Casa abierta al tiempo
Universidad Autónoma Metropolitana

Dr. José Raúl Montes de Oca Machorro
Jefe del Departamento
División de Ciencias Básicas e Ingeniería

C.B.I.MAT.070.2025
31 de julio 2025

Dr. Román Linares Romero
Presidente del Consejo Divisional
División de Ciencias Básicas e Ingeniería
Presente

Por medio del presente me permito solicitar, se incluya en el Orden del Día de la próxima Sesión del Consejo Divisional, el informe del periodo sabático que presenta el **Dr. Horacio Tapia Recillas (4619)**.

Agradeciendo la atención a la presente, quedo a sus órdenes para cualquier aclaración que requiera al respecto.

Atentamente
"Casa Abierta al Tiempo"

[redacted]

Anexo: Informe.
Probatorios

Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

CONSEJO DIVISIONAL DE CIENCIAS BÁSICAS E INGENIERIA

INFORME DE PERÍODO SABÁTICO

DATOS GENERALES

Nombre del profesor: HORACIO TAPIA RECILLAS Nº empleado: 4619

Departamento: MATEMÁTICAS Área: ÁLGEBRA

Teléfono particular: SIN Extensión UAM-I: [redacted] E-mail [redacted]@xanum.uam.mx

DATOS DEL PERÍODO SABÁTICO SOLICITADO

Nº meses solicitados: 20 Fecha de inicio: 6/11/2023 Fecha de terminación: 5/07/2025

Institución donde se realizará:

Depto., Laboratorio, etc.:

Domicilio de la institución:

Teléfono: Fax: E-mail

OBJETIVOS DEL PERÍODO SABÁTICO

REALIZAR INVESTIGACIÓN EN LA TEORIA DE CODIGOS ALGEBRAICOS

MIEMBRO DEL COMITE DEL XV COLOQUIO NACIONAL DE CODIGOS CRIPTOGRAFI/

Y AREAS RELACIONADAS DE 26-28 DE JUNIO DEL 2025. PRESENTACIÓN DE UNA PLATICA PONENTE

LA PUBLICACION DE CUATRO ARTICULOS

METAS ALCANZADAS EN EL PERÍODO SABÁTICO

□ Memorias in extenso en libro de resúmenes*

☑ Artículos de investigación en revista indexada*

☑ Presentaciones en congresos

□ Libros o capítulos de libros

□ Grado

□ % Avance de estudios de posgrado

☑ Otros (especifique): PARTICIPACIÓN EN SEMINARIO DE CRIPTOGRAFIA

* Indicar en anexo si se trata de trabajo publicado, aceptado o sometido

TIPO DE ACTIVIDADES ACADÉMICAS DESARROLLADAS

(Indique aquellas relacionadas con las actividades desarrolladas)

☑ Investigación　□ Docencia　☑ Difusión

☑ Formación académica　□ Formación profesional　□ Entrenamiento técnico

□ Otros (especifique): ______________________________

RESUMEN DEL PLAN DE ACTIVIDADES ACADÉMICAS DESARROLLADAS

(El llenado de esta sección no sustituye el informe detallado de actividades)

PUBLICACION DE CUATRO ARTICULOS DE INVESTIGACIÓN EN EL AREA DE CODIGOS.

PRESENTACIÓN DE UNA PONENCIA" CODIGOS DNA SOBRE EL CAMPO FINITO DE 16 ELEMENTOS"

MIEMBRO DEL COMITE ORGANIZADOR DE XV COLOQUIO NACIONAL DE CODIGOS CRIPTOGRAFIA Y AREAS RELACIONADAS

CONTINUE TRABAJANDO CON MI ALUMNO DE DOCTORADO (ARMANDO VELAZCO VELAZCO)

PARA USO DEL JEFE DE DEPARTAMENTO

Después de haber evaluado el informe detallado de actividades del período sabático del interesado según los lineamientos establecidos para tal efecto; informo al Consejo Divisional que:

(☒) Los objetivos SE cumplieron satisfactoriamente
(□) Los objetivos SE cumplieron parcialmente
(□) Los objetivos NO se cumplieron
(□) NO se cumplió el propósito del sabático

[redacted]
Firma del Jefe de Departamento

31/Julio/2025
Fecha

PARA USO DEL CONSEJO DIVISIONAL

El Consejo Divisional, en su Sesión No. ______________ del ______________________________ sobre el Período sabático del interesado acordó que:

(□) Los objetivos SE cumplieron satisfactoriamente
(□) Los objetivos SE cumplieron parcialmente
(□) Los objetivos NO se cumplieron
(□) NO se cumplió el propósito del sabático

____
Secretario del Consejo Divisional

*Además de este formato-resumen, el interesado deberá entregar su Informe detallado de actividades junto con la documentación probatoria correspondiente.

REPORTE DE ACTIVIDADES REALIZADAS DURANTE MI PERIODO SABÁTICO
(Horacio Tapia Recillas, 4619)

Investigación
Se han publicado los siguientes artículos de investigación:

H. Tapia-Recillas and J. A. and Velazco-Velazco. Cyclic Codes over the ring Z2k +uZ2k . São Paulo Journal of Mathematical Sciences, 18:14–27, march 2024. doi.org/10.1007/s40863-024-00412-z

H. Tapia-Recillas and J. A. Velazco-Velazco. Group structures of twistulant matrices over rings. International Electronic Journal of Algebra, Published Online: December 4, 2024
DOI: 10.24330/ieja.1596075

de Melo Hernández, F.D., Hernández Melo, C.A. and Tapia-Recillas, H. About quadratic residues in a class of rings. *São Paulo J. Math. Sci.* **18**, 28–47 (2024). https://doi.org/10.1007/s40863-024-00423-w

Horacio Tapia-Recillas and J. Armando Velazco-Velazco, A Note on Constacyclic Codes Over a Finite Commutative Local Ring with Residue Field Fp. International Journal of Algebra, Vol. 19, 2025, no. 2, 57 – 68, HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2025.91959

Docencia
Se participó en el seminario de Criptografía para estudiantes de Licenciatura en el Dpto. de Matemáticas de la UAM-I

Divulgación
Se formó parte del Comité Organizador del XV Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas celebrado en la Cd. de México del 26 al 28 de junio, 2025.

Se presentó una plática en el XV Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas celebrado en la Cd. de México del 26 al 28 de junio, 2025.

Se adjuntan comprobantes que avalan este reporte.

[redacted]

Horacio Tapia Recillas, 4619

[redacted]

International Journal of Algebra, Vol. 19, 2025, no. 2, 57 - 68
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2025.91959

A Note on Constacyclic Codes Over a Finite Commutative Local Ring with Residue Field $\mathbb{F}_p$

Horacio Tapia-Recillas

Departamento de Matemáticas
Universidad Autónoma Metropolitana-I
09340 CDMX, México

J. Armando Velazco-Velazco

Departamento de Computación
Universidad del Istmo - Campus Tehuantepec
70760, Tehuantepec Oaxaca, México

Abstract

Given a finite commutative local ring with identity, residue field $\mathbb{F}_p$, $p \geq 2$ a prime, and a length n such that $\gcd(p, n) = 1$, linear constacyclic codes over such rings are studied by means of idempotent elements. Under such conditions, the present work involves both: chain and non-chain rings.

Mathematics Subject Classification: 94B05, 94B60, 16U40

Keywords: Finite ring, constacyclic codes, idempotent elements

1 Introduction

Linear codes, cyclic and constacyclic codes over finite rings have been studied intensively in recent years. In particular, finite chain rings have been used as alphabets for this type of codes ([10], [3]). Constacylic codes are a generalization of cyclic codes and have been studied in contemporary papers by several research groups, for instance, over a finite chain ring we have the work [2], and some cases where the alphabet is a finite non-chain Frobenius ring were studied in [1].

In the present work we study the structure of constacyclic codes and their description by means of idempotent elements when the alphabet is a finite commutative local ring $\mathcal{R}$ with identity and residual field $\mathbb{F}_p$. The manuscript is organized as follows: In section 2 the necessary background material is given. In section 3 results on constacyclic codes are presented with emphasis on their description by means of idempotents elements. Finally, in section 4 examples illustrating the main results are presented.

2 Preliminaries

In this section definitions and basic results from algebra used in the manuscript are recalled. We refer the reader to [7] and [8] for details. By a ring $\mathcal{R}$ we mean a finite commutative ring with identity ($1 \in \mathcal{R}$). The set of units in $\mathcal{R}$ is denoted by $\mathcal{U}(\mathcal{R})$. An ideal I of $\mathcal{R}$ is generated by a nonempty $S \subseteq \mathcal{R}$, denoted by $I = \langle S \rangle$, if $I = \{\sum_{i=1}^{m} r_i s_i \mid r_i \in \mathcal{R}, s_i \in S, m \in \mathbb{N}\}$. If $S = \{s_1, \ldots, s_k\}$ we write $I = \langle s_1, \ldots, s_k \rangle$. If I is an ideal of a ring $\mathcal{R}$ and $\mathcal{R}$ is a subring of a ring $\mathcal{S}$, the ideal $I\mathcal{S}$, generated by the elements of I in $\mathcal{S}$, is called the extension of the ideal I to $\mathcal{S}$.

The ring $\mathcal{R}$ is called local if it has only one maximal ideal $\mathfrak{m}$. If $\mathcal{R}$ is a local ring with maximal ideal $\mathfrak{m}$ the quotient ring $\mathcal{R}/\mathfrak{m}$ is the residue field of $\mathcal{R}$, which is a finite field $\mathbb{F}_q$, where $q = p^m$ for some prime p. This information will be indicated by $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$. Given a finite local ring $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$, there is an integer $t \geq 1$ such that $\mathfrak{m}^t = \langle 0 \rangle$ and $\mathfrak{m}^{t-1} \neq \langle 0 \rangle$. Such integer t is called the nilpotency index of $\mathfrak{m}$. The (Jacobson) radical of $\mathcal{R}$, $\mathrm{Rad}(\mathcal{R})$, is defined as the intersection of all the maximal ideals of $\mathcal{R}$ and it is characterized in the following way: Let $\mathcal{R}$ be a ring. An element $r \in \mathcal{R}$ satisfies $r \in \mathrm{Rad}(\mathcal{R})$ if and only if $1 - rs$ is a unit in $\mathcal{R}$ for all $s \in \mathcal{R}$.

Let $\mathcal{R}$ be a finite local ring with residue field $\mathbb{F}_q$, with $q = p^m$ for some prime number p, and consider the corresponding rings of polynomials on one variable $\mathcal{R}[x]$ and $\mathbb{F}_q[x]$. The map $\bar{}\, : \mathcal{R} \longrightarrow \mathbb{F}_q$ is defined by $\overline{r} = r + \mathfrak{m}$. This map $\bar{}$ can be extended to a reduction map $\mathcal{R}[x] \longrightarrow \mathbb{F}_q[x]$ by $f(x) \mapsto \overline{f}(x)$ where $\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + \ldots + \overline{a}_{n-1} x^{n-1}$. If $f(x) \in \mathcal{R}[x]$ we will write f instead $f(x)$ as it is customary nowadays. Two polynomials $f, g \in \mathcal{R}[x]$ are relatively prime (or coprime) if $\langle f \rangle + \langle g \rangle = \langle 1 \rangle$. Also, f is regular if it is not a zero-divisor in $\mathcal{R}[x]$ which is equivalent with $\overline{f} \neq 0$, and $f \in \mathcal{R}[x]$ is basic irreducible if $\overline{f}$ is irreducible in $\mathbb{F}_q[x]$. If I is an ideal of a finite commutative ring with identity $\mathcal{R}$, then the set $I[x] = \{r_0 + r_1 x + \ldots + r_n x^n \in R[x] \mid r_i \in I, 0 \leq i \leq n\}$ is an ideal of $\mathcal{R}[x]$. From the definitions, the following lemma is easy to prove.

Lemma 2.1. *Let $f, g \in \mathcal{R}[x]$, where $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$ is a finite commutative local ring with identity. Then f, g are relatively prime in $\mathcal{R}[x]$ if and only if $\overline{f}$ and $\overline{g}$ are relatively prime in $\mathbb{F}_q[x]$.*

As mentioned, $\mathcal{R}$ will denote a finite commutative ring with identity unless othereise specified. From Hensel's lemma (theorem XIII.4) and theorems XIII.7. and XIII.11 in the reference [8] it is not difficult to see the following,

Proposition 2.2. *Let $f \in \mathcal{R}[x]$ be a monic regular polynomial, where $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_q)$ is a finite commutative local ring with identity. Suppose in $\mathbb{F}_q[x]$, $\overline{f} = \prod_{i=1}^{m} \overline{g}_i$ with the $\overline{g}_i$ monic, irreducible and pairwise relatively prime polynomials. Then, f has a factorization as a product of monic, basic irreducible and pairwise coprime polynomials.*

General definitions and results about idempotent elements in a ring are recalled. Let $\mathcal{R}$ be a commutative ring with unity. An element $e \in \mathcal{R}$ is called idempotent if $e^2 = e$. Two idempotent elements e and f are said to be orthogonal if $ef = 0$. An idempotent e is called primitive if $e = f + g$ with f and g orthogonal idempotent, then $f = 0$ or $g = 0$. A set of idempotent elements $\{e_1, e_2, \ldots, e_m\}$ such that $\sum_{i=1}^{m} e_i = 1$ is called a complete set. Furthermore, if $e_i e_j = 0$, $i \neq j$, the set is called a complete set of pairwise orthogonal idempotent elements. Additionally, if all the idempotents in such a set are primitive, the set is the complete set of primitive pairwise orthogonal idempotent elements and it is unique ([6] proposition 22.1). The set of idempotent elements of a ring $\mathcal{R}$ will be denoted by $E(\mathcal{R})$.

We recall the notion of a lifting idempotent. If I is an ideal of $\mathcal{R}$, let $\theta \in E(\mathcal{R}/I)$. It is said that θ is lifted to $\mathcal{R}$ if there is an $e \in E(\mathcal{R})$ such that $\pi(e) = \theta$, where π is the natural map $\mathcal{R} \to \mathcal{R}/I$. In this case we say $e \in E(\mathcal{R})$ is a lifting idempotent.

A ring $\mathcal{R}$ is decomposable if there are $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_l$ commutative nontrivial subrings of $\mathcal{R}$ with identity such that $\mathcal{R} \cong \oplus_{i=1}^{l} \mathcal{R}_i$.

Let $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_p)$ be a finite commutative local ring with identity. In particular, $\mathcal{R}$ is noetherian and artinian. Given a basic irreducible polynomial $f \in \mathcal{R}[x]$, let $\mathcal{R}_f = \mathcal{R}[x]/\langle f \rangle$. With the notation and definitions introduced above we establish the following,

Lemma 2.3. *Let $f \in \mathcal{R}[x]$ be a monic basic irreducible polynomial and let $\mathcal{R}_f = \mathcal{R}[x]/\langle f \rangle$. Then, for $g \in \mathcal{R}[x]$, $g + \langle f \rangle \in \mathcal{U}(\mathcal{R}_f)$ if and only if g is relatively prime with f in $\mathcal{R}[x]$.*

Proof. Suppose f, g are relatively prime in $\mathcal{R}[x]$. Then by definition $\langle g \rangle + \langle f \rangle = \langle 1 \rangle$ implies there are $h_0, h_1 \in \mathcal{R}$ such that $h_0 g + h_1 f = 1$. Thus, in $\mathcal{R}_f$ we have $h_0 g + \langle f \rangle = 1 + \langle f \rangle$, that is, $g + \langle f \rangle \in \mathcal{U}(\mathcal{R}_f)$. Conversely, suppose $g + \langle f \rangle \in \mathcal{U}(\mathcal{R}_f)$. Let $h + \langle f \rangle \in \mathcal{R}_f$ such that $gh + \langle f \rangle = 1 + \langle f \rangle$. Then

$hg + fF_0 = 1 + fF_1$ for some $F_0, F_1 \in \mathcal{R}[x]$. Rearranging the terms we have $hg + fF = 1$, with $F \in \mathcal{R}_f$ and then g and f are relatively prime by definition. □

Corollary 2.4. *Let $\mathcal{R}_f$ be as in lemma 2.3. If $f, h \in \mathcal{R}[x]$ are not relatively prime in $\mathcal{R}[x]$, then $(1 + h) + \langle f \rangle \in \mathcal{U}(\mathcal{R}_f)$.*

Proof. If $h \in \mathfrak{m}[x] \subset \mathcal{R}[x]$ there is nothing to prove: $(1 + h) + \langle f \rangle \in \mathcal{U}(\mathcal{R}_f)$ since $1 + \langle f \rangle$ is a unit and $h + \langle f \rangle$ is nilpotent. Let us suppose $h \notin \mathfrak{m}[x]$. By hypothesis $\overline{h}$ and $\overline{f}$ are not relatively prime in $\mathbb{F}_p[x]$ which, given $\overline{f}$ is irreducible, means that $\overline{h} = \overline{h}_0\overline{f}$ for some $\overline{h}_0 \in \mathbb{F}_p[x]$. Thus,

$$\overline{1 + h} - \overline{h}_0\overline{f} = 1 + \overline{h}_0\overline{f} - \overline{h}_0\overline{f} = 1 \in \mathbb{F}_p[x].$$

By lemma 2.1, $1 + h$ and f are relatively prime in $\mathcal{R}[x]$. The claim follows from lemma 2.3. □

Proposition 2.5. *Let $f \in \mathcal{R}[x]$ be a monic basic irreducible polynomial. Then $\mathcal{R}_f$ is a local ring.*

Proof. It will be shown that the set of non-units $\mathfrak{M}$ of $\mathcal{R}_f$ is an ideal. To prove the assertion we only need to show the set is closed under addition. Let $g + \langle f \rangle, h + \langle f \rangle$ be non-units. By lemma 2.3 g and h are not relatively prime with f in $\mathcal{R}[x]$. Suppose without loss of generality that $(g+h)+\langle f \rangle = 1+\langle f \rangle$. From this $g+\langle f \rangle = (1-h)+\langle f \rangle$, leading to an absurd. On one hand $g+\langle f \rangle$ is a non-unit and on the other hand $\langle 1-h \rangle+\langle f \rangle = \langle 1 \rangle$ in $\mathcal{R}[x]$, because $\overline{1-h}$ and $\overline{f}$ are relatively prime in $\mathbb{F}_p[x]$. However that means $(1-h)+\langle f \rangle \in \mathcal{U}(\mathcal{R}_f)$. Then the non-units of $\mathcal{R}_f$ form the ideal $\mathfrak{M}$ and, therefore, $\mathcal{R}_f$ is a local ring. □

Lemma 2.3 and proposition 2.5 imply the following claim. The proof is in essence the same as Proposition 11 of [12] and it is omitted.

Proposition 2.6. *Let $f \in \mathcal{R}_k[x]$ be a monic basic irreducible polynomial and $\mathcal{R}_f = \mathcal{R}[x]/\langle f \rangle$. Then any ideal $\mathcal{I}$ of $\mathcal{R}_f$ has the form*

$$\mathcal{I} = I\mathcal{R}_f,$$

where $I\mathcal{R}_f$ denotes the ideal extension of the ideal I of $\mathcal{R}$ to the ring $\mathcal{R}_f$.

