IMÁGENES LINEALES DE GRAY DE $\mathcal{R}-$CÓDIGOS CÍCLICOS LINEALES

TESIS QUE PRESENTA

HAYDEE HERNÁNDEZ SORIANO

PARA OBTENER EL GRADO DE
MAESTRA EN CIENCIAS MATEMÁTICAS

DIRECTOR DE TESIS: DR. CARLOS ALBERTO LÓPEZ ANDRADE

BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA ⟨BUAP⟩
Facultad de Ciencias Físico Matemáticas ⟨FCFM⟩
http://www.fcfm.buap.mx/
Noviembre 2020

Haydee Hernández Soriano : *Imágenes lineales de Gray de $\mathcal{R}$–códigos cíclicos lineales* , Benemérita Universidad Autónoma de Puebla (BUAP) , Facultad de Ciencias Físico Matemáticas (FCFM)

WEBSITE:
http://www.fcfm.buap.mx/

E-MAIL:
haydeehs03@gmail.com

DRA. LIDIA AURORA HERNÁNDEZ REBOLLAR
SECRETARIA DE INVESTIGACIÓN Y
ESTUDIOS DE POSGRADO, FCFM-BUAP
P R E S E N T E:

Por este medio le informo que la C:

HAYDEE HERNÁNDEZ SORIANO

estudiante de la Maestría en Ciencias (Matemáticas), ha cumplido con las indicaciones que el Jurado le señaló en el Coloquio que se realizó el día 30 de noviembre de 2020, con la tesis titulada:

Imágenes lineales de Gray de R-códigos cíclicos lineales

Por lo que se le autoriza a proceder con los trámites y realizar el examen de grado en la fecha que se le asigne.

A T E N T A M E N T E.
H. Puebla de Z. a 4 de diciembre de 2020

DRA. PATRICIA DOMÍNGUEZ SOTO
COORDINADORA DEL POSGRADO
EN MATEMÁTICAS.

Facultad
de Ciencias
Físico Matemáticas

Av. San Claudio y 18 Sur, edif. FM1
Ciudad Universitaria, Col. San
Manuel, Puebla, Pue. C.P. 72570
01 (222) 229 55 00 Ext. 7550 y 7552

A mis padres y hermano.

AGRADECIMIENTOS

De manera muy especial agradezco a mi asesor, el Dr. Carlos Alberto López Andrade, su compromiso con este trabajo. Le agradezco la opotunidad que me dió de trabajar bajo su dirección, la confianza y paciencia depósitadas en mi. Gracias por compartir conmigo sus conocimientos, por el tiempo invertido en este trabajo, por su apoyo y ánimos.

Agradezco a mis sinodales, los Drs. Carlos Guillén Galván, Iván Fernando Vilchis Montalvo y César Bautista Ramos, por su acompñamiento y observaciones emitidos en los foros de avance, así que como el tiempo dedicado a la lectura y revisión de este trabajo. Gracias a mi sinodal el M.C. Henry Chimal Dzul, por el tiempo dedicado a la revisión de este trabajo, por sus observaciones y comentarios , y por su disposición a atender mis dudas.

Agradezco a CONACYT por el apoyo económico brindado durante la realización de este trabajo.

Agradezco a mis padres por ser un ejemplo de determinación, valentía y tenacidad para mí. Gracias por alentarme a luchar por mis sueños y estar presentes en cada paso que doy.

Gracias a mi hermano por su complicidad en estos años. Te agradezco cada risa, cada ánimo, cada paso que diste a mi lado. Gracias por nunca dejarme sola y siempre motivarme y alentarme a seguir.

Agradezco a mi familia sus ánimos y compañía, de manera especial a mis tíos Francisco y Columba, y a mi prima Laura, por su asilo y hospitalidad.

Gracia a mis amigos y hermanos de comunidad por su apoyo y compañ̃ia.

INTRODUCCIÓN

La Teoría de Códigos Algebraicos está enfocada en la optimización de la fiabilidad de las comunicaciones dígitales. Es vista como una rama de las matemáticas puras. Sus fundamentos pueden encontrarse en el Álgebra, la Teoría de Números, la Geometría Finita y la Combinatoria.

En los años 90,el anillo $\mathbb{Z}/4\mathbb{Z}$ destacó mucho debido a que los códigos sobre este anillo fueron relacionados con códigos binarios a través de la función de Gray. Hammons et al. demostraron en [HKC+94] que los códigos no lineales de Nordstrom-Robinson, Kerdock, Preparata y Goethals pueden verse como la imagen de Gray de códigos cíclicos lineales sobre $\mathbb{Z}/4\mathbb{Z}$. Con esto se logró explicar la dualidad formal entre los códigos de Kerdock y Preparata. Este trabajo es importante porque dió origen a una nueva perspectiva del estudio de códigos sobre anillos finitos. Además, la función de Gray se volvió clave en el estudio de estos códigos, por la información que podrían aportar las imágenes de estos códigos bajo dicha función. Por ello fue generalizada para anillos finitos de cadena ([GS99]). A la par se estudiaba la estructura de códigos sobre distintos anillos finitos ([CS95], [KLP97], [PQ96], [DLP04]) y el comportamiento de sus imágenes bajo la función de Gray ([Wol01], [Wol99], [LB02], [LATR11], [LATR12]).

J. Wolfmann mostró que la imagen de Gray de un código negacíclico lineal sobre $\mathbb{Z}/4\mathbb{Z}$ es un código cíclico binario (no necesariamente lineal) de distancia invariante (c.f. [Wol99]). Más tarde, en [Wol01], Wolfmann estableció resultados importantes sobre la linealidad y cíclicidad de las imágenes de Gray de códigos cíclicos lineales de longiutd impar sobre $\mathbb{Z}/4\mathbb{Z}$. En particular, Wolfmann dio condiciones necesarias y suficientes para que la imagen de un código cíclico lineal de longiutd impar sobre $\mathbb{Z}/4\mathbb{Z}$ bajo la función de Gray sea un código cíclico lineal (c.f.[Wol01, Proposición 16, Teorema 21]).

Por su parte, Ling y Blackford en [LB02] generalizan varios resultados que J. Wolfmann presenta en [Wol01] para códigos sobre $\mathbb{Z}/p^2\mathbb{Z}$. En específico, Ling y Blackford dan condiciones necesarias y suficientes para que la imagen de Gray de un código cíclico lineal sobre $\mathbb{Z}/p^2\mathbb{Z}$ sea cíclica lineal ([LB02, Teorema 4.6, Teorema 4.13]).

En [LATR11], López-Andrade y Tapia-Recillas proporcionan condiciones necesarias y suficientes para que la imagen de Gray de un código cíclico lineal, definido sobre un anillo de Galois de índice de nilpotencia 2, sea lineal. Dicho teorema generaliza la Proposición 16 y el Teorema 4.6 de los artículos [Wol01] y [LB02].

Por otro lado, H. Q. Dinh y S. R. López-Permouth obtuvieron en [DLP04] la estructura de un código cíclico sobre un anillo finito de cadena. Muestran que un código cíclico sobre un anillo finito de cadena tiene una representación polinomial sobre cierto anillo cociente de ideales principales. Dicha representación es un ideal en el anillo cociente y por lo tanto tiene un polinomio generador. Los resultados que ellos establecen se cumplen para códigos cíclicos lineales sobre anillos de Galois de índice de nilpotencia 2. Con el trabajo de H. Q. Dinh y S. R. López-Permouth se puede establecer que cualquier código cíclico lineal de longitud n sobre un anillo de Galois de índice de nilpotencia 2, $GR(p^2, m)$, con n y p coprimos, tiene un polinomio generador de la forma $G(x) = A(x)(B(x) + p)$ en el anillo $GR(p^2, m)[x]/(x^n - 1)$, donde $A(x)B(x)C(x) = x^n - 1$, y $A(x), B(x), C(x)$ son polinomios mónicos coprimos por pares sobre el anillo $GR(p^2, m)$ (c.f. Teorema 1.5). Observemos que para el polinomio generador de un $GR(p^2, m)-$código cíclico lineal se tienen los siguientes casos:

i) Si $C(x) = 1$ entonces $G(x) = pA(x)$.

ii) Si $A(x) = 1$ entonces $G(x) = B(x) + p$.

Describir la imagen bajo la función de Gray de códigos cíclicos lineales sobre anillos de Galois de índice de nilpotencia 2 no es un trabajo sencillo. No obstante, con los resultados establecidos por López-Andrade y Tapia-Recillas en [LATR12] se da una respuesta parcial a dicho problema. Ya que, la imagen de Gray de un código cíclico lineal sobre un anillo de Galois $GR(p^2, m)$ con polinomio generador $G(x) = pA(x)$, es cíclica lineal sobre $\mathbb{F}_{p^m}$, y su polinomio generador es de la forma

$\overline{A}(x)(x^n-1)^{p^m-1} \in \mathbb{F}_{p^m}[x]$, con $\overline{A}(x)$ la μ—reducción de $A(x)$ (c.f. [LA13, Teorema 5.5]). Del problema original resta estudiar el comportamiento de las imágenes de Gray de $GR(p^2,m)$—códigos cíclicos lineales cuando el polinomio generador es $B(x)+p$.

Motivados por los resultados de Ling y Blackford [LB02] y Wolfmann [Wol01], en el presente trabajo estudiamos las imágenes bajo la función de Gray de códigos cíclicos lineales sobre anillos de Galois de índice de nilpotencia 2. De manera específica, nos enfocamos en estudiar códigos cíclicos con polinomio generador de la forma $B(x)+p$. En contraste con los resultados obtenidos por López-Andrade y Tapia-Recillas, en esta tesis demostramos que la imagen de Gray de estos códigos cíclicos no es necesariamente cíclica pero sí lineal.

Formalmente, demostraremos el siguiente teorema, el cual es nuestra principal aportación:

Teorema 1. *Sean $\mathcal{R} = GR(p^2,m)$ un anillo de Galois de índice de nilpotencia 2. Sea $\mathcal{C} \subseteq \mathcal{R}^n$ un $\mathcal{R}$—código cíclico lineal de longitud n tal que n es primo relativo con p, generado por el polinomio $G(x) = B(x)+p$ y Φ la función de Gray en $\mathcal{R}^n$. Entonces $\Phi(\mathcal{C})$ es $\mathbb{F}_{p^m}$— lineal.*

En esta tesis se abordan cinco capítulos, los cuales están conformados de la siguiente manera:

En el Capítulo 1 se estudian propiedades de los anillos de Galois. Además, se introduce la definición del Anillo de Vectores de Witt. Finalmente, se revisa la estructura de códigos sobre campos finitos y anillos finitos conmutativos con unidad.

El Capítulo 2 se enfoca en la definición y las propiedades más importantes de la función de Gray. En particular, estudiamos condiciones necesarias y suficientes para que la imagen de Gray de un código cíclico lineal sobre un anillo de Galois de índice de nilpotencia 2 , sea lineal. Dichas condiciones (c.f. Teorema 2.2) serán empleadas en el capítulo 3 para probar que la imagen de un código cíclico lineal generado por un polinomio de la forma $B(x)+p$, es lineal. Por último, se revisan detalladamente algunos de los resultados que J. Wolfmann establece en [Wol01], con el fin de entender el comportamiento de la función de Gray.

El Capítulo 3 es el centro de este trabajo. En él se prueba que la imágenes de Gray de códigos cíclicos lineales sobre anillos de Galois de índice de nilpotencia 2 y, cuyo polinomio generador es $B(x)+p$, es lineal sobre $\mathbb{F}_{p^m}$.

En el Capítulo 4 se realiza un análisis detallado de la primera sección del artículo [US98] donde se aborda un anillo de clases residuales muy particular. Esto se hace con el fin de exhibir un anillo sobre el cual la función de Gray es lineal, y por ello, la imagen de Gray de los códigos cíclicos lineales definidos sobre este anillo, es lineal.

Finalmente, en el Capítulo 5 mostramos el trabajo que se realizó en el software `MAGMA`, el cual fue relevante para el desarrollo de esta tesis, pues nos permitió descartar que las imágenes bajo la función de Gray de códigos cíclicos lineales sobre $GR(p^2,m)$ y, cuyo polinomio generador es $B(x)+p$, no son cíclicas. Además descubrimos que tras aplicar a dichas imágenes la permutación global de Nechaev, estas no eran cíclicas, por lo que en este tipo de códigos la permutación de Nechaev no resultó de gran utilidad.

ÍNDICE GENERAL

1 PRELIMINARES

En este capítulo se presentan las definiciones y los resultados más relevantes acerca de los anillos de Galois y la Teoría de Códigos, que serán utilizados en capítulos posteriores.

1.1 ANILLOS DE GALOIS

Los anillos de Galois son base primordial de esta tesis. Es por ello que en esta sección recopilamos los resultados de mayor relevancia para nuestros fines. Los resultados que se enuncian pueden consultarse en [Wan03] y [GR17].

Sean p un número primo, s un entero positivo, $\mathbb{Z}/p^s\mathbb{Z}$ el anillo de enteros módulo p^s, y $f(x)$ un polinomio en el anillo $(\mathbb{Z}/p^s\mathbb{Z})[x]$. Decimos que $f(x)$ es un *polinomio básico irreducible* si su reducción módulo p es un polinomio irreducible en el anillo de polinomios $\mathbb{F}_p[x]$. De manera análoga, decimos que $f(x)$ es un *polinomio básico primitivo* si su reducción módulo p es un polinomio primitivo sobre el campo $\mathbb{F}_p$.

De manera formal, un *anillo de Galois* es definido como un anillo finito con identidad 1, en el que el conjunto de sus divisores de cero, añadiendo el cero, forma un ideal principal, $\langle p1\rangle$, con p un número primo. Entiendase por $p1$ la suma del elemento identidad $p-$veces, es decir, $p1 = 1 + \cdots + 1$. Sin embargo, existe una caracterización de estos anillos, la cual afirma que cualquier anillo de Galois, R, con característica p^s y cardinalidad p^{sm}, donde p es un número primo y $s, m \in \mathbb{N}$, es isomorfo al anillo de clases residuales $\frac{(\mathbb{Z}/p^s\mathbb{Z})[x]}{(h(x))}$, donde $h(x)$ es un polinomio mónico básico irreducible de grado m con coeficientes en el anillo $\mathbb{Z}/p^s\mathbb{Z}$ y $(h(x))$ es el ideal del anillo $(\mathbb{Z}/p^s\mathbb{Z})[x]$ generado por $h(x)$ (c.f. [Wan03, Teorema 14.6]); es decir:

$$R \cong \frac{(\mathbb{Z}/p^s\mathbb{Z})[x]}{(h(x))}. \tag{1}$$

El conjunto de los divisores de cero del anillo $\frac{(\mathbb{Z}/p^s\mathbb{Z})[x]}{(h(x))}$, añadiendo el cero, forman el ideal $\langle p[1 + (h(x))]\rangle$, con $[1 + (h(x))]$ la unidad en el anillo. Identificaremos a $p[1 + (h(x))]$ por $p + (h(x)) \in \frac{(\mathbb{Z}/p^s\mathbb{Z})[x]}{(h(x))}$.

Denotaremos a los anillos de Galois de la siguiente manera: $GR(p^s, m)$, ó bien $GR(p, s, m)$, donde p^s es la característica del anillo $\mathbb{Z}/p^s\mathbb{Z}$ y m es el grado del polinomio $h(x)$, con $h(x)$ mónico básico irreducible sobre el anillo de enteros módulo p^s. Para los elementos del anillo de Galois omitiremos la notación de clase residual. Sin embargo, no perdamos de vista que el producto en el anillo $GR(p^s, m)$ es módulo $h(x)$.

Sea R el anillo de Galois $R = GR(p^s, m) = \frac{(\mathbb{Z}/p^s\mathbb{Z})[x]}{(h(x))}$, con $h(x)$ un polinomio mónico básico irreducible en $\mathbb{Z}/p^s\mathbb{Z}$, de grado m:

a) R tiene p^{sm} elementos y su característica es p^s.

b) Cuando $m = 1$, R es el anillo $\mathbb{Z}/p^s\mathbb{Z}$. Si $s = 1$, entonces R es isomorfo a una extensión de grado m del campo finito $\mathbb{F}_p$, es decir, $R \cong \mathbb{F}_{p^m}$.

c) Cuando $s > 1$, el anillo de Galois $R = GR(p^s, m)$ resulta ser un *anillo local*, ya que tiene un único ideal máximal, $\mathcal{M}$, cuyos elementos son el cero y sus divisores, más aún $\mathcal{M} = \langle p\rangle$.

d) Los ideales del anillo R, son de la forma $\langle p^i\rangle$, con $0 \leqslant i \leqslant s$. Además, satisfacen la *condición de cadena finita*, puesto que para cada $i \in \{0, 1, \ldots, s-1\}$ se cumple que $\langle p^{i+1}\rangle \subset \langle p^i\rangle$, es decir:

$$\{0\} = \langle p^s\rangle \subset \langle p^{s-1}\rangle \subset \cdots \langle p\rangle \subset \langle p^0\rangle = R.$$

Por lo que R es un *anillo finito de cadena*.

e) El *campo residual* del anillo R es definido como $RF = R/\langle p\rangle$. Se puede demostrar que $R/\langle p\rangle \cong \mathbb{F}_{p^m}$.

f) Sea $\mu\colon R \to RF$, donde $\mu(a) = a + \mathcal{M} := \overline{a}$, para cada $a \in R$. La función μ es el *homomorfismo canónico*, también llamada la μ*—reducción* del anillo de Galois R sobre su campo residual. Dicho homomorfismo se puede extender al anillo de polinomios con coeficientes en R, de la siguiente manera:

$$\begin{array}{rcl} \overline{\mu}\colon R[z] & \to & RF[z] \\ a(z) = \overline{\mu}(\sum_{i=0}^{n} a_i z^i) & \mapsto & \sum_{i=0}^{n} \mu(a_i) z^i := \overline{a}(z). \end{array}$$

g) El *conjunto de Teichmüler*, $\mathcal{T}$, del anillo de Galois R, es un conjunto de representantes del campo residual contenido en el anillo, por lo que $|\mathcal{T}| = p^m$.

Los elementos de un anillo de Galois, $GR(p^s, m)$, poseen dos representaciones. Una de ellas es la *representación multiplicativa*, la cual depende del conjunto de Teichmüller que se considere y está dada de la siguiente forma: para cada $a \in R$, existen únicos $\rho_0(a), \rho_1(a), \ldots, \rho_{s-1}(a) \in \mathcal{T}$ tales que

$$a = \rho_0(a) + p\rho_1(a) + \cdots + p^{s-1}\rho_{s-1}(a). \tag{2}$$

Esta representación es también conocida como la *representación* p*—ádica* ó *extensión* p*—ádica* de a.

Existe un elemento en $GR(p^s, m)$ distinto de cero, $v \in GR(p^s, m)$, tal que v es la raíz del polinomio $h(x)$ (c.f [Wan03, Teorema 14.1]) y todo $a \in GR(p^s, m)$ admite una respresentación única, de la siguiente manera:

$$a = a_0 + a_1 v + \cdots + a_{m-1} v^{m-1}, \tag{3}$$

donde $a_0, a_1, \ldots, a_{m-1} \in R_0$, con R_0 subanillo de $GR(p^s, m)$ tal que $R_0 \cong \mathbb{Z}/p^s\mathbb{Z}$. Esta representación es la *representación aditiva* de los elementos de un anillo de Galois (c.f. [Wan03, Teorema 14.1]). El isomorfismo entre los anillos R_0 y $\mathbb{Z}/p^s\mathbb{Z}$ nos permite establecer la relación $GR(p^s, m) = (\mathbb{Z}/p^s\mathbb{Z})[v]$, ya que al anillo de Galois $GR(p^s, m)$ es un $\mathbb{Z}/p^s\mathbb{Z}$—módulo.

En el anillo $GR(p^s, m)$ podemos encontrar un elemento ω cuyo orden sea $p^m - 1$, tal que ω es la raíz de un polinomio básico primitivo $f(x) \in (\mathbb{Z}/p^s\mathbb{Z})[x]$ de grado m el cual divide a $x^{p^m-1} - 1$ (c.f.[Wan03, Teorema 14.8]). Si con el polinomio $f(x)$ construimos el anillo de Galois $GR_1(p^s, m) = \frac{(\mathbb{Z}/p^s\mathbb{Z})[x]}{(f(x))}$, entonces $GR_1(p^s, m)$ es isomorfo a $GR(p^s, m)$, ya que cualesquiera dos anillos de Galois que tengan la misma cardinalidad y característica, son isomorfos. Es más conveniente trabajar con el anillo $GR_1(p^s, m)$ debido a que la μ—reducción del elemento ω, $\mu(\omega) = \overline{\omega}$, es un *elemento primitivo* del campo residual de $GR_1(p^s, m)$, $\mathbb{F}_{p^m}$, es decir, $\mathbb{F}_{p^m} \setminus \{0\} = \langle\overline{\omega}\rangle$. Así que un conjunto de Teichmüller de un anillo de Galois $GR(p^s, m)$, puede ser escogido de la siguiente manera:

$$\mathcal{T} = \{0, 1, \omega, \ldots, \omega^{p^m-2}\}.$$

En adelante, cuando hablemos de un anillo de Galois, estaremos pensado en uno de la forma

$$GR(p^s, m) = \frac{(\mathbb{Z}/p^s\mathbb{Z})[x]}{(f(x))},$$

donde $f(x)$ es un polinomio mónico básico primitivo de grado m tal que $f(x)$ divide $x^{p^m-1} - 1$ en el anillo $(\mathbb{Z}/p^s\mathbb{Z})[x]$. Ya que de esta manera podemos tener control sobre los elementos del conjunto de Teichmüller, como se mostró previamente.

1.1.1 Anillo de polinomios

Sean $R = GR(p^s, m)$ un anillo de Galois, F el campo residual del anillo R y μ el homomorfismo canónico de R sobre su campo resiudal.

Definición 1.1. *Sean* $R[z]$ *y* $F[z]$ *los anillos de polinomios con coeficientes en* R *y* F*, respectivamente, y* $\overline{\mu}$ *la extensión del homomorfismo canónico* μ*.*

i) *Un polinomio* $f(z) \in R[z]$ *es basico irreducible (primitivo) en el anillo* $R[z]$, *si* $\overline{f}(z)$ *es un polinomio irreducible (primitivo) en* $F[z]$.

ii) *Dos polinomios,* $f(z), g(z) \in R[z]$, *son coprimos si y sólo si,* $f(z)R[z] + g(z)R[z] = R[z]$.

iii) *Sea* I *un ideal de* R, *decimos que* I *es un ideal primario si* $I \neq A$ *y* $ab \in I$ *implica que* $a \in I$ *ó* $b^l \in I$ *para algún* $l \in \mathbb{N}$.

iv) *Sea* $f(z) \in R[z]$ *con* $f(z)$ *distinto del polinomio cero. Entonces* $f(z)$ *es un polinomio primario si* $\langle f(z) \rangle$ *es un ideal primario.*

Algunos resultados sobre polinomios primarios y coprimos son los siguientes:

Lema 1.1. *[Wano3, Lema 14.18] Sean* $f(z) \in R[z]$ *y* $\overline{\mu}(f(z)) = \overline{f}(z)$. *Si* $\overline{f}(z) = G^l(z)$, *con* $G(z)$ *un polinomio irreducible en* $F[z]$ *y* $l \in \mathbb{N}$, *entonces* $f(z)$ *es un polinomio primario.*

Lema 1.2. *[Wano3, Lema 14.19] Sean* $f(z), g(z) \in R[z]$. *Entonces* $f(z)$ *y* $g(z)$ *son coprimos en* $R[z]$ *si y sólo si* $\overline{f}(z)$ *y* $\overline{g}(z)$ *son coprimos en* $F[z]$.

