mathcal{M}_5(\mathbb{F}_{11})$ is diagonalizable. Let $\lambda_1 = 7$, then

$$\mathcal{F} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 7 & 8 & 6 & 10 & 2 \\ 5 & 9 & 3 & 1 & 4 \\ 2 & 6 & 7 & 10 & 8 \\ 3 & 4 & 9 & 1 & 5 \end{pmatrix} \text{ and } \mathcal{F}^{-1} = \begin{pmatrix} 9 & 6 & 4 & 10 & 3 \\ 9 & 8 & 1 & 7 & 5 \\ 9 & 7 & 3 & 6 & 1 \\ 9 & 2 & 9 & 2 & 9 \\ 9 & 10 & 5 & 8 & 4 \end{pmatrix}.$$

Thus $\mathcal{F}^{-1} J_{10} \mathcal{F} = 7D_9 = \mathrm{diag}(7, 8, 6, 10, 2)$. On the contrary, if $\beta = 6$, then $J_6 \in \mathcal{M}_5(\mathbb{F}_{11})$ is not diagonalizable since $\lambda^5 - 6 = 0$ has no solution in $\mathbb{F}_{11}$.

Example 5.3. Consider the field $\mathbb{F}_{11}$ and let $\mathbf{a} = (3,2,1,0,2) \in \mathbb{F}_{11}^5$. With the parameters given in the previous example, i.e., $\beta = 10, \omega = 9$ and $\lambda_1 = 7$,

$$\mathrm{rcirc}_{10}((a)) = \begin{pmatrix} 3 & 2 & 1 & 0 & 2 \\ 9 & 3 & 2 & 1 & 0 \\ 0 & 9 & 3 & 2 & 1 \\ 10 & 0 & 9 & 3 & 2 \\ 9 & 10 & 0 & 9 & 3 \end{pmatrix},$$

and from the Corollary 4.6

$$\mathrm{rcirc}_{10}(3,2,1,0,2)^{-1} = \mathcal{F}[3I_5 + 2(\lambda_1 D_9) + 1(\lambda_1 D_9)^2 + 0(\lambda_1 D_9)^3 + 2(\lambda_1 D_9)^4]^{-1}\mathcal{F}^{-1},$$

where $\mathcal{F}$ and $\mathcal{F}^{-1}$ are given in the mentioned example. Thus,

$$\mathrm{rcirc}_{10}(3,2,1,0,2)^{-1} = \begin{pmatrix} 9 & 2 & 2 & 4 & 9 \\ 2 & 9 & 2 & 2 & 4 \\ 7 & 2 & 9 & 2 & 2 \\ 9 & 7 & 2 & 9 & 2 \\ 9 & 9 & 7 & 2 & 9 \end{pmatrix}.$$

It can be seen that, for instance the third element in the diagonal matrix $\sum_{i=0}^4 a_i(\lambda_1 D_\omega)^i$ is, $f(\omega^2) = a_0 + a_1\lambda_1\omega^2 + a_2\lambda_1^2\omega^{2\cdot 2} + a_3\lambda_1^3\omega^{2\cdot 3} + a_4\lambda_1^4\omega^{2\cdot 4}$, i.e., $f(\omega^2) = 3+1+3+7 = 3$. In the same fashion it can be seen that $f(\omega^3) = 4$ and $f(\omega^4) = 10$, and also, from Corollary 4.7, $\det(\mathrm{rcirc}_{10}(\mathbf{a})) = 4 = \det(\mathrm{diag}(6,3,3,4,10))$.