Let $\mathfrak{R} = \mathcal{R}[x]/\langle F \rangle$, where $F \in \mathcal{R}[x]$.

Theorem 2.7. *Let $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_p)$ be a finite local commutative ring with identity. Let $F \in \mathcal{R}[x]$ be such that $\deg F = n$, $\gcd(p, n) = 1$, and $F = \prod_{i=1}^{m} f_i$ where the f_i are monic basic pairwise relatively prime polynomials in $\mathcal{R}[x]$. Then,*

$$\mathfrak{R} = \mathcal{R}[x]/\langle F \rangle \cong \bigoplus_{i=1}^{m} \mathcal{R}_{f_i}$$

where $\mathcal{R}_{f_i} = \mathcal{R}[x]/\langle f_i \rangle$ *for* $i = 1, \dots, m$*. Furthermore, there is a complete set of primitive pairwise orthogonal idempotents*

$$E_p = \{\hat{e}_1, \dots, \hat{e}_m\}$$

in $\mathcal{R}[x]/\langle F \rangle$ *such that* $\mathcal{R}_{f_i} \cong \hat{e}_i \mathfrak{R}$ *for* $i = 1, \dots, m$*, i.e,* $\mathfrak{R} \cong \bigoplus_{i=1}^m \mathcal{R}_{f_i} \cong \bigoplus_{i=1}^m \hat{e}_i \mathfrak{R}$*.*

Proof. As a direct consequence of the Chinese Remainder theorem we have

$$\mathfrak{R} = \mathcal{R}[x]/\langle F \rangle \cong \bigoplus_{i=1}^{m} \mathcal{R}_{f_i}.$$

Let $\mathbf{e}_i = (0, \dots, 1, \dots, 0)$ be the element of $\bigoplus_{i=1}^m \mathcal{R}_{f_i}$ with 1 at the *ith* coordinate and all the remains equal to zero. It is immediate to see that $\mathbf{e}_i$ is idempotent, $i = 1, \dots, m$ and the set $\{\mathbf{e}_1, \dots, \mathbf{e}_l\}$ is a complete set of pairwise orthogonal idempotents. We claim each $\mathbf{e}_i$ is primitive. Suppose $\mathbf{h}_i = (h_{i1}, \dots, h_{im}), \mathbf{g}_i = (g_{i1}, \dots, g_{im}) \in E(\bigoplus_{i=1}^m \mathcal{R}_{f_i})$ are orthogonal idempotents such that

$$\mathbf{e}_i = \mathbf{h}_i + \mathbf{g}_i,$$

then $(h_{i1}g_{i1} \dots, h_{im}g_{im}) = (0, \dots, 0)$ from which $h_{ij}g_{ij} = 0$, $j = 1, \dots, m$. Note $h_{ij}, g_{ij} \in \mathcal{R}_{f_i}$ are idempotents in a local ring, then $\mathbf{h}_i = \mathbf{0}$ or $\mathbf{g}_i = \mathbf{0}$, where $\mathbf{0}$ is the zero of $\bigoplus_{i=1}^l \mathcal{R}_{f_i}$. The existence of a complete set of primitive pairwise orthogonal idempotents $\{\hat{e}_1, \hat{e}_2, \dots, \hat{e}_l\} \subset \mathfrak{R}$ follows from the fact that $\hat{e}_i = \psi^{-1}(\mathbf{e}_i)$ where $\psi : \mathfrak{R} \longrightarrow \bigoplus_{i=1}^l \mathcal{R}_{f_i}$ is the Chinese Remainder Theorem isomorphism. Notice $(\hat{e}_i \mathfrak{R}, +, \cdot)$ is a finite commutative ring with identity $\hat{e}_i$. The isomorphism ψ^{-1} restricted to each summand of $\bigoplus_{i=1}^m \mathcal{R}_{f_i}$ induces a ring isomorphism ϕ_i in the obvious way between $\mathcal{R}_{f_i}$ and the ring $\hat{e}_i \mathfrak{R} = \langle \hat{e}_i \rangle$. □

3 Constacyclic Codes over a local ring with residual field $\mathbb{F}_p$

In this section, given a prime p, we consider linear constacyclic codes of length n, $\gcd(p, n) = 1$, defined over a local ring $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_p)$. An $\mathcal{R}$-submodule $\mathcal{C} \subset \mathcal{R}^n$ will be a linear code $\mathcal{C}$ over $\mathcal{R}$. A codeword will be denoted as $\mathbf{c} = (c_0, c_1, \dots, c_{n-1})$, $c_i \in \mathcal{R}$. Let $\gamma \in \mathcal{U}(\mathcal{R})$ be unit of $\mathcal{R}$. A linear code $\mathcal{C}$ of length n over $\mathcal{R}$ is constacyclic if it satisfied

$$(c_0, c_1, \dots, c_{n-1}) \text{ implies } (\gamma c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}.$$

By means of the polynomial representation associated to the elements of $\mathcal{R}^n$ and, in particular, with the elements of the code $\mathcal{C}$ ([5], [4]) a linear constacyclic code of length n, with $\gcd(p, n) = 1$, is identified with an ideal from the ring

$$\mathcal{R}_n = \mathcal{R}[x]/\langle x^n - \gamma \rangle, \gamma \in \mathcal{U}(\mathcal{R}).$$

Particular cases of linear constacyclic codes are called cyclic and negacyclic codes with $\gamma = 1, -1$ respectively.

From theorem 2.7, we have the following situation illustrated in the diagram,

$$\begin{tikzcd}
\mathcal{R}[x]/\langle x^n - \gamma\rangle \arrow[r, "\cong"] \arrow[d, "-"'] & \bigoplus_{i=1}^m \mathcal{R}[x]/\langle f_i\rangle \arrow[d, "-"] \\
\mathbb{F}_p[x]/\langle \overline{x^n - \gamma}\rangle \arrow[r, "\cong"'] & \bigoplus_{i=1}^m \mathbb{F}_p[x]/\langle \overline{f}_i\rangle .
\end{tikzcd}$$

Via the isomorphisms given by the Chinese Remainder theorem and the corresponding reduction maps, an explicit isomorphism $\phi : \bigoplus_{i=1}^m \hat{e}_i\mathcal{R}_n \longrightarrow \mathcal{R}_n$ is obtained. The map $\phi : \bigoplus_{i=1}^m \hat{e}\mathcal{R}_n \longrightarrow \mathcal{R}_n$ defined by

$$\phi(\hat{e}_1 c_1 + \langle x^n - \gamma\rangle, \ldots, \hat{e}_m c_m + \langle x^n - \gamma\rangle) = \sum_{i=1}^m \hat{e}_i c_i + \langle x^n - \gamma\rangle, \qquad (1)$$

where the $\hat{e}_i \in E_p$, the corresponding complete set of primitive pairwise orthogonal idempotents from $\mathcal{R}_n$.

That the map ϕ is an isomorphism, follows from the next theorem.

Theorem 3.1. *Let n be an integer such that $\gcd(p, n) = 1$, $x^n - \gamma = \prod_{i=1}^m f_i$ where the f_i's are distinct monic basic irreducible pairwise relatively prime polynomials in $\mathcal{R}[x]$ for $i \in \{1, 2, \ldots, m\}$, and $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_p)$ a local ring. The complete set of primitive pairwise orthogonal idempotents in $\mathcal{R}_n$*

$$E_p = \{\hat{e}_1, \hat{e}_2, \ldots, \hat{e}_m\}$$

is given explicitly by $\hat{e}_i = \hat{\lambda}_i \hat{f}_i + \langle x^n - \gamma\rangle$, for $i = 1, \ldots, m$, where $\hat{\lambda}_i \in \mathcal{R}[x]$ satisfy

$$\sum_{i=1}^m \hat{\lambda}_i \hat{f}_i = 1 \in \mathcal{R}[x].$$

Moreover, each one of the primitive $\hat{e}_i$ is a lifting idempotent from the ring $\mathbb{F}_p[x]/\langle \overline{x^n - \gamma}\rangle$.

Proof. Let $\overline{x^n - \gamma} = \prod_{i=1}^m F_i$ be the product of irreducible polynomials in $\mathbb{F}_p[x]$, with $F_i = \overline{f}_i$ and let $\hat{F}_i = \prod_{j \neq i} F_j$. Then $\gcd(\hat{F}_1, \hat{F}_2, \ldots, \hat{F}_m) = 1$ and from Lemma 2.1, the corresponding $\hat{f}_1, \ldots, \hat{f}_m$ where $\hat{f}_i = \prod_{j \neq i} f_j$, are relatively prime. Then there exist $\hat{\lambda}_i \in \mathcal{R}[x]$, $i = 1, \ldots, m$ such that

$$\hat{\lambda}_1 \hat{f}_1 + \hat{\lambda}_2 \hat{f}_2 + \ldots + \hat{\lambda}_m \hat{f}_m = 1.$$

Also, for $i = 1, \ldots, m$, from lemma 2.1 and theorem 2.7, there is a $\lambda_i \in \mathcal{R}[x]$ such that $\hat{\lambda}_i \hat{f}_i + \lambda_i f_i = 1$ in $\mathcal{R}[x]$ which implies $\hat{e}_i = \hat{\lambda}_i \hat{f}_i + \langle x^n - \gamma\rangle$ is idempotent in $\mathcal{R}_n$. This defined $\hat{e}_i\hat{e}_j = 0 + \langle x^n - \gamma\rangle$ for $i \neq j$ and by construction they are primitive. The idempotent $\hat{e}_i \in \mathcal{R}_n$ by definition is a lifting idempotent as a consequence of the reduction map $\mathcal{R}/\langle x^n - \gamma\rangle \to (\mathcal{R}/\langle x^n - \gamma\rangle)/\mathfrak{m}$. □

The previous theorem together with the next one will provide a way to determine the set of primitive idempotent elements in the ring $\mathcal{R}_n$ from the ring $\mathbb{F}_p[x]/\langle\overline{x^n - \gamma}\rangle$.

Proposition 3.2. *([9], Proposition 4.1) Let $\mathcal{R}$ be a commutative ring and N a nilpotent ideal of $\mathcal{R}$ with nilpotency index $t \geq 2$. Let $s > 1$ be the characteristic of the quotient ring $\mathcal{R}/N$. If e is an idempotent element of $\mathcal{R}/N$ then,*

$$e^{s^{t-1}}$$

is an idempotent element of the ring $\mathcal{R}$, called the lift of e. Moreover, if there is a collection of primitive orthogonal idempotent elements of $\mathcal{R}/N$ it lifts to a set of idempotent elements of $\mathcal{R}$ with the same property. Also, $|E(\mathcal{R})| = |E(\mathcal{R}/N)|$ where $E(\mathcal{R})$ is the set of idempotent elements of $\mathcal{R}$.

Now we apply the previous results to our situation. Recall that $(\mathcal{R}, \mathfrak{m}, \mathbb{F}_p)$ is a local ring, then $\mathcal{R}_n = \mathcal{R}[x]/\langle x^n - \gamma\rangle$, $\mathfrak{m}_n = \mathfrak{m}\mathcal{R}_n$ is an ideal with nilpotency index t, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{R}$ and $\mathcal{R}_n/\mathfrak{m}_n = \mathbb{F}_p[x]/\langle\overline{x^n - \gamma}\rangle$ has characteristic $s = p$. With the previous notation the following claim follows easily.

Theorem 3.3. *Let $E = \{\hat{\theta}_1, \hat{\theta}_2, \ldots \hat{\theta}_m\}$ be the complete set of primitive pairwise idempotent elements in the ring $\mathbb{F}_p[x]/\langle\overline{x^n - \gamma}\rangle$. Then*

$$E_p = \{\hat{e}_1 = \hat{\theta}_1^{p^{t-1}}, \hat{e}_2 = \hat{\theta}_2^{p^{t-1}}, \ldots, \hat{e}_m = \hat{\theta}_m^{p^{t-1}}\}$$

is the complete set of primitive pairwise orthogonal idempotent elements of the ring $\mathcal{R}_n$.

With notation as above, the following result is easy to prove.

Theorem 3.4. *Let n be an integer such that $\gcd(p, n) = 1$, and $x^n - \gamma = \prod_i^m f_i$ be a product of monic basic irreducible pairwise coprime polynomials.*

1. *The ring $\mathcal{R}_n$ is a principal ideal ring if and only if $\mathcal{R}$ is a principal ideal ring.*

2. *The ring $\mathcal{R}_n$ is a semi-local ring. Moreover, $\mathcal{R}_n$ has exactly m maximal ideals.*

3. *Let $\mathcal{L}$ be the set of ideals of the ring $\mathcal{R}$ (including $\langle 1\rangle$) and m the number of distinct monic basic irreducible coprime factors of $x^n - \gamma$ in $\mathcal{R}[x]$. Then the ring $\mathcal{R}_n$ has $|\mathcal{L}|^m$ ideals.*

Proof. With the notation as above, for $j = 1, \ldots, m$ consider the ideal

$$\mathfrak{M}_j = \langle 1 + \langle f_1 \rangle \rangle \oplus \ldots \oplus \mathfrak{M}\mathcal{R}_{f_j} \oplus \ldots \oplus \langle 1 + \langle f_m \rangle \rangle \subset \bigoplus_{i=1}^{m} \mathcal{R}_{f_i}.$$

This is a maximal ideal as, from propositions 2.5 and 2.6,

$$\left(\bigoplus_{i=1}^{m} \mathcal{R}_{f_i} \right) / \mathfrak{M}_j \cong \mathbb{F}_{p^{\deg f_j}}.$$

Therefore, from theorem 2.7 the ideal $\mathfrak{M}_j$ has the same number of generators under the isomorphism image $\phi(\mathfrak{M}_j)$. The second claim is a consequence of this fact. The third part follows from the Chine Remainder theorem. □

We recall that the ring $\mathcal{R}$ is local with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}_p$. If $f \in \mathcal{R}[x]$ its image under the reduction map modulo $\mathfrak{m}$ to $\mathbb{F}_p[x]$ is denoted by $\overline{f}$. We have the following.

Proposition 3.5. *Let γ be a unit of the ring $\mathcal{R}$, $x^n - \gamma = \prod_{i=1}^{m} f_i$ where n is such that $\gcd(p, n) = 1$ and f_i's are distinct monic basic irreducible pairwise relatively prime polynomials in $\mathcal{R}[x]$ for $i \in \{1, 2, \ldots, m\}$. Let $\overline{x^n - \gamma} = \Pi_{i=1}^{m} \overline{f}_i$ be the corresponding product of irreducible factors in $\mathbb{F}_p[x]$. Then a non-zero principal ideal $\mathcal{C} = \langle f + \langle x^n - \gamma \rangle \rangle \subseteq \mathcal{R}_n$ is trivial if and only if $\gcd(\overline{f}, \overline{x^n - \gamma}) = 1$ in $\mathbb{F}_p[x]$.*

Proof. If $\gcd(\overline{f}, \overline{x^n - \gamma}) = 1$, then $\gcd(\overline{f}, \overline{f_i}) = 1$ and from the lemma 2.1 we have $\langle f \rangle + \langle f_i \rangle = \langle 1 \rangle$ in $\mathcal{R}[x]$. Then, lemma 2.3 and theorem 2.7 imply

$$\langle f + \langle x^n - \gamma \rangle \rangle \cong \oplus_{i=1}^{m} \langle 1 + \langle f_i \rangle \rangle = \bigoplus_{i=1}^{m} \mathcal{R}_{f_i}.$$

□

Now we are able to give the following,

Theorem 3.6. *Let n be an integer such that $\gcd(p, n) = 1$, $\mathcal{R}_n = \mathcal{R}[x]/\langle x^n - \gamma \rangle$ and let $x^n - \gamma = \prod_{i=1}^{m} f_i$ be the representation of $x^n - \gamma$ as a product of distinct monic basic irreducible pairwise relatively prime polynomials in $\mathcal{R}[x]$. Let $\mathcal{C} = \langle f + \langle x^n - \gamma \rangle \rangle$ be a non-trivial principal ideal of $\mathcal{R}_n$ and assume $f = f_{j_1} f_{j_2} \cdots f_{j_s}$ where $j_l \in M = \{1, 2, ..., m\}, l = 1, 2, ..., s$. Then, the idempotent element $e_f + \langle x^n - \gamma \rangle \in E(\mathcal{R}_n)$ such that*

$$\mathcal{C} = \langle e_f + \langle x^n - \gamma \rangle \rangle$$

is given by

$$e_f + \langle x^n - \gamma \rangle = \sum_i \hat{e}_i + \langle x^n - \gamma \rangle,$$

where $\{\hat{e}_i + \langle x^n - \gamma \rangle \mid i \in M \setminus \{j_1, j_2, ..., j_s\}\} \subset E_p$ and the set E_p is the complete set of primitive pairwise orthogonal idempotent elements of $\mathcal{R}_n$.

Proof. Since $f = \prod_{l=1}^{s} f_{j_l}$, let $\hat{f} = \prod_i f_i$ with $i \in M \setminus \{j_1, j_2, ..., j_s\}$. Thus f and $\hat{f}$ are relatively prime and there are $\lambda, \hat{\lambda} \in \mathcal{R}[x]$ such that $\lambda f + \hat{\lambda}\hat{f} = 1$. Let $e_f + \langle x^n - \gamma\rangle = \lambda f + \langle x^n - \gamma\rangle \in \mathcal{R}_n$. It is easy to see that this is an idempotent element. Observe that

$$\lambda f \equiv 1 \equiv \hat{\lambda}_i \hat{f}_i \mod \langle f_i\rangle, i \in M \setminus \{j_1, j_2, \ldots, j_s\},$$

and

$$\lambda f \equiv 0 \mod \langle f_{j_l}\rangle, l = 1, 2, \ldots, s.$$

Using the isomorphism (1) from $\bigoplus_{i=1}^{m} \mathcal{R}_{f_i} \to \mathcal{R}_n$ the expression for $e_f + \langle x^n - \gamma\rangle$ is obtained. Also, by construction,

$$fe_f + \langle x^n - \gamma\rangle = f(\lambda f) + \langle x^n - \gamma\rangle = f(1 - \hat{\lambda}\hat{f}) + \langle x^n - \gamma\rangle = f + \langle x^n - \gamma\rangle.$$

It follows that $\langle f + \langle x^n - \gamma\rangle\rangle = \langle e_f + \langle x^n - \gamma\rangle\rangle$. □

4 Examples of constacyclic codes over local rings and their idempotents

SageMath ([13]) was utilized to develop the computations in the following examples.