El siguiente Teorema nos proporciona las condiciones bajo las cuales una factorización sobre el anillo R es única.

Teorema 1.1. *[Wano3, Teorema 14.21] Sea* $f(z)$ *un polinomio mónico de grado* $l \geqslant 1$ *en* $R[z]$. *Entonces:*

i) $f(z)$ *puede ser factorizado como producto de algunos, dígamos* r *polinomios primarios mónicos coprimos por pares* $f_1(z), f_2(z), \ldots, f_r(z)$ *sobre* R, *es decir:*

$$f(z) = f_1(z)f_2(z)\cdots f_r(z),$$

y para cada $i = 1, 2, \ldots, r$, $\overline{\mu}(f_i(z))$ *es potencia de algún polinomio mónico irreducible sobre* $F[z]$.

ii) *Si* $f(z) = f_1(z)f_2(z)\cdots f_r(z) = h_1(z)h_2(z)\cdots h_t(z)$ *son dos factorizaciones de* $f(z)$ *en producto de polinomios mónicos primarios coprimos por pares en* $R[z]$, *entonces* $r = t$ *y salvo re-ordenamiento* $f_i(z) = h_i(z)$ *para* $i = 1, 2, \ldots, r$.

1.1.2 Anillo de Witt $\mathcal{W}_2(\mathbb{F})$

Sea $R = GR(p^2, m)$. A continuación definiremos el anillo de vectores (truncado) de Witt, $\mathcal{W}_2(\mathbb{F})$, ya que más adelante enunciaremos algunos resultados importantes cuyas pruebas requieren trabajar con este anillo. Si se desea más información sobre este anillo se puede consultar [Jac89] [GRLAVHon].

Sea $\mathbb{F} = \mathbb{F}_{p^m}$ un campo finito. El anillo de Witt $\mathcal{W}_2(\mathbb{F})$ es el producto cartesiano $\mathbb{F} \times \mathbb{F}$ dotado con la suma "$+_{\mathcal{W}}$" y el producto "$*_{\mathcal{W}}$", definidos de la siguiente manera:

$$(x_0, x_1) +_{\mathcal{W}} (y_0, y_1) = (S_0(x_0, x_1, y_0, y_1), S_1(x_0, x_1, y_0, y_1))$$

donde

$$\begin{aligned} S_0(x_0, x_1, y_0, y_1) &= x_0 + y_0, \\ S_1(x_0, x_1, y_0, y_1) &= (x_1 + y_1) + h(x_0, y_0) \end{aligned}$$

con $h(a, b) = \frac{1}{p}((a+b)^p - a^p - b^p) \in \mathbb{Q}[a, b]$, y

$$(x_0, x_1) *_{\mathcal{W}} (y_0, y_1) = (x_0y_0, x_0^p y_1 + y_0^p x_1).$$

Cuando $\mathbb{F}$ es el campo residual del anillo R, es decir, $\mathbb{F} = R/\mathcal{M}$, entonces el anillo de Galois R y el anillo de Witt $\mathcal{W}_2(\mathbb{F})$ son isomorfos. El isomorfismo está dado por:

$$\begin{aligned} \Psi\colon R &\to \mathcal{W}_2(\mathbb{F}) \\ a &\mapsto (a_0, a_1^p) \end{aligned}$$

donde $a_i = \mu(\rho_i(a))$ para $i = 0, 1$, con μ el homomorfismo canónico de R en su campo residual y $\rho_0(a_i), \rho_1(a_i)$ las componentes $p-$ádicas de a. La función inversa de Ψ es la siguiente:

$$\begin{aligned} \Psi^{-1}\colon \mathcal{W}_2(\mathbb{F}) &\to R \\ (b_0, b_1) &\mapsto B_0 + pB_1^{1/p} \end{aligned}$$

con $B_0, B_1 \in \mathcal{T}$ tales que $\mu(B_0) = b_0$ y $\mu(B_1) = b_1$, y $\mathcal{T}$ es el conjunto de Teichmüller del anillo de Galois R.

Recordemos que el conjunto de Teichmüler, $\mathcal{T}$, del anillo R se puede ver de la forma $\mathcal{T} = \langle\omega\rangle \cup \{0\}$, donde $\langle\overline{\omega}\rangle = \mathbb{F}^*$ con $\overline{\omega} = \mu(\omega)$ y $\mathbb{F}^*$ es el grupo multiplicativo del campo residual, $\mathbb{F}$, del anillo de Galois $R = GR(p^2, m)$. Así que $\Psi(\mathcal{T}) = \{(0,0), (1,0), (\overline{\omega}, 0), \ldots, (\overline{\omega}^{p^m-2}, 0)\} \subseteq \mathcal{W}_2(\mathbb{F})$.

Del resultado que a continuación se enuncia (c.f. [LATR11]) se proporciona un esbozo de su demostración. Además, dicho resultado se empleará en los siguientes capítulos.

Proposición 1.1. *Sean* $\mathbf{a} = \rho_0(\mathbf{a}) + p\rho_1(\mathbf{a}), \mathbf{b} = \rho_0(\mathbf{b}) + p\rho_1(\mathbf{b}) \in R$, *con* $\rho_i(\mathbf{a}), \rho_i(\mathbf{b}) \in \mathcal{T}$, $\mu(\rho_i(\mathbf{a})) = r_i(\mathbf{a})$, $\mu(\rho_i(\mathbf{b})) = r_i(\mathbf{b})$ *para* $i = 0, 1$. *Sea* $\mathbf{a} + \mathbf{b} = \rho_0(\mathbf{a}+\mathbf{b}) + p\rho_1(\mathbf{a}+\mathbf{b})$ *con* $\rho_i(\mathbf{a}+\mathbf{b}) \in \mathcal{T}$ *y* $\mu(\rho_i(\mathbf{a}+\mathbf{b})) = r_i(\mathbf{a}+\mathbf{b})$ *para* $i = 0, 1$. *Entonces*

$$\begin{aligned} r_0(\mathbf{a}+\mathbf{b}) &= r_0(\mathbf{a}) + r_0(\mathbf{b}) \\ r_1(\mathbf{a}+\mathbf{b}) &= [r_1(\mathbf{a})^p + r_1(\mathbf{b})^p - h(r_0(\mathbf{a}), r_0(\mathbf{b}))]^{1/p}. \end{aligned}$$

Demostración. Por el isomorfismo, Ψ, que existe entre el anillo de Galois $R = GR(p^2, m)$ y el anillo de Witt $\mathcal{W}_2(\mathbb{F})$, donde $\mathbb{F}$ es el campo residual de R, sabemos que $\Psi(\mathbf{a}+\mathbf{b}) = \Psi(\mathbf{a}) +_{\mathcal{W}} \Psi(\mathbf{b})$. Desarrollando ambos lados obtenemos lo siguiente:

$$\begin{aligned} \Psi(\mathbf{a}+\mathbf{b}) &= (r_0(\mathbf{a}+\mathbf{b}), r_1(\mathbf{a}+\mathbf{b})^p) \\ \Psi(\mathbf{a}) +_{\mathcal{W}} \Psi(\mathbf{b}) &= (r_0(\mathbf{a}), r_1(\mathbf{a})^p) +_{\mathcal{W}} (r_0(\mathbf{b}), r_1(\mathbf{b})^p) \\ &= (r_0(\mathbf{a}) + r_0(\mathbf{b}), r_1(\mathbf{a})^p + r_1(\mathbf{b})^p + h(r_0(\mathbf{a}), r_0(\mathbf{b}))). \end{aligned}$$

Así que

$$\begin{aligned} r_0(\mathbf{a}+\mathbf{b}) &= r_0(\mathbf{a}) + r_0(\mathbf{b}) \\ r_1(\mathbf{a}+\mathbf{b})^p &= r_1(\mathbf{a})^p + r_1(\mathbf{b})^p + h(r_0(\mathbf{a}), r_0(\mathbf{b})). \end{aligned}$$

□

1.2 TEORÍA DE CÓDIGOS

Las definiciones y propiedades más relevantes de la Teoría de Códigos para códigos sobre anillos y campos finitos se presentan a continuación. Si se desea profundizar en el tema, puede consultarse [MA78], [Ple89], [BF02] y [DLP04].

Sean $\mathcal{A}$ un alfabeto finito (para nuestros fines $\mathcal{A}$ será un anillo finito ó un campo finito), n un entero positivo y $\mathcal{A}^n$ el conjunto de $n-$adas sobre $\mathcal{A}$.

Definición 1.2. *Sea* $\mathcal{C}$ *un subconjunto no vacío de* $\mathcal{A}^n$. *Entonces* $\mathcal{C}$ *es llamado un código de longitud* n *sobre* $\mathcal{A}$. *Un elemento* $\mathbf{c} \in \mathcal{C}$ *es llamado palabra-código . Si* M *es la cardinalidad de* $\mathcal{C}$, *entonces se dice que* $\mathcal{C}$ *es un* (n, M)*-código sobre* $\mathcal{A}$.

i) Si $\mathcal{A} = \mathbb{F}_q$ *es un campo finito, entonces* $\mathcal{A}^n = \mathbb{F}_q^n$ *es un* $\mathbb{F}_q-$*espacio vectorial de dimensión* n. *Un subespacio* $\mathcal{C} \subseteq \mathbb{F}_q^n$ *de dimensión* k *es llamado un* $\mathbb{F}_q-$*código lineal*

ii) Si $\mathcal{A} = \mathcal{R}$ *es un anillo conmutativo finito con unidad, entonces* $\mathcal{R}^n$ *es un* $\mathcal{R}-$*módulo. Decimos que* $\mathcal{C} \subseteq \mathcal{R}^n$ *es un* $\mathcal{R}-$*código lineal de longitud* n *si* $\mathcal{C}$ *es un* $\mathcal{R}-$ *submódulo de* $\mathcal{R}^n$.

La función:

$$\begin{aligned} \sigma : \mathcal{A}^n &\to \mathcal{A}^n \\ \mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) &\mapsto \sigma(\mathbf{c}) = (c_{n-1}, c_0, \ldots, c_{n-2}) \end{aligned} \tag{4}$$

recibe el nombre de *corrimiento cíclico*. Dado un código $\mathcal{C} \subseteq \mathcal{A}^n$, diremos que $\mathcal{C}$ es un $\mathcal{A}-$*código cíclico* si $\sigma(\mathcal{C}) = \{\sigma(\mathbf{c}) : \mathbf{c} \in \mathcal{C}\} = \mathcal{C}$.

Para cualesquiera enteros positivos s y t, sea

$$\begin{aligned} \sigma^{\otimes t} : \mathcal{A}^{st} &\to \mathcal{A}^{st} \\ \mathbf{a} = \left(a^{(1)}|a^{(2)}|\ldots|a^{(t)}\right) &\mapsto \sigma^{\otimes t}(\mathbf{a}) = \left(\sigma(a^{(1)})|\sigma(a^{(2)})|\ldots|\sigma(a^{(t)})\right), \end{aligned} \tag{5}$$

donde $a^{(1)}, a^{(2)}, \ldots, a^{(t)} \in \mathcal{A}^s$, σ es el corrimiento cíclico como en (4) y "|" representa la concatenación. La función $\sigma^{\otimes t}$ es llamada un *corrimiento cuasi-cíclico* . Observemos que cuando $t = 1$, entonces $\sigma^{\otimes t} = \sigma$, es decir, $\sigma^{\otimes t}$ es un corrimiento cíclico. Un código $\mathcal{C} \subseteq \mathcal{A}^n$ es llamado un *código cuasi-cíclico de índice* t si t divide a n y $\sigma^{\otimes t}(\mathcal{C}) = \mathcal{C}$.

1.2.1 Códigos cíclicos lineales sobre campos finitos

Sea $\mathbb{F}_q$ un campo finito con $q = p^m$, donde p es un número primo y m un entero positivo, y sea n un entero positivo. Consideremos el anillo de clases polinomiales módulo $x^n - 1$:

$$\mathcal{A}_n = \frac{\mathbb{F}_q[x]}{(x^n - 1)},$$

y definimos

$$\begin{aligned} \mathcal{P}^n_{\mathbb{F}_q} &: \mathbb{F}_q^n \to \mathcal{A}_n \\ \mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) &\mapsto \mathcal{P}^n_{\mathbb{F}_q}(\mathbf{c}) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + (x^n - 1). \end{aligned} \tag{6}$$

Entonces $\mathcal{P}^n_{\mathbb{F}_q}$ es un isomorfismo de $\mathbb{F}_q-$espacios vectoriales, llamado la *representación polinomial* de los elementos de $\mathbb{F}_q^n$ en el anillo $\mathcal{A}_n$. Dicha representación nos permite identificar de manera única a los elementos de un código como clases polinomiales. Por ello, dado un código $\mathcal{C} \subseteq \mathbb{F}_q^n$, usaremos $\mathcal{C}$ y $\mathcal{P}^n_{\mathbb{F}_q}(\mathcal{C})$ indistintamente.

Un resultado muy útil sobre $\mathbb{F}_q-$ códigos cíclicos lineales nos dice que: $\mathcal{C} \subseteq \mathbb{F}_q^n$ es un $\mathbb{F}_q-$ código cíclico lineal de longitud n, si y sólo si, $\mathcal{P}^n_{\mathbb{F}_q}(\mathcal{C})$ es un ideal del anillo $\mathcal{A}_n$. Dado que $\mathcal{A}_n$ es un anillo de ideales principales entonces $\mathcal{P}^n_{\mathbb{F}_q}(\mathcal{C})$ tiene un único elemento generador $g(x) + I$, con $I = (x^n - 1)$, tal que $g(x)$ es un polinomio mónico de grado más pequeño en $\mathcal{P}^n_{\mathbb{F}_q}(\mathcal{C})$. Además, el polinomio generador $g(x)$ divide a $x^n - 1$ en $\mathbb{F}_q[x]$ y el código $\mathcal{C}$ tiene dimensión $n - grad(g(x))$. Por otro lado, si $g(x) = g_0 + g_1 x + \cdots + g_k x^k$ entonces, $g_0 \neq 0$ y el código $\mathcal{C}$ tiene la siguiente matriz generadora:

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_k & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \cdots & g_k & & \vdots \\ & & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_k \end{pmatrix}.$$

El peso de Hamming de un vector $\mathbf{u} \in \mathbb{F}_q^n$, denotado por $wt_H(\mathbf{u})$, es el número de componentes distintas de cero que tiene $\mathbf{u}$. La distancia de Hamming entre dos vectores $\mathbf{u}, \mathbf{v} \in \mathbf{F}_q^n$ es determinada por $d_H(\mathbf{u}, \mathbf{v}) = wt_H(\mathbf{u} - \mathbf{v})$. La distancia mínima de Hamming d, definida como $d = mín\{d_H(\mathbf{u}, \mathbf{v}) : \mathbf{u}, \mathbf{v} \in \mathcal{C},\ \mathbf{u} \neq \mathbf{v}\}$, es el tercer parámetro de un código, es decir, si $\mathcal{C} \subseteq \mathbb{F}_q^n$ es un $[n, k, d]-$código, entonces la longitud de $\mathcal{C}$ es n, $\mathcal{C}$ es $k-$dimensional y d es la distacia mínima de Hamming.

1.2.2 Códigos cíclicos lineales sobre anillos finitos

Sean $\mathcal{R}$ un anillo finito conmutativo con unidad, y n un entero positivo. Definimos el anillo $\mathcal{R}_n$, de la siguiente manera:

$$\mathcal{R}_n = \frac{\mathcal{R}[x]}{(x^n - 1)}.$$

De manera similar a como se hizó en (6), podemos definir la representación polinomial de $\mathcal{R}^n$ en el anillo $\mathcal{R}_n$ como sigue:

$$\begin{aligned} \mathcal{P}^n_{\mathcal{R}} &: \mathcal{R}^n \to \mathcal{R}_n \\ \mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) &\mapsto \mathcal{P}^n_{\mathcal{R}}(\mathbf{c}) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + (x^n - 1). \end{aligned} \tag{7}$$

Es fácil demostrar que $\mathcal{P}^n_{\mathcal{R}}$ es un isomorfismo de $\mathcal{R}-$módulos. De igual forma, $\mathcal{C} \subseteq \mathcal{R}^n$ es un código cíclico lineal de longitud n si y sólo si $\mathcal{P}^n_{\mathcal{R}}(\mathcal{C})$ es un ideal en el anillo $\mathcal{R}_n$. En algunas ocasiones, haciendo

abuso de la notación, sólo escribiremos $\mathcal{C}$ para referirnos a la representació polinomial del código, en lugar de escribir $\mathcal{P}^n_{\mathcal{R}}(\mathcal{C})$.

H. Q. Dinh y S. R. López-Permouth, obtuvieron en [DLP04], la estructura de un código cíclico sobre un anillo finito de cadena. Ya que los anillos de Galois son anillos finitos de cadena, entonces los resultados que ellos muestran tambien se satisfacen para códigos cíclicos sobre anillos de Galois. A nosotros nos interesan dos de sus resultados, dado que proporcionan el polinomio generador de la representación polinomial de un código cíclico.

El teorema que a continuación enunciamos nos muestra como son los ideales del anillo $R_n = R[x]/(x^n - 1)$ y se emplea para la prueba del Teorema 1.3.

Teorema 1.2. *[DLP04, Teorema 3.2] Asumimos que R es un anillo finito de cadena cuyo ideal maximal es $M = (a)$; sea t la nilpotencia de a. Sea $x^n - 1 = f_1 f_2 \cdots f_r$ una factorización de $x^n - 1$ en $R_n[x]$ en términos de polinomios mónicos básicos irreducibles y coprimos por pares. Entonces cualquier ideal en el anillo $R[x]/(x^n - 1)$ es una suma de ideales de la forma $\langle a^j \hat{f}_i + (x^n - 1)\rangle$ donde $0 \leqslant j \leqslant t$, $0 \leqslant i \leqslant r$ y $\hat{f}_i = \prod_{k \neq i} f_k$.*

Teorema 1.3. *[DLP04, Teorema 3.4] Sea $\mathcal{C}$ un código cíclico lineal de longitud n sobre un anillo finito de cadena R. Entonces existe una única familia de polinomios mónicos coprimos por parejas $F_0, F_1, \ldots, F_t$ en $R[x]$ tales que $F_0 F_1 \cdots F_t = x^n - 1$ y $\mathcal{C} = \langle \hat{F}_1, a\hat{F}_2, \ldots, a^{t-1}\hat{F}_t\rangle$ donde $\hat{F}_i = (x^n - 1)/F_i = \prod_{k \neq i} F_k$, para $1 \leqslant i \leqslant t$. Más aún,*

$$|\mathcal{C}| = |R|^{\sum_{i=0}^{t-1} (t-i)\,grad(F_{i+1})}.$$

Nota 1.1. *Cuando se trabaja con $\mathcal{C}$ como un ideal, nos referimos a su representación polinomial, la cual está determinada por el isomorfismo que se mostró en (7). Además recordemos que cuando decimos que $\mathcal{C} = \langle \hat{F}_1, a\hat{F}_2, \ldots, a^{t-1}\hat{F}_t\rangle$ nos referimos a las clases polinomiales cuyos representantes son los polinomios $\hat{F}_1$ y $a^{j-1}\hat{F}_j$ con $2 \leqslant j \leqslant t$.*

El siguiente resultado nos muestra como es el polinomio generador de la representación polinomial de un código cíclico definido sobre un anillo finito de cadena.

Teorema 1.4. *[DLP04, Teorema 3.6] Sea $\mathcal{C}$ un código cíclico de logitud n, con la notación como en el Teorema 1.3 y $F = \hat{F}_1 + a\hat{F}_2 + \cdots + a^{t-1}\hat{F}_t$. Entonces $\mathcal{C} = \langle F\rangle$.*

Con los teorema previos se prueba lo siguiente:

Teorema 1.5. *Sean $\mathcal{R} = GR(p^2, m)$ y $\mathcal{C}$ un $\mathcal{R}$–código cíclico lineal de longitud n, con n coprimo con p. Entonces existen $A(x), B(x), C(x) \in \mathcal{R}[x]$ polinomios mónicos coprimos por pares tales que $x^n - 1 = A(x)B(x)C(x)$ y $\mathcal{C} = \langle A(x)(B(x) + p)\rangle$ en $\mathcal{R}_n = \mathcal{R}[x]/(x^n - 1)$.*

Demostración. Sabemos que todo anillo de Galois es un anillo finito de cadena donde el ideal maximal es (p) y en particular, en el anillo $\mathcal{R} = GR(p^2, m)$ se tiene que $p^2 = 0$. Así que por el Teorema 1.3 existen polinomios mónicos coprimos por pares $A(x), B(x), C(x) \in \mathcal{R}[x]$ tales que $x^n - 1 = A(x)B(x)C(x)$ y $\mathcal{C} = \langle \hat{C}(x), p\hat{B}(x)\rangle \subseteq \mathcal{R}_n$, donde $\hat{B}(x) = A(x)C(x)$ y $\hat{C}(x) = A(x)B(x)$. Más aún, por el Teorema 1.4, podemos considerar que $\mathcal{C} = \langle \hat{C}(x) + p\hat{B}(x)\rangle$. Sea $\mathcal{D} = \langle G(x)\rangle$ con $G(x) = A(x)(B(x) + p)$, deseamos probar que $\mathcal{C} = \mathcal{D}$. Para ello primero probemos la inclusión $\mathcal{D} \subseteq \mathcal{C}$. Dado que $B(x)$ y $C(x)$ son coprimos, exiten $U(x), V(x) \in \mathcal{R}[x]$ tales que $U(x)B(x) + V(x)C(x) = 1$, haciendo reducción módulo $(x^n - 1)$ y mulplicando por la clase polinomial $pA(x)$ ambos lados tenemos que,

$$pU(x)A(x)B(x) + pV(x)A(x)C(x) = pA(x) \mod (x^n - 1). \tag{8}$$

Sumando $A(x)B(x) \mod (x^n - 1)$ en ambos lados se tiene que,

$$\begin{aligned} A(x)B(x) + pA(x) &\equiv A(x)B(x) + pU(x)A(x)B(x) + pV(x)A(x)C(x) && \mod (x^n - 1) \\ &\equiv (1 + pU(x))A(x)B(x) + pV(x)A(x)C(x) && \mod (x^n - 1) \\ &\equiv (1 + pU(x))\hat{C}(x) + pV(x)\hat{B}(x) && \mod (x^n - 1). \end{aligned}$$

Así, en $\mathcal{R}_n$ se cumple $G(x) = (1 + pU(x))\hat{C}(x) + V(x)p\hat{B}(x)$, donde $(1 + pU(x))\hat{C}(x) + pV(x)\hat{B}(x) \in \mathcal{C} = \langle \hat{C}(x), p\hat{B}(x)\rangle$, por lo que $\mathcal{D} \subseteq \mathcal{C}$.

Por otro lado, dado que $x^n - 1 = A(x)B(x)C(x)$ en $\mathcal{R}[x]$, entonces $C(x)G(x) = C(x)A(x)(B(x) + p) = A(x)B(x)C(x) + pA(x)C(x)$, así que

$$C(x)G(x) \equiv p\hat{B}(x) \quad \text{mód } (x^n - 1). \tag{9}$$

Además $pG(x) = p(A(x)B(x) + pA(x)) = pA(x)B(x)$, por lo que

$$pG(x) \equiv p\hat{C}(x) \quad \text{mód } (x^n - 1). \tag{10}$$

De (9) y (10) se tiene que $p\hat{B}(x), p\hat{C}(x) \in \mathcal{D}$, luego, $pU(x)A(x)B(x)$ y $pV(x)A(x)C(x)$ son elementos de $\mathcal{D}$. Así que por (8) se tiene que $pA(x) \in \mathcal{D}$. Como $\hat{C}(x) = A(x)B(x) = G(x) - pA(x)$, entonces $\hat{C}(x) \in \mathcal{D}$. Por lo tanto $\hat{C}(x) + p\hat{B}(x) \in \mathcal{D}$ y así $\mathcal{C} \subseteq \mathcal{D}$. □

En [LATR12] se puede consultar una versión del Teorema 1.5 para anillos finitos de cadena de índice de nilpotencia 2.