Example 5.4. Consider the finite field $\mathbb{F}_9 = \mathbb{F}_3[X]/\langle X^2+2X+2\rangle$ with $3^2 = 9$ elements. Then $\mathbb{F}_9 = \{a_0 + a_1 x \mid a_0, a_1 \in \mathbb{F}_3, x^2+2x+2 = 0$. Let $\omega = 1 + x \in \mathbb{F}_9$ which is a 4^{th}-root of unity and let $\beta = 2$. Note that $\lambda_1 = 2^{\frac{1}{4}} = x \in \mathbb{F}_9$. Then,

$$J_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \end{pmatrix},$$

while

$$\mathcal{F} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ x & 1+2x & 2x & 2+x \\ 1+x & 2+2x & 1+x & 2+2x \\ 1+2x & x & 2+x & 2x \end{pmatrix} \text{ and } \mathcal{F}^{-1} = \begin{pmatrix} 1 & 2+x & 2+2x & 2x \\ 1 & 2x & 1+x & 2+x \\ 1 & 1+2x & 2+2x & x \\ 1 & x & 1+x & 1+2x \end{pmatrix}.$$

Then, $\mathcal{F}^{-1}J_\beta\mathcal{F} = \begin{pmatrix} x & 0 & 0 & 0 \\ 0 & 1+2x & 0 & 0 \\ 0 & 0 & 2x & 0 \\ 0 & 0 & 0 & 2+x \end{pmatrix}$.

6. Final comments

It is shown that twistulant matrices over a ring can be thought as elements of a finitely generated algebra, fact that is used to prove that the set of these matrices is closed under the usual multiplication, and that if a twistulant matrix is invertible its inverse is also twistulant. In the case where the ring is a field, particularly a finite field, it is shown that the twistulant matrices can be diagonalized by means of a Discrete Fourier Transform-type matrix. This fact is used to show that the group of twistulant matrices over a finite field is commutative with the usual matrix multiplication though this is a direct consequence from Proposition 3.3 and Theorem 3.4.

Acknowledgement. The authors extend heartfelt gratitude to the anonymous referee for his/her careful reading, valuable feedback and suggestions.

Disclosure statement. The authors report there are no competing interests to declare.

References

[1] N. Aydin, N. Connolly and M. Grassl, *Some results on the structure of constacyclic codes and new linear codes over* $GF(7)$ *from quasi-twisted codes*, Adv. Math. Commun., 11(1) (2017), 245-258.

[2] R. E. Blahut, Algebraic Codes on Lines, Planes and Curves: An Engineering Approach, Cambridge University Press, Cambridge, 2008.

[3] B. Chen, Y. Fan, L. Lin and H. Liu, *Constacyclic codes over finite fields*, Finite Fields Appl., 18(6) (2012), 1217-1231.

[4] P. J. Davis, Circulant Matrices, A Wiley-Interscience Publication, Pure and Applied Mathematics, John Wiley & Sons, New York-Chichester-Brisbane, 1979.

[5] *Discrete Fourier Transform*, (2024, February 15) in Wikipedia, https://en.wikipedia.org/wiki/DFT_matrix.

[6] S. Jitman, S. Ruangpum and T. Ruangtrakul, *Group structures of complex twistulant matrices*, AIP Conf. Proc., 1775 (2016), 030016 (8 pp).

[7] S. Jitman, *Vector-circulant matrices and vector-circulant based additive codes over finite fields*, Information, 8(3) (2017), 82 (7 pp).

[8] I. Kra and S. R. Simanca, *On circulant matrices*, Notices Amer. Math. Soc., 59(3) (2012), 368-377.

[9] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, New York: Elsevier/North Holland, 1977.

[10] H. Tapia-Recillas and J. A. Velazco-Velazco, *Diagonalización de matrices circulantes por medio de la Transformada Discreta de Fourier sobre campos finitos*, Rev. Met. de Mat., 13(1) (2022), 95-98.

[11] The Sage Developers, *SageMath, the Sage Mathematics Software System* (Version 10.0) (2023), https://www.sagemath.org.

Horacio Tapia-Recillas and **J. Armando Velazco-Velazco** (Corresponding Author)
Departamento de Matemáticas
Universidad Autónoma Metropolitana-I
09340 México City, MÉXICO
e-mails: htr@xanum.uam.mx (H. Tapia-Recillas)
oczalevaj@gmail.com (J. A. Velazco-Velazco)