Example 4.1. *Let $\mathcal{R} = \mathbb{F}_2 + u\mathbb{F}_2 = \{a + bu \mid a, b \in \mathbb{F}_2, u^2 = 0\} = \{0, 1, u, 1 + u\}$. This is a finite commutative local chain ring with identity, whose maximal ideal is $\mathfrak{m} = \langle u\rangle$ with nilpotency index $t = 2$, and residue field $\mathcal{R}/\mathfrak{m} = \mathbb{F}_2$. Let $n = 15, \gamma = 1$ and $p = 2$, i.e, we describe the cyclic codes of length $n = 15$. In $\mathcal{R}[x]$ the polynomial $x^{15} - 1 = \prod_{i=1}^{5} f_i$ where $f_1 = x + 1, f_2 = x^2 + x + 1, f_3 = x^4 + x + 1,\ f_4 = x^4 + x^3 + 1, f_5 = x^4 + x^3 + x^2 + x + 1$. From theorem 2.7 we have*

$$\mathcal{R}_{15} = \mathcal{R}[x]/\langle x^{15} - 1\rangle \cong \bigoplus_{i=1}^{5} \mathcal{R}_{f_i} \cong \bigoplus_{i=1}^{5} \hat{e}_i \mathcal{R}_{15},$$

where $\hat{e}_i \in E_2$, the complete set of primitive pairwise orthogonal idempotents of $\mathcal{R}_{15}$, set which we will proceed to determine. Let $R_{15} = \mathbb{F}_2[x]/\langle x^{15} + 1\rangle$. We have $\overline{x^{15} - 1} = x^{15}+1$ and $x^{15}+1 = \prod_{i=1}^{5} f_i \in \mathbb{F}_2[x]$. By means of the Euclidean algorithm, the complete set of primitive pairwise orthogonal idempotents in R_{15} is given by $\{\hat{\theta}_i, i = 1, 2, 3, 4, 5\}$, where

$$\begin{aligned}
\hat{\theta}_1 &= \prod_{j \neq 1}^{5} f_j + \langle x^{15} + 1\rangle,\\
\hat{\theta}_2 &= x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + \langle x^{15} + 1\rangle,\\
\hat{\theta}_3 &= x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x + \langle x^{15} + 1\rangle,\\
\hat{\theta}_4 &= x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^6 + x^3 + \langle x^{15} + 1\rangle,\\
\hat{\theta}_5 &= x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x + \langle x^{15} + 1\rangle.
\end{aligned}$$

with $\hat{\theta}_1 = x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1+\langle x^{15}+1\rangle$*. Then, by theorem 3.3,* $E_2 = \{\hat{\theta}_i^2, i = 1,2,3,4,5\} \subset \mathcal{R}_{15}$*. From proposition 2.6 each* $\mathcal{R}_{f_i} = \mathcal{R}[x]/\langle f_i\rangle$, $i = 1,\dots,5$ *has the same set of ideals* $\mathcal{L} = \{\langle 0\rangle, \langle 1\rangle, \langle u\rangle, \langle 1+u\rangle\}$ *as* $\mathcal{R}$*. By means of the isomorphism (1) the generator for a non trivial cyclic code* $\mathcal{C}$ *in* $\mathcal{R}_{15}$ *is given by*

$$\mathcal{C} = \langle \sum_{i=1}^{5} g_i\hat{e}_i + \langle x^{15}-1\rangle\rangle$$

where $g_i \in \{0,1,u,1+u\}$*, this last set the collection of ideal generators in the ring* $\mathcal{R}$*. Notice, by theorem 3.4, each cyclic code* $\mathcal{C}$ *in* $\mathcal{R}_{15}$ *is principal since* $\mathcal{R} = \mathbb{F}_2 + u\mathbb{F}_2$ *is a principal ideal ring.*

Example 4.2. *From the ring in example 4.1, i.e.* $\mathcal{R} = \mathbb{F}_2 + u\mathbb{F}_2$ *where* $u^2 = 0$*, take* $\gamma = 1+u$*. We will determine the complete set of primitive pairwise orthogonal idempotent elements for the ring*

$$\mathcal{R}_{15} = \mathcal{R}[x]/\langle x^{15} - (1+u)\rangle.$$

In this case we have the factorization $x^{15} - (1+u) = \prod_{i=1}^{5} h_i$ *as a product of monic basic irreducible pairwise coprime polynomials in* $\mathcal{R}[x]$*, where* $h_1 = x+(1+u)$, $h_2 = x^2+(1+u)x+1$, $h_3 = x^4+(1+u)x+1$, $h_4 = x^4+(1+u)x^3+1$ *and* $h_5 = x^4+(1+u)x^3+x^2+(1+u)x+1$*. In the ring* $R_{15} = \mathbb{F}_2[x]/\langle x^{15}+1\rangle$ *we have the complete set of primitive pairwise orthogonal idempotent elements* $\{\hat{\theta}_1, \hat{\theta}_2, \hat{\theta}_3, \hat{\theta}_4, \hat{\theta}_5\}$ *(see previous example 4.1) from where by means of theorem 3.3 the corresponding complete set of primitive pairwise orthogonal idempotent elements in* $\mathcal{R}_{15}$ *is given by*

$\hat{e}_1 = x^{14}+(1+u)x^{13}+x^{12}+(1+u)x^{11}+x^{10}+(1+u)x^9+x^8+(1+u)x^7+x^6+(1+u)x^5+x^4+(1+u)x^3+x^2+(1+u)x+1.$

$\hat{e}_2 = x^{14}+(1+u)x^{13}+(1+u)x^{11}+x^{10}+x^8+(1+u)x^7+(1+u)x^5+x^4+x^2+(1+u)x.$

$\hat{e}_3 = x^{12}+(1+u)x^9+x^8+x^6+x^4+(1+u)x^3+x^2+(1+u)x.$

$\hat{e}_4 = x^{14}+(1+u)x^{13}+x^{12}+(1+u)x^{11}+(1+u)x^9+(1+u)x^7+x^6+(1+u)x^3.$

$\hat{e}_5 = x^{14}+(1+u)x^{13}+x^{12}+(1+u)x^{11}+(1+u)x^9+x^8+(1+u)x^7+x^6+x^4+(1+u)x^3+x^2+(1+u)x.$

Notice we have omitted the part '$+\langle x^{15}-(1+u)\rangle$*' on each idempotent for sake of space and notation clarity. It is worth mentioning the idempotent elements obtained in this work and those obtained from proposition 3.1 appearing in [11] where the authors prove* $\mathcal{R}[x]/\langle x^n-1\rangle \cong \mathcal{R}[x]/\langle x^{15}-(1+u)\rangle$ *in case n is an odd integer. The isomorphism* $\mu : \mathcal{R}[x]/\langle x^n-1\rangle \longrightarrow \mathcal{R}[x]/\langle x^{15}-(1+u)\rangle$ *given in such work and defined by* $\mu(c(x)) = c((1+u)x)$ *maps each* $\hat{e}_i \in \mathcal{R}[x]/\langle x^n-1\rangle$ *to* $\hat{e}_i \in \mathcal{R}[x]/\langle x^{15}-(1+u)\rangle$*.*

Example 4.3. *Let* $p = 5, \gamma = 8$ *and* $n = 6$ *and consider the non-chain ring* $\mathcal{R} = \mathbb{Z}_{25} + u\mathbb{Z}_{25} = \{a+bu \mid a,b \in \mathbb{Z}_{25}, u^2 = 0\}$*.* $\mathcal{R}$ *is a finite commutative local ring with identity and maximal ideal* $\mathfrak{m} = \langle 5, u\rangle$ *whose nilpotency index* *is $t = 3$. The ring operations are the natural ones derived from the sum and product in $\mathbb{Z}_{25}$. With these parameters, the ring $\mathcal{R}_6 = \mathcal{R}[x]/\langle x^6 - 8\rangle$. In $\mathcal{R}[x]$, $x^6 - 8 = f_1 f_2 f_3$ where $f_1 = x^2 + 23$, $f_2 = x^2 + 12x + 23$, $f_3 = x^2 + 13x + 23$. The residue field is $\mathcal{R}/\mathfrak{m} = \mathbb{F}_5$. Under the reduction map, in $\mathbb{F}_5[x]$,*

$$\overline{x^6 - 8} = x^6 + 2 = \overline{f}_1 \overline{f}_2 \overline{f}_3$$

where $\overline{f}_1 = x^2 + 3$, $\overline{f}_2 = x^2 + 2x + 3$, $\overline{f}_3 = x^2 + 3x + 3$. Then let $R_6 = \mathbb{F}_5[x]/\langle x^6 + 2\rangle$. The complete set of primitive pairwise orthogonal idempotent elements in R_6 is $\{\hat{\theta}_1 = 3x^4 + x^2 + 2 + \langle x^6 + 2\rangle, \hat{\theta}_2 = x^5 + x^4 + 2x^2 + x + 2 + \langle x^6 + 2\rangle, \hat{\theta}_3 = 4x^5 + x^4 + 2x^2 + 4x + 2 + \langle x^6 + 2\rangle\}$. From theorem 3.3 we have

$$E_5 = \{\hat{e}_1, \hat{e}_2, \hat{e}_3\} = \{\hat{\theta}_1^{25}, \hat{\theta}_2^{25}, \hat{\theta}_3^{25}\}$$

where $\hat{e}_i = \hat{\theta}_i^{25}$, $i = 1, 2, 3$, and

$$\begin{aligned} \hat{\theta}_1^{25} &= 23x^4 + 21x^2 + 17 + \langle x^6 - 8\rangle, \\ \hat{\theta}_2^{25} &= 6x^5 + x^4 + 2x^2 + x + 17 + \langle x^6 - 8\rangle, \\ \hat{\theta}_3^{25} &= 19x^5 + x^4 + 2x^2 + 24x + 17 + \langle x^6 - 8\rangle. \end{aligned}$$

With the previous information, using theorem 3.6, the idempotents associated to the ideal of $\mathcal{R}_6$

$$\mathcal{C} = \langle x^4 + 2x^2 + 4 + \langle x^6 - 8\rangle, u(x^2 + 23) + \langle x^6 - 8\rangle\rangle = \langle f + \langle x^6 - 8\rangle, ug + \langle x^6 - 8\rangle\rangle$$

are determined. Observe that $f = f_2 f_3$, $g = f_1$ in $\mathcal{R}[x]$. Then $e_f = \hat{e}_1 = 23x^4 + 21x^2 + 17 + \langle x^6 - 8\rangle$, and similarly, $e_g = \hat{e}_2 + \hat{e}_3 = 2x^4 + 4x^2 + 9 + \langle x^6 - 8\rangle$. Thus, since $e_f, e_g \in \mathcal{C}$, $e_f(f + \langle x^6 - 8\rangle) = f + \langle x^6 - 8\rangle$, $e_g(ug + \langle x^6 - 8\rangle) = ug + \langle x^6 - 8\rangle$, then

$$\mathcal{C} = \langle f + \langle x^6 - 8\rangle, ug + \langle x^6 - 8\rangle\rangle = \langle e_f, ue_g\rangle.$$

Acknowledgements. The first author was partially supported by Sistema Nacional de Investigadoras e Investigadores (SNII), México, Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT).

References

[1] C. A. Castillo-Guillén, C. Rentería-Márquez, and H. Tapia-Recillas, Constacyclic codes over finite local Frobenius non-chain rings with nilpotency index 3., *Finite Fields and Their Applications,* **43** (2017), 1–21. https://doi.org/10.1016/j.ffa.2016.08.004

[2] M. Charkani and J. Kabore, Primitive idempotents and constacyclic codes over finite chain rings, *Gulf Journal of Mathematics,* **8** (2) (2020), 55–67. https://doi.org/10.56947/gjom.v8i2.434

[3] Hai Q. Dinh and S. R. López-Permouth, Cyclic and Negacyclic codes over finite chain rings, *IEEE Transactions on Information Theory,* **50(8)** (2004), 1728–1744. https://doi.org/10.1109/TIT.2004.831789

[4] S. T. Dougherty, *Algebraic Coding Theory over Finite Commutative Rings,* Springer International Publishing AG, first edition, 2017

[5] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes,* Cambridge University Press, first edition, 2003.

[6] T. Y. Lam, *A First Course in Noncommutative Rings,* volume 131, *Graduated Texts in Mathematics*, Springer Verlag New York, Inc., 1991.

[7] S. Lang, *Algebra,* volume 211, *Graduate Text in Mathematics.* Springer New York, NY, third edition, 2012.

[8] B. R. McDonald, *Finite Rings with Identity,* Number 28 in Pure and Applied Mathematics. Marcel Dekker Inc., 1974.

[9] F. D. Melo-Hernández, C. A. Hernández-Melo, and H. Tapia-Recillas, On idempotents of a class of commutative rings, *Communications in Algebra,* **48** (2020), 4013–4026. https://doi.org/10.1080/00927872.2020.1754424

[10] G. H. Norton and A. Sălăgean, On the structure of linear and cyclic codes over a finite chain ring, *Applicable Algebra in Engineering, Communication and Computing,* **10** (2000), 489–506.
https://doi.org/10.1007/PL00012382

[11] J.F. Qian, L.N. Zhang, and S.X. Zhu, $(1+u)$-constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *Applied Mathematics Letters,* **19(8)** (2006), 820–823. https://doi.org/10.1016/j.aml.2005.10.011

[12] H. Tapia-Recillas and J. A. Velazco-Velazco, Cyclic Codes over the ring $\mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$, *São Paulo Journal of Mathematical Sciences,* **18** (2024), 14–27. https://doi.org/10.1007/s40863-024-00412-z

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

Received: May 17, 2025; Published: May 31, 2025

São Paulo Journal of Mathematical Sciences
https://doi.org/10.1007/s40863-024-00423-w

ORIGINAL ARTICLE

About quadratic residues in a class of rings

Fernanda D. de Melo Hernández[1] · César A. Hernández Melo[1] · Horacio Tapia-Recillas[2]

Accepted: 21 March 2024

Abstract
Let R be a commutative ring with a collection of ideals $\{N_1, N_2, \ldots, N_{k-1}\}$ satisfying certain conditions, properties of the set of invertible quadratic residues of the ring R are described in terms of properties of the set of invertible quadratic residues of the quotient ring R/N_1

Keywords Lifting method · Units · Quadratic residues

1 Introduction

Quadratic residues [1] have been studied since the 17th and 18th century by P. de Fermat, L. Euler, J.L. Lagrange A.M. Legendre, among other mathematicians. Nowadays quadratic residues are still a topic of study ([2]),[3–6]) and they have applications in areas which include acoustical engineering ([7]), cryptography ([8, 9]), in the study of Paley (conference) graphs, primality testing (Solovay-Strassen, Miller-Rabin), and integer factorization (quadratic sieve, number field sieve).

In this note, by considering R a commutative ring with a collection of ideals $\{N_1, N_2, \ldots, N_{k-1}\}$ satisfying the CNC-condition given in Definition 1, properties of

Communicated by Francisco Cesar Polcino Milies.

César A. Hernández Melo and Horacio Tapia-Recillas have contributed equally to this work.

✉ Fernanda D. de Melo Hernández
fdmelo@uem.br

César A. Hernández Melo
cahmelo@uem.br

Horacio Tapia-Recillas
htr@xanum.uam.mx

[1] Departamento de Matemática, Universidade Estadual de Maringá, Av. Colombo 5790, Maringá, PR 87020-900, Brazil

[2] Departamento de Matemáticas, Universidad Autónoma Metropolitana-Iztapalapa, Av. San Rafael Atlixco 186, 09340 Mexico, Cdmx, Mexico

Published online: 02 May 2024

invertible quadratic residues in R are described in terms of properties of invertible quadratic residues in the quotient ring R/N_1, i.e., the properties are "lifted" from those of a quotient ring. Recently, this class of rings has been studied in ([10–12]) to obtain properties of idempotent elements, invertible elements and a generalization of the Euler-Fermat Theorem using lifting method. In essence, the proof of the results discussed in those works are based on the existence of a multiplicative function H from R/N_1 to R that preservers the essencial characteristics of the elements in the quotient ring R/N_1, for more details see Proposition 5. In this manuscript, the ideas in the works cited above are adapted to the study of invertible quadratic residues.

Examples of rings that satisfy the CNC-conditions include the integer modules p^k, $\mathbb{Z}_{p^k}$, where p is a prime number and k is a positive integer, finite chain rings, the ring group RG with Galois ring R and commutative group G and the polynomial ring $R[x]$ where R is a commutative ring containing a collection of ideals satisfying the CNC-condition.

The manuscript is divided in four sections. In Sect. 2 notation and facts needed in the rest of the manuscript are presented. In section 3 the main results are given and in Sect. 4 applications of the results previously discussed are considered. Examples are given to illustrate the main results.

2 Notations and basic facts

Given R an associative ring with identity and N a nil ideal of R, we begin our discussion recalling that units of the quotient ring R/N can be lifted to the ring R. More precisely, if R^* and $(R/N)^*$ denote the group of units of the ring R and R/N respectively, the following result holds.

Proposition 1 *Let R be an associative ring with identity, N a nil ideal of R and $\bar{\ }: R \longrightarrow R/N$ the canonical homomorphism from R to the quotient ring R/N. Then,*

1. $\bar{f} = f + N \in (R/N)^*$ *if and only if* $f + N \subset R^*$.
2. *If R is finite the cardinality of R^* and the cardinality of $(R/N)^*$ are related by the relation*

$$\mid R^* \mid = \mid N \mid\mid (R/N)^* \mid . \tag{1}$$

Proof The proof of this proposition can be found in [11], Proposition 2.1 and Remark 2.2. □

Recall that an element a of a ring R is a *quadratic residue*, if there exists $x \in R$ such that $x^2 = a$ ([1, 13, 14]). Given N an ideal of R, it is clear that if a is a quadratic residue in the ring R, then $a + N$ is a quadratic residue in the quotient ring R/N. The following proposition provides sufficient conditions to prove the converse of this statement, as it will be seen, proposition 1 will be essential in the proof that will be presented.

Proposition 2 *Let R be a commutative ring with identity and N a nil ideal of R. If $(g+N)^2 = a+N$ and $2g+N$ is an invertible element in R/N, then the function*

$$\eta : g+N \to a+N \quad \text{given by} \quad \eta(g+m) = (g+m)^2,$$

is bijective. In other words, if $a+N$ is a quadratic residue in R/N, then every element $b \in a+N$ is a quadratic residue in the ring R and, and for all $b \in a+N$ the quadratic equation

$$y^2 = b$$

has a unique solution in the set $g+N \subset R$.

Proof Since $(g+N)^2 = a+N$, it is clear that the function η is well defined. Since N is a nil ideal of R and $2g+N$ is an invertible element in R/N it follows from Proposition 1 that for all $p \in N$, the element $2g+p$ is an invertible element in R. Thus, if $\eta(g+m_1) = \eta(g+m_2)$ then,

$$(2g+m_1+m_2)(m_1-m_2) = 0.$$

Since $2g+m_1+m_2$ is an invertible element in the ring R, it is concluded that $m_1 = m_2$. Therefore η is an injective function. Now, we show that η is surjective. First of all, note that since $(g+N)^2 = a+N$, there exists $n_0 \in N$, such that $g^2 = a+n_0$. Now, given $n \in N$, it is easy to see that

$$\eta(g+(2g)^{-1}(n-n_0)) = a+n,$$

which proves the claim. □

Now, definitions and notation that will be useful in the rest of the manuscript are introduced. The set $q(R^*)$ will denote the quadratic residues in the ring R that are also units in R, that is

$$q(R^*) = \{a \in R; a \text{ is a quadratic residue in } R \, \text{and} \, a \in R^*\}.$$

For a a quadratic residue in the ring R, $s(a)$ will denote the set of solutions of the equation $x^2 = a$ in the ring R. In other words,

$$s(a) = \{x \in R; x^2 = a\}.$$

Finally, if N is an ideal in ring R and $a \in R$, $T(a+N)$ will be denote the set of solutions of the equation $x^2 = b$, when b varies in the equivalence class $a+N \in R/N$, in other words

$$T(a+N) = \{y \in R; y^2 \in a+N\}.$$

Based on propositions 1 and 2, sufficient conditions to lift quadratic residues from the quotient ring *R*/*N* in ring *R*, where *N* is a nil ideal of the ring *R* are established. In addition if *R* is finite, formulas relating the cardinality of the sets $N, s(b), s(b+N), R^*, (R/N)^*, q(R^*)$ and $q((R/N)^*)$ are given.