Observación 1.1. *Si el polinomio generador de un* $GR(p^2, m)$*—código cíclico lineal es como en el Teorema 1.5, se tienen los siguientes casos:*

i) Si $C(x) = 1$ *entonces* $G(x) = pA(x)$.

ii) Si $A(x) = 1$ *entonces* $G(x) = B(x) + p$.

Cuando $G(x) = pA(x)$, la imagen de Gray del código cíclico lineal generado por $G(x)$, es cíclica lineal sobre $\mathbb{F}_{p^m}$, y su polinomio generador es de la forma $\overline{A}(x)(x^n - 1)^{p^m - 1} \in \mathbb{F}_{p^m}[x]$, con $\overline{A}(x)$ la μ—reducción de $A(x)$ (c.f. [LA13, Teorema 5.5]). En el capítulo 3 se muestra el comportamiento de las imágenes de Gray de códigos cíclicos lineales, cuando su polinomio generador es $G(x) = B(x) + p$.

2 IMÁGENES DE GRAY DE $\mathcal{R}-$CÓDIGOS LINEALES

Este capítulo tiene como objetivo principal mostrar como está definida la función de Gray sobre anillos de Galois de índice de nilpotencia 2. Además, se enuncian algunas propiedades importantes de la función de Gray. Por último, estudiaremos algunos resultados del artículo [Wolo1], donde se analiza la estructura de las imágenes de Gray de códigos cíclicos lineales sobre el anillo $\mathbb{Z}/4\mathbb{Z}$.

En este capítulo $\mathcal{R}$ es un anillo de Galois de índice de nilpotencia 2, es decir, $\mathcal{R} = GR(p^2, m)$ a menos que se especifique otra cosa.

2.1 LA FUNCIÓN DE GRAY

Comenzamos definiendo el producto de Kronecker expandido de derecha a izquierda.

Definición 2.1. *Sean* $k, l \in \mathbb{N}$, $\mathbf{x} = (x_0, x_1, \cdots, x_{k-1}) \in \mathcal{R}^k$ *y* $\mathbf{y} = (y_0, y_1, \cdots, y_{l-1}) \in \mathcal{R}^l$, *el producto de Kronecker de* $\mathbf{x}$ *con* $\mathbf{y}$ *está definido como:*

$$\mathbf{x} \otimes \mathbf{y} = (x_1\mathbf{y}|x_2\mathbf{y}|\ldots|x_n\mathbf{y}), \tag{11}$$

donde "|" representa la concatenación.
El producto $\mathbf{x} \otimes \mathbf{y}$ *tiene* kl *entradas.*

El producto de Kronecker expandido de izquiera a derecha se define de la siguiente manera:

$$\mathbf{x} \otimes \mathbf{y} = (\mathbf{x}y_1|\mathbf{x}y_2|\ldots|\mathbf{x}y_n),$$

con $\mathbf{x}$ y $\mathbf{y}$ como en la Definición 2.1. Sin embargo nosotros trabajaremos con el producto expandido de derecha a izquierda.
Algunas de las propiedades que posee el producto de Kronecker se enuncian en el siguiente lema.

Lema 2.1. *Sean* $\mathbf{X}, \mathbf{Y}, \mathbf{Z}, \mathbf{X_1}, \mathbf{X_2} \in \mathcal{R}^n$ *y* $\alpha \in \mathcal{R}$. *El producto de Kronecker definido como en (11) satisface las siguientes propiedades::*

i) $\mathbf{X} \otimes (\mathbf{Y} + \mathbf{Z}) = \mathbf{X} \otimes \mathbf{Y} + \mathbf{X} \otimes \mathbf{Z}$,

ii) $(\mathbf{X} + \mathbf{Y}) \otimes \mathbf{Z} = \mathbf{X} \otimes \mathbf{Z} + \mathbf{Y} \otimes \mathbf{Z}$,

iii) $\alpha(\mathbf{X} \otimes \mathbf{Y}) = (\alpha\mathbf{X}) \otimes \mathbf{Y} = \mathbf{X} \otimes (\alpha\mathbf{Y})$,

iv) $(\mathbf{X_1}|\mathbf{X_2}) \otimes \mathbf{Y} = (\mathbf{X_1} \otimes \mathbf{Y}|\mathbf{X_2} \otimes \mathbf{Y})$.

No es difícil verificar las propiedades exhibidas en el Lema 2.1, ya que estas dependen únicamente de la aplicación correcta de la definición del producto de Kronecker.

Sea $\mathbb{F}_q$ el campo residual del anillo $\mathcal{R}$. Denotamos por $\mathbf{C_0} \in \mathbb{F}_q^q$ al vector que enlista a todos los elementos de $\mathbb{F}_q$ y por $\mathbf{C_1} = \mathbf{1_q} \in \mathbb{F}_q^q$ al vector cuyas entradas son todas iguales a 1. Ambos vectores son de longitud $q = p^m$, es decir, $\mathbf{C_0}, \mathbf{C_1} \in \mathbb{F}_{p^m}^q$.

Sean $\mathcal{T} \subseteq \mathcal{R}$ el conjunto de Teichmüller del anillo y $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1})$ un elemento de $\mathcal{R}^n$. Con la representación $p-$ádica de los elementos del anillo $\mathcal{R}$ podemos definir una *"extensión" de la representación* $p-$*ádica* para los elementos del $\mathcal{R}-$módulo $\mathcal{R}^n$ de la siguiente manera:

$$\mathbf{A} = \rho_0(\mathbf{A}) + p\rho_1(\mathbf{A}), \tag{12}$$

donde para $k = 0, 1$, $\rho_k(\mathbf{A}) = (\rho_k(a_0), \rho_k(a_1), \ldots, \rho_k(a_{n-1}))$ y $\rho_0(a_i), \rho_1(a_i)$ son las componentes de la representación p—ádica de cada a_i con $i = 0, \ldots, n-1$, es decir, $a_i = \rho_0(a_i) + p\rho_1(a_i)$. Notemos que $\rho_k(\mathbf{A}) \in \mathcal{T}^n$, ya que $\rho_0(a_i), \rho_1(a_i) \in \mathcal{T}$. Sustituyendo $\rho_0(\mathbf{A})$ y $\rho_0(\mathbf{A})$ en (12) tenemos que

$$\mathbf{A} = (\rho_0(a_0), \rho_0(a_1), \ldots, \rho_0(a_{n-1})) + p(\rho_1(a_0), \rho_1(a_1), \ldots, \rho_1(a_{n-1})), \tag{13}$$

Sea μ el homormofismo canónico del anillo $\mathcal{R}$ en su campo residual. Denotamos a $\mu(\rho_k(a_i))$ por $r_k(a_i)$ para cada $i = 0, \ldots, n-1$ y $k = 0, 1$ ($\mu(\rho_k(a_i)) = r_k(a_i)$). Ya que $\rho_k(\mathbf{A}) = (\rho_k(a_0), \rho_k(a_1), \ldots, \rho_k(a_{n-1}))$ entonces $r_k(\mathbf{A}) = (r_k(a_0), r_k(a_1), \ldots, r_k(a_{n-1}))$ para $k = 0, 1$.

Definición 2.2. *La función de Gray sobre $\mathcal{R}^n$ está dada por:*

$$\begin{aligned} \Phi : \mathcal{R}^n &\longrightarrow \mathbb{F}_q^{nq} \\ \mathbf{A} &\longmapsto \mathbf{C_0} \otimes r_0(\mathbf{A}) + \mathbf{C_1} \otimes r_1(\mathbf{A}) \end{aligned} \tag{14}$$

donde $\mathbf{A} = (a_0, \ldots, a_{n-1}) \in \mathcal{R}^n$ y "$\otimes$" es el producto de Kronecker definido en (11).

Definimos el peso homogéneo en $\mathcal{R}$ de la siguiente manera (c.f.[GS99]):

$$wt_h(a) = \begin{cases} (q-1), & \text{si } a \in R \setminus \langle p \rangle, \\ q, & \text{si } a \in \langle p \rangle, \\ 0, & \text{de otro modo,} \end{cases} \tag{15}$$

con $q = p^m$. El peso homogéneo de los elementos de $\mathcal{R}^n$ está dado por:

$$wt_h(\mathbf{A}) = wt_h(a_0) + wt_h(a_1) + \cdots + wt_h(a_{n-1}), \tag{16}$$

donde $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n$.

El peso homogéneo en $\mathcal{R}^n$, wt_h, induce la métrica $d_h(\mathbf{A}, \mathbf{B}) = wt_h(\mathbf{A} - \mathbf{B})$ en $\mathcal{R}^n$. En el Capítulo 1 se definió la distancia de Hamming, d_H, que es una métrica en $\mathbb{F}_q^{nq}$ ($q = p^m$). La función de Gray posee una propiedad que relaciona estás dos métricas, tal como lo establece el siguiente resultado:

Teorema 2.1. *[GS99, Teorema 1.1] La función de Gray es una isometría inyectiva entre $(\mathcal{R}^n, d_h)$ y $(\mathbb{F}_q^{qn}, d_H)$.*

Otras propiedades de la función de Gray son las que se enuncian en la siguiente proposición.

Proposición 2.1. *[LATR11] Sean $\mathbf{A} = \rho_0(\mathbf{A}) + p\rho_1(\mathbf{A})$ y $\mathbf{B} = \rho_0(\mathbf{B}) + p\rho_1(\mathbf{B})$ elementos cualesquiera de $\mathcal{R}^n$. Entonces:*

$$\begin{aligned} \Phi(p\mathbf{B}) &= (r_0(\mathbf{B}), r_0(\mathbf{B}), \ldots, r_0(\mathbf{B})) \\ \Phi(\mathbf{A} + p\mathbf{B}) &= \Phi(\mathbf{A}) + \Phi(p\mathbf{B}), \end{aligned}$$

donde $\mu(\rho_0(\mathbf{B})) = r_0(\mathbf{B})$.

Demostración. Notemos que $p\mathbf{B} = p(\rho_0(\mathbf{B}) + p\rho_1(\mathbf{B})) = p\rho_0(\mathbf{B})$, es decir $\rho_0(p\mathbf{B}) = 0_{\mathcal{R}^n}$ y $\rho_1(p\mathbf{B}) = \rho_0(\mathbf{B})$, donde $0_{\mathcal{R}^n} \in \mathcal{T}^n \subseteq \mathcal{R}^n$ es la n—ada cuyas entradas son todas iguales a 0. Entonces

$$\begin{aligned} \Phi(p\mathbf{B}) &= \mathbf{C_0} \otimes r_0(p\mathbf{B}) + \mathbf{C_1} \otimes r_1(p\mathbf{B}) \\ &= \mathbf{C_0} \otimes 0_{\mathbb{F}_q^n} + \mathbf{C_1} \otimes r_0(\mathbf{B}), \end{aligned}$$

pero $\mathbf{C_0} \otimes 0_{\mathbb{F}_q^n} = 0_{\mathbb{F}_q^{nq}}$ y $\mathbf{C_1} \otimes r_0(\mathbf{B}) = (r_0(\mathbf{B}), \ldots, r_0(\mathbf{B})) \in \mathbb{F}_q^{nq}$ pues $\mathbf{C_1} \in \mathbb{F}_q^q$ es el vector cuyas entradas son todas iguales a 1. Por lo tanto $\Phi(p\mathbf{B}) = (r_0(\mathbf{B}), \ldots r_0(\mathbf{B}))$.

La prueba de la segunda igualdad es un poco más elaborada. A continuación mostramos un esbozo de su prueba. Primero debemos probar con ayuda de la Proposición 1.1 que $r_0(\mathbf{A} + p\mathbf{B}) = r_0(\mathbf{A})$ y $r_1(\mathbf{A} + p\mathbf{B}) = r_1(\mathbf{A}) + r_0(\mathbf{B})$, despues aplicamos la función de Gray a $\mathbf{A} + p\mathbf{B}$, y sustituimos $r_0(\mathbf{A} + p\mathbf{B})$ y $r_1(\mathbf{A} + p\mathbf{B})$, obteniendo lo siguiente:

$$\Phi(\mathbf{A} + p\mathbf{B}) = \mathbf{C_0} \otimes r_0(\mathbf{A}) + \mathbf{C_1} \otimes (r_1(\mathbf{A}) + r_0(\mathbf{B})),$$

desarrollando el lado derecho de la igualdad tenemos que

$$\Phi(\mathbf{A} + p\mathbf{B}) = (\mathbf{C_0} \otimes r_0(\mathbf{A}) + \mathbf{C_1} \otimes r_1(\mathbf{A})) + \mathbf{C_1} \otimes r_0(\mathbf{B}),$$

por lo que $\Phi(\mathbf{A} + p\mathbf{B}) = \Phi(\mathbf{A}) + \Phi(p\mathbf{B})$. □

2.2 IMÁGENES LINEALES DE UN $\mathcal{R}$—CÓDIGO LINEAL

A continuación se introduce un poco de notación que se empleará en los siguientes resultados:

- $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1})$, $\mathbf{B} = (b_0, b_1, \ldots, b_{n-1})$ son elementos de $\mathcal{R}^n$,
- para cada $i \in \{0, \ldots, n-1\}$, $a_i = \rho_0(a_i) + p\rho_1(a_i) \in \mathcal{R}$ es la expansión p-ádica de a_i,
- $r_k(a_i) = \mu(\rho_k(a_i))$ con $k = 0, 1$,
- $\rho_k(\mathbf{A}) = (\rho_k(a_0), \rho_k(a_1), \ldots, \rho_k(a_{n-1}))$ y $r_k(\mathbf{A}) = (r_k(a_0), r_k(a_1), \ldots, r_k(a_{n-1}))$ para $k = 0, 1$.

Tambien consideremos lo anterior para $\mathbf{B}$, $\mathbf{A}+\mathbf{B}$ y $\mathbf{A}+p\mathbf{B}$.

Sean $\theta(a_i, b_i) = r_1(a_i) + r_1(b_i) - [r_1(a_i)^p + r_1(b_i)^p - h(r_0(a_i), r_0(b_i))]^{\frac{1}{p}}$, donde $h(r_0(a_i), r_0(b_i))$ es como se definió en la Sección 1.1.2, $\Theta(a_i, b_i) \in \mathcal{T}$ y $\mu(\Theta(a_i, b_i)) = \theta(a_i, b_i) \in \mathbb{F}_{p^m}$ tales que:

Proposición 2.2. *[LATR11] Sea Φ la función de Gray en $\mathcal{R}^n$ introducida anteriormente en (2.2). Con la notación anterior para elementos cualesquiera $\mathbf{A} = (a_0, \ldots, a_{n-1})$, $\mathbf{B} = (b_0, \ldots, b_{n-1}) \in \mathcal{R}^n$ se tiene que:*

$$\Phi(\mathbf{A}) + \Phi(\mathbf{B}) - \Phi(\mathbf{A}+\mathbf{B}) = \Phi(p\Theta(\mathbf{A}, \mathbf{B})), \tag{17}$$

donde

$$\begin{aligned} \Theta(\mathbf{A}, \mathbf{B}) &= (\Theta(a_0, b_0), \ldots, \Theta(a_{n-1}, b_{n-1})) \in \mathcal{T}^n, \\ \theta(\mathbf{A}, \mathbf{B}) &= (\theta(a_0, b_0), \ldots, \theta(a_{n-1}, b_{n-1})) \in \mathbb{F}_{p^m}^n, \text{ y} \\ \Phi(p\Theta(\mathbf{A}, \mathbf{B})) &= (\theta(\mathbf{A}, \mathbf{B}), \ldots, \theta(\mathbf{A}, \mathbf{B})). \end{aligned}$$

Demostración. Para demostrar (17) se requiere desarrollar el lado izquierdo de la igualdad,

$$\begin{aligned} \Phi(\mathbf{A}) + \Phi(\mathbf{B}) - \Phi(\mathbf{A}+\mathbf{B}) &= (\mathbf{C_0} \otimes r_0(\mathbf{A}) + \mathbf{C_1} \otimes r_1(\mathbf{A})) + (\mathbf{C_0} \otimes r_0(\mathbf{B}) + \mathbf{C_1} \otimes r_1(\mathbf{B})) \\ &\quad -(\mathbf{C_0} \otimes r_0(\mathbf{A}+\mathbf{B}) + \mathbf{C_1} \otimes r_1(\mathbf{A}+\mathbf{B})) \\ &= (\mathbf{C_0} \otimes (r_0(\mathbf{A}) + r_0(\mathbf{B})) + \mathbf{C_1} \otimes (r_1(\mathbf{A}) + r_1(\mathbf{B})) \\ &\quad -\mathbf{C_0} \otimes r_0(\mathbf{A}+\mathbf{B}) - \mathbf{C_1} \otimes r_1(\mathbf{A}+\mathbf{B})). \end{aligned}$$

Extendiendo los resultados de la Proposición 1.1 a $\mathbf{A}$ y $\mathbf{B}$ podemos decir que $r_0(\mathbf{A}+\mathbf{B}) = r_0(\mathbf{A}) + r_0(\mathbf{B})$ y $r_1(\mathbf{A}+\mathbf{B}) = [r_1(\mathbf{A})^p + r_1(\mathbf{B})^p - h(r_0(\mathbf{A}), r_0(\mathbf{B}))]^{1/p}$ donde

$$\begin{aligned} r_1(\mathbf{A})^p &= (r_1(a_0)^p, r_1(a_1)^p, \ldots, r_1(a_{n-1})^p) \text{ (análogo para } r_1(\mathbf{B})^p) \text{ y} \\ h(r_0(\mathbf{A}), r_0(\mathbf{B})) &= (h(r_0(a_0), r_0(b)), \ldots, h(r_0(a_{n-1}), r_0(b_{n-1}))). \end{aligned}$$

Por lo que, la entrada i—ésima de la n—ada $[r_1(\mathbf{A})^p + r_1(\mathbf{B})^p - h(r_0(\mathbf{A}), r_0(\mathbf{B}))]^{1/p}$ es :

$$[r_1(a_i)^p + r_1(b_i)^p - h(r_0(a_i), r_0(b_i))]^{1/p}.$$

Sustituyendo $r_0(\mathbf{A}+\mathbf{B})$ y $r_1(\mathbf{A}+\mathbf{B})$ y asociando de manera adecuada, se sigue que :

$$\begin{aligned} \Phi(\mathbf{A}) + \Phi(\mathbf{B}) - \Phi(\mathbf{A}+\mathbf{B}) &= \mathbf{C_1} \otimes (r_1(\mathbf{A}) + r_1(\mathbf{B}) - [r_1(\mathbf{A})^p + r_1(\mathbf{B})^p - h(r_0(\mathbf{A}), r_0(\mathbf{B}))]^{1/p}) \\ &= r_1(\mathbf{A}) + r_1(\mathbf{B}) - [r_1(\mathbf{A})^p + r_1(\mathbf{B})^p - h(r_0(\mathbf{A}), r_0(\mathbf{B}))]^{1/p}. \end{aligned}$$

Notemos que la i—ésima entrada de la n—ada $r_1(\mathbf{A}) + r_1(\mathbf{B}) - [r_1(\mathbf{A})^p + r_1(\mathbf{B})^p - h(r_0(\mathbf{A}), r_0(\mathbf{B}))]^{1/p}$ es:

$$r_1(a_i) + r_1(b_i) - [r_1(a_i)^p + r_1(a_i)^p - h(r_0(a_i), r_0(b_i))]^{1/p} = \theta(a_i, b_i).$$

De ahí que, $r_1(\mathbf{A}) + r_1(\mathbf{B}) - [r_1(\mathbf{A})^p + r_1(\mathbf{B})^p - h(r_0(\mathbf{A}), r_0(\mathbf{B}))]^{1/p} = \theta(\mathbf{A}, \mathbf{B})$. Por lo tanto,

$$\Phi(\mathbf{A}) + \Phi(\mathbf{B}) - \Phi(\mathbf{A}+\mathbf{B}) = \theta(\mathbf{A}, \mathbf{B}) = \Phi(p\Theta(\mathbf{A}, \mathbf{B})).$$

□

El siguiente teorema nos da las condiciones necesarias y suficientes para que la imagen de un $\mathcal{R}$—código lineal sea $\mathbb{F}_{p^m}$—lineal.

Teorema 2.2. *Sea $\mathcal{C}$ un $\mathcal{R}$—código lineal de longitud n y sea Φ la función de Gray en $\mathcal{R}^n$. Entonces $\Phi(\mathcal{C})$ es un $\mathbb{F}_{p^m}$—código lineal si y sólo si $p\Theta(A,B) \in \mathcal{C}$ para toda $A, B \in \mathcal{C}$.*

En la prueba del teorema emplearemos la notación $\underline{\mathbf{A}}$ para denotar a los elementos del espacio vectorial $\mathbb{F}_{p^m}$.

Demostración. Saen $\mathbf{U}, \mathbf{V} \in \mathcal{R}^n$. Por la Proposición 2.2 sabemos que $\Phi(\mathbf{U}) + \Phi(\mathbf{V}) = \Phi(\mathbf{U}+\mathbf{V}) + \Phi(p\Theta(\mathbf{U},\mathbf{V}))$ y por la Proposición 2.1 se sigue que

$$\Phi(\mathbf{U}) + \Phi(\mathbf{V}) = \Phi(\mathbf{U}+\mathbf{V}+p\Theta(\mathbf{U},\mathbf{V})). \tag{18}$$

Supongamos que $\Phi(\mathcal{C})$ es $\mathbb{F}_{p^m}$—lineal. Sean $\mathbf{A},\mathbf{B} \in \mathcal{C}$, entonces $\Phi(\mathbf{A}), \Phi(\mathbf{B}) \in \Phi(\mathcal{C})$. Más aún, por hipótesis, $\Phi(\mathbf{A}) + \Phi(\mathbf{B}) \in \Phi(\mathcal{C})$, así que por (18), $\Phi(\mathbf{A}+\mathbf{B}+p\Theta(\mathbf{A},\mathbf{B})) \in \Phi(\mathcal{C})$. De ahí que, $\mathbf{A}+\mathbf{B}+p\Theta(\mathbf{A},\mathbf{B}) \in \mathcal{C}$. Como $\mathcal{C}$ es $\mathcal{R}$—lineal, entonces $p\Theta(\mathbf{A},\mathbf{B}) \in \mathcal{C}$.