Proposition 3 *Let R be a commutative ring with identity and N a nil ideal of R such that* $2+N$ *is an invertible element in R/N. The following statements hold,*

1. $a+N \in q((R/N)^*)$ *if and only if* $a+N \subset q(R^*)$.
2. *The cardinality of the set* $q(R^*)$ *satisfies*

$$\mid q(R^*) \mid = \mid N \mid\mid q((R/N)^*) \mid . \tag{2}$$

3. *If* $a+N \in q((R/N)^*)$, *then for all* $b \in a+N$ *the number of solutions of the quadratic equation*

$$y^2 = b$$

in the ring *R* is equal to the number of solutions of the quadratic equation

$$y^2 = b+N$$

in the ring *R*/*N*. In other words

$$\mid s(b) \mid = \mid s(a+N) \mid$$

for all $b \in a+N$.

4. *The cardinality of the set* R^* *satisfies the following relation*

$$\mid R^* \mid = \mid N \mid \sum_{a+N \in q((R/N)^*)} \mid s(a+N) \mid . \tag{3}$$

5. *If in addition, there exists* α *such that* $\mid s(a+N) \mid = \alpha$ *for all* $a+N \in q((R/N)^*)$,

$$\begin{aligned} &a)\ \mid q((R/N)^*) \mid = \frac{\mid (R/N)^* \mid}{\alpha} \\ &b)\ \mid q(R^*) \mid = \frac{\mid N \mid\mid (R/N)^* \mid}{\alpha} \\ &c)\ \mid q(R^*) \mid = \frac{\mid R^* \mid}{\alpha}. \end{aligned} \tag{4}$$

Proof 1. It is easy to see that if $a+N \subset q(R^*)$, then $a+N \in q((R/N)^*)$. Now we proved the other implication. Assuming $a+N \in q((R/N)^*)$, there exists $g+N \in R/N$ such that $(g+N)^2 = a+N$. Since $a+N$ and $2+N$ are invertible elements in the ring *R*/*N*, it follows that

$$(2+N)(g+N) = 2g+N$$

is an invertible element in R/N, thus proposition 2 implies that every element $b \in a+N$ is a quadratic residue in the ring R. In addition, since $a+N \in (R/N)^*$ and N is a nil ideal of the ring R, proposition 1 implies that for all $b \in a+N$, $b \in R^*$. This proofs that $a+N \subset q(R^*)$.

2. From claim 1, it follows that

$$q(R^*) = \bigcup_{a+N \in q((R/N)^*)} (a+N). \tag{5}$$

Then,

$$\mid q(R^*) \mid = \sum_{a+N \in q((R/N)^*)} \mid a+N \mid = \mid N \mid \sum_{a+N \in q((R/N)^*)} 1 = \mid N \mid\mid q((R/N)^*) \mid,$$

which proves relation (2).

3. Note that since $a+N \in q((R/N)^*)$, for all $b \in a+N$, $s(b) \neq \emptyset$. In order to prove that $\mid s(b) \mid = \mid s(a+N) \mid$, it will be shown that the canonical homomorphism $\phi : R \to R/N$ restricted to the set $s(b)$, namely

$$x \in s(b) \to \phi(x) = x+N$$

determines a bijection between $s(b)$ and $s(b+N)$. In fact, if $x \in s(b)$ then $x+N \in s(b+N)$, thus the function ϕ is well defined. Now, if $\phi(x) = \phi(y) = x+N$ with $x, y \in s(b)$, then $(x+N)^2 = b+N = a+N$ with $2x+N$ an invertible element in the ring R/N. So, proposition 2 implies that the function

$$z \in x+N \to \eta_1(z) = z^2 \in b+N$$

is bijective, hence, since $x, y \in x+N$ and $x^2 = y^2 = b$, the injectivity of the function η_1 implies that $x = y$. Now, if $t+N \in s(b+N)$, then $(t+N)^2 = b+N = a+N$. Since $2t+N$ is an invertible element in the ring R/N, proposition 2 implies that the function

$$z \in t+N \to \eta_2(z) = z^2 \in b+N$$

is bijective. Thus there exists $n_0 \in N$, such that $\eta_2(t+n_0) = (t+n_0)^2 = b$. Hence, $t+n_0 \in s(b)$ and $\phi(t+n_0) = t+N$, hence ϕ is a surjective function.

4. Note that the set R^* is a disjoint union of the sets $T(a+N)$ with $a+N \in q((R/N)^*)$, that is

$$R^* = \bigcup_{a+N \in q((R/N)^*)} T(a+N).$$

From this fact, it follows that

$$\mid R^* \mid = \sum_{a+N \in q((R/N)^*)} \mid T(a+N) \mid . \tag{6}$$

In order to compute $\mid T(a+N) \mid$, observe that $T(a+N)$ can be written as a disjoint union of the sets $s(b)$ with $b \in a+N$,

$$T(a+N) = \bigcup_{b \in a+N} s(b). \tag{7}$$

Thus, since for all $b \in a+N, \mid s(b) \mid = \mid s(a+N) \mid$,

$$\mid T(a+N) \mid = \sum_{b \in a+N} \mid s(b) \mid = \mid s(a+N) \mid \sum_{b \in a+N} 1 = \mid s(a+N) \mid\mid N \mid . \tag{8}$$

Finally, combining (6) and (8), relation in (3) follows easily.

5. Since $|s(a+N)| = \alpha$ for all $a+N \in q((R/N)^*)$, from relation (3), it follows that

$$\mid R^* \mid = \alpha \mid N \mid\mid q((R/N)^*) \mid, \tag{9}$$

and proposition (1) implies that,

$$\mid R^* \mid = \mid N \mid\mid (R/N)^* \mid . \tag{10}$$

Thus, by combining (9) and (10), relation in (5)-*a*) is obtained. The relation in (5)-*b*) is obtained from (2) and (5)-*a*). Finally, relation in (5)-*c*) is obtained from (10) and (5)-*b*). □

In the next lines the results in proposition 3 are illustrated with an example. Let p be a prime number different from 2, k a natural number and let $R = \mathbb{Z}_{p^k}$ be the ring of integers modulo p^k. It is clear that the ideal $N = \langle p \rangle$, is a nilpotent ideal of index k of the ring R. In addition,

$$\frac{R}{N} = \frac{\mathbb{Z}_{p^k}}{\langle p \rangle} \cong \mathbb{Z}_p,$$

thus $\mid (R/N)^* \mid = p-1$ and from Lagrange's theorem it follows that $\mid N \mid = p^{k-1}$. From the identity in (1), we have that $\mid R^* \mid = p^{k-1}(p-1)$. In addition, since, $R/N \cong \mathbb{Z}_p$ is a field of characteristic different from 2, it follows that the number α appearing in claim 5 of proposition 3 is $\alpha = 2$. From proposition 4, we conclude that:

- If $a \in \mathbb{Z}_{p^k}^*$, and $a \equiv b \mod (p)$, then a is a quadratic residue in $\mathbb{Z}_{p^k}$ if and only if b is a quadratic residue in the ring $\mathbb{Z}_p$.
- If $a \in q(\mathbb{Z}_{p^k}^*)$ and $a \equiv b \mod (p)$, then the number of solutions of the equation $x^2 = a$ in the ring $\mathbb{Z}_{p^k}$ is equal to the number of solutions of the equation $x^2 = b$ in the field $\mathbb{Z}_p$, which is equal to 2, in other words

  $$s(a) = s(b) = 2.$$

- The cardinality of the sets $q(\mathbb{Z}_p^*)$, $q(\mathbb{Z}_{p^k}^*)$ are given by

  $$\mid q(\mathbb{Z}_p^*) \mid = \frac{p-1}{2} \text{ and } \mid q(\mathbb{Z}_{p^k}^*) \mid = \frac{p^{k-1}(p-1)}{2},$$

  respectively.

Next, the previous proposition is extended to a direct product of a finite collection of rings.

Proposition 4 *Let $R_1, R_2, \dots, R_m$, be commutative rings with identity and let N_i be a nil ideal of the ring R_i, such that $2 + N_i \in (R_i/N_i)^*$ for each $i = 1, 2, \dots, m$. The following statements hold*:

1. $(a_1, \dots, a_m) \in q((R_1 \times \cdots \times R_m)^*)$ *if and only if* $a_i + N_i \in q((R/N_i)^*)$ *for every* i=1,2,...,m.
2. *If* $(a_1, \dots, a_m) \in q((R_1 \times \cdots \times R_m)^*)$ *then*
$$\mid s((a_1, \dots, a_m)) \mid = \mid s(a_1 + N_1) \mid \cdots \mid s(a_m + N_m) \mid . \tag{11}$$
3. *The cardinality of* $q((R_1 \times \cdots \times R_m)^*)$ *satisfies the following relation*
$$\mid q((R_1 \times \cdots \times R_m)^*) \mid = \mid N_1 \mid\mid q((R/N_1)^*) \mid \cdots \mid N_m \mid\mid q((R/N_m)^*) \mid \tag{12}$$
4. *If* $\mid s(a + N_i) \mid = \alpha_i$ *for all* $a + N_i \in q((R/N_i)^*)$, *then*
$$\mid q((R_1 \times \cdots \times R_m)^*) \mid = \frac{\mid N_1 \mid\mid (R/N_1)^* \mid \cdots \mid N_m \mid\mid (R/N_m)^* \mid}{\alpha_1 \alpha_2 \cdots \alpha_m}, \tag{13}$$
and
$$\mid q((R_1 \times \cdots \times R_m)^*) \mid = \frac{\mid (R_1 \times \cdots \times R_m)^* \mid}{\alpha_1 \alpha_2 \cdots \alpha_m}. \tag{14}$$

Proof The proof of this proposition is a simple consequence of the results above, so details are left to the reader. □

In the following lines the results of the previous proposition are illustrated with an example. Given n an odd natural number, if $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ denotes the prime factorization of n. The Chinese Remainder Theorem implies that

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

By setting $R_i = \mathbb{Z}_{p_i^{k_i}}$ and $N_i = \langle p_i \rangle$ for $i = 1, 2, \dots, m$, it is clear that $R_i/N_i \cong \mathbb{Z}_{p_i}$ and that $2 + N_i \in (R_i/N_i)^*$. Thus, from proposition 4, it is concluded that:

- If $a \in \mathbb{Z}_n^*$, and $a \equiv a_i \mod (p_i)$ for $i = 1, 2, \dots, m$, a is a quadratic residue in $\mathbb{Z}_n$ if and only if a_i is a quadratic residue in the ring $\mathbb{Z}_{p_i}$ for all $i = 1, 2, \dots, m$.
- If $a \in q(\mathbb{Z}_n^*)$ and $a \equiv b_i \mod (p_i^{k_i})$ for $i = 1, 2, \dots, m$, since $s(b_i + N_i) = 2$ for all $i = 1, 2, \dots, m$, the number of solutions of the equation $x^2 = a$ in the ring $\mathbb{Z}_n$ is equal to 2^m, in other words

$$s(a) = 2^m.$$

- The cardinality of the set $q(\mathbb{Z}_n^*)$ is given by

$$\mid q(\mathbb{Z}_n^*) \mid = \frac{p_1^{k_1-1}(p_1 - 1) \cdots p_m^{k_m-1}(p_m - 1)}{2^m}.$$

3 Main results

In this section we present our main results. For R a commutative ring containing a collection of ideals $\{N_1, N_2, \dots, N_{k-1}\}$ satisfying a certain condition (the CNC condition, Definition 1), properties of the set of invertible quadratic residues of the ring R are described in terms of properties of the set of invertible quadratic residues of the quotient ring R/N_1.

Proposition 5 *Let R be a commutative ring and N a nilpotent ideal of index $t \geq 2$ in R. Then the following statements hold*:

1. *For any prime number p such that $p \geq t$, for all $n \in N$ and $a \in R$,*

$$(a + n)^p = a^p + pnr,$$

   for some $r \in R$.
2. *In addition, assuming there exists a natural number $s > 1$ such that $sN = \{0\}$ and such that all the prime factors of s are greater than or equal to the nilpotency index t of the ideal N. The function $H : R/N \to R$ given by*

$$H(x + N) = x^s$$

   is well defined and it is multiplicative, i.e., it satisfies $H((x + N)(y + N)) = H(x + N)H(y + N)$, for all $x, y \in R$.
3. *Under the assumptions of claim* 1, *if $a + N$ is a quadratic residue in the quotient ring R/N, then $H(a + N) = a^s$ is a quadratic residue in R. More precisely, if $g \in R$ is such that $(g + N)^2 = a + N$, then*

$$(g^s)^2 = a^s.$$

Proof

1. Since $n^t = 0$,

$$(a+n)^p = \sum_{j=0}^{p} \binom{p}{j} a^{p-j}n^j = a^p + \sum_{j=1}^{t-1} \binom{p}{j} a^{p-j}n^j.$$

Since p is a prime number, p divides $\binom{p}{j}$ for all $1 \leq j \leq p-1$. Also, since $t \leq p$,

$$(a+n)^p = a^p + pn\left(k_1a^{p-1} + k_2a^{p-2}n + \cdots + k_{t-1}a^{p-t+1}n^{t-2}\right)$$

where $k_i = \binom{p}{i}/p$. Therefore,

$$(a+n)^p = a^p + pnr,$$

with $r = k_1a^{p-1} + k_2a^{p-2}n + \cdots + k_{t-1}a^{p-t+1}n^{t-2} \in R$.

2. Let $p_1, p_2, p_3, \ldots, p_m$ be the prime numbers, not necessarily different, appearing in the prime factor decomposition of the integer s, with $p_i \geq t$, for $i = 1, 2, 3, \cdots, m$. Since $y + N = x + N$, there exists $n \in N$ such that $y = x + n$. Since $p_1 \geq t$, from claim 1,

$$y^{p_1} = (x+n)^{p_1} = x^{p_1} + p_1nr_1,$$

for some $r_1 \in R$. Similarly, since $p_2 \geq t$ and $p_1nr_1 \in N$, it follows from claim 1 and the previous relation that

$$y^{p_1p_2} = (x^{p_1} + p_1nr_1)^{p_2} = x^{p_1p_2} + p_2(p_1nr_1)r_2,$$

for some $r_2 \in R$. In the same way, it is possible to verify that

$$y^{p_1p_2\cdots p_m} = x^{p_1p_2\cdots p_m} + (p_1p_2\cdots p_m)n(r_1r_2\cdots r_m),$$

with $r_1, r_2, \ldots, r_m \in R$. In other words,

$$y^s = x^s + sh,$$

where $h = nr_1r_2\cdots r_m \in N$. Finally, since $h \in N$ and $sN = 0$, it follows that $y^s = x^s$. Hence, the function H is well defined and it is easily verified that it is multiplicative.

3. Since $(g+N)^2 = a + N$, it follows that $(H(g+N))^2 = H(a+N)$, thus $(g^s)^2 = a^s$, i.e., a^s is a quadratic residue in the ring R.

□

An example illustrating the previous proposition is presented which it allows to discuss additional properties of the function H. Consider $R = \mathbb{Z}_{25}$ and $N = \langle 5 \rangle = \{0, 5, 10, 15, 20\}$. It is clear that N has nilpotency index $t = 2$, $sN = 0$ for $s = 5$ and

$$\frac{\mathbb{Z}_{25}}{\langle 5\rangle} \cong \mathbb{Z}_5.$$

- By setting $x + N = \overline{x}$, it is not difficult to see that $H(\overline{0}) = 0$, $H(\overline{1}) = 1$, $H(\overline{2}) = 7$, $H(\overline{3}) = 18$ and $H(\overline{4}) = 24$. Since, $\overline{0}, \overline{1}$ and $\overline{4}$ are the quadratic residues in the ring $\mathbb{Z}_{25}/\langle 5\rangle$, then 0, 1 and 24 are quadratic residues in the ring $\mathbb{Z}_{25}$.
- Since $(3+N)^2 = 4+N$ in $\mathbb{Z}_{25}/\langle 5\rangle$. From proposition 2, it follows that the function $\eta : \{3, 8, 13, 18, 23\} \to \{4, 9, 14, 19, 24\}$ given by $\eta(x) = x^2 \mod (25)$ is a bijective function, in particular, all the elements in the equivalence class $4+N$ are quadratic residues in the ring $\mathbb{Z}_{25}$. Thus, the only quadratic residue in the equivalence class $4+N$ that is mapping by the function H is 24.
- Since $H(1+N+1+N) = 7$ and $H(1+N) + H(1+N) = 1+1 = 2$, then the function H is not in general a ring homomorphism.

It is to be noticed that the hypothesis in claim 1 of Proposition 5, which requires that all prime factors of s be greater or equal than the nilpotency index t of the ideal N, restricts enormously the number of applications of that proposition. For instance, if we consider $R = \mathbb{Z}_{2^t}$ with $2 \leq t$ and $N = \langle 2\rangle$, it is clear that $N^t = \{0\}$ and $sN = \{0\}$ for $s = 2^{t-1}$. Thus, according to claim 1 of Proposition 5, in order to get quadratic residues in the ring R by computing the quadratic residues in the ring $R/N \cong \mathbb{Z}_2$, it is necessary that $t \leq 2$, therefore $t = 2$. Hence, we can only obtain quadratic residues in the ring $\mathbb{Z}_4$, which is easily done by hand. In the following lines, we show how to overcome such restrictions.

Definition 1 [10, Definition 3.2] We say that a collection $\{N_1, ..., N_k\}$ of ideals of a ring R satisfies the *CNC-condition* if the following properties hold:

1. **Chain condition:** $\{0\} = N_k \subset N_{k-1} \subset \cdots \subset N_2 \subset N_1 \subset R$.
2. **Nilpotency condition:** for $i = 1, 2, 3, \dots, k-1$, there exists $t_i \geq 2$ such that $N_i^{t_i} \subset N_{i+1}$.
3. **Characteristic condition:** for $i = 1, 2, 3, \dots, k-1$, there exists $s_i \geq 1$ such that $s_i N_i \subset N_{i+1}$. In addition, the prime factors of s_i are greater than or equal to t_i.

The minimum number t_i satisfying the nilpotency condition will be called the nilpotency index of the ideal N_i in the ideal N_{i+1}. Similarly, the minimum number s_i satisfying the characteristic condition will be called the characteristic of the ideal N_i in the ideal N_{i+1}.

The nilpotency condition and the characteristic condition of the previous definition can be stated as follows:

a. The nilpotency condition is equivalent to the following condition: for $i = 1, 2, \dots, k-1$, N_i/N_{i+1} is a nilpotent ideal of index t_i in the ring R/N_{i+1}, (for details see [10, Definition 3.2]).

b. The characteristic condition is equivalent to the following condition: for $i = 1, 2, \dots, k-1$, there exists a natural number $s_i \geq 1$ such that $s_i(N_i/N_{i+1}) = 0$ in the ring R/N_{i+1}, (for details see [10, Definition 3.2]).

Theorem 6 *Let R be a commutative ring, $\{N_1, N_2, \dots, N_k\}$ a collection of ideals of R satisfying the CNC-condition and let s_i be the characteristic of the ideal N_i in the ideal N_{i+1}. If $a + N_1$ is a quadratic residue in R/N_1, then $a^{s_1 s_2 \cdots s_{k-1}}$ is a quadratic residue in R. More precisely, if $g \in R$ is such that $(g + N_1)^2 = a + N_1$, then*

$$(g^{s_1 s_2 \cdots s_{k-1}})^2 = a^{s_1 s_2 \cdots s_{k-1}}. \tag{15}$$

Proof Note first that since the ideals N_i satisfy the chain condition given in definition 1, for all $i = 1, 2, \dots, k-1$, the following isomorphism holds

$$R/N_i \cong \frac{(R/N_{i+1})}{(N_i/N_{i+1})}. \tag{16}$$

In addition, since the ideals N_i satisfy the nilpotency condition and characteristic condition with characteristics s_i respectivelly, from claim 1 of proposition 5, it follows that for $i = 1, 2, \dots, k-1$, the functions

$$H_i : R/N_i \to R/N_{i+1}, \qquad H_i(x + N_i) = x^{s_i} + N_{i+1}$$

are well defined and multiplicative. Hence, if $(g + N_1)^2 = a + N_1$,

$$H_{k-1} \circ \cdots \circ H_1((g + N_1)^2) = H_{k-1} \circ \cdots \circ H_1(a + N_1),$$

whence the identity in (15) is obtained. □

Remark 1 It follows from the proof of the Theorem (6) that, if $a \in R$ is such that $a + N_1$ is a quadratic residue in R/N_1, then $H_1(a + N_1) = a^{s_1} + N_2$ is a quadratic residue in R/N_2. In the same way, $H_2(a^{s_1} + N_2) = a^{s_1 s_2} + N_3$ is a quadratic residue in R/N_3, and so on. At the end of this process, it is obtained that $a^{s_1 s_2 \cdots s_{k-1}}$ is a quadratic residue in R. The following chain of multiplicative functions,

$$\frac{R}{N_1} \xrightarrow{H_1} \frac{R}{N_2} \xrightarrow{H_2} \cdots \xrightarrow{H_{k-2}} \frac{R}{N_{k-1}} \xrightarrow{H_{k-1}} \frac{R}{N_k} = R, \quad \text{with} \quad H_i(x + N_i) = x^{s_i} + N_{i+1}$$

appears naturally in that process.

Theorem 7 *Let R be a commutative ring with identity, $\{N_1, N_2, \dots, N_k\}$ a collection of ideals of R satisfying both the Chain condition and the Nilpotency condition. Assuming that $2 + N_1 \in (R/N_1)^*$, the following claims hold*

1. *$a + N_1 \in q((R/N_1)^*)$ if and only if $a + N_1 \subset q(R^*)$.*
2. *The cardinality of the set $q(R^*)$ is given by*

$$| q(R^*) |=| N_1 || q((R/N_1)^*) | \tag{17}$$

3. *If* $a + N_1 \in q((R/N_1)^*)$, *then*

$$s(a) = s(a + N_{k-1}) = \cdots = s(a + N_1). \tag{18}$$

4. *If for each* $i = 1, 2, 3, \ldots, k - 1$, *there exists* α_i *such that,* $| s(a + N_i) |= \alpha_i$ *for all* $a + N_i \in q((R/N_i)^*)$, *then*

$$| (R/N_{i+1})^* |= \alpha_i | q((R/N_{i+1})^*) | . \tag{19}$$

In particular,

$$| R^* |= \alpha_{k-1} | q(R^*) | . \tag{20}$$

Proof 1. It is easy to see that if $a + N_1 \subset q(R^*)$, then $a + N_1 \in q((R/N_1)^*)$. Now, we proceed to prove the other implication of the statement. From the isomorphism given in (16), the fact that N_i/N_{i+1} is a nilpotent ideal of index t_i in the ring R/N_{i+1} and the fact that $2 + N_1 \in (R/N_1)^*$, from proposition (1), it follows that

$$(2 + N_{i+1}) + N_i/N_{i+1} \in ((R/N_{i+1})/(N_i/N_{i+1}))^*$$

for all $i \in 1, 2, 3, \ldots, k$. Now, let $b \in a + N_1$, since $b + N_1 = a + N_1 \in q((R/N_1)^*)$, it follows from the isomorphism

$$R/N_1 \cong \frac{(R/N_2)}{(N_1/N_2)},$$

that $(b + N_2) + N_1/N_2 \in q(((R/N_2)/(N_1/N_2))^*)$, thus, from claim 1 of proposition 3, it follows that

$$(b + N_2) + N_1/N_2 = \{b + n + N_2 ; n \in N_1\} \subset q((R/N_2)^*),$$

in particular, it is concluded that $b + N_2 \in q((R/N_2)^*)$. Similarly, from the isomorphism

$$R/N_2 \cong \frac{(R/N_3)}{(N_2/N_3)},$$

it follows that $(b + N_3) + N_2/N_3 \in q(((R/N_3)/(N_2/N_3))^*)$, thus, from item 1 of proposition 3, it follows that

$$(b + N_3) + N_2/N_3 = \{b + n + N_3 ; n \in N_2\} \subset q((R/N_3)^*),$$

in particular, we concluded that $b + N_3 \in q((R/N_3)^*)$. Continuing this process, it is finally shown that $b + N_k = \{b\} \in q((R/N_k)^*)$, which immediately implies that $b \in q(R^*)$. This shows that $a + N_1 \subset q(R^*)$, as we wanted to prove.

2. From the isomorphism given in (16) and item 2 of proposition 3, it follows that

$$\mid N_i/N_{i+1} \mid\mid q((R/N_i)^*) \mid = \mid q(((R/N_{i+1})/(N_i/N_{i+1}))^*) \mid = \mid q((R/N_{i+1})^*) \mid, \quad (21)$$

thus from Lagrange's theorem,

$$\begin{aligned} \mid q(R^*) \mid = \mid q((R/N_k)^*) \mid &= \frac{\mid N_{k-1} \mid}{\mid N_k \mid} \mid q((R/N_{k-1})^*) \mid \\ &= \frac{\mid N_{k-1} \mid}{\mid N_k \mid} \frac{\mid N_{k-2} \mid}{\mid N_{k-1} \mid} \cdots \frac{\mid N_1 \mid}{\mid N_2 \mid} \mid q((R/N_1)^*) \mid, \end{aligned}$$

whence the identity in (17) is obtained.

3. Again, from the isomorphism given in (16), it follows that

$$s(a+N_i) = s(a+N_{i+1}+N_i/N_{i+1})$$

for all $i = 1, 2, 3, \dots, k-1$. On the other hand, since N_i/N_{i+1} is a nilpotent ideal of index t_i in the ring R/N_{i+1} and the fact that $(2+N_{i+1})+N_i/N_{i+1} \in ((R/N_{i+1})/(N_i/N_{i+1}))^*$, from claim 3 of proposition 3, it follows that

$$s(a+N_{i+1}+N_i/N_{i+1}) = s(a+N_{i+1}).$$

for $i = 1, 2, 3, \dots, k-1$. From the previous identities, it follows that $s(a+N_i) = s(a+N_{i+1})$ for $i = 1, 2, 3, \dots, k-1$, this of course implies the equalities appearing in (18).

4. It follows from the isomorphism given in (16) and claim 4 of proposition 3 that

$$\mid (R/N_{i+1})^* \mid = \mid N_i/N_{i+1} \mid \sum_{a+N_i \in q((R/N_i)^*)} \mid s(a+N_i) \mid .$$

Since, $\mid s(a+N_i) \mid = \alpha_i$, it is deduced from the former identity that

$$\mid (R/N_{i+1})^* \mid = \alpha_i \mid N_i/N_{i+1} \mid\mid q((R/N_i)^*) \mid .$$

Finally, identity in (19) follows from (21). □

4 Applications of the main results

In this section Theorems 6 and 7 will be used in order to describe properties of the set of invertible quadratic residues for several classes of rings which include: rings containing a nilpotent ideal; group rings RG where R is a commutative ring containing a collection of ideals satisfying the CNC-condition and G is a commutative group; polynomial ring $R[x]$ where R is a commutative ring containing a collection of ideals satisfying the CNC-condition. Examples are given illustrating the results.

4.1 Rings containing a nilpotent ideal

If R is a commutative ring containing a nilpotent ideal N, by invoking Theorems 6 and 7, properties of the set of invertible quadratic residues of the ring R are described.

Proposition 8 *Let R be a commutative ring and N a nilpotent ideal of nilpotency index $k \geq 2$ in R. Then, the following statements hold,*

1. *Let $s > 1$ be the characteristic of the quotient ring R/N. If $a + N$ is a quadratic residue in R/N, then $a^{s^{k-1}}$ is a quadratic residue in R. More precisely, if $g \in R$ is such that $(g + N)^2 = a + N$, then*

$$\left(g^{s^{k-1}}\right)^2 = a^{s^{k-1}}. \tag{22}$$

2. *Assuming that $2 + N \in (R/N)^*$, the following claims hold,*

   a). $a + N \in q((R/N)^*)$ if and only if $a + N \subset q(R^*)$.
   b). The cardinality of the set $q(R^*)$ is given by

$$\mid q(R^*) \mid=\mid N \mid\mid q((R/N)^*) \mid \tag{23}$$

   c). If $a + N \in q((R/N)^*)$, then

$$s(a) = s(a + N^{k-1}) = \cdots = s(a + N). \tag{24}$$

   d). If there exists β such that, $|s(a + N)| = \beta$ for all $a + N \in q((R/N)^*)$, then

$$\mid (R/N^{i+1})^* \mid= \beta \mid q((R/N^{i+1})^*) \mid . \tag{25}$$

   In particular,

$$\mid R^* \mid= \beta \mid q(R^*) \mid . \tag{26}$$

Proof First it is shown that the collection $B = \{N, N^2, ..., N^k\}$ of ideals of the ring R satisfies the CNC-condition with nilpotency index and characteristic of the ideal N^i in the ideal N^{i+1} being $t_i = 2$ and $s_i = s$ for all $i = 1, 2, 3, \ldots, k - 1$. Thus,

1. It is clear that the collection B satisfies the chain condition.
2. Since $(N^i)^2 = N^{2i}$ and $i + 1 \leq 2i$ for all $i = 1, 2, 3, \ldots, k - 1$, it follows that $(N^i)^2 \subset N^{i+1}$. Hence, the collection B satisfies the nilpotency condition.
3. Since the ring R/N has characteristic s, there exists $n \in N$ such that $\sum_{i=1}^{s} 1_R = n$. Since

$$sN^i = (1_R + \cdots + 1_R)N^i = nN^i \subset N^{i+1}, \tag{27}$$

it follows that $sN^i \subset N^{i+1}$ for all $i = 1, 2, 3, \dots, k-1$. In addition, all prime factors of $s_i = s$ are greater or equal to the nilpotency index $t_i = 2$, proving that the collection B satisfies the characteristic condition.

Therefore, the proof of this proposition is now a clear consequence of Theorems 6 and 7 □

Example 1 Let p be an odd prime number, $i \in \mathbb{N}$ and let $R = \{a + bu{:}a, b \in \mathbb{Z}_{p^i}, u^2 = 0\}$. It is readily seen that R with the (obvious) addition and multiplication operations is a commutative ring with cardinality $|R| = p^{2i}$. It is also easily seen that R is isomorphic to the ring of polynomials with coefficients in $\mathbb{Z}_{p^i}$ modulo the ideal generated by x^2, that is $\mathbb{Z}_{p^i}[x]/\langle x^2\rangle$. It is readely seen that

$$R^* = \{a + bu;a \in (\mathbb{Z}_{p^i})^*, b \in \mathbb{Z}_{p^i}\},$$

so the cardinality of R^* is $\mid R^* \mid = \varphi(p^i)p^i = (p-1)p^{2i-1}$, where φ denotes the Euler totient function. On the other hand, it is verified that the ideal $N = \langle p, u\rangle$ has nilpotency index $k = i + 1$ and that $\mid N \mid = p^{2i-1}$, then it follows that N is a maximal ideal of R with

$$\frac{R}{N} \cong \mathbb{Z}_p,$$

whence $\mid (R/N)^* \mid = p - 1$ and the characteristic of the quotient ring R/N is $s = p$. From the latter isomorphism and proposition 8, it is concluded that

- $a + bu \in q(R^*)$ if and only if $a \mod (p) \in q(\mathbb{Z}_p^*)$.
- Let $a + bu \in R$ if $a \mod (p) \in q(\mathbb{Z}_p^*)$ then for all $b \in \mathbb{Z}_{p^i}$

  $$(a + bu)^{p^i} = (a \mod (p))^{p^i}$$

  is an invertible quadratic residue in R.
- The number of invertible quadratic residues of the ring R is given by

  $$\mid q(R^*) \mid = \mid N \mid\mid q((R/N)^*) \mid = \frac{p^{2i-1}(p-1)}{2}$$

- Let $a + bu \in R$, if $a \mod (p) \in q(\mathbb{Z}_p^*)$ then for all $b \in \mathbb{Z}_{p^i}$ the number of solutions in R of the equation $x^2 = a + bu$ is equal to 2, in other words

  $$s(a + bu) = 2.$$

An easy application of the previous result is the following:

Corollary 9 *Let R be a commutative ring and c a nilpotent element of index $k \geq 2$ in R. Then, the following statements hold*:

1. *Let $s > 1$ be the characteristic of the quotient ring $R/\langle c\rangle$. If $a + \langle c\rangle$ is a quadratic residue in $R/\langle c\rangle$, then $a^{s^{k-1}}$ is a quadratic residue in R. More precisely, if $g \in R$ is such that $(g + \langle c\rangle)^2 = a + \langle c\rangle$, then*

$$\left(g^{s^{k-1}}\right)^2 = a^{s^{k-1}}. \tag{28}$$

2. *Assuming that $2 + \langle c\rangle \in (R/\langle c\rangle)^*$, the following claims hold:*

   a. *$a + \langle c\rangle \in q((R/\langle c\rangle)^*)$ if and only if $a + \langle c\rangle \subset q(R^*)$.*

   b. *The cardinality of the set $q(R^*)$ is given by*

$$\mid q(R^*) \mid=\mid \langle c\rangle \mid\mid q((R/\langle c\rangle)^*) \mid . \tag{29}$$

   c. *If $a + \langle c\rangle \in q((R/\langle c\rangle)^*)$, then*

$$s(a) = s(a + \langle c^{k-1}\rangle) = \cdots = s(a + \langle c\rangle). \tag{30}$$

   d. *If there exists β such that $\mid s(a + \langle c\rangle) \mid= \beta$ for all $a + \langle c\rangle \in q((R/\langle c\rangle)^*)$, then*

$$\mid (R/\langle c^{i+1}\rangle)^* \mid= \beta \mid q((R/\langle c^{i+1}\rangle)^*) \mid . \tag{31}$$

   In particular,

$$\mid R^* \mid= \beta \mid q(R^*) \mid . \tag{32}$$

Proof Since R is a commutative ring, $\langle c\rangle$ is a nilpotent ideal of nilpotency index k in R, and the result follows immediately from Proposition 8 □

4.2 Group rings

If R is a commutative ring containing a collection of ideals satisfying the CNC-condition and G is a commutative group, by invoking Theorems 6 and 7, properties of the set of invertible quadratic residues of the group ring RG are described.

Proposition 10 *Let R be a commutative ring and G a commutative group. Let $\{N_1, N_2, \ldots, N_k\}$ be a collection of ideals of R satisfying the CNC-condition. Then, the following statements hold:*

1. *Let s_i be the characteristic of the ideal N_i in the ideal N_{i+1}. If $a + N_1G$ is a quadratic residue in $(R/N_1)G$, then $a^{s_1s_2\cdots s_{k-1}}$ is a quadratic residue in RG. More precisely, if $g \in RG$ is such that $(g + N_1G)^2 = a + N_1G$, then*

$$(g^{s_1s_2\cdots s_{k-1}})^2 = a^{s_1s_2\cdots s_{k-1}}. \tag{33}$$

2. *Assuming that $2 + N_1G \in ((R/N_1)G)^*$, then the following claims hold:*

a. $a+N_1G \in q(((R/N_1)G)^*)$ *if and only if* $a+N_1G \subset q((RG)^*)$.

b. *The cardinality of the set* $q((RG)^*)$ *is given by*

$$\mid q((RG)^*) \mid = \mid N_1 \mid^{|G|} \mid q(((R/N_1)G)^*) \mid . \tag{34}$$

c. *If* $a+N_1G \in q(((R/N_1)G)^*)$ *then*,

$$s(a) = s(a+N_{k-1}G) = \cdots = s(a+N_1G). \tag{35}$$

d. *If there exists* β *such that* $|s(a+N_1G)| = \beta$ *for all* $a+N_1G \in q(((R/N_1)G)^*)$ *then*,

$$\mid ((R/N_{i+1})G)^* \mid = \beta \mid q(((R/N_{i+1})G)^*) \mid, \tag{36}$$

for $i = 1, 2, \cdots, k-1$. In particular,

$$\mid (RG)^* \mid = \beta \mid q((RG)^*) \mid . \tag{37}$$

Proof In [11] (Proposition 4.9), it is shown that the collection

$$B = \{N_1G, N_2G, \ldots, N_kG\}$$

of ideals of the ring RG satisfies the CNC-condition with nilpotency index and characteristic of the ideal N_iG in the ideal $N_{i+1}G$ being exactly the same nilpotency index and characteristic of the ideal N_i in the ideal N_{i+1}. Therefore, the proof of this proposition is a direct conequence of Theorems 6 and 7. □

Corollary 11 *Let G be a commutative group*, *R be a commutative ring and N a nilpotent ideal of index k in R*. *Then*, *the following statements hold*:

1. *Let* $s > 1$ *be the characteristic of the quotient ring R/N. If* $a+NG$ *is a quadratic residue in* $(R/N)G$, *then* $a^{s^{k-1}}$ *is a quadratic residue in RG*. *More precisely*, *if* $g \in RG$ *is such that* $(g+NG)^2 = a+NG$, *then*

$$\left(g^{s^{k-1}}\right)^2 = a^{s^{k-1}}. \tag{38}$$

2. *Assuming that* $2+NG \in ((R/N)G)^*$, *the following claims hold*

a. $a+NG \in q(((R/N)G)^*)$ *if and only if* $a+NG \subset q((RG)^*)$.

b. *The cardinality of the set* $q((RG)^*)$ *is given by*

$$\mid q((RG)^*) \mid = \mid N \mid^{|G|} \mid q(((R/N)G)^*) \mid . \tag{39}$$

c. *If* $a+NG \in q(((R/N)G)^*)$, *then*

$$s(a) = s(a+N^{k-1}G) = \cdots = s(a+NG). \tag{40}$$

d. *If there exists β such that* $\mid s(a+NG) \mid = \beta$ *for all* $a+NG \in q(((R/N)G)^*)$ *then,*

$$\mid ((R/N^{i+1})G)^* \mid = \beta \mid q(((R/N^{i+1})G)^*) \mid, \tag{41}$$

for $i = 1, 2, \cdots, k-1$. In particular,

$$\mid (RG)^* \mid = \beta \mid q((RG)^*) \mid . \tag{42}$$

Proof The proof of this corollary is a direct consequence of Proposition 10 and the fact that the collection $\{N, N^2, ..., N^k\}$ of ideals of the ring R satisfies the CNC-condition with constant characteristic $s_i = s$ for all $i = 1, 2, 3, \cdots, k-1$. □