Ahora, supongamos que para cualesquiera $\mathbf{A},\mathbf{B} \in \mathcal{C}$ se cumple que $p\Theta(\mathbf{A},\mathbf{B}) \in \mathcal{C}$. Sean $\underline{\mathbf{A}}, \underline{\mathbf{B}} \in \Phi(\mathcal{C})$ y $\alpha \in \mathbb{F}_{p^m}$. Dado que $\underline{\mathbf{A}}, \underline{\mathbf{B}} \in \Phi(\mathcal{C})$, existen $\mathbf{A},\mathbf{B} \in \mathcal{C}$ tales que $\Phi(\mathbf{A}) = \underline{\mathbf{A}}$ y $\Phi(\mathbf{B}) = \underline{\mathbf{B}} \in \Phi(\mathcal{C})$. Por hipótesis tenemos que $p\Theta(\mathbf{A},\mathbf{B}) \in \mathcal{C}$ y como $\mathcal{C}$ es $\mathcal{R}$—lineal, entonces $\mathbf{A}+\mathbf{B}+p\Theta(\mathbf{A},\mathbf{B}) \in \mathcal{C}$. Por lo que $\Phi(\mathbf{A}+\mathbf{B}+p\Theta(\mathbf{A},\mathbf{B})) \in \Phi(\mathcal{C})$. Así que $\Phi(\mathbf{A}) + \Phi(\mathbf{B}) \in \Phi(\mathcal{C})$ (por (18)). Por otro lado, ya que $\alpha \in \mathbb{F}_{p^m}$ entonces $\alpha = 0$ ó $\alpha \in \mathbb{F}_{p^m}^*$. Si $\alpha = 0$ hemos terminado, pero si $\alpha \in \mathbb{F}_{p^m}^* = \langle\overline{\omega}\rangle$ entonces existe $s \in \{0,1,\ldots,p^m-2\}$ tal que $\alpha = \overline{\omega}^s$ donde $\overline{\omega} = \mu(\omega)$ con $\omega \in \mathcal{R}$ de tal forma que $\mathcal{T} = \langle\omega\rangle \cup \{0\}$. Ya sabemos que para $\underline{\mathbf{A}} \in \Phi(\mathcal{C})$ existe $\mathbf{A} \in \mathcal{C}$ tal que $\Phi(\mathbf{A}) = \underline{\mathbf{A}}$. Entonces

$$\begin{aligned} \alpha\underline{\mathbf{A}} &= \overline{\omega}^s\Phi(\mathbf{A}) \\ &= \overline{\omega}^s(\mathbf{C_0} \otimes r_0(\mathbf{A}) + \mathbf{C_1} \otimes r_1(\mathbf{A})) \\ &= \mathbf{C_0} \otimes \overline{\omega}^s r_0(\mathbf{A}) + \mathbf{C_1} \otimes \overline{\omega}^s r_1(\mathbf{A}), \end{aligned}$$

donde

$$\overline{\omega}^s r_i(\mathbf{A}) = (\overline{\omega}^s r_i(a_0), \ldots, \overline{\omega}^s r_i(a_{n-1})),$$

para $i = 0, 1$. Pero, recordemos que para cada $j \in \{0,1,\ldots,n-1\}$, $r_i(a_j) = \mu(\rho_i(a_j))$, así que $\overline{\omega}^s r_i(a_j) = \mu(\omega^s)\mu(\rho_i(a_j)) = \mu(\omega^s\rho_i(a_j))$, con $i = 0,1$ y $j = 0,1,\ldots,n-1$. Dado que, $\omega^s \in \mathcal{T}$ y $\rho_i(a_j) \in \mathcal{T} = \langle\omega\rangle \cup \{0\}$, entonces $\omega^s\rho_i(a_j) \in \mathcal{T}$ para cada i y cada j. Sea $\mathbf{B} = (\omega^s a_0, \omega^s a_1, \ldots, \omega^s a_{n-1}) = \omega^s\mathbf{A}$, como $\mathbf{A} \in \mathcal{C}$ y $\mathcal{C}$ es $\mathcal{R}$—lineal, se sigue que $\mathbf{B} = \omega^s\mathbf{A} \in \mathcal{C}$. Por lo que $\Phi(\mathbf{B}) \in \Phi(\mathcal{C})$, y por la construcción de $\mathbf{B}$ se cumple que $r_i(\mathbf{B}) = \alpha r_i(\mathbf{A})$. Por lo que $\Phi(\mathbf{B}) = \alpha\Phi(\mathbf{A}) = \alpha\underline{\mathbf{A}} \in \Phi(\mathcal{C})$. Por lo tanto $\Phi(\mathcal{C})$ es $\mathbb{F}_{p^m}$—lineal. □

2.2.1 Permutación de Nechaev

Al estudiar las imágenes de Gray de $\mathcal{R}$—códigos cíclicos una permutación que suele destacar, es la permutación de Nechaev, ya que en algunos casos, las imágenes de Gray de ciertos códigos cíclicos se vuelve cíclica bajo esta permutación. Es por eso que a conitnuación damos la definición de esta permutación.

Sean $n \in \mathbb{N}$ tal que $(n,p) = 1$ y n' su inverso módulo p, es decir, $nn' \equiv 1 \mod p$. Además, sea $q = p^m$.

Definición 2.3. *Sea π la permutación definida sobre $\{0,1,\ldots,nq-1\}$:*

$$\forall u: \ 0 \leqslant u \leqslant p-1 \ y \ \forall v: \ un \leqslant v \leqslant (u+1)n-1$$

$$\pi(v) = \left((vn' - u)_p n + v\right)_{np},$$

donde $(\bullet)_p$ denota la reducción módulo p y $(\bullet)_{np}$ denota la reducción módulo np.

Se define la permutación global de Nechaev Π en $\mathbb{F}_q^{nq}$, con $q = p^m$, como

$$\Pi(c_0, c_1, \ldots, c_v, \ldots, c_{nq-1}) = (c_{\pi(0)}, c_{\pi(1)}, \ldots, c_{\pi(v)}, \ldots, c_{\pi(nq-1)}).$$

Sin embargo, como se muestra en los ejemplos que se implementaron en MAGMA, para el tipo de códigos cíclicos lineales que trabajaremos en el Capíutlo 3 la permutación de Nechaev no aporta información extra.

2.3 IMÁGENES DE GRAY DE UN $\mathbb{Z}/4\mathbb{Z}$–CÓDIGO CÍCLICO LINEAL

Jacques Wolfman en [Wolo1] determina como son todos los $\mathbb{Z}/4\mathbb{Z}$−códigos cíclicos de longitud impar, tales que sus imágenes bajo la función de Gray son códigos cíclicos lineales. Estudiar y comprender los resultados que este artículo exhibe nos brindó un primer acercamiento al comportamiento de la función de Gray sobre anillos de Galois de la forma $GR(p^2, m)$, donde, para $\mathbb{Z}/4\mathbb{Z}$, $p = 2$ y $m = 1$. Es por ello que a continuación se muestran los resultados que, para nuestros fines, resultaron más relevantes.

En esta sección $\mathcal{R}$ denotará el anillo de enteros módulo 4, es decir $\mathcal{R} = \mathbb{Z}/4\mathbb{Z}$ y n será un entero positivo coprimo con 2.

- El ideal maximal de $\mathcal{R}$ es $\langle 2\rangle$.
- El campo residual del anillo $\mathcal{R}$ es isomorfo a $\mathbb{F}_2 = \{0, 1\}$.
- El conjunto de Teichmüller del anillo $\mathcal{R}$, con el que trabajaremos, es $\mathcal{T} = \{0, 1\}$.
- Sea $\overline{\mu}$ el homomorfismo canónico de $\mathcal{R}[x]$ en $\mathbb{F}_2[x]$. Entonces a las imágenes bajo dicho homomorfismo las denotaremos por $\overline{A}(x) \in \mathbb{F}_2[x]$, con $A(x) \in \mathcal{R}[x]$. Más aún, a los elementos del anillo de polinomios $\mathbb{F}_2[x]$, los denotaremos con una barra superior, es decir $\overline{F}(x) \in \mathbb{F}_2[x]$.

Definimos el anillo de clases residuales

$$\mathcal{R}_n = \frac{\mathcal{R}[x]}{(x^n - 1)}.$$

Para referirnos a los elementos del anillo $\mathcal{R}_n$ denotaremos a $F(x) + (x^n - 1)$ por $F(x) + I_4^n$, donde I_4^n es el ideal $(x^n - 1)$ en el anillo $\mathcal{R}[x]$.

Y para los elementos del anillo

$$\mathcal{F}_{2n} = \frac{\mathbb{F}_2[x]}{(x^{2n} - 1)},$$

la notación que emplearemos será de la forma $\overline{F}(x) + (x^{2n} - 1) = \overline{F}(x) + I_2^{2n}$ donde I_2^{2n} hace referencia al ideal generado por el polinomio $x^{2n} - 1$ sobre el anillo $\mathbb{F}_2[x]$ y $\overline{F}(x) \in \mathbb{F}_2[x]$.

Sea A un anillo conmutativo. Si $\mathbf{U} = (u_0, u_1, \ldots, u_{t-1})$ y $\mathbf{V} = (v_0, v_1, \ldots, v_{t-1})$ son dos elementos en A^t con $t \in \mathbb{N}$, entonces

$$\mathbf{U} * \mathbf{V} = (u_0v_0, u_1v_1, \ldots, u_{t-1}v_{t-1}). \tag{19}$$

Similarmente, para dos polinomios en $A[x]$, tenemos que

$$\left(\sum_{i=0}^{t-1} u_i x^i\right) * \left(\sum_{i=0}^{t-1} v_i x^i\right) = \sum_{i=0}^{t-1} u_i v_i x^i. \tag{20}$$

Si $\mathcal{U}$ y $\mathcal{V}$ son dos subconjuntos de A^t entonces

$$\mathcal{U} * \mathcal{V} = \{\mathbf{U} * \mathbf{V} | \mathbf{U} \in \mathcal{U},\ \mathbf{V} \in \mathcal{V}\}.$$

En los siguientes dos resultados omitiremos la notación de clase residual para los elementos de los anillos $\mathcal{R}_n$ y $\mathbb{F}_2[x]/(x^n - 1)$. Denotando a los elementos de $\mathcal{R}_n$ de la forma $F(x) + (x^n - 1) := \mathbf{F}(x)$, y a los del anillo $\mathbb{F}_2[x]/(x^n - 1)$ por $\overline{F}(x) + (x^n - 1) = \overline{\mathbf{F}}(x)$.

Observación 2.1. *Sea* $a \in \mathcal{R} = \mathbb{Z}/4\mathbb{Z}$, *sabemos que* $a = \rho_0(a) + 2\rho_1(a)$, *donde* $\rho_0(a), \rho_1(a) \in \mathcal{T} = \{0, 1\}$. *Entonces* $\mu(a) = \mu(\rho_0(a) + 2\rho_1(a)) = \mu(\rho_0(a))$, *es decir* $\mu(a) = \mu(\rho_0(a))$. *Por lo que si tomamos* $F(x) \in \mathcal{R}[x]$, *se sigue que* $\overline{F}(x) = \overline{\mu}(F(x)) = \overline{\mu}(\rho_0(F(x)) + 2\rho_1(F(x)))$ *donde* $\rho_j(F(x)) = \sum_{i=0}^{n-1} \rho_j(f_i)x^i$ *para* $j = 0, 1$.

Proposición 2.3. *[Wolo1, Proposición 1]*

i) Si $\mathbf{U}(x) \in \mathcal{R}_n$ *entonces* $2\mathbf{U}(x) = 2\rho_0(\mathbf{U}(x))$ *en* $\mathcal{R}_n$.

ii) *Si* $\overline{\mathbf{U}}(x), \overline{\mathbf{V}}(x) \in \mathbb{F}_2[x]/(x^n-1)$, *entonces* $2\rho_0(\mathbf{U}(x)) = 2\rho_0(\mathbf{V}(x))$ *en* $\mathcal{R}_n$ *implica que* $\overline{\mathbf{U}}(x) = \overline{\mathbf{V}}(x)$.

iii) *Si* $\mathbf{U}(x) \in \mathcal{R}_n$ *entonces* $\langle 2\mathbf{U}(x)\rangle = \langle 2\rho_0(\mathbf{U}(x))\rangle$.

Demostración. i) Sea $\mathbf{U}(x) \in \mathcal{R}_n$ con $\mathbf{U}(x) = \sum_{i=0}^{n-1} u_i x^i$, para cada $0 \leqslant i \leqslant n-1$, $u_i = \rho_0(u_i) + 2\rho_1(u_i)$ con $\rho_0(u_i)\rho_1(u_i) \in \mathcal{T}$. Entonces $2u_i = 2\rho_0(u_i)$ en $\mathcal{R}$, por lo que

$$2\mathbf{U}(x) = \sum_{i=0}^{n-1} 2\rho_0(u_i)x^i = 2\sum_{i=0}^{n-1} \rho_0(u_i)x^i = 2\rho_0(\mathbf{U}(x)).$$

ii) Sean $\overline{\mathbf{U}}(x), \overline{\mathbf{V}}(x) \in \mathbb{F}_2[x]/(x^n-1)$, con $\overline{\mathbf{U}}(x) = \sum_{i=0}^{n-1} \overline{u}_i x^i$ y $\overline{\mathbf{V}}(x) = \sum_{i=0}^{n-1} \overline{v}_i x^i$.Si $2\rho_0(\mathbf{U}(x)) = 2\rho_0(\mathbf{V}(x))$, entonces para cada $i \in \{0, 1, \ldots, n-1\}$ se cumple que $2u_i = 2v_i$. Por lo que $2u_i - 2v_i \equiv 0 \mod 4$. Entonces $2(u_i - v_i) = 4k_i$ para algún $k_i \in \mathbb{Z}$. De ahí que $u_i - v_i = 2k_i$ y así, $u_i = v_i$ en $\mathbb{F}_2$, es decir, $\overline{u}_i = \overline{v}_i$. Por lo tanto $\overline{\mathbf{U}}(x) = \overline{\mathbf{V}}(x)$ en $\mathbb{F}_2[x]/(x^n-1)$.

iii) Sea $\mathbf{U}(x) \in \mathcal{R}_n$. Del inciso i) tenemos que $2\mathbf{U}(x) = 2\rho_0(\mathbf{U}(x))$. Así que $\langle 2\mathbf{U}(x)\rangle = \langle 2\rho_0(\mathbf{U}(x))\rangle$. □

Proposición 2.4. *[Wolo1, Proposición 6] Si* $G(x) = A(x)(B(x)+2)$ *es el polinomio generador de un código cíclico lineal sobre* $\mathcal{R}$ *de longitud impar* n, *entonces*

$$\mathcal{P}_{\mathcal{R}}^n(\mathcal{C}) \cap 2\mathcal{R}_n = \langle 2\mathbf{A}(x)\rangle,$$

donde $2\mathcal{R}_n = \{2\mathbf{F}(x) \mid \mathbf{F}(x) \in \mathcal{R}_n\}$ *y* $A(x)B(x)C(x) = x^n - 1$ *en* $\mathcal{R}[x]$.

Demostración. Si $\mathbf{U}(x) \in \mathcal{P}_{\mathcal{R}}^n(\mathcal{C}) \cap 2\mathcal{R}_n$, entonces $\mathbf{U}(x) = \mathbf{G}(x)\mathbf{T}(x)$ y $\mathbf{U}(x) = 2\mathbf{S}(x)$ para algunos $\mathbf{T}(x), \mathbf{S}(x) \in \mathcal{R}_n$, así que $U(x) - G(x)T(x), U(x) - 2S(x) \in (x^n-1)$. Como $grad(U(x) - G(x)T(x)) < n$ y $grad(U(x) - 2S(x)) < n$, entonces $U(x) - G(x)T(x) = 0$ y $U(x) - 2S(x) = 0$. Por lo que

$$U(x) = G(x)T(x) \text{ y } U(x) = 2S(x). \tag{21}$$

Ya que $C(x)$ es un polinomio mónico, entonces podemos dividir a $T(x)$ por $C(x)$ en $\mathcal{R}[x]$. Así que existen $Q(x), R(x) \in \mathcal{R}[x]$ tales que $T(x) = Q(x)C(x) + R(x)$ con $grad(R(x)) < grad(C(x))$ ó $R(x) = 0$. Sustituyendo $G(x)$ y $T(x)$ en (21) se sigue que

$$\begin{aligned} U(x) &= (A(x)B(x) + 2A(x))(Q(x)C(x) + R(x)) \\ &= Q(x)(x^n-1) + R(x)A(x)B(x) + 2A(x)[Q(x)C(x) + R(x)]. \end{aligned}$$

Sean $D(x) = R(x)A(x)B(x)$ y $H(x) = A(x)[Q(x)C(x) + R(x)]$, entonces $U(x) = Q(x)(x^n-1) + D(x) + 2H(x)$. Dado que $U(x) = 2S(x)$, tenemos que

$$Q(x)(x^n-1) + D(x) + 2H(x) - 2S(x) = 0,$$

todo esto en $\mathcal{R}[x]$. Aplicando $\overline{\mu}$ en ambos lados, se cumple que

$$\overline{Q}(x)(x^n-1) + \overline{D}(x) = 0.$$

Entonces $\overline{A}(x)\overline{B}(x)\overline{R}(x) = \overline{Q}(x)(x^n-1)$ en $\mathbb{F}_2[x]$, es decir, $\overline{A}(x)\overline{B}(x)\overline{R}(x) \in (x^n-1)$. Como $grad(R(x)) < grad(C(x))$ entonces $grad(D(x)) < n$, así que $\overline{A}(x)\overline{B}(x)\overline{R}(x) = 0$ en $\mathbb{F}_2[x]$. Recordemos que $A(x)$ y $B(x)$ dividen a x^n-1 en $\mathcal{R}[x]$, por lo que $\overline{A}(x)$ y $\overline{B}(x)$ son distintos de cero. Así que $\overline{A}(x)\overline{B}(x) \neq 0$ y $\overline{A}(x)\overline{B}(x)\overline{R}(x) = 0$. Dado que $\mathbb{F}_2[x]$ es un dominio entero entonces $\overline{R}(x) = 0$. Por lo que, en $\mathcal{R}_n$, se sigue que $R(x) \in \langle 2\rangle = \{2F(x) \mid F(x) \in \mathcal{R}\} \subseteq \mathcal{R}[x]$. De ahí que $R(x) = 2K(x)$ para algún $K(x) \in \mathcal{R}][x]$. Así que $D(x) = 2K(x)A(x)B(x)$. Entonces $U(x) = Q(x)(x^n-1) + 2K(x)A(x)B(x) + 2H(x)$. Por lo que

$$\begin{aligned} \mathbf{U}(x) &= 2\mathbf{A}(x)(\mathbf{K}(x)\mathbf{B}(x)) + 2\mathbf{A}(x)(\mathbf{Q}(x)\mathbf{C}(x) - \mathbf{R}(x)) \\ &= 2\mathbf{A}(x)[\mathbf{K}(x)\mathbf{B}(x) + \mathbf{Q}(x)\mathbf{C}(x) - \mathbf{R}(x)] \\ &\in \langle 2\mathbf{A}(x)\rangle. \end{aligned}$$

Por lo tanto $\mathbf{U}(x) \in \langle 2\mathbf{A}(x)\rangle$. Así, $\mathcal{P}_{\mathcal{R}}^n \cap 2\mathcal{R}_n \subseteq \langle 2\mathbf{A}(x)\rangle$.

Para probar la otra inclusión observemos que $\langle 2\mathbf{A}(x)\rangle \subseteq \mathcal{P}_{\mathcal{R}}^n(\mathcal{C})$ (ver prueba del Teorema 1.5) y $\langle 2\mathbf{A}(x)\rangle \subseteq 2\mathcal{R}_n$, por lo que $\langle 2\mathbf{A}(x)\rangle \subseteq \mathcal{P}_{\mathcal{R}}^n(\mathcal{C}) \cap 2\mathcal{R}_n$. □

La función:

$$\begin{aligned} \nu\colon \mathcal{R}^n &\to \mathcal{R}^n \\ \mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) &\mapsto \sigma(\mathbf{c}) = (-c_{n-1}, c_0, \ldots, c_{n-2}) \end{aligned} \tag{22}$$

es llamada *nega-corrimiento cíclico* . Un código $\mathcal{C} \subseteq \mathcal{R}^n$ se dice *negacíclico* si $\nu(\mathcal{C}) = \mathcal{C}$.

La función de Gray sobre $\mathcal{R}^n$ es:

$$\begin{aligned} \Phi\colon \mathcal{R}^n &\to \mathbb{F}_2^{2n} \\ \mathbf{A} &\mapsto \mathbf{C_0} \otimes r_0(\mathbf{A}) + \mathbf{C_1} \otimes r_1(\mathbf{A}), \end{aligned} \tag{23}$$

donde $\mathbf{C_0} = (0,1) \in \mathbb{F}_2^2$ y $\mathbf{C_1} = (1,1) \in \mathbb{F}_2^2$. Por lo que

$$\begin{aligned} \mathbf{C_0} \otimes r_0(\mathbf{A}) + \mathbf{C_1} \otimes r_1(\mathbf{A}) &= (0,1) \otimes r_0(\mathbf{A}) + (1,1) \otimes r_1(\mathbf{A}) \\ &= (\mathbf{o}_{\mathbb{F}_2^n}, r_0(\mathbf{A})) + (r_1(\mathbf{A}), r_1(\mathbf{A})) \\ &= (r_1(\mathbf{A}), r_0(\mathbf{A}) + r_1(\mathbf{A})). \end{aligned}$$

De ahí que para cualquier elemento $\mathbf{A} \in \mathcal{R}^n$ su imagen bajo la función de Gray es de la forma:

$$\Phi(\mathbf{A}) = (r_1(\mathbf{A}), r_0(\mathbf{A}) + r_1(\mathbf{A})) \tag{24}$$

J. Wolfmann en la [Wolo1, Proposición 8], enuncia las siguientes propiedades de la función de Gray:

$$\begin{aligned} \Phi(2\mathbf{A}) &= (r_0(\mathbf{A}), r_0(\mathbf{A})), \\ \Phi(\mathbf{A} + 2\mathbf{B}) &= \Phi(\mathbf{A}) + \Phi(p\mathbf{B}). \end{aligned} \tag{25}$$

Observemos que en la Proposición 2.1 dichas propiedades son generalizadas.

Por otro lado, definimos sobre el conjunto $\{0, 1, \ldots, 2n-1\}$ la siguiente permutación:

$$\pi = (1, n+1)(3, n+3)\cdots(2i+1, n+2i+1)\cdots(n-2, 2n-2). \tag{26}$$

Haciendo los cálculos pertinentes se puede comprobar que esta permutación es un caso particular, cuando $q = 2$, de la permutación dada en la Definición 2.3. Con ella se define la permutación de Nechaev sobre $\mathcal{R}^{2n}$,

$$\begin{aligned} \Pi(a_0, a_1, \ldots, a_{2n-1}) &= (a_{\pi(0)}, a_{\pi(1)}, \ldots, a_{\pi(2n-1)}) \\ &= (a_0, a_{n+1}, a_2, \ldots, a_{2n-2}, a_{n-1}, a_n, a_1, a_{n+2}, \ldots, a_{n-2}, a_{2n-1}). \end{aligned} \tag{27}$$

La *función de Nechaev-Gray* es la función $\Psi\colon \mathcal{R}^n \to \mathbb{F}_2^{2n}$ definida por $\Psi = \Pi\Phi$, donde Π es la permutación de Nechaev y Φ es la función de Gray.

Dado que existe un isormorfismo entre $\mathcal{R}_n$ y $\mathcal{R}^n$, el cual es $\mathcal{P}_{\mathcal{R}}^n$ (ver (7)), y uno entre $\mathbb{F}_2^{2n}$ y $\mathcal{F}_{2n}$ que está denotado por $\mathcal{P}_{\mathbb{F}_2}^{2n}$ (ver (6)), podemos tener la representación polinomial de la función de Gray y de la función de Nechaev-Gray, la cuales son:

$$\begin{aligned} \Phi_{\mathcal{P}} &= \mathcal{P}_{\mathbb{F}_2}^{2n} \Phi (\mathcal{P}_{\mathcal{R}}^n)^{-1}, \\ \Psi_{\mathcal{P}} &= \mathcal{P}_{\mathbb{F}_2}^{2n} \Psi (\mathcal{P}_{\mathcal{R}}^n)^{-1}. \end{aligned}$$

A partir de ahora $\mathcal{C}$ será un $\mathcal{R}$—código cíclico lineal de longitud impar n, a menos que se diga otra cosa.

Dado que $\mathcal{R}$ es un anillo de Galois de índice de nilpotencia 2, entonces por el Teorema 1.5 existen polinomios mónicos básicos coprimos por pares $A(x), B(x), C(x) \in \mathcal{R}[x]$ tales que $x^n - 1 = A(x)B(x)C(x)$ y $\mathcal{C} = \langle A(x)(B(x)+2)+^n \rangle$.

Un resultado que J. Wolfmann prueba y que atrae nuestra atención, nos muestra que la imagen de un código cíclico (no necesariamente lineal) bajo la función de Nechaev-Gray es cíclica.