Example 2 Let p be an odd prime number, $i \in \mathbb{N}$ and let $R = \{a + bu{:}a, b \in \mathbb{Z}_{p^i}, u^2 = 1\}$ be the group ring $\mathbb{Z}_{p^i}G$ where $G = \{1, u\}$ is the cyclic group of order $n = 2$. It is readily seen that R with the (obvious) addition and multiplication operations is a commutative ring with cardinality $\mid R \mid = p^{2i}$. It is also easily seen that R is isomorphic to the ring of polynomials with coefficients in $\mathbb{Z}_{p^i}$ modulo the ideal generated by $x^2 - 1$ in R, that is $\mathbb{Z}_{p^i}G \cong \mathbb{Z}_{p^i}[x]/\langle x^2 - 1\rangle$. It is readily seen that

$$(\mathbb{Z}_p G)^* = \{a + bu \,:\, a \neq b, a \neq -b\},$$

so the cardinality of $(\mathbb{Z}_p G)^*$ is $\mid (\mathbb{Z}_p G)^* \mid = (p-1)^2$. In addition, since $N = \langle p \rangle$ has nilpotency index $k = i$ in $\mathbb{Z}_{p^i}$, and

$$\frac{\mathbb{Z}_{p^i}G}{\langle p \rangle G} \cong \mathbb{Z}_p G,$$

then it is deduced that $\mid (\mathbb{Z}_{p^i}G)^* \mid = \mid (\mathbb{Z}_p G)^* \mid\mid \langle p \rangle G \mid = (p-1)^2 p^{2(i-1)}$. From the latter isomorphism and the proposition 11, it is concluded that:

- $a + bu \in q((\mathbb{Z}_{p^i}G)^*)$ if and only if $(a \mod (p)) + (b \mod (p))u \in q((\mathbb{Z}_p G)^*)$.
- Let $a + bu \in \mathbb{Z}_{p^i}G$, if $(a \mod (p)) + (b \mod (p))u \in q((\mathbb{Z}_p G)^*)$, then

  $$(a + bu)^{p^{i-1}} = ((a \mod (p)) + (b \mod (p))u)^{p^{i-1}}$$

  is an invertible quadratic residue in $R = \mathbb{Z}_{p^i}G$.
- The number of invertible quadratic residues of the ring R is given by

  $$\mid q((\mathbb{Z}_{p^i}G)^*) \mid = \mid N \mid^{|G|} \mid q((\mathbb{Z}_p G)^*) \mid = p^{2(i-1)} \mid q((\mathbb{Z}_p G)^*) \mid$$

- Let $a + bu \in \mathbb{Z}_{p^i}G$, if $(a \mod (p)) + (b \mod (p))u \in q((\mathbb{Z}_p G)^*)$ and $\mid s((a \mod (p)) + (b \mod (p))u) \mid = \beta$, then

  $$\mid s(a + bu) \mid = \beta.$$

If additionally, $\mid s((a \mod (p)) + (b \mod (p))u) \mid = \beta$ for all $(a \mod (p)) + (b \mod (p))u \in q((\mathbb{Z}_p G)^*)$ then,

$$\mid (\mathbb{Z}_{p^i} G)^* \mid = \beta \mid q((\mathbb{Z}_{p^i} G)^*) \mid .$$

For instance, if $p = 3$, it is easy to see that $q((\mathbb{Z}_3 G)^*) = \{1\}$ and the number of solutions in $\mathbb{Z}_3 G$ of the equation $x^2 = 1$ is equal to 4, in other words $|s(1)| = 4$. Thus, if $a + bu \in \mathbb{Z}_{3^i} G$ is such that $a \equiv 1 \mod (3)$ and $b \equiv 0 \mod (3)$, then

$$(a + bu)^{3^{i-1}} = 1,$$

$\mid s(a + bu) \mid = 4, \mid q((\mathbb{Z}_{3^i} G)^*) \mid = 3^{2(i-1)}$ and $\mid (\mathbb{Z}_{3^i} G)^* \mid = (4)3^{2(i-1)}$.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no Conflict of interest.

References

1. Ireland, K., Rosen, M.: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics, vol. 84. Springer, New York (1990)
2. Chowla, S., Friedlander, J.: Class number and quadratic residues. Glasgow Math. J. **17**(1), 47–52 (1976)
3. Lev, V.F., Sonn, J.: Quadratic residues and difference sets. Q. J. Math. **68**(1), 79–95 (2017)
4. Burgess, D.A.: A note on the distribution of quadratic residues and non-residues. J. London Math. Soc. **38**, 253–256 (1963)
5. Petrov, F., Sun, Z.: Proof of some conjectures involving quadratic residues. Electron. Res. Arc. **28**(2), 589–597 (2020)
6. Sárközy, A.: On additive decompositions of the set of quadratic residues modulo *p*. Acta Arith. **155**, 41–51 (2012)
7. Schroeder, M.R.: The distribution of quadratic residues and non-residues in the Goldwasser-Micali type of cryptosystem. J. Acoust. Soc. Am. **65**(4), 958–963 (1979)
8. Jusutus, B.: The distribution of quadratic residues and non-residues in the Goldwasser-Micali type of cryptosystem. J. Math. Cryptol. **29**(2), 115–137 (2015)
9. Hofheinz, D., Kiltz, E.: The group of signed quadratic residues and applications. In: Halevi, S. (ed.) Advances in Cryptology - CRYPTO 2009, pp. 637–653. Springer, Berlin, Heidelberg (2009)
10. de Melo Hernández, F., Hernández Melo, C.A., Tapia-Recillas, H.: On idempotents of a class of commutative rings. Commun. Algebra (2020). https://doi.org/10.1080/00927872.2020.1754424
11. de Melo Hernández, F., Hernández Melo, C.A., Tapia-Recillas, H.: A recursive construction of units in a class of rings. Preprint at arXiv:1911.07743 (2020)
12. de Melo Hernández, F., Hernández Melo, C.A., Tapia-Recillas, H.: Fermat's little theorem and Euler's theorem in a class of rings. Commun. Algebra (2022). https://doi.org/10.1080/00927872.2021.2024841
13. Niven, I., Zuckerman, H.S., Montgomery, H.L.: An Introduction to the Theory of Numbers. Wiley, New York (1991)
14. Wright, S.: Quadratic Residues and Non-residues: Selected Topics. Lecture Notes in Mathematics, vol. 2171. Springer, Cham (2016)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

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 $\lambda_k = \beta^{\frac{k}{n}}$, $k = 2, \ldots, n-1$ and let $\omega \in \mathbb{F}$ be an n$^{\text{th}}$-root of unity. Let $\mathcal{F} \in \mathcal{M}_n(\mathbb{F})$ be defined by

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

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 $D_\lambda = \operatorname{diag}(1, \lambda_1, \lambda_2, \ldots, \lambda_{n-1})$ *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 $D_\lambda = \operatorname{diag}(1, \lambda_1, \lambda_2, \ldots, \lambda_{n-1})$. 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 $D_{\lambda^{-1}} = \operatorname{diag}(1, \lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_{n-1}^{-1})$. □

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* $\operatorname{rcirc}_\beta(\mathbf{a}) \in \mathcal{M}_n(\mathbb{F})$ *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 $\mathbb{F}_9 = \{a_0 + a_1x \mid a_0, a_1 \in \mathbb{F}_3, x^2 + 2x + 2 = 0$. 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)

São Paulo Journal of Mathematical Sciences
https://doi.org/10.1007/s40863-024-00412-z

ORIGINAL ARTICLE

Cyclic codes over the ring $\mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$

Horacio Tapia-Recillas[1] · J. Armando Velazco-Velazco[1]

Accepted: 12 February 2024

Abstract

The purpose of this manuscript is two-fold. First, properties of the ring $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$ and the set of ideals are established. Second, results on cyclic codes of length n, $\gcd(2, n) = 1$, over the non-chain Frobenius ring $\mathcal{R}_k$ and their description by means of idempotent elements are presented.

Keywords Finite ring · Frobenius ring · Cyclic codes · Idempotent elements

Mathematics Subject Classification 94B05 · 94B15 · 94B99

1 Introduction

Cyclic codes over finite rings have been studied intensively during the last decades after the seminal work of Hammons et al. [1]. Results on cyclic codes over finite chain rings appear in several manuscripts such as [2–4]. Cyclic and constacyclic codes over some non-chain finite commutative Frobenius rings with identity have been discussed in various papers including [5]. Results on linear and cyclic codes over the ring $\mathbb{Z}_q + u\mathbb{Z}_q$ where u satisfies $u^2 = 0$ and $q = p^m$, p a prime, are presented in [6, 7] and [8] for the case $q = 4$ and in [9] for the case $q = 8$.

The present work is two-fold. First, properties of the ring $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$, $k > 1$, including the fact that it is a finite non-chain Frobenius ring, and the set of ideals, particularly principal ideals, are given. Second, results on cyclic codes of odd length over this ring are presented which are described by means of idempotent elements.

Communicated by Sergio R. López-Permouth.

J. Armando Velazco-Velazco contributed equally to this work.

✉ J. Armando Velazco-Velazco
oczalevaj@gmail.com

Horacio Tapia-Recillas
htr@xanum.uam.mx

[1] Departamento de Matemáticas, Universidad Autónoma Metropolitana-I,
Ciudad de México 09340, México

Published online: 18 March 2024

The manuscript is organized as follows: In Sect. 2 the necessary background material is given. In Sect. 3 results on the ring $\mathcal{R}_k$, $k > 1$, are presented and in Sect. 4 we give results about the set of ideals of the ring, particularly principal ideals. Section 5 is devoted to results on cyclic codes of odd length over the mentioned ring, described by means of idempotent elements. In Sect. 6 examples are provided illustrating the main results of the manuscript, and the Conclusions are given in Sect. 7.

2 Preliminaries

In this section definitions and basic results from commutative algebra used in the manuscript are recalled. We refer the reader to [10] and [11] for details. By a ring R we mean a commutative ring with identity ($1 \in R$). Given a nonempty subset $S \subseteq R$, the ideal generated by S will be denoted by $\langle S \rangle$, i.e., $\langle S \rangle = \{\sum_{i=1}^{m} r_i s_i \mid r_i \in R, s_i \in S, m \in \mathbb{N}\}$. If $S = \{s_1, \dots, s_n\}$, it will be written $\langle s_1, \dots, s_n \rangle$ for $\langle S \rangle$. The annihilator of an R-module M is the ideal $Ann(M) = \{r \in R \mid r \cdot M = 0\}$.

An R-module M is simple if and only if $M \cong R/\mathfrak{m}$, where $\mathfrak{m}$ is a maximal ideal of R, i. e., M has no nonzero submodules. The length of M, $\ell_R(M)$, is the number of links of the composition series for M or ∞ if M has no a finite composition series, where by a composition series we mean a chain $M = M_0 \supset M_1 \supset \dots \supset M_{l-1} \supset M_l = \langle 0 \rangle$ such that each M_i/M_{i+1} is a nonzero simple module. When $\ell_R(M) < \infty$ this number is unique by the Jordan–Hölder theorem (see [10], Proposition 6.7).

The ring R is called local if it has a unique maximal ideal $\mathfrak{m}$. If R is a local ring with maximal ideal $\mathfrak{m}$, the quotient ring $R/\mathfrak{m}$ is the residue field of R, which is a finite field $\mathbb{F}_q$ where $q = p^m$ for some prime p and m a positive integer. This information is indicated by $(R, \mathfrak{m}, R/\mathfrak{m})$ or $(R, \mathfrak{m}, \mathbb{F}_q)$.

One of the algebraic structures to be considered in this work is the Frobenius ring. There are several (equivalent) definitions of a Frobenius ring (see [12, 13]), although for our purpose the following is enough: let $(R, \mathfrak{m}, R/\mathfrak{m})$ be a finite local ring. Then R is Frobenius if and only if $Soc(R)$ is a simple R-module. In particular $\dim_{R/\mathfrak{m}} Ann(\mathfrak{m}) = 1$ where $Ann(\mathfrak{m})$ is the annihilator ideal of $\mathfrak{m}$. The group of units of R is denoted by $\mathcal{U}(R)$. A ring R is called a chain ring if its collection of ideals is totally ordered by inclusion. Given a finite local ring $(R, \mathfrak{m}, \mathbb{F}_q)$, there is a natural homomorphism $\mu : R \longrightarrow \mathbb{F}_q$ given by $\mu(r) = \overline{r} = r + \mathfrak{m}$, which extends naturally to $\mu : R[x] \longrightarrow \mathbb{F}_q[x]$ as: if $f(x) = a_0 + a_1 x + \dots + a_n x^n \in R[x]$ then $\mu(f)(x) = \overline{f} = \overline{a_0} + \overline{a_1} x + \dots + \overline{a_n} x^n$, where $\mu(a_i) = \overline{a_i}$. We say that a monic polynomial $f(x) \in R[x]$ is basic irreducible if $\overline{f}(x) \in \mathbb{F}_q[x]$ is irreducible. Hensel's lemma (see [11], Theorem XIII.4) guarantees that given a factorization as a product of pairwise coprime polynomials over $\mathbb{F}_q[x]$ it lifts to a factorization of basic irreducible coprime polynomials over $R[x]$. If I is an ideal of a ring R, the set $I[x] = \{r_0 + r_1 x + \dots + r_n x^n \in R[x] \mid r_i \in I, 0 \le i \le n\}$ is an ideal of $R[x]$. If I is an ideal of a ring R and R a subring of a ring S, the ideal IS is called the extension of I to S.

3 The ring $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$

Let $\mathcal{R}_k := \{a + ub \mid a, b \in \mathbb{Z}_{2^k}, k > 1, u^2 = 0\}$ where $\mathbb{Z}_{2^k}$ is the ring of integers modulo 2^k. As usual we take the complete residual system $\{0, 1, 2, \dots, 2^k - 1\}$ as the respective set of class representatives for $\mathbb{Z}_{2^k}$.

Some properties of the ring $\mathcal{R}_k$ are sumarized in the following,

Proposition 1 *Let $\mathcal{R}_k = \{a + ub \mid a, b \in \mathbb{Z}_{2^k}, k > 1, u^2 = 0\}$. Then*

(i)*The ring $\mathcal{R}_k$ has cardinality 2^{2k} and it is isomorphic to $\mathbb{Z}_{2^k}[U]/\langle U^2 \rangle$.*
(ii)The ring $(\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}, \mathfrak{m} = \langle 2, u \rangle, \mathcal{R}_k/\mathfrak{m} \cong \mathbb{F}_2)$ is a local non-chain Frobenius ring with nilpotency index of $\mathfrak{m}$ equal to $t = k + 1$.
(iii)The group of units of the ring is $\mathcal{U}(\mathcal{R}_k) = \{a + ub \mid a \in \mathcal{U}(\mathbb{Z}_{2^k})\}$ with $|\mathcal{U}(\mathcal{R}_k)| = \varphi(2^{2k}) = 2^{2k-1}$.
(iv)The j-power of the maximal ideal $\mathfrak{m}$ is $\mathfrak{m}^j = \langle 2^j, 2^{j-1}u \rangle$ and it has cardinality $2^{2(k-j)+1}$ for $j = 1, 2, \dots, k$.
(v)*The ring $\mathcal{R}_k$ has length $\ell_{\mathcal{R}_k}(\mathcal{R}_k) = 2k$.*

Proof It is easy to see that the ideal $\langle 2, u \rangle$ generated by 2 and u is the unique maximal ideal of $\mathcal{R}_k$. Observe that the ideals $\langle u \rangle$ and $\langle 2^j \rangle$ for $1 \le j \le k - 1$ are not comparable by inclusion so $\mathcal{R}_k$ is not a chain ring. By observing that $Ann(\langle 2, u \rangle) = \langle 2^{k-1}u \rangle$, the fact the ring is Frobenius follows from the definition. In order to prove (v), just note that

$$\mathcal{R}_k \supset \mathfrak{m} \supset \langle 2 \rangle \supset \cdots \supset \langle 2^{j-1} \rangle \supset \mathfrak{m}^j = \langle 2^j, 2^{j-1}u \rangle \supset \langle 2^j \rangle \supset \cdots \supset \mathfrak{m}^k \supset \mathfrak{m}^{k+1} = \langle 0 \rangle$$

is a composition series for the ring $\mathcal{R}_k$. The rest of the claims are obvious. □

4 The set of ideals of $\mathcal{R}_k$

Since the maximal ideal of $\mathcal{R}_k$ is generated by two elements, the other ideals of the ring are also generated by at most two elements. In the following lines results on the set $\mathcal{L}_k$ of ideals of the ring $\mathcal{R}_k$ are presented, in particular the number of principal ideals is determined.

4.1 Principal ideals

We observe that if $I = \langle 2^d\alpha + \beta u \rangle$ is a principal ideal of $\mathcal{R}_k$ with $\alpha \in \mathcal{U}(\mathbb{Z}_{2^k})$, $\beta \in \mathbb{Z}_{2^k}$, then $I = \langle 2^d + \nu u \rangle$ for some $\nu \in \{0, 1, 2, \dots, 2^d - 1\}$.

Table 1 Number of fixed elements $|X^\gamma|$ in the ring $\mathcal{R}_3$ by each unit γ

γ	$\|X^\gamma\|$	γ	$\|X^\gamma\|$	γ	$\|X^\gamma\|$	γ	$\|X^\gamma\|$
1	64	$1+5u$	8	$3+6u$	4	$5+7u$	8
3	4	$1+6u$	16	$3+7u$	4	$7+u$	4
5	16	$1+7u$	8	$5+u$	8	$7+2u$	4
7	4	$3+u$	4	$5+2u$	16	$7+3u$	4
$1+u$	8	$3+2u$	4	$5+3u$	8	$7+4u$	4
$1+2u$	16	$3+3u$	4	$5+4u$	16	$7+5u$	4
$1+3u$	8	$3+4u$	4	$5+5u$	8	$7+6u$	4
$1+4u$	32	$3+5u$	4	$5+6u$	16	$7+7u$	4

Since $\mathcal{R}_k$ is finite and local, observe that two principal ideals are the same if and only if their generators are associated. Let $\Gamma = \mathcal{U}(\mathcal{R}_k)$ be the group of units of $\mathcal{R}_k$ acting by translation on $\mathcal{R}_k$ (Table 1).

By the Frobenius–Burnside Lemma (see [14], Theorem 3.22) we can state the following:

Theorem 2 *Let $\gamma \in \Gamma$, $X^\gamma = \{x \in \mathcal{R}_k \mid \gamma \cdot x = x\}$ be the set of elements fixed by γ under the considered action. Then the number N of principal ideals I of $\mathcal{R}_k$, such that*

$$I = \langle 2^d + vu\rangle,\ 0 \le d \le k,\ v \in \mathbb{Z}_{2^k} \text{ or } I = \langle 2^d u\rangle,$$

is

$$N = \frac{1}{2^{2k-1}} \sum_{\gamma\in\Gamma} |X^\gamma|.$$

Example 3 Let $\mathcal{R}_3 = \mathbb{Z}_8 + u\mathbb{Z}_8$. For each $\gamma \in \mathcal{U}(\mathcal{R}_3)$, using SageMath [15], it is seen that,

where $X^\gamma = \{x \in X \mid \gamma \cdot x = x\}$. Thus $\sum_{\gamma\in\Gamma} |X^\gamma| = 320$ and by Theorem 2, there are:

$$\frac{1}{2^5} \sum_{\gamma\in\Gamma} |X^\gamma| = \frac{320}{32} = 10$$

principal ideals. Note that the trivial ideals $\langle 0\rangle$ and $\langle 1\rangle$ are included.

4.2 Two-element generated ideals

The cardinality of the ring $\mathcal{R}_k$ increases with the values of k, as are the number of ideals, both, those generated by one element and those generated by two elements. In the following, general results about the two-element generated ideals are given.

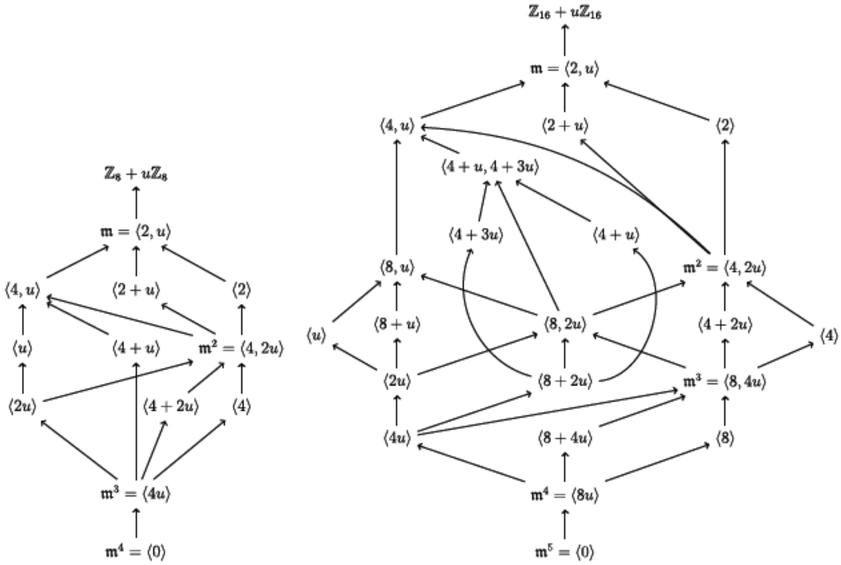

Fig. 1 The set of ideals of the ring $\mathcal{R}_3$ (left) and for the ring $\mathcal{R}_4$ (right)

For small values of k with the help of SageMath ([15]) we were able to give the complete set of ideals. See the Fig. 1.

Proposition 4 *Let $\lambda_0, \lambda_1 \in \mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$. Then, the ideal $I = \langle \lambda_0, \lambda_1\rangle$ is a two-element generated ideal of $\mathcal{R}_k$ if and only if $\lambda_0 \notin \langle \lambda_1\rangle$ and $\lambda_1 \notin \langle \lambda_0\rangle$. Consequently, for $1 \leq d \leq k-1$, the ring $\mathcal{R}_k$ has at least the following two-element generated ideals*:

$$\langle 2^d, u\rangle,\ \langle 2^d, 2u\rangle,\ \langle 2^d, 2^2u\rangle,\ \ldots,\ \langle 2^d, 2^{d-1}u\rangle.$$

Given d, e such that $0 \leq d, e \leq k$, let $I^{d,e}_{\nu,\rho} = \langle 2^d + \nu u, 2^e + \rho u\rangle$ with $\nu, \rho \in \mathbb{Z}_{2^k}$. In the case where $d = e$ we write $I^d_{\nu,\rho}$ for $I^{d,d}_{\nu,\rho}$.

Proposition 5 *Let $I^d_{\nu,\rho} = \langle 2^d + \nu u, 2^d + \rho u\rangle$ be a two-element generated ideal. If $\nu \not\equiv \rho \bmod 2$, then*

$$I^d_{\nu,\rho} = \langle 2^d, u\rangle.$$

Proof From the hypothesis it follows that $\nu - \rho$ is a unit and since $(2^d + \nu u) - (2^d + \rho u) = (\nu - \rho)u \in I^d_{\nu,\rho}$, $u \in I^d_{\nu,\rho}$. If $u \in I^d_{\nu,\rho}$ it can be easily seen that $2^d \in I^d_{\nu,\rho}$. □

The next results are easily proven.

Proposition 6 *Let $I^{d,e}_{\nu,\rho}$, $d < e$, be an ideal of the ring $\mathcal{R}_k$. Then if there is an $\alpha \in \mathbb{Z}_{2^k}$ such that $\rho - 2^{e-d}\nu = 2^d\alpha$, $I^{d,e}_{\nu,\rho} = \langle 2^d + \nu u\rangle$.*

Proposition 7 *Let $I^{d,e}_{\nu,\rho}$, $d < e$, be an ideal of the ring $\mathcal{R}_k$. If $\rho \in \mathcal{U}(\mathbb{Z}_{2^k})$ the ideal is generated by two elements and $I^{d,e}_{\nu,\rho} = I^{d}_{0,1}$.*

As an example of the previous proposition we have the following

Example 8 Let $I^{d}_{\nu,\rho}$ be an ideal of $\mathcal{R}_k$, $k > 1$, as in Proposition 5. Given $\rho = \delta\nu$, $\delta = 2^l\alpha$, then

$$I^{d}_{\nu,\rho} = \langle 2^d, \nu u\rangle = I^{d,k}_{0,\nu}.$$

5 Cyclic codes over $\mathcal{R}_k$

In this section cyclic codes over the ring $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$ are considered and described by means of idempotent elements. Results about constacyclic codes and their idempotents over finite chain rings are given in [16].

5.1 Basic results

Let R be a finite commutative local ring with identity, maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}_q = R/\mathfrak{m}$. The image of an element $r \in R$ under the canonical mapping $R \longrightarrow \mathbb{F}_q$ will be denoted by $\overline{r}$. Let $R[x]$ be the polynomial ring over R. Recall that an element $f(x) \in R[x]$ is called basic irreducible if its image $\overline{f}(x) \in \mathbb{F}_q[x]$ is irreducible. The following result is easy to prove.

Lemma 9 *Let R be as above. Then $f(x), g(x) \in R[x]$ are relatively prime if and only if $\overline{f}(x)$ and $\overline{g}(x)$ are relatively prime in $\mathbb{F}_q[x]$.*

Let R be as above. An R-submodule $\mathcal{C} \subset R^n$ is called a linear code of length n. Let τ be the standard cyclic shift operator on R^n: $(r_0, r_1, \dots, r_{n-1}) \overset{\tau}{\to} (r_{n-1}, r_0, r_1, \dots, r_{n-2})$. A linear code $\mathcal{C}$ of length n over R is cyclic if $\tau(\mathbf{c}) \in \mathcal{C}$ whenever $\mathbf{c} \in \mathcal{C}$.

For a ring R the polynomial representation of R^n is the R-isomorphism given by $\mathcal{P} : R^n \longrightarrow R[x]/\langle x^n - 1\rangle$, $\mathcal{P}(a_0, a_1, ..., a_{n-1}) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$. By means of the polynomial representation of R^n a cyclic code of length n can be regarded as an ideal of the polynomial ring $R_n = R[x]/\langle x^n - 1\rangle$.

We have the following,

Proposition 10 *The ring $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - 1\rangle$ is not a principal ideal ring.*

Proof The map $\gamma : \mathcal{R}_{k,n} \longrightarrow \mathcal{R}_k$ given by $\sum_{i=0}^{n-1} a_i x^i \mapsto \sum_{i=0}^{n-1} a_i$ is a surjective ring homomorphism. The ideal $\gamma^{-1}(\mathfrak{m})$ of $\mathcal{R}_{k,n}$ is not principal, otherwise if $\gamma^{-1}(\mathfrak{m}) = \langle r \rangle$ for some $r \in \mathcal{R}_{n,k}$,

$$\langle \gamma(r) \rangle = \gamma(\langle r \rangle) = \gamma(\gamma^{-1}(\mathfrak{m})) = \mathfrak{m} = \langle 2, u \rangle,$$

would be principal, a contradiction. □

Now consider the ring $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$ which is local with maximal ideal $\mathfrak{m} = \langle 2, u \rangle$, and observe that by means of the inclusion map ι, $\mathcal{R}_k$ can be considered as a subring of $\mathcal{R}_k[x]$. If f is a basic irreducible polynomial of $\mathcal{R}_k[x]$, there is the canonical mapping $\pi : \mathcal{R}_k[x] \longrightarrow \mathcal{R}_{k,f} = \mathcal{R}_k[x]/\langle f \rangle$.

The next proposition will be useful for describing cyclic codes.

Proposition 11 *Let $f \in \mathcal{R}_k[x]$ be a monic basic irreducible polynomial and $\mathcal{R}_{k,f} = \mathcal{R}_k[x]/\langle f \rangle$. Then any ideal $\mathcal{I}$ of $\mathcal{R}_{k,f}$ is of the form*

$$\mathcal{I} = I\mathcal{R}_{k,f},$$

where $I\mathcal{R}_{k,f}$ is the ideal extension of the ideal I of $\mathcal{R}_k$ to the ring $\mathcal{R}_{k,f}$.

Proof Given f and $\mathcal{R}_{k,f}$ as above, since $\mathcal{R}_k$ is local then $\mathcal{R}_{k,f}$ is an unramified extension ring over $\mathcal{R}_k$, i.e., $(\mathcal{R}_{k,f}, \mathfrak{M}, \mathcal{R}_{k,f}/\mathfrak{M})$ is a local commutative ring, with maximal ideal $\mathfrak{M} = \mathfrak{m}\mathcal{R}_{k,f}$ (see [11], XIV.8 for details). In particular any ideal $\mathcal{I}$ of $\mathcal{R}_{k,f}$ is such that $\mathcal{I} \subseteq \mathfrak{M}$. Let $g \in \mathcal{R}_k[x]$ and consider $g + \langle f \rangle \in \mathcal{R}_{k,f}$. Since f is basic irreducible, there are two possibilities, $\gcd(\overline{g},\overline{f}) = 1$ or $\gcd(\overline{g},\overline{f}) = \overline{f}$. If the first possibility holds, from Lemma 9, g and f are relatively prime in $\mathcal{R}_k[x]$, i. e., there are $\lambda_1, \lambda_2 \in \mathcal{R}_k[x]$ such that $\lambda_1 g + \lambda_2 f = 1$ which implies $\lambda_1 g \equiv 1 \mod \langle f \rangle$, thus g is a unit and hence $\mathcal{I} = \langle 1 + \langle f \rangle \rangle$.

If on the contrary, $\gcd(\overline{g},\overline{f}) = \overline{f}$ we can write in $\mathcal{R}_k[x]$, $g = fq + r$, $r \in \mathfrak{m}[x]$ but that means $g + \langle f \rangle \in \mathfrak{m}\mathcal{R}_{k,f} = \mathfrak{M}$. Let $\mathcal{I} \subset \mathfrak{M}$ be an ideal such that $g + \langle f \rangle \in \mathcal{I}$ and let $I = \pi^{-1}(\mathcal{I})$ which is an ideal of $\mathcal{R}_k[x]$. Since in particular $r \in \pi^{-1}(g + \langle f \rangle) \subset I$ then $\pi(\pi^{-1}(g + \langle f \rangle)) = \pi(r) \subset \pi(\pi^{-1}(\mathcal{I})) = \pi(I) = I\mathcal{R}_{k,f}$ then $\mathcal{I} \subseteq I\mathcal{R}_{k,f}$. Let $s + \langle f \rangle \in I\mathcal{R}_{k,f} = \pi(I)$, we have $\pi^{-1}(s + \langle f \rangle) \subset I = \pi^{-1}(\mathcal{I})$ from which it follows that $s + \langle f \rangle \in \mathcal{I}$ and hence $I\mathcal{R}_{k,f} \subseteq \mathcal{I}$. Thus $\mathcal{I} = I\mathcal{R}_{k,f}$ □

From the previous proposition it follows that the configuration of the set of ideals of the ring $\mathcal{R}_{k,f}$ is the same as that of the ring $\mathcal{R}_k$.

Let n be an odd integer, $x^n - 1 = f_1 f_2 \dots f_m$ where the f_i's are distinct monic basic irreducible pairwise relatively prime polynomials in $\mathcal{R}_k[x]$ for $i \in \{1, 2, \dots, m\}$, and let $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - 1 \rangle$. The following result is a direct consequence of the Chinese Remainder Theorem (CRT).

Theorem 12 *Let n and $x^n - 1$ be as above. Then,*

$$\mathcal{R}_{k,n} \cong \bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i},$$

where $\mathcal{R}_{k,f_i} = \mathcal{R}_k[x]/\langle f_i \rangle$*. In particular, any ideal* I *of* $\mathcal{R}_{k,n}$ *is such that*

$$I \cong \bigoplus_{i=1}^{m} I_i \mathcal{R}_{k,f_i},$$

where I_i *is an ideal of* $\mathcal{R}_k$*.*

Corollary 13 *Let* n *be odd,* $\mathcal{L}_k$ *be the set of ideals of the ring* $\mathcal{R}_k$ *and* m *the number of distinct monic basic irreducible coprime factors of* $x^n - 1$*. Then the ring* $\mathcal{R}_{k,n}$ *has* $|\mathcal{L}_k|^m$ *ideals.*

We recall that the ring $\mathcal{R}_k$ is local with maximal ideal $\mathfrak{m} = \langle 2, u \rangle$ and residue field $\mathbb{F}_2$. If $f \in \mathcal{R}_k[x]$ its image under the reduction map to $\mathbb{F}_2[x]$ is denoted by $\bar{f}$. The following result is easy to prove.

Proposition 14 *Let* $x^n - 1 = f_1 f_2 \ldots f_m$ *where* n *is odd and the* f_j*'s are distinct monic basic irreducible pairwise relatively prime polynomials in* $\mathcal{R}_k[x]$ *for* $j \in \{1, 2, \ldots, m\}$*. Let* $\overline{x^n - 1} = \Pi_{i=1}^{m} \bar{f}_i$ *be the corresponding product of irreducible factors in* $\mathbb{F}_2[x]$*. Then a non-zero principal ideal* $\mathcal{C} = \langle f + \langle x^n - 1 \rangle \rangle \subset \mathcal{R}_{k,n}$ *is trivial if and only if* $gcd(\bar{f}, \overline{x^n - 1}) = 1$ *in* $\mathbb{F}_2[x]$*.*

5.2 Idempotents and cyclic codes

In this section cyclic codes over the ring $\mathcal{R}_k$ are described by means of idempotent elements. First, general definitions and results are recalled.

Let R be a commutative ring with unity. An element $e \in R$ is called idempotent if $e^2 = e$. Two idempotent elements e and f are said to be orthogonal if $ef = 0$. An idempotent e is called primitive if $e = f + g$ with f and g orthogonal idempotent, then $f = 0$ or $g = 0$. A set of idempotent elements $\{e_1, e_2, \ldots, e_m\}$ such that $\sum_{i=1}^{m} = 1$ is called a complete set. Furthermore if $e_i e_j = 0$, $i \neq j$, the set is called a complete set of pairwise orthogonal idempotent elements. The set of idempotent elements of a ring R will be denoted by $E(R)$.

We recall that a ring R is said to be decomposable if there exist a finite collection $\{R_1, \ldots, R_t\}$ of non-trivial rings such that $R \cong \oplus_{i=1}^{t} R_i$.

Proposition 15 *Let* R *be a commutative ring with identity. Then* R *is decomposable,* $R \cong \oplus_{i=1}^{t} R_i$*, if and only if there is a complete set of non-trivial pairwise orthogonal idempotent elements* $\{e_1, e_2, \ldots, e_t\}$ *of* R *such that* $R_i \cong e_i R$*.*

Proof Suppose R is decomposable and let $\mathbf{e}_i = (0, \ldots, 1, \ldots, 0)$ be the element of $\oplus_{i=1}^{t} R_i$ with 1 at the *ith* coordinate and zero elsewhere. Then $\{\mathbf{e}_1, ..., \mathbf{e}_t\}$ is a complete set of pairwise orthogonal idempotent elements of $\bigoplus_{i=1}^{t} R_i$. It follows that if η is an isomorphism between R and $\bigoplus_{i=1}^{t} R_i$, the elements $\{\eta^{-1}(\mathbf{e}_i),\ i = 1, 2, ..., t\}$ comprise the desired set of idempotent elements of R. The converse is obvious. □

The following result is easy to prove from the definitions.

Proposition 16 *Let R be a commutative ring with identity. The following statements are equivalent*:

(i) *R is local.*

(ii) *R has no non-trivial idempotent elements.*

(iii) *R is indecomposable.*

In order to give a set of idempotent elements of the ring $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - 1\rangle$, an explicit isomorphism determining the Chinese Remainder Theorem is recalled (Theorem 12).

Let n be an odd integer, $x^n - 1 = f_1 \cdots f_m$ a product of distinct monic basic irreducible pairwise coprime polynomials in $\mathcal{R}_k[x]$ and define $\psi : \mathcal{R}_{k,n} \longrightarrow \bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i}$ by

$$\psi(c + \langle x^n - 1\rangle) = (c_1 + \langle f_1\rangle, ..., c_m + \langle f_m\rangle)$$

where $c \equiv c_i \mod \langle f_i\rangle$ for $i = 1, 2, ..., m$.

It is easy to see that ψ is an isomorphism whose inverse is given as follows. Let $\overline{x^n - 1} = \prod_{i=1}^{m} \bar{f}_i$ be the product of irreducible polynomials in $\mathbb{F}_2[x]$. Let $\overline{\hat{f}}_i = \prod_{i \neq j} \bar{f}_j$, then $\gcd\{\overline{\hat{f}}_i, ..., \overline{\hat{f}}_m\} = 1$ and from Lemma 9, $\hat{f}_1, ..., \hat{f}_m$ where $\hat{f}_i = \Pi_{i \neq j} f_j$, are relatively prime. Then there exist $\lambda_i \in \mathcal{R}_k[x]$ such that

$$\lambda_1 \hat{f}_1 + \lambda_2 \hat{f}_2 + \cdots + \lambda_m \hat{f}_m = 1.$$

Observe that $\sum_{j=1}^{m} \lambda_j \hat{f}_j \equiv \lambda_i \hat{f}_i \equiv 1 \mod \langle f_i\rangle,\ i = 1, 2, ..., m.$ The map $\phi : \bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i} \longrightarrow \mathcal{R}_{k,n}$. defined as

$$\phi(c_1 + \langle f_1\rangle, c_2 + \langle f_2\rangle, ..., c_m + \langle f_m\rangle) = \sum_{i=1}^{m} \lambda_i \hat{f}_i c_i + \langle x^n - 1\rangle,$$

is the inverse of the map ψ defined above.