Teorema 2.3. *[Wolo1, Teorema 14]*

i) $\Phi(\mathcal{C})$ *es un código cíclico si y sólo si* $\mathcal{C}$ *es negacíclico.*

ii) $\Psi(\mathcal{C})$ *es un código cíclico si y sólo si* $\mathcal{C}$ *es un código cíclico.*

En este primer teorema la permutación de Nechaev es relevante y se seguirá viendo su importancia en los siguientes resultados.

El siguiente teorema afirma que la imagen bajo la función de Nechaev-Gray de un $\mathcal{R}$—código cíclico lineal está contenida en un $\mathbb{F}_2$—código cíclico lineal de longitud $2n$, no trivial, y la prueba de dicho resultado puede consultarse en [Wol01].

Teorema 2.4. *[Wol01, Teorema 15] La representación polinomial de* $\Psi(\mathcal{C})$ *es un subconjunto del código cíclico lineal de longitud* $2n$ *generado por* $\overline{A}(x)\overline{B}(x) + I_2^{2n}$.

La siguiente proposición nos da una condición para la linealidad de $\Phi(\mathcal{C})$.

Proposición 2.5. *[Wol01, Proposición 16]* $\Phi(\mathcal{C})$ *es un* $\mathbb{F}_2$*—código lineal si y sólo si* $\langle \overline{A}(x)\overline{B}(x) + I_2^n \rangle * \langle \overline{A}(x)\overline{B}(x) + I_2^n \rangle \subseteq \langle \overline{A}(x) + I_2^n \rangle$, *donde* I_2^n *es el ideal principal generado por* $x^n - 1$ *en el anillo* $\mathbb{F}_2[x]$.

La prueba de está proposición se puede consultar en la referencia mencionada y parte fundamental de dicha prueba es un teorema que Hammons et. al probaron en [HKC+94]. Dicho teorema toma relevancia para nosotros pues da condiciones necesarias y suficientes para que la imagen bajo la función de Gray de un código cuaternario sea lineal. Además resulta ser un caso particular del Teorema 2.2.

Teorema 2.5. *[HKC+94, Teorema 5] La imagen binaria,* $\Phi(\mathcal{C})$, *de un código lineal cuaternario* $\mathcal{C}$ *es lineal si y sólo si*

$$\mathbf{A}, \mathbf{B} \in \mathcal{C} \Rightarrow 2\rho_0(\mathbf{A}) * \rho_1(\mathbf{A}) \in \mathcal{C}.$$

Demostración. En la siguiente tabla se muestran las representaciones 2—ádicas de los elementos del anillo $\mathcal{R}$.

c	$\rho_0(c)$	$\rho_1(c)$	$r_0(c) + r_1(c)$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	0

Tabla 1: Representación 2—ádica de los elementos de $\mathcal{R}$

Con apoyo de la tabla se puede probar que para cada $a, b \in \mathcal{R}$

$$\begin{aligned} r_0(a+b) &= r_0(a) + r_0(b), \\ r_1(a+b) &= r_1(a) + r_1(b) + r_1(2\rho_0(a)\rho_0(b)). \end{aligned} \tag{28}$$

Recordemos que $r_i(a), r_i(b) \in \mathbb{F}_2$ para $i = 0, 1$, por lo que las sumas se hacen reducción módulo 2. Las igualdades mostradas en (28) se pueden extender de manera que para cualesquiera $\mathbf{A}, \mathbf{B} \in \mathcal{R}^n$ se cumple lo siguiente:

$$\begin{aligned} r_0(\mathbf{A}+\mathbf{B}) &= r_0(\mathbf{A}) + r_0(\mathbf{B}), \\ r_1(\mathbf{A}+\mathbf{B}) &= r_1(\mathbf{A}) + r_1(\mathbf{B}) + r_1(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B})), \end{aligned} \tag{29}$$

donde $*$ es el producto que se definió en (19). Luego,

$$\begin{aligned} \Phi(\mathbf{A}) + \Phi(\mathbf{B}) + \Phi(\mathbf{A}+\mathbf{B}) &= (r_1(\mathbf{A}), r_0(\mathbf{A}) + r_1(\mathbf{A})) + (r_1(\mathbf{B}), r_0(\mathbf{B}) + r_1(\mathbf{B})) + \\ &\quad (r_1(\mathbf{A}+\mathbf{B}), r_0(\mathbf{A}+\mathbf{B}) + r_1(\mathbf{A}+\mathbf{B})) \\ &= (r_1(\mathbf{A}) + r_1(\mathbf{B}), r_0(\mathbf{A}) + r_1(\mathbf{A}) + r_0(\mathbf{B}) + r_1(\mathbf{B})) + \\ &\quad (r_1(\mathbf{A}) + r_1(\mathbf{B}) + r_1(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B})), r_0(\mathbf{A}) + r_0(\mathbf{B}) + \\ &\quad r_1(\mathbf{A}) + r_1(\mathbf{B}) + r_1(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B}))) \\ &= (r_1(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B})), r_1(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B}))). \end{aligned}$$

Por otro lado, sea $\mathbf{C} = 2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B}) \in \mathcal{R}^n$. Observemos que para cada $i \in \{0, 1, \ldots, n-1\}$, $c_i = 2\rho_0(a_i)\rho_0(b_i)$ y dado que $\rho_0(a_i), \rho_0(b_i) \in \mathcal{T} = \{0, 1\}$, entonces $2\rho_0(a_i)\rho_0(b_i) \in \{0, 2\}$. Así que, con

apoyo de la Tabla 1, se puede probar que $\rho_0(c_i) = 0$, por lo que $r_0(c_i) = 0$. De ahí que $r_0(\mathbf{C}) = 0_{\mathbb{F}_2^n}$. Entonces

$$\begin{aligned} \Phi(\mathbf{C}) &= (r_1(\mathbf{C}), r_0(\mathbf{C}) + r_1(\mathbf{C})) \\ &= (r_1(\mathbf{C}), r_1(\mathbf{C})) \\ \Phi(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B})) &= (r_1(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B})), r_1(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B}))). \end{aligned}$$

De lo anterior se sigue que

$$\Phi(\mathbf{A}) + \Phi(\mathbf{B}) + \Phi(\mathbf{A} + \mathbf{B}) = \Phi(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B})). \tag{30}$$

Supongamos que $\Phi(\mathcal{C})$ es lineal. Sean $\mathbf{A}, \mathbf{B} \in \mathcal{C}$, dado que $\mathcal{C}$ es lineal, entonces $\mathbf{A} + \mathbf{B} \in \mathcal{C}$. Por lo que $\Phi(\mathbf{A}) + \Phi(\mathbf{B}) + \Phi(\mathbf{A} + \mathbf{B}) \in \Phi(\mathcal{C})$. Por (30) se cumple que $\Phi(2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B})) \in \Phi(\mathcal{C})$ y por lo tanto $2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B}) \in \mathcal{C}$.

Ahora supongamos que $2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B}) \in \mathcal{C}$ para cualesquiera $\mathbf{A}, \mathbf{B} \in \mathcal{C}$. Sean $\underline{\mathbf{A}}, \underline{\mathbf{B}} \in \Phi(\mathcal{C})$, entonces existen $\mathbf{A}, \mathbf{B} \in \mathcal{C}$ tales que $\Phi(\mathbf{A}) = \underline{\mathbf{A}}$ y $\Phi(\mathbf{B}) = \underline{\mathbf{B}}$. Por (25) y (30) se obtiene que

$$\Phi(\mathbf{A}) + \Phi(\mathbf{B}) = \Phi(\mathbf{A} + \mathbf{B} + (2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B}))).$$

Por hipótesis $2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B}) \in \mathcal{C}$, así que $\mathbf{A} + \mathbf{B} + (2\rho_0(\mathbf{A}) * \rho_0(\mathbf{B})) \in \Phi(\mathcal{C})$. Por lo que su imagen bajo la función de Gray es un elemento de $\Phi\mathcal{C}$. Por lo tanto $\Phi(\mathbf{A}) + \Phi(\mathbf{B}) \in \Phi(\mathcal{C})$. Así $\underline{\mathbf{A}} + \underline{\mathbf{B}} \in \Phi(\mathcal{C})$, es decir, $\Phi(\mathcal{C})$ es lineal. □

Observemos que en la la Proposición 2.2 se da una generalización del resultado que se muestra en (30).

Como se mencionó antes, la permutación de Nechaev arroja información valiosa cuando se aplica a las imágenes de Gray de un código. En este caso, cuando $\mathcal{R} = \mathbb{Z}/4\mathbb{Z}$, el resultado de aplicar dicha permutación a las imágenes de un $\mathcal{R}-$código cíclico lineal nos da un $\mathbb{F}_2-$código cíclico lineal de longitud $2n$, tal como se muestra en el siguiente teorema y su prueba se puede consultar en la referencia indicada.

Teorema 2.6. *[Wolo1, Teorema 17] Si $\Psi(\mathcal{C})$ es un código lineal, entonces $\Psi(\mathcal{C})$ es el código cíclico lineal de longitud $2n$ generado por $\overline{A}(x)^2\overline{B}(x) + I_2^{2n}$.*

Los teoremas que se muestran más adelante nos proporcionan todos los códigos cíclicos lineales sobre $\mathcal{R}$ de longitud impar tales que sus imágenes bajo la función de Gray son $\mathbb{F}_2-$códigos cíclicos lineales. Para la prueba de dichos resultados haremos uso de la transformada de Mattson-Solomon (ó bien, polinomio de Mattson-Solomon), la cual está determinada de la siguiente manera:

Sean n impar, $\mathbb{F}_{2^t}$ el campo de descomposición de $x^n - 1$ sobre $\mathbb{F}_2$ y β una $n-$ésima raíz primitiva de la unidad en $\mathbb{F}_{2^t}$. La transformada (polinomio) de Mattson-Solomon es la transformación biyectiva $\mathbf{T}$ de $(\mathbb{F}_{2^t}[x]/(x^n - 1), +, \cdot)$ en $(\mathbb{F}_{2^t}[x]/(x^n - 1), +, *)$, donde $*$ es el producto que se definió en (20), tal que, si $U(x) \in \mathbb{F}_{2^t}[x]$ es la representación polinomial de $\mathbf{U} \in \mathbb{F}_{2^t}^n$, entonces la transformada de Mattson-Solomon es

$$\mathbf{T}(U(x) + (x^n - 1)) = \sum_{k=0}^{n-1} U_k x^{n-k} + (x^n - 1),$$

donde cada $U_k = U(\beta^k)$. Por propiedades de la transformada se cumple que

$$\mathbf{T}(U(x) + (x^n - 1)) = \sum_{k=0}^{n-1} U_{-k} x^k + (x^n - 1),$$

donde $U_{-k} = U(\beta^k)$. Así que podemos escribir dicha transformada como

$$\mathbf{U}(x) + (x^n - 1) = \mathbf{T}(U(x) + (x^n - 1)) = \sum_{k=0}^{n-1} U(\beta^k) x^k + (x^n - 1). \tag{31}$$

La inversa de dicha de transformada es de la forma:

$$U(x) + (x^n - 1) = \mathbf{T}^{-1}(\mathbf{U}(x) + (x^n - 1)) = \frac{1}{n} \sum_{i=0}^{n-1} \mathbf{U}(\beta^i) x^i + (x^n - 1)$$

es decir, $nU(x) + (x^n - 1) = \sum_{i=0}^{n-1} \mathbf{U}(\beta^i)x^i + (x^n - 1)$. Observemos que $nU(x) = U(x) \in \mathbb{F}_2[x]$, pues n es impar, por lo que

$$U(x) + (x^n - 1) = \mathbf{T}^{-1}(\mathbf{U}(x) + (x^n - 1)) = \sum_{i=0}^{n-1} \mathbf{U}(\beta^i)x^i + (x^n - 1).$$

La propiedad que más nos interesa de esta transformada es la siguiente: Sean $U(x), V(x) \in \mathbb{F}_2[x]$, entonces

$$\mathbf{T}(U(x)V(x) + (x^n - 1)) = \mathbf{T}(U(x) + (x^n - 1)) * (\mathbf{T}(V(x) + (x^n - 1))). \tag{32}$$

De manera análoga, para $\mathbf{T}^{-1}$ tenemos que

$$\mathbf{T}^{-1}(\mathbf{U}(x) * \mathbf{V}(x) + (x^n - 1)) = \mathbf{T}^{-}1(\mathbf{U}(x) + (x^n - 1))(\mathbf{T}^{-1}(\mathbf{V}(x) + (x^n - 1))). \tag{33}$$

Definición 2.4. *Sea $\overline{U}(x)$ un divisor de $x^n - 1$ en $\mathbb{F}_2[x]$ con n impar y sea β una n—ésima raíz primitiva de la unidad sobre $\mathbb{F}_2$. Entonces $(\overline{U} \otimes \overline{U})(x)$ es el divisor de $x^n - 1$ en $\mathbb{F}_2[x]$ cuyas raíces son los $\beta^i\beta^j$ tales que β^i y β^j son raíces de $\overline{U}(x)$.*

Ejemplo 2.1. *Sea $\overline{U}(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$, $\overline{U}(x)$ divide a $x^n - 1$, con $n = 7$ y β, β^2, β^4 son raíces de $\overline{U}(x)$. Por lo que $\beta^3 + \beta + 1 = 0$. Así que*

$$\begin{aligned} \beta^3 &= \beta + 1, \\ \beta^4 &= \beta^2 + \beta, \\ \beta^5 &= \beta^2 + \beta + 1, \\ \beta^6 &= \beta^2 + 1, \\ \beta^7 &= 1. \end{aligned}$$

Como β, β^2 y β^4 son las raíces de $\overline{U}(x)$, entonces $\beta\beta = \beta^2$, $\beta\beta^2 = \beta^3$, $\beta\beta^4 = \beta^5$, $\beta^2\beta^2 = \beta^4$, $\beta^2\beta^4 = \beta^6$ y $\beta^4\beta^4 = \beta^8 = \beta$ son las raíces de $(\overline{U} \otimes \overline{U})(x)$. Por lo que

$$\begin{aligned} (\overline{U} \otimes \overline{U})(x) &= (x - \beta)(x - \beta^2)(x - \beta^3)(x - \beta^4)(x - \beta^5)(x - \beta^6) \\ &= \overline{U}(x)(x - \beta^3)(x - \beta^5)(x - \beta^6) \\ &= (x^3 + x + 1)(x^3 + x^2 + 1) \\ &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \end{aligned}$$

es decir, $(\overline{U} \otimes \overline{U})(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$. Observemos que $(\overline{U} \otimes \overline{U})(x)(x + 1) = x^7 + 1$.

Parte de la prueba del siguiente lema se empleará en la demostración del Teorema **??**, es por ello que a continuación se escribe su demostración.

Lema 2.2. *[Wolo1, Lema 19] Sean $\overline{D}(x)$ y $\overline{C}(x)$ en $\mathbb{F}_2[x]$ tales que $x^n - 1 = \overline{D}(x)\overline{C}(x)$ con n impar. Sea $\overline{E}(x)$ tal que $x^n - 1 = (\overline{C}(x) \otimes \overline{C}(x))\overline{E}(x)$. Entonces*

$$\langle \overline{D}(x) + I_2^n \rangle * \langle \overline{D}(x) + I_2^n \rangle \subseteq \langle \overline{E}(x) + I_2^n \rangle.$$

Demostración. Sea $\overline{S}(x) = \overline{M}_1(x)\overline{D}(x) * \overline{M}_1(x)\overline{D}(x) + I_2^n \in \langle \overline{D}(x) + I_2^n \rangle * \langle \overline{D}(x) + I_2^n \rangle \subseteq \langle \overline{E}(x) + I_2^n \rangle$, con $I_2^n = (x^n - 1)$ en $\mathbb{F}]_2[x]$. Usando la transformada inversa del polinomio de Mattson-Solomon y la propiedad vista en (33) se sigue que, $\mathbf{T}^{-}1(\overline{S}(x)) = \mathbf{T}^{-1}(\overline{M}_1(x)\overline{D}(x) + I_2^n)\mathbf{T}^{-1}(\overline{M}_1(x)\overline{D}(x) + I_2^n)$, es decir,

$$\sum_{k=0}^{n-1} \overline{S}(\beta^k)x^k + I_2^n = \left(\sum_{i=0}^{n-1} \overline{M}_1(\beta^i)\overline{D}(\beta^i)x^i\right)\left(\sum_{j=0}^{n-1} \overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n. \tag{34}$$

Observemos que $\overline{D}(\beta^t) = 0$ para algún $0 \leqslant t \leqslant n - 1$, ya que $\overline{D}(x)$ divide a $x^n - 1$ en $\mathbb{F}_2[x]$. cuando esto sucede entonces $\overline{M}_1(\beta^t)\overline{D}(\beta^t) = 0 = \overline{M}_2(\beta^t)\overline{D}(\beta^t)$. Por lo que (34) se puede reescribir de la siguiente manera

$$\sum_{k=0}^{n-1} \overline{S}(\beta^i)x^k + I_2^n = \left(\sum_{\overline{D}(\beta^i)\neq 0} \overline{M}_1(\beta^i)\overline{D}(\beta^i)x^i\right)\left(\sum_{\overline{D}(\beta^j)\neq 0} \overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n. \tag{35}$$

Además, observemos que $\overline{D}(\beta^t) \neq 0$ si y sólo si, $\overline{C}(\beta^t) = 0$, ya que $\overline{C}(x)\overline{D}(x) = x^n - 1$ y β genera a todas las raíces $n-$ésimas de la unidad, pues es primitiva. Así que reescribiendo la ecuación (35), tenemos que:

$$\sum_{k=0}^{n-1} \overline{S}(\beta^k)x^k + I_2^n = \left(\sum_{\overline{C}(\beta^i)=0} \overline{M}_1(\beta^i)\overline{D}(\beta^i)x^i\right)\left(\sum_{\overline{C}(\beta^j)=0} \overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n. \tag{36}$$

Sea $I = \{i_1, i_2, \ldots, i_r\} \subseteq \{0, 1, \ldots, n-1\}$, tal que cada $i_k \in I$ es una raíz de $\overline{C}$, es decir, $\overline{C}(\beta^{i_k}) = 0$. Entonces la parte derecha de la igualdad (36) se puede desarrollar de la siguiente manera

$$\begin{aligned}
& \overline{M}_1(\beta^{i_1})\overline{D}(\beta^{i_1})x^{i_1}\left(\sum_{\overline{C}(\beta^j)=0} \overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n \\
+ \;& \overline{M}_1(\beta^{i_2})\overline{D}(\beta^{i_2})x^{i_2}\left(\sum_{\overline{C}(\beta^j)=0} \overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n \\
& \vdots \\
+ \;& \overline{M}_1(\beta^{i_r})\overline{D}(\beta^{i_r})x^{i_r}\left(\sum_{\overline{C}(\beta^j)=0} \overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n \\
= \;& \left(\sum_{\overline{C}(\beta^j)=0} \overline{M}_1(\beta^{i_1})\overline{D}(\beta^{i_1})x^{i_1}\overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n \\
+ \;& \left(\sum_{\overline{C}(\beta^j)=0} \overline{M}_1(\beta^{i_2})\overline{D}(\beta^{i_2})x^{i_2}\overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n \\
& \vdots \\
+ \;& \left(\sum_{\overline{C}(\beta^j)=0} \overline{M}_1(\beta^{i_r})\overline{D}(\beta^{i_r})x^{i_r}\overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n.
\end{aligned}$$

Observemos que para cada $j \in I$ y cada $1 \leqslant t \leqslant r$, se cumple que $\beta^{i_t}\beta^j$ es una raíz del polinomio $(\overline{C} \otimes \overline{C})(x)$ (ver Definición 2.4). Así que lo anterior puede escribirse como

$$\begin{aligned}
= \;& \left(\sum_{(\overline{C}\otimes\overline{C})(\beta^{i_1}\beta^j)=0} \overline{M}_1(\beta^{i_1})\overline{D}(\beta^{i_1})x^{i_1}\overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n \\
+ \;& \left(\sum_{(\overline{C}\otimes\overline{C})(\beta^{i_2}\beta^j)=0} \overline{M}_1(\beta^{i_2})\overline{D}(\beta^{i_2})x^{i_2}\overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n \\
& \vdots \\
+ \;& \left(\sum_{(\overline{C}\otimes\overline{C})(\beta^{i_r}\beta^j)=0} \overline{M}_1(\beta^{i_r})\overline{D}(\beta^{i_r})x^{i_r}\overline{M}_2(\beta^j)\overline{D}(\beta^j)x^j\right) + I_2^n \\
= \;& \sum_{(\overline{C}\otimes\overline{C})(\beta^i\beta^j)=0} \sum_{i+j} \overline{M}_1(\beta^i)\overline{D}(\beta^i)\overline{M}_2(\beta^j)\overline{D}(\beta^j)x^{i+j} + I_2^n.
\end{aligned}$$

Por lo que

$$\sum_{k=0}^{n-1} \overline{S}(\beta^k)x^k + I_2^n = \sum_{(\overline{C}\otimes\overline{C})(\beta^k)=0} \sum_{i+j=k} \overline{M}_1(\beta^i)\overline{D}(\beta^i)\overline{M}_2(\beta^j)\overline{D}(\beta^j)x^k + I_2^n. \tag{37}$$

Notemos que si $\overline{S}(\beta^k) \neq 0$ entonces el coeficiente de x^k de la expresión del lado derecho es distinto de cero, por lo que $(\overline{C} \otimes \overline{C})(\beta^k) = 0$ ya que $k = i + j$ con β^i y β^j raíces de $\overline{C}(x)$.

Si $\overline{E}(\beta^k) = 0$, entonces β^k es raíz de $\overline{E}(x)$ pero no es raíz de $(\overline{C} \otimes \overline{C})(x)$. Así que $\overline{S}(\beta^k) = 0$. De ahí que, $\overline{E}(\beta^k) = 0$ implica que $\overline{S}(\beta^k) = 0$. Por lo que toda raíz de $\overline{E}(x)$ es raíz de $\overline{S}(x)$. Así que $\overline{E}(x)$ divide a $\overline{S}(x)$. Por lo tanto $\overline{S}(x) + I_2^n \in \langle \overline{E}(x) + I_2^n \rangle$.

□

Los siguientes dos teoremas nos dan las condiciones requeridas para que la imagen de un $\mathcal{R}-$código cíclico lineal bajo la función Φ, sea un $\mathbb{F}_{p^m}-$código cíclico lineal.

Demostración. Sabemos que π (ver (26)) es una permutación en $\{0,1,\ldots,2n-1\}$, por lo que π es biyectiva y con ello se puede probar que la función $\Pi\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ (ver(27)) es biyectiva. Por otro lado, sean $\overline{\mathbf{A}} = (\overline{a_0}, \overline{a_1}, \ldots, \overline{a_{2n-1}}), \overline{\mathbf{B}} = (\overline{b_0}, \overline{b_1}, \ldots, \overline{b_{2n-1}}) \in \mathbb{F}_2^{2n}$ y $\overline{\alpha} \in \mathbb{F}_2$, entonces

$$\begin{aligned}
\Pi(\overline{\mathbf{A}} + \overline{\alpha}\overline{\mathbf{B}}) &= \Pi((\overline{a}_0 + \overline{\alpha}\overline{b}_0, \overline{a}_1 + \overline{\alpha}\overline{b}_1, \ldots, \overline{a}_{2n-1} + \overline{\alpha}\overline{b}_{2n-1})) \\
&= (\overline{a}_0 + \overline{\alpha}\overline{b}_0, \overline{a}_{n+1} + \overline{\alpha}\overline{b}_{n+1}, \overline{a}_2 + \overline{\alpha}\overline{b}_2, \ldots, \overline{a}_{n-2} + \overline{\alpha}\overline{b}_{n-2}, \overline{a}_{2n-1} + \overline{\alpha}\overline{b}_{2n-1}) \\
&= (\overline{a}_0, \overline{a}_{n+1}, \overline{a}_2, \ldots, \overline{a}_{n-2}, \overline{a}_{2n-1}) + \overline{\alpha}(\overline{b}_0, \overline{b}_{n+1}, \overline{b}_2, \overline{b}_{n-2}, \overline{b}_{2n-1}) \\
&= \Pi(\overline{\mathbf{A}}) + \overline{\alpha}\Pi(\overline{\mathbf{B}})
\end{aligned}$$

Por lo que Π es una función $\mathbb{F}_2$—lineal biyectiva. Así que existe $\Pi^{-1}\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ lineal.

La equivalencia (**??**⇔**??**) se deriva de la linealidad de Π. Si $\Phi(\mathcal{C})$ es un código lineal binario entonces $\Pi\Phi(\mathcal{C})$ es un código lineal binario. Dado que $\Pi\Phi = \Psi$, se sigue que $\Psi(\mathcal{C})$ es un código lineal binario. Por el Teorema 2.3 tenemos que $\Psi(\mathcal{C})$ es un código cíclico. Por lo tanto $\Psi(\mathcal{C})$ es un $\mathbb{F}_2$—código cíclico lineal. Por otro lado, si suponemos que $\Psi(\mathcal{C})$ es un código cíclico lineal binario entonces $\Pi^{-1}\Psi(\mathcal{C}) = \Pi^{-1}\Pi\Phi(\mathcal{C}) = \Phi(\mathcal{C})$ es un código lineal binario.

Ahora probemos (**??**⇔**??**).

$$\begin{aligned}
\overline{B}(x)\overline{C}(x) = (\overline{C} \otimes \overline{C})(x)\overline{K}(x) \text{ para algún } \overline{K}(x) \in \mathbb{F}_2[x] \quad &\Leftrightarrow \quad \overline{A}(x)\overline{B}(x)\overline{C}(x) = (\overline{C} \otimes \overline{C})(x)\overline{K}(x)\overline{A}(x) \\
&\Leftrightarrow \quad x^n - 1 = (\overline{C} \otimes \overline{C})(x)\overline{K}(x)\overline{A}(x) \\
&\Leftrightarrow \quad (\overline{C} \otimes \overline{C})(x)\overline{E}(x) = (\overline{C} \otimes \overline{C})(x)\overline{K}(x)\overline{A}(x) \\
&\Leftrightarrow \quad \overline{E}(x) = \overline{K}(x)\overline{A}(x) \text{ para algún } \overline{K}(x) \in \mathbb{F}_2[x].
\end{aligned}$$

Por lo tanto $(\overline{C} \otimes \overline{C})(x)$ divide a $\overline{B}(x)\overline{C}(x)$ si y sólo si, $\overline{A}(x)$ divide a $\overline{E}(x)$.

Si $\overline{A}(x)$ divide $\overline{E}(x)$ entonces existe $\overline{K}(x) \in \mathbb{F}_2[x]$ tal que $\overline{E}(x) = \overline{A}(x)\overline{K}(x)$. Así que $\overline{E}(x) + I_2^n = \overline{A}(x)\overline{K}(x) + I_2^n$, donde $I_2^n = (x^n - 1) \subseteq \mathbb{F}_2[x]$. Por lo que $\langle \overline{E}(x) + I_2^n \rangle \subseteq \langle \overline{A}(x) + I_2^n \rangle$. Sea $\overline{D}(x) = \overline{A}(x)\overline{B}(x)$, se sigue que $x^n - 1 = \overline{D}(x)\overline{C}(x)$. Entonces por el Lema 2.2 $\langle \overline{D}(x) + I_2^n \rangle * \langle \overline{D}(x) + I_2^n \rangle \subseteq \langle \overline{E}(x) + I_2^n \rangle \subseteq \langle \overline{A}(x) + I_2^n \rangle$. Luego $\langle \overline{A}(x)\overline{B}(x) + I_2^n \rangle * \langle \overline{A}(x)\overline{B}(x) + I_2^n \rangle \subseteq \langle \overline{A}(x) + I_2^n \rangle$. Por lo tanto, por la Proposición 2.5 , $\Phi(\mathcal{C})$ es un $\mathbb{F}_2$—código lineal. Con lo cual se prueba (**??**⇒ **??**).

Ahora supongamos que $\Phi(\mathcal{C})$ es un código lineal binario. Notemos que si $\overline{A}(x) = 1$ entonces $\overline{A}(x)$ divide $\overline{E}(x)$ y si $\overline{C}(x) = 1$ entonces $\overline{E}(x) = x^n - 1$, así $\overline{A}(x)$ divide a $\overline{E}(x)$. Por otro lado, definimos

$$\mathcal{K} = \{k \mid 0 \leqslant k \leqslant n-1,\ (\overline{C} \otimes \overline{C})(\beta^k) = 0\} \text{ y}$$
$$\mathcal{J}(k) = \{j \mid 0 \leqslant j \leqslant n-1,\ \overline{C}(\beta^j) = 0 \text{ y } \overline{C}(\beta^{k-j}) = 0\}.$$

Sea β una raíz n—ésima primitiva de la unidad sobre $\mathbb{F}_2$. Como $\overline{C}(x) \neq 1$ y $\overline{C}(x)$ divide a $x^n - 1$, entonces, existe $i \in \{0,1,\ldots,n-1\}$ tal que $\overline{C}(\beta^i) = 0$. Por la definición de $(\overline{C} \otimes \overline{C})(x)$ se tiene que $\beta^i\beta^i = \beta^{2i}$ es una raíz de $(\overline{C} \otimes \overline{C})(x)$, es decir, $(\overline{C} \otimes \overline{C})(\beta^{2i}) = 0$. Por lo que existe $0 \leqslant k \leqslant n-1$ ($k \equiv 2i$ mód n) tal que $(\overline{C} \otimes \overline{C})(\beta^k) = 0$. De ahí que $\mathcal{K} \neq \emptyset$. Más aún, sea $k \in \mathcal{K}$, tenemos que $(\overline{C} \otimes \overline{C})(\beta^k) = 0$. Así que existen $0 \leqslant i, j \leqslant n-1$ tales que $i + j = k$, $\overline{C}(\beta^i) = 0$ y $\overline{C}(\beta^j) = 0$, ya que $i = k - j$. Entonces $\overline{C}(\beta^j) = 0$ y $\overline{C}(\beta^{k-j}) = 0$, por lo que $j \in \mathcal{J}(k)$. Por lo tanto $\mathcal{J}(k) \neq \emptyset$.

Sea m un entero tal que $0 \leqslant m \leqslant n-1$. Tenemos que $(\overline{A}(x)\overline{B}(x) * x^m\overline{A}(x)\overline{B}(x)) + I_2^n \in \langle \overline{A}(x)\overline{B}(x) + I_2^n \rangle * \langle \overline{A}(x)\overline{B}(x) + I_2^n \rangle$. Por la Proposición 2.5 se sigue que

$$(\overline{A}(x)\overline{B}(x) * x^m\overline{A}(x)\overline{B}(x)) + I_2^n \in \langle \overline{A}(x) + I_2^n \rangle.$$

Así que, existe $\overline{\lambda}_m(x) \in \mathbb{F}_2[x]$ tal que $(\overline{A}(x)\overline{B}(x) * x^m\overline{A}(x)\overline{B}(x)) = \overline{A}(x)\overline{\lambda}_m(x)$. Sea $\overline{D}(x) = \overline{A}(x)\overline{B}(x)$, entonces $\overline{D}(x) * x^m\overline{D}(x) = \overline{A}(x)\overline{\lambda}_m(x)$. Sea $\overline{S}(x) = \overline{A}(x)\overline{\lambda}_m(x)$. Por la prueba del Lema 2.2, sabemos que aplicando la transformada inversa de Mattson-Solomon a $\overline{S}(x)$, obtenemos

$$\sum_{k=0}^{n-1} \overline{A}(\beta^k)\overline{\lambda}_m(\beta^k)x^k = \sum_{(\overline{C}\otimes\overline{C})(\beta^k)=0} \sum_{i+j=k} \overline{D}(\beta^i)(\beta^j)^m\overline{D}(\beta^j)x^k.$$

Si β^k es tal que $(\overline{C} \otimes \overline{C})(\beta^k) = 0$ entonces $k \in \mathcal{K}$. Si $k = i + j$, en particular $i = k - j$, se tiene que la última suma es igual a

$$\sum_{k\in\mathcal{K}} \sum_{i=k-j} \overline{D}(\beta^{k-j})(\beta^m)^j\overline{D}(\beta^j)x^k.$$

Observemos que si $\overline{D}(\beta^{k-j}) = 0$ ó $\overline{D}(\beta^j) = 0$, entonces el término k–ésimo es cero, por lo que podemos restringir la suma a los $0 \leqslant j \leqslant n-1$ tales que $\overline{C}(\beta^j) = 0$ y $\overline{C}(\beta^{k-j}) = 0$, es decir, $j \in \mathcal{J}(k)$. Por lo que la suma quedaría de la siguiente manera,

$$\sum_{k\in\mathcal{K}} \sum_{j\in\mathcal{J}(k)} \mathcal{A}_j(k)(\beta^m)^j x^k,$$

donde $\mathcal{A}_j(k) = \overline{D}(\beta^{k-j})\overline{D}(\beta^j)$. Por lo que

$$\sum_{k=0}^{n-1} \overline{A}(\beta^k)\overline{\lambda}_m(\beta^k)x^k = \sum_{k\in\mathcal{K}} \sum_{j\in\mathcal{J}(k)} \mathcal{A}_j(k)(\beta^m)^j x^k.$$

Observemos que si $k \notin \mathcal{K}$ entonces el termino k–ésimo en la segunda suma es cero, por lo que podemos restringir la suma en ambos lados para los $k \in \mathcal{K}$, es decir,

$$\sum_{k\in\mathcal{K}} \overline{A}(\beta^k)\overline{\lambda}_m(\beta^k)x^k = \sum_{k\in\mathcal{K}} \sum_{j\in\mathcal{J}(k)} \mathcal{A}_j(k)(\beta^m)^j x^k.$$

Sea $k \in \mathcal{K}$, definimos $\mathcal{S}_k(x) = \sum_{j\in\mathcal{J}(k)} \mathcal{A}_j(k)x^j$. Como $k \in \mathcal{K}$, entonces $(\overline{C} \otimes \overline{C})(\beta^k) = 0$. Por lo que existe $j \in \{0, 1, \ldots, n-1\}$ tal que $\overline{C}(\beta^j) = 0$ y $\overline{C}(\beta^{k-j}) = 0$. Así que β^{k-j} y β^j no pueden ser raíces de $\overline{D}(x) = \overline{A}(x)\overline{B}(x)$. De ahí que $\overline{D}(\beta^j)\overline{D}(\beta^{k-j}) \neq 0$. Entonces $\mathcal{A}_j(K) \neq 0$ para toda $k \in \mathcal{K}$ y cada $j \in \mathcal{J}(k)$. Por lo tanto $\mathcal{S}_k(x) \neq 0$.

Observemos que el grado de $\mathcal{S}_k(x)$ es a lo más $n-1$ y por tanto tiene a lo más $n-1$ raíces. Por lo que existe m en $\{0, 1, \ldots, n-1\}$ tal que $\mathcal{S}_k(\beta^m) \neq 0$. Entonces $\overline{\lambda}_m(\beta^k)\overline{A}(\beta^k) \neq 0$. Así, $\overline{\lambda}_m(\beta^k) \neq 0$ y $\overline{A}(\beta^k) \neq 0$. De ahí que para cada $k \in \mathcal{K}$ y cada $j \in \mathcal{J}(k)$ se tiene que $\overline{A}(\beta^k) \neq 0$, es decir, para cada $k \in \{0, 1, \ldots, n-1\}$ tal que $(\overline{C} \otimes \overline{C})(\beta^k) = 0$ se tiene que $\overline{A}(\beta^k) \neq 0$. Así que, si $\overline{A}(\beta^k) = 0$ entonces $(\overline{C} \otimes \overline{C})(\beta^k) \neq 0$, por lo que $\overline{E}(\beta^k) = 0$. Por lo tanto $\overline{A}(x)$ divide a $\overline{E}(x)$. Hemos probado (**??**⇒**??**).

?? Si una de las condiciones del inciso **??** se cumple, entonces $\Psi(\mathcal{C})$ es un código cíclico lineal y por tanto, por el Teorema 2.6, $\Psi_{\mathcal{P}}(\mathcal{C}) = \langle \overline{A}^2(x)\overline{B}(x) + I_2^{2n} \rangle$.

□

Teorema 2.7. *[Wolo1, Teorema 21] Sea $\mathcal{C}$ un código cíclico lineal sobre $\mathcal{R}$ de longitud impar n. Sea Φ la función de Gray:*

I) Las siguientes propiedades son equivalentes:

- *i) $\Phi(\mathcal{C})$ es un código cíclico lineal binario,*
- *ii) $\mathcal{C}$ es un código negacíclico,*
- *iii) el polinomio generador de $\mathcal{C}$ es $G(x) = 2D(x)$ ó $G(x) = D(x) + 2$, donde $D(x)$ divide $x^n - 1$ en $\mathcal{R}[x]$.*

II) Si $G(x) = 2D(x)$ entonces $\Phi(\mathcal{C})$ es el código cíclico lineal binario de longitud $2n$ generado por $\overline{D}(x)(x^n - 1) \in \mathbb{F}_2[x]$. Si $G(x) = D(x) + 2$ entonces $\Phi(\mathcal{C})$ es el código cíclico lineal binario de longitud $2n$ generado por $\overline{D}(x) \in \mathbb{F}_2[x]$.

Demostración. Por el Teorema 2.3 sabemos que si $\Phi(\mathcal{C})$ es un código cíclico binario entonces $\mathcal{C}$ es un código negacíclico. Por lo que i) ⇒ ii).

Ahora supongamos que $\mathcal{C}$ es un $\mathcal{R}$–código negacíclico. Dado que $\mathcal{C}$ es un $\mathcal{R}$–código cíclico (por hipótesis), existe $G(x) \in \mathbb{Z}_4[x]$ tal que $\mathcal{C} = \langle G(x) + I_4^n \rangle$.

Supongamos que $G(x) + I_4^n \notin 2\mathcal{R}_n = \{2F(x) + I_4^n \,|\, F(x) + I_4^n \in \mathcal{R}_n\}$. Así que $\langle G(x) + I_4^n \rangle \nsubseteq 2\mathcal{R}_n$, es decir, $\mathcal{C} \nsubseteq 2\mathcal{R}_n$. Por lo que existe una palabra código $\mathbf{V} = (v_0, v_1, \ldots, v_{n-1}) \in \mathcal{C}$ tal que $\mathbf{V} \notin 2\mathcal{R}_n$. Así que para algún $i \in \{0, 1, \ldots, n-1\}$, la i–ésima ordena de $\mathbf{V}$ es distinta de 0 y 2, es decir, $v_i = 1$ ó $v_i = 3$. Aplicando el corrimiento cíclico, σ (ver (4)), $n - (i+1)$ veces a $\mathbf{V}$, tenemos que:

$$\sigma^{n-(i+1)}(\mathbf{V}) = (v_{i+1}, \ldots, v_{n-1}, v_0, \ldots, v_i) = \mathbf{U}$$

Ya que $\mathcal{C}$ es un código cíclico, entonces $\mathbf{U} \in \mathcal{C}$. Además

$$\begin{aligned} \sigma(\mathbf{U}) &= (v_i, v_{i+1}, \ldots, v_{n-1}, v_0, \ldots, v_{i-1}) \in \mathcal{C} \text{ y} \\ \nu(\mathbf{U}) &= (-v_i, v_{i+1}, \ldots, v_{n-1}, v_0, \ldots, v_{i-1}) \in \mathcal{C}, \end{aligned}$$

donde ν es el nega-corrimiento cíclico. Como $\mathcal{C}$ es $\mathcal{R}$—lineal entonces $\sigma(\mathbf{U}) - \nu(\mathbf{U}) \in \mathcal{C}$, con

$$\begin{aligned} \sigma(\mathbf{U}) - \nu(\mathbf{U}) &= (v_i + v_i, v_{i+1} - v_{i+1}, \ldots, v_{n-1} - v_{n-1}, v_0 - v_0, \ldots, v_{i-1} - v_{i-1}) \\ &= (2v_i, 0, \ldots, 0). \end{aligned}$$

Observemos que $2v_i = 2$, ya que $v_i = 1$ ó $v_i = 3$. Así que $(2, 0, \ldots, 0) \in \mathcal{C}$. Entonces $\mathcal{P}_{\mathcal{R}}^n((2v_i, 0, \ldots, 0)) = 2 + I_4^n \in \langle G(x) + I_4^n \rangle$, por lo que $2 + I_4^n \in \mathcal{P}_{\mathcal{R}}^n(\mathcal{C}) \cap 2\mathcal{R}_n = \langle 2A(x) + I_4^n \rangle$ (por Proposición 2.4). De ahí que $2 + I_4^n = 2A(x)H(x) + I_4^n$ para algún $H(x) \in \mathcal{R}[x]$. Por la Proposición 2.3, tenemos que $2A(x)H(x) = 2\rho_0(A(x)B(x))$ y notemos que $\rho_0(1) = 1$, así que

$$2\rho_0(1) + I_4^n = 2\rho_0(A(x)H(x)) + I_4^n.$$

Por lo que $1 + I_2^n = \overline{A}(x)\overline{H}(x) + I_2^n$ (por Proposición 2.3), donde $I_2^n = (x^n - 1) \subseteq \mathbb{F}_2[x]$. Entonces $1 - \overline{A}(x)\overline{H}(x) \in (x^n - 1)$. Como $\mathrm{grad}(A(x)H(x)) < n$, se sigue que $\mathrm{grad}(\overline{A}(x)\overline{H}(x)) < n$. Así que $1 - \overline{A}(x)\overline{H}(x) = 0$. De ahí que $1 = \overline{A}(x)\overline{H}(x)$ en $\mathbb{F}_2[x]$.

Afirmación. Si $\overline{A}(x)\overline{H}(x) = 1$ entonces $\overline{A}(x) = 1$.

Probaremos que: $\overline{A}(x) \neq 1$ implica que $1 \neq \overline{A}(x)\overline{H}(x)$. Observemos que si $\mathrm{grad}(\overline{A}(x)) = 0$ entonces $\overline{A}(x) = 1$, ya que $A(x)$ es un polinomio mónico en $\mathcal{R}[x]$. Dado que nuestra hipótesis es $\overline{A}(x) \neq 1$, entonces $\mathrm{grad}(\overline{A}(x)) \neq 0$. Por lo tanto, $\mathrm{grad}(\overline{A}(x)) \geqslant 1$.

Caso 1. Si $\overline{H}(x) = 0$ ó $\overline{H}(x) = 1$, entonces $\overline{A}(x)\overline{H}(x) = 0 \neq 1$ ó $\overline{A}(x)\overline{H}(x) = \overline{A}(x) \neq 1$. Por lo que el resultado se sigue.

Caso 2. Supongamos que $\mathrm{grad}(\overline{H}(x)) \geqslant 1$. Entonces $\mathrm{grad}(\overline{A}(x)\overline{H}(x)) = \mathrm{grad}(\overline{A}(x)) + \mathrm{grad}(\overline{H}(x)) \geqslant 2$. Así que $\overline{A}(x)\overline{H}(x) \neq 1$.

Por lo tanto la afirmación se cumple.

De la afirmación se sigue $\overline{A}(x) = 1$. Aplicando el levantamiento de Hensel (c.f. [Wan03]) a el polinomio $\overline{A}(x)$, tenemos que $A(x) = 1$, ya que $A(x)$ es un polinomio mónico en $\mathcal{R}[x]$. Así que $G(x) = A(x)[B(x) + 2] = B(x) + 2$, donde $B(x)$ divide a $x^n - 1$ sobre $\mathcal{R}$. Por lo tanto $G(x) = D(x) + 2$ con $D(x) = B(x)$.

Por otra parte, si $G(x) + I_4^n \in 2\mathcal{R}_n$, entonces $\langle G(x) + I_4^n \rangle \subseteq 2\mathcal{R}_n$. Así que $\mathcal{P}_{\mathcal{R}}^n(\mathcal{C}) \cap 2\mathcal{R}_n = \mathcal{P}_{\mathcal{R}}^n(\mathcal{C})$. Además, por la Proposición 2.4, $\mathcal{P}_{\mathcal{R}}^n(\mathcal{C}) \cap 2\mathcal{R}_n = \langle 2A(x) + I_4^n \rangle$. Se sigue que

$$\langle A(x)[B(x) + 2] + I_4^n \rangle = \langle 2A(x) + I_4^n \rangle.$$

Entonces, existe $K(x) + I_4^n \in \mathcal{R}_n$ tal que $2A(x)K(x) + I_4^n = A(x)B(x) + 2A(x) + I_4^n$. Supongamos que $C(x) \neq 1$, así que $\mathrm{grad}(A(x)B(x)) < n$ y $A(x)B(x) + I_4^n \neq 0 + I_4^n$. Por lo que $2A(x)K(x) - A(x)B(x) - 2A(x) \in (x^n - 1)$. Ya que $\mathrm{grad}(2A(x)K(x) - A(x)B(x) - 2A(x)) < n$, debido a que podemos escoger $K(x)$ de tal forma que $\mathrm{grad}(A(x)K(x)) < n$, entonces $2A(x)K(x) - A(x)B(x) - 2A(x) = 0$. Multiplicando por $C(x)$ en ambos lados tenemos que, $2A(x)C(x)K(x) - A(x)B(x)C(x) - 2A(x)C(x) = 0$. Así que, $\overline{\mu}(2A(x)C(x)K(x)) - \overline{\mu}(A(x)B(x)C(x)) - \overline{\mu}(2A(x)C(x)) = 0$, es decir, $\overline{A}(x)\overline{B}(x)\overline{C}(x) = 0$. Lo cual no es posible ya que $A(x), B(x)$ y $C(x)$ son polinomios mónicos que dividen a $x^n - 1$ en $\mathcal{R}[x]$. Por lo tanto $C(x) = 1$, y así $A(x)[B(x) + 2] = A(x) + 2$ en $\mathcal{R}_n$. De ahí que $G(x) = A(x) + 2$ donde $A(x)$ divide a $x^n - 1$ en $\mathcal{R}$. Así que $G(x) = 2D(x)$ con $D(x) = A(x)$.

Con lo anterior se prueba ii)⇒iii).

Ahora probaremos iii) ⇒ i).