Proposition 17 *With the notation as above let $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$, n a positive odd integer and $x^n - 1 = f_1 f_2 \ldots f_m$ the decomposition of $x^n - 1$ as a product of monic distinct basic irreducible pairwise coprime polynomials. Then*

$$E_{k,n} = \{\hat{e}_1, \hat{e}_2, \ldots, \hat{e}_m\}$$

where $\hat{e}_i = \lambda_i \hat{f}_i$, $\hat{f}_i = \frac{x^n - 1}{f_i}$, and λ_i, $i = 1, 2, ..., m$ as above is a complete set of primitive orthogonal idempotent elements of $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - 1\rangle$.

Proof Let $\hat{e}_i = \phi(\mathbf{e}_i)$ where $\mathbf{e}_i$ is the i-th coordinate vector of $\bigoplus_{i=1}^{m} \mathcal{R}_{k,f_i}$ and ϕ is as defined above. From the definition of ϕ it can be seen that $\hat{e}_i = \lambda_i \hat{f}_i$. □

The following easy result will be used later.

Lemma 18 *Let $\mathcal{C} = \langle f \rangle$ be a principal ideal of a commutative ring R with identity and let e be a nontrivial idempotent element in $\mathcal{C}$. Then,*

(a) *$\mathcal{C} = \langle e \rangle$ if and only if $f = ef$. Moreover, $ec = c$ for all $c \in \mathcal{C}$.*
(b) *The idempotent e such that $\langle f \rangle = \langle e \rangle$ is unique.*

Now we have,

Theorem 19 *Let n be an odd integer, $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - 1 \rangle$ and $x^n - 1 = \prod_{i=1}^{m} f_i$ be the representation of $x^n - 1$ as a product of distinct monic basic irreducible pairwise relatively prime polynomials in $\mathcal{R}_k[x]$. Let $\mathcal{C} = \langle f + \langle x^n - 1 \rangle \rangle$ be a non-trivial principal ideal of $\mathcal{R}_{k,n}$ and assume $f = f_{j_1} f_{j_2} \cdots f_{j_s}$ where $j_l \in M = \{1, 2, ..., m\}, l = 1, 2, ..., s$. Then, the idempotent $e_f + \langle x^n - 1 \rangle \in \mathcal{R}_{k,n}$ such that*

$$\mathcal{C} = \langle e_f + \langle x^n - 1 \rangle \rangle$$

is given by

$$e_f + \langle x^n - 1 \rangle = \sum_i \hat{e}_i + \langle x^n - 1 \rangle,$$

where $i \in M \backslash \{j_1, j_2, ..., j_s\}$ and $\{\hat{e}_i + \langle x^n - 1 \rangle\}$ is the complete set of primitive pairwise orthogonal idempotent elements given in Proposition 17.

Proof Since $f = \prod_{l=1}^{s} f_{j_l}$, let $\hat{f} = \prod_i f_i$ with $i \in M \backslash \{j_1, j_2, ..., j_s\}$. Thus f and $\hat{f}$ are relatively prime and there are $\lambda, \hat{\lambda} \in \mathcal{R}_k[x]$ such that $\lambda f + \hat{\lambda} \hat{f} = 1$. Let $e_f + \langle x^n - 1 \rangle = \lambda f + \langle x^n - 1 \rangle \in \mathcal{R}_{k,n}$. It is easy to see that this is an idempotent element. Observe that

$$\lambda f \equiv 1 \equiv \hat{\lambda}_i \hat{f}_i \bmod \langle f_i \rangle, i \in M \setminus \{j_1, j_2, ..., j_s\},$$

and

$$\lambda f \equiv 0 \bmod \langle f_{j_l} \rangle, l = 1, 2, ..., s.$$

By construction,

$$f e_f + \langle x^n - 1 \rangle = f(\lambda f) + \langle x^n - 1 \rangle = f(1 - \hat{\lambda} \hat{f}) + \langle x^n - 1 \rangle = f + \langle x^n - 1 \rangle.$$

and from Lemma 18 it follows that $\langle f + \langle x^n - 1 \rangle \rangle = \langle e_f + \langle x^n - 1 \rangle \rangle$. □

Corollary 20 *With the above notation, $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - 1\rangle$ has 2^m idempotent elements, where m is the number of basic irreducible factors of $x^n - 1$ in $\mathcal{R}_k[x]$.*

The general idea of the proof of the following result is easy or it can be found in ([17], Theorems 4.3.2 and 4.3.8).

Proposition 21 *Let n be an odd integer, $R_n = \mathbb{F}_2[x]/\langle x^n - 1\rangle$ and let $x^n - 1 = g_1 g_2 \cdots g_m$ be the expression of $x^n - 1$ as a product of distinct monic irreducible pairwise relatively prime polynomials in $\mathbb{F}_2[x]$, and let $\hat{g}_i = \frac{x^n-1}{g_i}$. Then the set $\{\theta_1, ..., \theta_m\}$ with $\theta_i = \Lambda_i \hat{g}_i$, $i = 1, 2, ..., m$, Λ_i such that $\Lambda_i \hat{g}_i \equiv 1$ mod $\langle g_i\rangle$ is a complete set of primitive pairwise orthogonal idempotent elements in R_n.*

The previous result together with the next one will provide a way to determine the set of primitive idempotent elements in the ring $\mathcal{R}_{k,n}$.

Proposition 22 ([18], Proposition 4.1) *Let R be a commutative ring and N a nilpotent ideal of R with nilpotency index $t \geq 2$. Let $s > 1$ be the characteristic of the quotient ring R/N. If e is an idempotent element of R/N then,*

$$e^{s^{t-1}}$$

is an idempotent element of the ring R. Moreover, if there is a collection of primitive orthogonal idempotent elements of R/N it lifts to a set of idempotent elements of R with the same property. Also, $|E(R)| = |E(R/N)|$ where $E(R)$ is the set of idempotent elements of R.

Now we apply the previous results to our situation. Recall that $\mathcal{R}_{k,n} = \mathcal{R}_k[x]/\langle x^n - 1\rangle$, $\mathfrak{m}_{k,n} = \mathfrak{m}\mathcal{R}_{k,n}$ is an ideal with nilpotency index $t = k + 1$, where $\mathfrak{m}$ is the maximal ideal of $\mathcal{R}_k$ and $\mathcal{R}_{k,n}/\mathfrak{m}_{k,n} = \mathbb{F}_2[x]/\langle x^n - 1\rangle$ has characteristic $s = 2$.

Theorem 23 *With the notation as in Proposition 21,*

$$E(\mathcal{R}_{k,n}) = \{(\theta_1)^{2^k}, (\theta_2)^{2^k}, ..., (\theta_m)^{2^k}\}$$

is the complete set of primitive pairwise orthogonal idempotent elements of the ring $\mathcal{R}_{k,n}$.

From Theorems 19 and 23 we have the following,

Theorem 24 *Let $\mathcal{C} = \langle f + \langle x^n - 1\rangle, ug + \langle x^n - 1\rangle\rangle$ be a two-element generated ideal of $\mathcal{R}_{k,n}$. Then*

$$\mathcal{C} = \langle e_f + \langle x^n - 1\rangle, ue_g + \langle x^n - 1\rangle\rangle,$$

where $e_f + \langle x^n - 1\rangle$ and $e_g + \langle x^n - 1\rangle\rangle$ are the idempotent elements associated to $f + \langle x^n - 1\rangle$ and $g + \langle x^n - 1\rangle$ respectively, in the sense of Theorem 19.

6 Examples

In this section examples illustrating the previous results are provided in which the calculations were carried out with SageMath ([15]).

Example 25 The following illustrates Theorem 19. Let $\mathcal{R}_3 = \mathbb{Z}_8 + u\mathbb{Z}_8$ and $x^{15} - 1 = f_1 f_2 f_3 f_4 f_5$ where

$$f_1 = x + 7,\ f_2 = x^2 + x + 1,\ f_3 = x^4 + 4x^3 + 6x^2 + 3x + 1$$
$$f_4 = x^4 + 3x^3 + 6x^2 + 4x + 1,\ f_5 = x^4 + x^3 + x^2 + x + 1$$

in $\mathcal{R}_3[x]$. The idempotent generator for the ideal $\mathcal{C} = \langle x^6 + 5x^5 + 3x^4 + 5x^3 + 2x^2 + 4x + 1\rangle = \langle f_2 f_3\rangle$ will be determined. Observe that under the reduction map, $\overline{x^{15} - 1} = g_1 g_2 g_3 g_4 g_5$ where

$$g_1 = x + 1,\ g_2 = x^2 + x + 1,\ g_3 = x^4 + x + 1$$
$$g_4 = x^4 + x^3 + 1,\ g_5 = x^4 + x^3 + x^2 + x + 1.$$

A complete set of idempotent elements in $R_{15} = \mathbb{F}_2[x]/\langle x^{15} - 1\rangle$ is $E(R_{15}) = \{\theta_1, \theta_2, \theta_3, \theta_4, \theta_5\}$ where,

$$\begin{aligned}
\theta_1 =& x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\\
\theta_2 =& x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x,\\
\theta_3 =& x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x,\\
\theta_4 =& x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^7 + x^6 + x^3,\\
\theta_5 =& x^{14} + x^{13} + x^{12} + x^{11} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + x.
\end{aligned}$$

Since the ring R_{15} has characteristic $s = 2$, and the maximal ideal $\mathfrak{m}$ of $\mathcal{R}_3$ has nilpotency index $t = 4$, from this complete set of pairwise primitive idempotent elements and Theorem 23, a complete set of idempotent elements of $\mathcal{R}_{3,15} = \mathcal{R}_3[x]/\langle x^{15} - 1\rangle$ can be given: $E_{3,15} = \{e_1, e_2, e_3, e_4, e_5\}$ with $e_i = (\theta_i)^8$, $i = 1, 2, \ldots, 5$. Specifically,

$$\begin{aligned}
e_1 =& 7(x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1),\\
e_2 =& x^{14} + x^{13} + 6x^{12} + x^{11} + x^{10} + 6x^9 + x^8 + x^7 + 6x^6 + x^5 + x^4 + 6x^3 + x^2 + x + 6,\\
e_3 =& 4x^{14} + 4x^{13} + x^{12} + 4x^{11} + 2x^{10} + x^9 + 3x^8 + 4x^7 + x^6 + 2x^5 + 3x^4 + x^3 + 3x^2 + 3x + 4,\\
e_4 =& 3x^{14} + 3x^{13} + x^{12} + 3x^{11} + 2x^{10} + x^9 + 4x^8 + 3x^7 + x^6 + 2x^5 + 4x^4 + x^3 + 4x^2 + 4x + 4,\\
e_5 =& x^{14} + x^{13} + x^{12} + x^{11} + 4x^{10} + x^9 + x^8 + x^7 + x^6 + 4x^5 + x^4 + x^3 + x^2 + x + 4.
\end{aligned}$$

Since $f = f_2 f_3$, with the notation as in Theorem 19, it follows that $e_f = \hat{e}_1 + \hat{e}_4 + \hat{e}_5$, i. e.,

$$e_f = 3x^{14} + 3x^{13} + x^{12} + 3x^{11} + 5x^{10} + x^9 + 4x^8 + 3x^7 + x^6 + 5x^5 + 4x^4 + x^3 + 4x^2 + 4x + 7.$$

Note that $f = fe_f$, therefore $\langle f\rangle = \langle e_f\rangle$.

The following example illustrates Theorem 24.

Example 26 Let $k = 2, n = 7$, $\mathcal{R}_2 = \mathbb{Z}_4 + u\mathbb{Z}_4$ and $\mathcal{R}_{2,7} = \mathcal{R}_2[x]/\langle x^7 - 1\rangle$. In $\mathcal{R}_2[x]$ we have $x^7 - 1 = f_1 f_2 f_3$ where $f_1 = x + 3$, $f_2 = x^3 + 2x^2 + x + 3$, $f_3 = x^3 + 3x^2 + 2x + 3$. Thus, in $\mathbb{F}_2[x]$, $x^7 - 1 = \bar{f}_1\bar{f}_2\bar{f}_3$ with $\bar{f}_1 = x + 1$, $\bar{f}_2 = x^3 + x + 1$, $\bar{f}_3 = x^3 + x^2 + 1$. Then, $E = \{\theta_1, \theta_2, \theta_3\}$ where

$$\theta_1 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,\ \theta_2 = x^4 + x^2 + x + 1, \theta_3 = x^6 + x^5 + x^3 + 1.$$

Since the nilpotency index of the maximal ideal of $\mathcal{R}_2$ is $t = 3$ and the characteristic of the ring $\mathbb{F}_2[x]/\langle x^7 - 1\rangle$ is $s = 2$, from Theorem 23, $E_{2,7} = \{e_1, e_2, e_3\} = \{(\theta_1)^4, (\theta_2)^4, (\theta_3)^4\}$ where

$$\begin{aligned}(\theta_1)^4 =&3(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1),\\ (\theta_2)^4 =&2x^6 + 2x^5 + 3x^4 + 2x^3 + 3x^2 + 3x + 1,\\ (\theta_3)^4 =&3x^6 + 3x^5 + 2x^4 + 3x^3 + 2x^2 + 2x + 1.\end{aligned}$$

With the previous information, the idempotent generators of the ideal $\mathcal{C} = \langle 1 + 2x + x^2 + 3x^3, u(x-1)\rangle = \langle f, ug\rangle$ of the ring $\mathcal{R}_{2,7}$ are determined. Observe that $f = 3f_3$, $g = f_1$ and from Theorems 19 and 24, $e_{f_3} = e_1 + e_2 = x^6 + x^5 + 2x^4 + x^3 + 2x^2 + 2x$, and $e_g = x^6 + x^5 + x^4 + x^3 + x^2 + x + 2$. Thus,

$$\langle f, ug\rangle = \langle e_f, ue_g\rangle.$$

7 Conclusions

This manuscript approaches the study of the finite non-chain Frobenius ring $\mathcal{R}_k = \mathbb{Z}_{2^k} + u\mathbb{Z}_{2^k}$, with $u^2 = 0$ and $k > 1$ an integer and the number of principal ideals is given. Partial results on the ideals generated by two elements are provided. Cyclic codes over this ring are also considered, and it is shown that these codes can be described by means of idempotent elements. Examples are included illustrating the main results of the paper.

Acknowledgements The first author was partially supported by Sistema Nacional de Investigadores, SNI, México and the second author by Fellowship No. 764803, Consejo Nacional de Ciencia y Tecnología, CONACYT, México.

Declarations

Conflict of interest The authors have no conflicts of interest to disclose.

References

1. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. IEEE Trans. Inf. Theory **40**(2), 301–319 (1994)
2. Pless, V.S., Quian, Z.: Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$. IEEE Trans. Inf. Theory **42**(5), 1594–1600 (1996)
3. Norton, G.H., Sălăgean, A.: On the structure of linear and cyclic codes over a finite chain ring. Appl. Algebra Eng. Commun. Comput. **10**(1), 489–506 (2000). https://doi.org/10.1007/PL00012382
4. Kanwar, P., López-Permouth, S.R.: Cyclic codes over the integers modulo p^m. Finite Fields Appl. **3**(4), 334–352 (1997). https://doi.org/10.1006/ffta.1997.0189
5. Castillo-Guillén, C.A., Rentería-Márquez, C., Tapia-Recillas, H.: Constacyclic codes over finite local Frobenius non-chain rings with nilpotency index 3. Finite Fields Appl. **43**(X), 1–21 (2017). https://doi.org/10.1016/j.ffa.2016.08.004
6. Gao, J., Fu, F., Xiao, L., Bandi, R.: Some results on cyclic codes over $\mathbb{Z}_q + u\mathbb{Z}_q$. Discrete Math. Algorithms Appl. **7**(4), 1550058–115500589 (2015). https://doi.org/10.1142/S1793830915500585
7. Bandi, R., Bhaintwal, M.: Cyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$. In: Proceedings of IWSDA'15 (2015). https://doi.org/10.1109/IWSDA.2015.7458411
8. Yildiz, B., Karadeniz, S.: Linear codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$: MacWilliams identities, projections, and formally self-dual codes. Finite Fields Appl. **27**(4), 24–40 (2014). https://doi.org/10.1016/j.ffa.2013.12.007
9. Li, W., Yue, M., Huang, Z., Li, Z.: Linear codes over the ring $\mathbb{Z}_8 + u\mathbb{Z}_8$. In: Paper presented at the 2018 International Conference on Information, Electronic and Communication Engineering (2018)
10. Atiyah, M.F., MacDonald, I.G.: Introduction to Commutative Algebra. Addison–Wesley–Longman, Great Britain (1969)
11. McDonald, B.R.: Finite Rings with Identity. Pure and Applied Mathematics, vol. 28. Marcel Dekker Inc., New York (1974)
12. Lam, T.Y.: Lectures on Modules and Rings. Graduated Texts in Mathematics, vol. 189. Springer, New York (1999)
13. Wood, J.A.: Duality for modules over finite rings and applications to coding theory. Am. J. Math. **121**(3), 555–575 (1999). https://doi.org/10.1353/ajm.1999.0024
14. Rotman, J.J.: An Introduction to the Theory of Groups. Graduated Texts in Mathematics, vol. 148. Springer, New York (1994)
15. The Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.3). https://www.sagemath.org (2021)
16. Charkani, M.E., Kabore, J.: Primitive idempotents and constacyclic codes over finite chain rings. Gulf J. Math. **8**(2), 55–67 (2020). https://doi.org/10.56947/gjom.v8i2.434
17. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes, 1st edn. Cambridge University Press, Cambridge (2003)
18. Melo-Hernández, F.D., Hernández-Melo, C.A., Tapia-Recillas, H.: On idempotents of a class of commutative rings. Commun. Algebra **48**, 4013–4026 (2020). https://doi.org/10.1080/00927872.2020.1754424

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

15º CNCCAR COLOQUIO NACIONAL DE CÓDIGOS, CRIPTOGRAFÍA Y ÁREAS RELACIONADAS

04 de julio de 2025, CDMX

A quien corresponda
Presente

Por medio de la presente se hace constar que el

Dr. Horacio Tapia Recillas

formó parte del comité organizador del 15º Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas, celebrado de forma remota del 23 al 25 de junio de 2025.

Se expide la presente constancia al interesado en CDMX, a los 4 días del mes de julio de 2025.

[redacted] –

Dra. Gina Gallegos García
CIC, IPN

[redacted]

Dr. José Noé Gutiérrez Herrera
Depto. de Matemáticas, UAM-I

Universidad Nacional Autónoma de México

Instituto Politécnico Nacional
“La Técnica al Servicio de la Patria”

Cinvestav

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa

15° CNCCAR

COLOQUIO NACIONAL DE
CÓDIGOS, CRIPTOGRAFÍA
Y ÁREAS RELACIONADAS

El Comité Organizador otorga la presente

CONSTANCIA

A: *Horacio Tapia-Recillas*

por haber impartido la conferencia

Códigos DNA y el campo de Galois $\mathbb{F}_{16}$

en el 15º Coloquio Nacional de Códigos, Criptografía y Áreas Relacionadas, celebrado del 25 al 27 de junio de 2025, de forma remota desde CDMX, MÉXICO

[redacted]

Dra. Gina Gallegos García
Por el Comité Organizador
CIC-IPN

[redacted]

Dr. José Noé Gutiérrez Herrera
Por el Comité Organizador
UAM-Iztapalapa