Primero supongamos que $G(x) = 2D(x)$ con $D(x)$ divisor de $x^n - 1$ en $\mathcal{R}[x]$. Sabemos que $G(x) = A(x)B(x) + 2A(x)$, así que $A(x)B(x) + 2A(x) + I_4^n = 2D(x) + I_4^n$. Entonces $A(x)B(x) + I_4^n = 2(D(x) - A(x)) + I_4^n$. Observemos que si $A(x)B(x) \neq x^n - 1$ se sigue que $A(x)B(x) + I_4^n \neq 0 + I_4^n$. Luego $A(x)B(x) - 2(D(x) - A(x)) \in I_4^n = (x^n - 1)$, y como $\mathrm{grad}(A(x)B(x) - 2(D(x) - A(x))) < n$ entonces $A(x)B(x) - 2(D(x) - A(x)) = 0$ en $\mathcal{R}[x]$. Así que $A(x)B(x) = 2(D(x) - A(x))$, pero esto no es posible ya que $A(x)B(x)$ es un polinomio mónico pues $A(x)$ y $B(x)$ son polinomios mónicos y $2(D(x) - A(x))$ no lo es. Por lo que $A(x)B(x) = x^n - 1$ en $\mathcal{R}[x]$. Entonces $\overline{A}(x)\overline{B}(x) = x^n - 1$ en $\mathbb{F}_2[x]$. De ahí que

$\overline{A}(x)\overline{B}(x) + I_2^n = 0 + I_2^n$ en $\mathbb{F}_2[x]/(x^n-1)$ con $I_2^n = (x^n-1)$. Dado que $\langle \overline{A}(x)\overline{B}(x) + I_2^n\rangle * \langle \overline{A}(x)\overline{B}(x) + I_2^n\rangle = \langle 0 + I_2^n\rangle \subseteq \langle \overline{A}(x) + I_2^n\rangle$, se sigue, por la Proposición 2.5, que $\Phi(\mathcal{C})$ es un código lineal binario. Sea $\mathbf{U} \in \mathcal{C}$, entonces $U(x) + I_4^n \in \langle 2D(x) + I_4^n\rangle$, así que $U(x) + I_4^n = 2K(x) + I_4^n$ con $K(x) = D(x)H(x)$ para algún $H(x) \in \mathcal{R}[x]$. Sabemos que existe $\mathbf{K} \in \mathcal{R}^n$ tal que $(\mathcal{P}_{\mathcal{R}}^n)^{-1}(K(x) + I_4^n) = \mathbf{K}$. Por lo que $\mathbf{U} = 2\mathbf{K}$. De ahí que $\mathbf{U} = (2k_0, 2k_1, \ldots, 2k_{n-1})$. Luego

$$\begin{aligned} \nu(\mathbf{U}) &= \nu((2k_0, 2k_1, \ldots, 2k_{n-1})) \\ &= (-2k_{n-1}, 2k_0, \ldots, 2k_{n-2}) \\ &= (2k_{n-1}, 2k_0, \ldots, 2k_{n-2}) \\ &= \sigma((2k_0, 2k_1, \ldots, 2k_{n-1})) \\ &= \sigma(2\mathbf{K}) = \sigma(\mathbf{U}). \end{aligned}$$

Dado que $\sigma(\mathbf{U}) \in \mathcal{C}$, pues $\mathcal{C}$ es cíclico lineal, entonces $\nu(\mathbf{U}) \in \mathcal{C}$, con $\mathbf{U}$ un elemento arbitrario en $\mathcal{C}$. Así que $\mathcal{C}$ es negacíclico. Luego, por el Teorema 2.3, $\Phi(\mathcal{C})$ es un código cíclico. Por lo tanto $\Phi(\mathcal{C})$ es un $\mathbb{F}_2-$código cíclico lineal.

Por último, supongamos que $G(x) = D(x) + 2$. Ya que $G(x) = A(x)(B(x) + 2)$ entonces cuando consideramos $A(x) = 1$ tenemos que $G(x) = B(x) + 2$, donde $B(x)$ es un divisor de $x^n - 1$, así que $B(x) = D(x)$. Como $B(x)C(x) = x^n - 1$ en $\mathcal{R}[x]$, entonces $\overline{B}(x)\overline{C}(x) = x^n - 1$ en $\mathbb{F}_2[x]$. Por lo que $\overline{B}(x)\overline{C}(x) + I_2^n = 0 + I_2^n$ con $I_2^n = (x^n - 1) \subseteq \mathbb{F}_2[x]$ y $\overline{A}(x) + I_2^n = 1 + I_2^n$. Así que $\langle \overline{A}(x)\overline{B}(x) + I_2^n\rangle * \langle \overline{A}(x)\overline{B}(x) + I_2^n\rangle = \langle \overline{B} + I_2^n\rangle * \langle \overline{B}(x) + I_2^n\rangle \subseteq \frac{\mathbb{F}_2[x]}{(x^n-1)} = \langle \overline{A}(x) + I_2^n\rangle$. De ahí que, por la Proposición 2.5, $\Phi(\mathcal{C})$ es un código lineal binario. Sean $\mathbf{U} \in \mathcal{C}$ y $U(x) + I_4^n \in \mathcal{R}_n$ su representación polinomial, entonces $U(x) + I_4^n \in \mathcal{P}_{\mathcal{R}}^n(\mathcal{C}) = \langle B(x) + 2\rangle$. Por lo que $U(x) + I_4^n = B(x)K(x) + 2K(x) + I_4^n$ para algún $K(x) \in \mathcal{R}[x]$, es decir, $U(x) + I_4^n = H(x) + 2K(x) + I_4^n$, con $H(x) = B(x)K(x)$. Entonces $(\mathcal{P}_{\mathcal{R}}^n)^{-1}(H(x) + 2K(x) + I_4^n) = \mathbf{H} + 2\mathbf{K}$, con $\mathbf{H}, \mathbf{K} \in \mathcal{R}^n$ y además $\mathbf{U} = \mathbf{H} + 2\mathbf{K} = (h_0 + 2k_0, h_1 + 2k_1, \ldots, h_{n-1} + 2k_{n-1}) \in \mathcal{C}$. Luego

$$\begin{aligned} \nu(\mathbf{U}) &= \nu((h_0 + 2k_0, h_1 + 2k_1, \ldots, h_{n-1} + 2k_{n-1})) \\ &= (-h_{n-1} - 2k_{n-1}, h_0 + 2k_0, h_1 + 2k_1, \ldots, h_{n-1} + 2k_{n-1}) \\ &= (3h_{n-1} + 2k_{n-1}, h_0 + 2k_0, h_1 + 2k_1, \ldots, h_{n-2} + 2k_{n-2}). \end{aligned}$$

Por otro lado, al final de la prueba del Teorema 1.5 se exhibió que $A(x)B(x) + I_4^n, 2A(x) + I_4^n \in \langle A(x)B(x) + 2A(x) + I_4^n\rangle$, en este caso, dado que $A(x) = 1$, entonces $B(x) + I_4^n, 2 + I_4^n \in \langle B(x) + 2 + I_4^n\rangle = \mathcal{P}_{\mathcal{R}}^n(\mathcal{C})$. Por lo que $H(x) + I_4^n = B(x)K(x) + I_4^n, 2K(x) + I_4^n \in \mathcal{P}_{\mathcal{R}}^n(\mathcal{C}) \subseteq \mathcal{R}^n$. Así que $\mathbf{H}, 2\mathbf{K}, (2, 0, \ldots, 0) \in \mathcal{C}$. Luego, $\sigma(\mathbf{H}), \sigma(2\mathbf{K})$ y $(2h_{n-1}, 0, \ldots, 0)$ son elementos de $\mathcal{C}$, pues $\mathcal{C}$ es un $\mathcal{R}-$código cíclico lineal. Por lo que $\sigma(\mathbf{H}) + \sigma(2\mathbf{K}) + (2h_{n-1}, 0, \ldots, 0) = (3h_{n-1} + 2k_{n-1}, h_0 + 2k_0, h_1 + 2k_1, \ldots, h_{n-2} + 2k_{n-2}) \in \mathcal{C}$, pero $(3h_{n-1} + 2k_{n-1}, h_0 + 2k_0, h_1 + 2k_1, \ldots, h_{n-2} + 2k_{n-2}) = \nu(\mathbf{U})$. De ahí que, $\nu(\mathbf{U}) \in \mathcal{C}$ con $\mathbf{U}$ un elemento arbitrario de $\mathcal{C}$. Por lo tanto $\mathcal{C}$ es un código negacíclico. Así que por el Teorema 2.3, $\Phi(\mathcal{C})$ es un $\mathbb{F}_2-$código cíclico lineal.

Resta probar el inciso II). Para ello probemos que si $\mathcal{C}$ es generado por $G(x) = D(x) + 2$ ó $G(x) = 2D(x)$ entonces $\Psi(\mathcal{C}) = \Phi(\mathcal{C})$.

Sea $\overline{\gamma}\colon \mathcal{R}^n \to \mathcal{R}^n$ la función dada por $\overline{\gamma}(\mathbf{A}) = (a_0, -a_1, \ldots, (-1)^i a_i, \ldots, a_{n-1})$ con $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n$. Probaremos lo siguiente:

- $\Psi(\mathcal{C}) = \Phi\overline{\gamma}(\mathcal{C})$ y
- $\overline{\gamma}(\mathcal{C}) = \mathcal{C}$.

Sea $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{R}^n$, entonces $\overline{\gamma}(\mathbf{A}) = (a_0, -a_1, \ldots, (-1)^i a_i, \ldots, a_{n-1})$. Así que

$$\Phi(\overline{\gamma}(\mathbf{A})) = (r_1(\overline{\gamma}(\mathbf{A})), r_0(\overline{\gamma}(\mathbf{A})) + r_1(\overline{\gamma}(\mathbf{A}))).$$

Con ayuda de la Tabla 1 podemos probar que para cada $\alpha \in \mathcal{R}$, $r_0(-\alpha) = r_0(\alpha)$ y $r_1(-\alpha) = r_0(\alpha) + r_1(\alpha)$. De ahí que $r_0(-\alpha) + r_1(-\alpha) = r_1(\alpha)$ en $\mathbb{F}_2$. Aplicando estas igualdades a $r_1(\overline{\gamma}(\mathbf{A}))$ y $r_0(\overline{\gamma}(\mathbf{A})) + r_1(\overline{\gamma}(\mathbf{A}))$ tenemos que:

$$\begin{aligned} r_1(\overline{\gamma}(\mathbf{A})) &= (r_1(a_0), r_1(-a_1), \ldots, r_1(-a_{n-2}), r_1(a_{n-1})) \\ &= (r_1(a_0), r_0(a_1) + r_1(a_1), r_1(a_2), \ldots, r_0(a_{n-2}) + r_1(a_{n-2}), r_1(a_{n-1})), \end{aligned}$$

y

$$\begin{aligned} r_0(\overline{\gamma}(\mathbf{A})) + r_1(\overline{\gamma}(\mathbf{A})) &= (r_0(a_0) + r_1(a_0), r_1(-a_1) + r_1(-a_1), \ldots, r_0(a_{n-1}) + r_1(a_{n-1})) \\ &= (r_0(a_0) + r_1(a_0), r_1(a_1), \ldots, r_1(a_{n-2}), r_0(a_{n-1}) + r_1(a_{n-1})). \end{aligned}$$

Entonces

$$\begin{aligned} \Phi(\overline{\gamma}(\mathbf{A})) = (&r_1(a_0), r_0(a_1) + r_1(a_1), r_1(a_2), \ldots, r_0(a_{n-2}) + r_1(a_{n-2}), r_1(a_{n-1}), \\ &r_0(a_0) + r_1(a_0), r_1(a_1), \ldots, r_1(a_{n-2}), r_0(a_{n-1}) + r_1(a_{n-1})). \end{aligned}$$

Por otro lado, notemos que

$$\begin{aligned} \Pi(\Phi(\mathbf{A})) &= \Pi((r_1(a_0), r_1(a_1), \ldots, r_1(a_{n-1}), r_0(a_0) + r_1(a_0), r_0(a_1) + r_1(a_1), \ldots, r_0(a_{n-1}) + r_1(a_{n-1}))) \\ &= (r_1(a_0), r_0(a_1) + r_1(a_1), r_1(a_2), \ldots, r_0(a_{n-2}) + r_1(a_{n-2}), r_1(a_{n-1}), \\ &\quad r_0(a_0) + r_1(a_0), r_1(a_1), \ldots, r_1(a_{n-2}), r_0(a_{n-1}) + r_1(a_{n-1}))). \end{aligned}$$

Por lo tanto, $\Psi(\mathbf{A}) = \Pi\Phi(\mathbf{A}) = \Phi\overline{\gamma}(\mathbf{A})$. Así que $\Psi = \Phi\overline{\gamma}$ para cada $\mathbf{A} \in \mathcal{R}^n$.

Ahora probemos que $\mathcal{C} = \overline{\gamma}(\mathcal{C})$. Como el polinomio generador de $\mathcal{C}$ es $G(x) = D(x) + 2$ ó $G(x) = 2D(x)$, entonces por el inciso I), ya que iii) $\Rightarrow$ ii), tenemos que $\mathcal{C}$ es tambien negacíclico. Sea $\mathbf{C} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, entonces

$$\begin{aligned} \sigma(\mathbf{C}) &= (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}, \\ \nu\sigma(\mathbf{C}) &= (-c_{n-2}, c_{n-1}, c_0, c_1, \ldots, c_{n-3}) \in \mathcal{C}, \\ \sigma\nu\sigma(\mathbf{C}) &= (c_{n-3}, -c_{n-2}, c_{n-1}, c_0, \ldots, c_{n-4}) \in \mathcal{C}. \end{aligned}$$

Observemos que si seguimos repitiendo este procedimiento tendremos que

$$\delta_{n-i}\delta_{n-i-1}\cdots\delta_2\delta_1(\mathbf{C}) = ((-1)^i c_i, (-1^)i + 1c_{i+1}, \ldots, -c_{n-2}, c_{n-1}, c_0, c_1, \ldots, c_{i-1}) \in \mathcal{C},$$

donde $\delta_1 = \sigma$, $\delta_2 = \nu$,

$$\delta_{n-i} = \begin{cases} \sigma, & \text{si} \quad i \text{ es par}, \\ \nu, & \text{si} \quad i \text{ es impar}. \end{cases} \tag{38}$$

Así que

$$\delta_n\delta_{n-1}\cdots\delta_i\cdots\delta_2\delta_1(\mathbf{C}) = (c_0, -c_1, \ldots, (-1)^i c_i, \ldots, -c_{n-2}, c_{n-1}) \in \mathcal{C}.$$

Por otro lado, tenemos que $\overline{\gamma}(\mathbf{C}) = (c_0, -c_1, \ldots (-1)^i c_i, \ldots, -c_{n-2}, c_{n-1})$, entonces por (38) se sigue que $\overline{\gamma}(\mathbf{C}) \in \mathcal{C}$. Por lo tanto $\overline{\gamma}(\mathcal{C}) = \mathcal{C}$.

Como $\Psi(\mathcal{C}) = \Phi(\overline{\gamma}(\mathcal{C}))$ y $\overline{\gamma}(\mathcal{C}) = \mathcal{C}$, entonces $\Psi(\mathcal{C}) = \Phi(\mathcal{C})$, lo cual deseabamos probar.

Por el Teorema 2.6 sabemos que $\Psi(\mathcal{C}) = \langle \overline{A}^2(x)\overline{B}(x) + I_2^{2n} \rangle$ cuando $G(x) = A(x)[B(x) + 2]$. Así que, si $G(x) = 2D(x)$ entonces $D(x) = A(x)$ y $A(x)B(x) = x^n - 1$. Además, se cumple que $\Psi(\mathcal{C}) = \langle \overline{A}^2(x)\overline{B}(x) + I_2^{2n} \rangle = \langle \overline{A}(x)(x^n - 1) + I_2^{2n} \rangle = \langle \overline{D}(x)(x^n - 1) + I_2^{2n} \rangle$, pues $\overline{A}(x)\overline{B}(x) = x^n - 1$ en $\mathbb{F}_2[x]$, es decir,

$$\Psi(\mathcal{C}) = \langle \overline{D}(x)(x^n - 1) + I_2^{2n} \rangle.$$

Cuando $G(x) = D(x) + 2$, sabemos que $D(x) = B(x)$ y $A(x) = 1$. Así que $\Psi(\mathcal{C}) = \langle \overline{A}^2(x)\overline{B}(x) + I_2^{2n} \rangle = \langle \overline{B}(x) + I_2^{2n} \rangle = \langle \overline{D}(x) + I_2^{2n} \rangle$, es decir,

$$\Psi(\mathcal{C}) = \langle \overline{D}(x) + I_2^{2n} \rangle.$$

□

3 IMÁGENES LINEALES BAJO LA FUNCIÓN DE GRAY DE $\mathcal{R}-$CÓDIGOS CÍCLICO LINEALES

En este capítulo se prueba que la imagen bajo la función de Gray de un código cíclico lineal sobre un anillo de Galois de índice de nilpotencia 2 y, cuyo polinomio generador es $B(x)+p$, es lineal sobre $\mathbb{F}_{p^m}$.

En este Capítulo $\mathcal{R}$ denotará un anillo de Galois de índice de nilpotencia 2, es decir, $\mathcal{R} = GR(p^2, m)$, con p un número primo y m un entero positivo. Además, sean n un entero positivo coprimo con p y, $A(x), B(x), C(x) \in \mathcal{R}[x]$ polinomios mónicos coprimos por pares tales que $x^n - 1 = A(x)B(x)C(x)$ (dichos polinomios existen por el Teorema 1.5). Asumiremos que $A(x)$ es el polinomio constante 1, esto es $A(x) = 1$. El ideal principal generado por el polinomio $x^n - 1 \in \mathcal{R}[x]$ lo denotamos por I, es decir, $I = (x^n - 1)$, y al anillo de clases residuales $\mathcal{R}[x]/(x^n - 1)$ lo denotamos por $\mathcal{R}_n$.

Sea $\mathcal{C} \subseteq \mathcal{R}^n$ un $\mathcal{R}-$código cíclico lineal. Sabemos que dicho código tiene su representación polinomial en el anillo $\mathcal{R}_n$, denotada por $\mathcal{P}_\mathcal{C}$, i.e., $\mathcal{P}^n_\mathcal{R}(\mathcal{C}) = \mathcal{P}_\mathcal{C}$. Dicha representación es el ideal principal generado por el polinomio $B(x)+p$, por lo que $\mathcal{P}_\mathcal{C} = \langle B(x)+p+I\rangle$.

Proposición 3.1. *Sea $\mathcal{C} \subseteq \mathcal{R}^n$ un $\mathcal{R}-$código cíclico lineal de longitud n tal que $\mathcal{P}_\mathcal{C} = \langle B(x)+p+I\rangle$. Entonces $\langle p+I\rangle \subseteq \mathcal{P}_\mathcal{C}$.*

Demostración. Dado que $B(x)$ y $C(x)$ son polinomios coprimos en $\mathcal{R}[x]$, entonces existen $S(x), T(x) \in \mathcal{R}[x]$ tales que $1 = S(x)B(x) + T(x)C(x)$. Multiplicando por p ambos lados se obtiene que $p = pS(x)B(x) + pT(x)C(x)$. Pasando a clases polinomiales en el anillo $\mathcal{R}_n$, se cumple que

$$p + I = pS(x)B(x) + pT(x)C(x) + I. \tag{39}$$

Por otro lado, observemos que $C(x)[B(x)+p] = C(x)B(x) + pC(x)$ y $p[B(x)+p] = pB(x) + p^2 = pB(x)$ en $\mathcal{R}[x]$. Por lo que $[C(x)+I][B(x)+p+I] = pC(x) + I$ y $[p+I][B(x)+p+I] = pB(x) + I$. De ahí que $pB(x)+I, pC(x)+I \in \mathcal{R}_n$. Entonces $pS(x)B(x)+I, pT(x)C(x)+I \in \mathcal{R}_n$. Así que por (39), $p+I \in \mathcal{P}_\mathcal{C}$. Por lo tanto $\langle p+I\rangle \subseteq \mathcal{P}_\mathcal{C}$. □

Teorema 3.1. *Sean $\mathcal{C}$ un $\mathcal{R}-$código cíclico lineal de longitud n tal que n es primo relativo con p, generado por el polinomio $G(x) = B(x)+p$ y Φ la función de Gray en $\mathcal{R}^n$. Entonces $\Phi(\mathcal{C})$ es $\mathbb{F}_{p^m}-$ lineal.*

Demostración. Sean $\mathbf{F}, \mathbf{G} \in \mathcal{C}$ cualesquiera. Tomemos $\mathbf{H} = \Theta(\mathbf{F}, \mathbf{G})$. Por definición de Θ tenemos que $\mathbf{H} \in \mathcal{T}^n \subseteq \mathcal{R}^n$. Sea $\mathcal{P}^n_\mathcal{R}$ como en (7). Entonces existe $H(x)+I \in \mathcal{R}_n$ tal que $\mathcal{P}^n_\mathcal{R}(\mathbf{H}) = H(x)+I$. Dado que $\mathcal{P}^n_\mathcal{R}$ es un isomorfimos de $\mathcal{R}-$módulos y $p \in \mathcal{R}$, se tiene que $\mathcal{P}^n_\mathcal{R}(p\mathbf{H}) = p\mathcal{P}^n_\mathcal{R}(\mathbf{H})$, donde $p\mathcal{P}^n_\mathcal{R}(\mathbf{H}) = pH(x)+I$. Observemos que $pH(x)+I \in \langle p+I\rangle$. Así, por la Proposición 3.1 se sigue que $pH(x)+I \in \mathcal{P}_\mathcal{C} = \mathcal{P}^n_\mathcal{R}(\mathcal{C})$. Por consiguiente, $\mathcal{P}^n_\mathcal{R}(p\mathbf{H}) \in \mathcal{P}^n_\mathcal{R}(\mathcal{C})$, y ya que, $\mathcal{P}^n_\mathcal{R}$ es un isomorfismo, entonces $(\mathcal{P}^n_\mathcal{R})^{-1}(\mathcal{P}^n_\mathcal{R}(p\mathbf{H})) \in (\mathcal{P}^n_\mathcal{R})^{-1}(\mathcal{P}^n_\mathcal{R}(\mathcal{C}))$, es decir, $p\mathbf{H} \in \mathcal{C}$. Por lo tanto, para cualesquiera $\mathbf{F}, \mathbf{G} \in \mathcal{C}$ se cumple que $p\Theta(\mathbf{F}, \mathbf{G}) \in \mathcal{C}$. Así que, por el Teorema 2.2, se sigue que $\Phi(\mathcal{C})$ es un $\mathbb{F}_{p^m}-$ lineal. □

En el siguiente ejemplo se ilustra el comportamiento de las imágenes de Gray de dos $GR(p^2, m)-$ códigos cíclicos lineales distintos.

Ejemplo 3.1. *Sean $\mathcal{R} = GR(3^2, 2) = \frac{(\mathbb{Z}/3^2\mathbb{Z})[\xi]}{(\xi^2+4\xi+8)}$ y $n = 2$. El campo residual del anillo $\mathcal{R}$ es isomorfo al campo finito $\mathbb{F}_9$. Construimos el anillo*

$$\mathcal{R}_2 = \frac{\mathcal{R}[z]}{(z^2-1)}.$$

Sabemos que $\mathcal{R}_2$ es un anillo de ideales principales. Observemos que $z^2 - 1 = (z+1)(z+8)$ en $\mathcal{R}[z]$.

Sean $A(z) = z+1$ y $G_1(z) = 2A(z) = 3z+3$. Sea $\mathcal{C}_1 \subseteq \mathcal{R}^2$ el código cíclico lineal de longitud 2 cuyo polinomio generador es $G_1(z)$, es decir, $\mathcal{C}_1 = \langle 2A(z)\rangle$. Entonces su imagen bajo la función de Gray es un código cíclico lineal de longitud 18. Además, el polinomio generador de $\Phi(\mathcal{C}_1)$ es $\overline{A}(z)(z^2-1)^8 \in \mathbb{F}_9[z]$, con $\overline{A}(z)$

la μ—reducción de $A(z) \in \mathcal{R}[z]$ en el campo residual. Esto por los resultados establecidos por López-Andrade y Tepia-Recillas en [LATR12].

Por otro lado, si consideramos a $B(z) = z+1$, $G_2(z) = B(z)+3 = z+4$ y denotamos por $\mathcal{C}_2$ al código cíclico lineal sobre $\mathcal{R}$ de longitud 2, generado por $G_2(z)$. Es decir, $\mathcal{C}_2 = \langle z+4 \rangle \subseteq \mathcal{R}_2$. Observemos que en el anillo $\mathcal{R}_2$ se cumple lo siguiente:

$$3 = 6(z+1) + 6z(z+8).$$

Además, notemos que $6(z+1) = 6z+6 = 6(z+4) = 6G_2(z)$ y $6z(z+8) = 2z(3z+24) = 2z(3z+6) = 2z(z+8)(z+4) = 2z(z+8)G_2(z)$ en $\mathcal{R}_2$. Por lo que $6(z+1), 6z(z+8) \in \mathcal{C}_2$. Así que $3 \in \mathcal{C}_2$. Más aún, $3 = (z+5)(z+4) \mod (z^2-1)$.

Las imágenes de Gray del código $\mathcal{C}_2$ son $\mathbb{F}_9$—lineales pero no cíclicas, tal como se muestra en el Código 9.

4 LA LINEALIDAD DE LA FUNCIÓN DE GRAY SOBRE CIERTO ANILLO COCIENTE

Como sabemos la función de Gray, en general, no es una función lineal. En este capítulo estudiamos a un anillo de clases residuales sobre el cual la función de Gray resulta ser lineal. Esto debido a que el conjunto de Teichmüller es un campo, el cual es isomorfo al campo residual de nuestro anillo. Para ver esto, se estudia de manera más profunda el grupo de unidades del anillo. Cabe mencionar que el anillo de clases residuales que se analiza en este capítulo se deriva de un estudio detallado de la primera sección del artículo [US98].

Definición 4.1. *Sae* $GF(p)[\xi]$ *el anillo de todos los polinomios sobre* $GF(p)$, p *un primo y* $w(\xi)$ *un polinomio irreducible de grado* m *sobre* $GF(p)$, $m \geqslant 1$. *Entonces* $\mathcal{A}$ *es definido como el anillo cociente*

$$\mathcal{A} = \frac{GF(p)[\xi]}{\left(w(\xi)^k\right)},$$

con k *un entero tal que* $k \geqslant 1$.

En particular, los elementos del anillo $\mathcal{A}$ son clases polinomiales y para cada clase se puede escoger un representate polinomial de grado menor que $n = mk$, por otro lado los polinomio de grado menor que n se encuentra en diferentes clases. En adelante, cuando se tome un elemento de $\mathcal{A}$, el representante con el que se trabajará será de grado menor que n.

A los elementos del anillo $\mathcal{A}$ los denotaremos de la siguiente manera, $f(\xi) + \left(w(\xi)^k\right) := \overline{f(\xi)}$.

Observación 4.1. *i) El anillo* $\mathcal{A}$ *es un espacio vectorial sobre el campo* $GF(p)$, *con el siguiente producto escalar* $\mathbf{a} \cdot \overline{f(\xi)} := \overline{af(\xi)}$ *para cada* $\mathbf{a}$ *en* $GF(p)$ *y cada* $\overline{f(\xi)}$ *en* $\mathcal{A}$.

ii) El conjunto $\{\overline{1}, \overline{\xi}, \ldots, \overline{\xi^{n-1}}\}$ *es una base de* $\mathcal{A}$ *sobre* $GF(p)$.

iii) $|\mathcal{A}| = p^n$.

Notemos que de la Observación 4.1 se obtiene la primer representación de los elementos del anillo $\mathcal{A}$, la cual llamaremos *representación base estándar*, y es la siguiente: Sea $\overline{f(\xi)} \in \mathcal{A}$ entonces existen $\mathbf{a_0}, \mathbf{a_1} \ldots, \mathbf{a_{n-1}} \in GF(p)$ tales que

$$\overline{f(\xi)} = \mathbf{a_0}\overline{1} + \mathbf{a_1}\overline{\xi} + \cdots + \mathbf{a_{n-1}}\overline{\xi^{n-1}}. \tag{40}$$

Proposición 4.1. *$\mathcal{A}$ es un anillo de ideales principales.*

Demostración. Sea $\mathcal{I}$ un ideal de $\mathcal{A}$. Observemos que si $\mathcal{I} = \{\overline{0}\}$ entonces $\mathcal{I} = \langle\overline{0}\rangle$, es decir, $\mathcal{I}$ es un ideal principal, y si $\mathcal{I} = \mathcal{A}$ entonces $\mathcal{I} = \langle\overline{1}\rangle$. Por lo que, $\mathcal{I}$ es principal, así que supongamos que $\mathcal{I}$ es un ideal no trivial. Sea $N = \{grad(f(\xi)) | \overline{f(\xi)} \in \mathcal{I} \setminus \{\overline{0}\}\}$, observemos que $N \subseteq \mathbb{N} \cup \{0\}$ y además $N \neq \emptyset$ pues $\mathcal{I} \neq \{\overline{0}\}$. Luego por el principio del buen orden existe $g(\xi) \in GF(p)[\xi]$ tal que $\overline{g(\xi)} \in \mathcal{I}$ y $grad(g(\xi)) \leqslant l$ para cada $l \in N$.

Como $\overline{g(\xi)} \in \mathcal{I}$ entonces $\langle\overline{g(\xi)}\rangle \subseteq \mathcal{I}$, resta probar que $\mathcal{I} \subseteq \langle\overline{g(\xi)}\rangle$. Para ello tomemos $\overline{f(\xi)} \in \mathcal{I} \setminus \{\overline{0}\}$, se tiene que $grad(g(\xi)) \leqslant grad(f(\xi))$, así que por el algoritmo de la división, existen $q(\xi), r(\xi) \in GF(p)[\xi]$ tales que $f(\xi) = q(\xi)g(\xi) + r(\xi)$ donde $r(\xi) = 0$ ó $grad(r(\xi)) < grad(g(\xi))$,

$$\begin{aligned} \Rightarrow r(\xi) &= f(\xi) - q(\xi)g(\xi) \\ \Rightarrow \overline{r(\xi)} &= \overline{f(\xi)} - \overline{q(\xi)g(\xi)} \\ \Rightarrow \overline{r(\xi)} &\in \mathcal{I} \text{ ya que } \overline{f(\xi)}, \overline{g(\xi)} \in \mathcal{I}, \end{aligned}$$

luego $grad(r(\xi)) \in N$. Por lo que, $grad(g(\xi)) \leqslant grad(r(\xi))$, y entonces $r(\xi) = 0$ pues de lo contrario tendríamos que $grad(r(\xi)) \leqslant grad(g(\xi))$ lo cual es una contradicción. Así $g(\xi)$ divide a $f(\xi)$, entonces $\overline{f(\xi)} \in \langle\overline{g(\xi)}\rangle$, de ahí que $\mathcal{I} \subseteq \langle\overline{g(\xi)}\rangle$. Por lo tanto, $\mathcal{A}$ es un anillo de ideales principales. □

El lema que a continuación se enuncia es importante para poder probar que $\mathcal{A}$ es un anillo local.

Lema 4.1. *Sea* $\mathcal{M} = \langle \overline{w(\xi)} \rangle$ *un ideal de* $\mathcal{A}$. *Entonces para todo* $\overline{f(\xi)} \in \mathcal{A} \setminus \mathcal{M}$, $\overline{f(\xi)}$ *es una unidad en* $\mathcal{A}$.

Demostración. Sea $\overline{f(\xi)} \in \mathcal{A} \setminus \mathcal{M}$ arbitrario, sabemos que podemos escoger a $f(\xi) \in GF(p)[\xi]$ de tal manera que $grad f(\xi) < n = mk$. Veamos que $f(\xi)$ y $w(\xi)$ son coprimos en el anillo $GF(p)[\xi]$, es decir, $(f(\xi), w(\xi)) = 1$. Sea $d(\xi) \in GF(p)[\xi]$ tal que $d(\xi) = (f(\xi), w(\xi))$, entonces $d(\xi)$ divide a $f(\xi)$ y $w(\xi)$, pero recordemos que $w(\xi)$ es irreducible sobre $GF(p)[\xi]$, por lo que, $d(\xi) = 1$ ó $d(\xi) = w(\xi)$. Supongamos que $d(\xi) \neq 1$, es decir, $d(\xi) = w(\xi)$ y dado que $d(\xi)$ divide a $f(\xi)$, se tiene que $f(\xi) = w(\xi)g(\xi)$ para algún $g(\xi)GF(p)[\xi]$, así $\overline{f(\xi)} = \overline{w(\xi)g(\xi)}$, por lo que $\overline{f(\xi)} \in \mathcal{M}$, lo cual no es posible pues $\overline{f(\xi)} \in \mathcal{A} \setminus \mathcal{M}$. Por lo tanto, $d(\xi) = 1$.

Afirmación. $(f(\xi), w^l(\xi)) = 1$ para cada $l \in \mathbb{N}$.

Por lo anterior sabemos que para $l = 1$ se cumple que $(f(\xi), w^l(\xi)) = 1$. Ahora probaremos el resultado para $l = 2$. Dado que $(f(\xi), w(\xi)) = 1$ existen $s(\xi), t(\xi) \in GF(p)[\xi]$ tales que $1 = s(\xi)f(\xi) + t(\xi)w(\xi)$. Entonces

$$\begin{aligned} 1 &= s^2(\xi)f^2(\xi) + 2s(\xi)f(\xi)t(\xi)w(\xi) + t^2(\xi)w^2(\xi) \\ &= [s^2(\xi)f(\xi) + 2s(\xi)t(\xi)w(\xi)]f(\xi) + t^2(\xi)w^2(\xi) \\ &= s'(\xi)f(\xi) + t'(\xi)w^2(\xi) \end{aligned}$$

con $s'(\xi) = s^2(\xi)f(\xi) + 2s(\xi)t(\xi)w(\xi)$ y $t'(\xi) = t^2(\xi)$ polinomios en $GF(p)[\xi]$. Así que el resultado se sigue para $l = 2$.

Supongamos que $(f(\xi), w^l(\xi)) = 1$ con $l > 2$ y veamos que se cumple para $l + 1$. Dado que $(f(\xi), w^l(\xi)) = 1$ y $(f(\xi), w(\xi)) = 1$ existen $s(\xi), t(\xi), u(\xi), v(\xi) \in GF(p)[\xi]$ tales que $1 = u(\xi)f(\xi) + v(\xi)w^l(\xi)$ y $1 = s(\xi)f(\xi) + t(\xi)w(\xi)$. Entonces

$$\begin{aligned} 1 &= [u(\xi)f(\xi) + v(\xi)w^l(\xi)][s(\xi)f(\xi) + t(\xi)w(\xi)] \\ &= u(\xi)s(\xi)f^2(\xi) + v(\xi)w^l(\xi)s(\xi)f(\xi) + u(\xi)f(\xi)t(\xi)w(\xi) + v(\xi)t(\xi)w^{l+1}(\xi) \\ &= [u(\xi)s(\xi)f(\xi) + v(\xi)w^l(\xi)s(\xi) + u(\xi)t(\xi)w(\xi)]f(\xi) + [v(\xi)t(\xi)]w^{l+1}(\xi) \\ &= u'(\xi)f(\xi) + v'(\xi)w^{l+1}(\xi) \end{aligned}$$

con $u'(\xi) = u(\xi)s(\xi)f(\xi) + v(\xi)w^l(\xi)s(\xi) + u(\xi)t(\xi)w(\xi)$ y $v'(\xi) = v(\xi)t(\xi)$ polinomios en $GF(p)[\xi]$. Por lo tanto, para toda $l \in \mathbb{N}$, $(f(\xi), w^l(\xi)) = 1$.

Por la afirmación se tiene que $(f(\xi), w^k(\xi)) = 1$, así que existen $a(\xi), b(\xi) \in GF(p)[\xi]$ tales que $1 = a(\xi)f(\xi) + b(\xi)w^k(\xi)$. Entonces

$$\begin{aligned} & 1 - a(\xi)f(\xi) &&= b(\xi)w^k(\xi) \\ \Rightarrow\ & \overline{1 - a(\xi)f(\xi)} &&= \overline{0} \\ \Rightarrow\ & \overline{1} &&= \overline{a(\xi)f(\xi)}. \end{aligned}$$

Por lo tanto, $\overline{f(\xi)}$ es una unidad en $\mathcal{A}$.

□

Proposición 4.2. *$\mathcal{A}$ es un anillo local.*

Demostración. Por el lema previo y haciendo uso de la Propocisión 1.6 de [AM69], se sigue que $\mathcal{A}$ es un anillo local, y además $\mathcal{M}$ es su ideal maximal. □

Proposición 4.3. *Sea* $\mathcal{I}$ *un ideal de* $\mathcal{A}$, *entonces* $\mathcal{I} = \langle \overline{w^j(\xi)} \rangle$ *con* $0 \leqslant j \leqslant k$.

Demostración. Sea $\mathcal{I}$ un ideal de $\mathcal{A}$. Notemos que $\overline{w^0(\xi)} = \overline{1}$ y $\overline{w^k(\xi)} = \overline{0}$. Por lo que, si $\mathcal{I} = \langle \overline{1} \rangle$ ó $\mathcal{I} = \langle \overline{0} \rangle$ el resultado se sigue. Así que supongamos que $\mathcal{I}$ es un ideal no trivial, por la Proposición 4.1 sabemos que existe $\overline{f(\xi)} \in \mathcal{A}$ tal que $\mathcal{I} = \langle \overline{f(\xi)} \rangle$ y como $\mathcal{M} = \langle \overline{w(\xi)} \rangle$ es el ideal maximal de $\mathcal{A}$ entonces $\mathcal{I} \subseteq \mathcal{M}$, de ahí que existe $\overline{g_1(\xi)} \in \mathcal{A}$ tal que

$$\overline{f(\xi)} = \overline{w(\xi)g_1(\xi)},$$

si $\overline{g_1(\xi)} \notin \mathcal{M}$, por el Lema 4.1, existe $\overline{h_1(\xi)} \in \mathcal{A}$ tal que $\overline{g_1(\xi)h_1(\xi)} = \overline{1}$, entonces $\overline{f(\xi)h_1(\xi)} = \overline{w(\xi)}$, así que $\mathcal{I} = \mathcal{M}$ y el resultado se cumple. Pero si $\overline{g_1(\xi)} \in \mathcal{M}$ entonces $\overline{g_1(\xi)} = \overline{w(\xi)g_2(\xi)}$ para algún $\overline{g_2(\xi)} \in \mathcal{A}$, luego

$$\overline{f(\xi)} = \overline{w^2(\xi)g_2(\xi)},$$

de ahí que $\mathcal{I} = \langle \overline{f(\xi)} \rangle \subseteq \langle \overline{w^2(\xi)} \rangle$ y además si $\overline{g_2(\xi)} \notin \mathcal{M}$, existe $\overline{h_2(\xi)} \in \mathcal{A}$ tal que $\overline{g_2(\xi)h_2(\xi)} = \overline{1}$, así $\overline{f(\xi)h_2(\xi)} = \overline{w^2(\xi)}$, y entonces $\langle \overline{w^2(\xi)} \rangle = \mathcal{I}$, en caso contrario, si $\overline{g_2(\xi)} \in \mathcal{M}$, repetimos el análisis previo.

Observemos que dicho análisis sólo se puede realizar a lo más $k-1$ veces hasta encontrar $\overline{g_{k-1}(\xi)} \in \mathcal{A}$ tal que

$$\overline{f(\xi)} = \overline{w^{k-1}(\xi)}\overline{g_{k-1}(\xi)}$$

y $\overline{g_{k-1}(\xi)} \in \mathcal{A} \setminus \mathcal{M}$ (pues de lo contrario podríamos obtener un $\overline{g_k(\xi)} \in \mathcal{A}$ tal que $\overline{g_{k-1}(\xi)} = \overline{w(\xi)g_k(\xi)}$ y así $\overline{f(\xi)} = \overline{w^k(\xi)}\overline{g_k(\xi)} = \overline{0}$, lo cual es una contradicción pues $\mathcal{I} \neq \{\overline{0}\}$), entonces existe $\overline{h_{k-1}(\xi)} \in \mathcal{A}$ tal que $\overline{g_{k-1}(\xi)h_{k-1}(\xi)} = \overline{1}$, luego $\overline{f(\xi)h_{k-1}(\xi)} = \overline{w^{k-1}(\xi)}$ y por lo tanto, $\mathcal{I} = \langle\overline{w^{k-1}(\xi)}\rangle$.

Así que para cualquier ideal $\mathcal{I}$ de $\mathcal{A}$ existe $j \in \{0, 1, \ldots, k\}$ tal que $\mathcal{I} = \langle\overline{w^j(\xi)}\rangle$.

□

Observación 4.2. *Los ideales de $\mathcal{A}$ satisfacen la condición de cadena finita ya que para cada $j \in \{0, 1, \ldots, k-1\}$, se tiene que $\overline{w^{j+1}(\xi)} = \overline{w^j(\xi)}\overline{w(\xi)}$ y de ahí que $\langle\overline{w^{j+1}(\xi)}\rangle \subset \langle\overline{w^j(\xi)}\rangle$.*

Observación 4.3. *Los elementos del ideal $\mathcal{M} = \langle\overline{w(\xi)}\rangle$ son todos los divisores de cero del anillo $\mathcal{A}$.*

Proposición 4.4. *Sea $\overline{a(\xi)} \in \mathcal{M}$ un divisor de cero, entonces*

$$\overline{a(\xi)} = \overline{w^t(\xi)a_u(\xi)} \tag{41}$$

con $0 < t \leqslant k-1$ y $\overline{a_u(\xi)}$ una unidad de $\mathcal{A}$.

Demostración. Como $\overline{a(\xi)}$ es un divisor de cero, se tiene que $\overline{a(\xi)} \neq \overline{0}$ y además, por la Observación 4.3, $\overline{a(\xi)} \in \mathcal{M}$, así que existe $\overline{g_1(\xi)} \in \mathcal{A} \setminus \{\overline{0}\}$ tal que

$$\overline{a(\xi)} = \overline{w(\xi)g_1(\xi)},$$

notemos que si $\overline{g_1(\xi)} \notin \mathcal{M}$ el resultado se sigue, pero si $\overline{g_1(\xi)} \in \mathcal{M}$ entonces $\overline{g_1(\xi)} = \overline{w(\xi)g_2(\xi)}$ para algún $\overline{g_2(\xi)} \in \mathcal{A}$, por lo que

$$\overline{a(\xi)} = \overline{w^2(\xi)}\overline{g_2(\xi)},$$

y una vez más se tienen dos casos, $\overline{g_2(\xi)} \in \mathcal{M}$ ó $\overline{g_2(\xi)}$ es una unidad de $\mathcal{A}$. Si se cumple lo segundo habremos terminado, y si $\overline{g_2(\xi)} \in \mathcal{M}$ entonces repetimos el procedimiento anterior. Observemos que el análisis previo se puede realizar a lo más $k-1$ veces y obtendríamos un $\overline{g_{k-1}(\xi)} \in \mathcal{A}$ tal que

$$\overline{a(\xi)} = \overline{w^{k-1}(\xi)}\overline{g_{k-1}(\xi)},$$

y además $\overline{g_{k-1}(\xi)}$ es unidad, pues de lo contario podríamos hallar un $\overline{g_k(\xi)} \in \mathcal{A}$ tal que $\overline{g_{k-1}(\xi)} = \overline{w(\xi)g_k(\xi)}$ y así $\overline{a(\xi)} = \overline{w^k(\xi)}\overline{g_k(\xi)} = \overline{0}$ lo cual no es posible. Por lo tanto, $\overline{a(\xi)} = \overline{w^t(\xi)}\overline{a_u(\xi)}$ con $0 < t \leqslant k-1$ y $\overline{a_u(\xi)}$ una unidad de $\mathcal{A}$.

□

4.1 EL CAMPO RESIDUAL DEL ANILLO $\mathcal{A}$

Definición 4.2. *Sea $\mathcal{A}$ un anillo local y $\mathcal{M}$ su ideal maximal, el campo $\mathcal{A}/\mathcal{M}$ es llamado el campo residual del anillo $\mathcal{A}$, y es denotado por RF, es decir,*

$$RF = \frac{\mathcal{A}}{\mathcal{M}}.$$

Dado que el ideal maximal del anillo $\mathcal{A} = GF(p)[\xi]/\left(w(\xi)^k\right)$ es $\mathcal{M} = \langle\overline{w(\xi)}\rangle$, se tiene que su campo residual es:

$$RF = \frac{\mathcal{A}}{\mathcal{M}} = \frac{\dfrac{GF(p)[\xi]}{\overline{\left(w(\xi)^k\right)}}}{\langle\overline{w(\xi)}\rangle}.$$

El cual resulta ser isomorfo a $\mathbb{F}_{p^m}$. Para establecer dicho resultado veamos que la siguiente función es un homomorfismo sobreyectivo de anillos cuyo Kernel resulta ser el ideal $\mathcal{M} = \langle\overline{w(\xi)}\rangle$ donde $w(\xi)$ es irreducible en $GF(p)[\xi]$ y $grad(w(\xi)) = m$. Definimos al función φ de la siguiente manera:

$$\begin{array}{rccc} \varphi\colon & \dfrac{GF(p)[\xi]}{\left(w(\xi)^k\right)} & \longrightarrow & \dfrac{GF(p)[\xi]}{(w(\xi))} \\ & f(\xi)+\left(w(\xi)^k\right) & \longmapsto & f(\xi)+(w(\xi))\,. \end{array} \tag{42}$$

Veamos que φ está bien definida. Sean $f_1(\xi)+\left(w(\xi)^k\right), f_2(\xi)+\left(w(\xi)^k\right) \in \mathcal{A}$ tales que $f_1(\xi)+\left(w(\xi)^k\right) = f_2(\xi)+\left(w(\xi)^k\right)$,

$$\begin{array}{rrcl} \Rightarrow & [f_1(\xi)-f_2(\xi)]+\left(w(\xi)^k\right) & = & 0+\left(w(\xi)^k\right) \\ \Rightarrow & \varphi\left([f_1(\xi)-f_2(\xi)]+\left(w(\xi)^k\right)\right) & = & \varphi\left(0+\left(w(\xi)^k\right)\right) \\ \Rightarrow & [f_1(\xi)-f_2(\xi)]+(w(\xi)) & = & 0+(w(\xi)) \\ \Rightarrow & f_1(\xi)+(w(\xi)) & = & f_2(\xi)+(w(\xi)) \\ \Rightarrow & \varphi\left(f_1(\xi)+\left(w(\xi)^k\right)\right) & = & \varphi\left(f_2(\xi)+\left(w(\xi)^k\right)\right) \end{array}$$

De ahí que φ está bien definida. Por otro lado, sean $\overline{f(\xi)} = f(\xi)+\left(w(\xi)^k\right), \overline{g(\xi)} = g(\xi)+\left(w(\xi)^k\right) \in \mathcal{A}$ tales que $grad(f(\xi)), grad(g(\xi)) < n = mk$, entonces

i) $\varphi\left(\overline{f(\xi)}+\overline{g(\xi)}\right) = \varphi\left(\overline{f(\xi)+g(\xi)}\right) = \varphi\left([f(\xi)+g(\xi)]+\left(w(\xi)^k\right)\right) = [f(\xi)+g(\xi)]+(w(\xi)) = [f(\xi)+(w(\xi))]+[g(\xi)+(w(\xi))] = \varphi\left(\overline{f(\xi)}\right)+\varphi\left(\overline{g(\xi)}\right)$,

ii) $\varphi\left(\overline{f(\xi)}\cdot\overline{g(\xi)}\right) = \varphi\left(\overline{f(\xi)g(\xi)}\right) = \varphi\left([f(\xi)g(\xi)]+\left(w(\xi)^k\right)\right) = [f(\xi)g(\xi)]+(w(\xi)) = [f(\xi)+(w(\xi))]\cdot[g(\xi)+(w(\xi))] = \varphi\left(\overline{f(\xi)}\right)\cdot\varphi\left(\overline{g(\xi)}\right)$,

iii) $\varphi\left(\overline{1}\right) = \varphi\left(1+\left(w(\xi)^k\right)\right) = 1+(w(\xi))$.

Por i), ii) y iii) se tiene que φ es un homomorfismo de anillos. Para probar que es sobreyectiva tomemos $h(\xi)+(w(\xi)) \in GF(p)[\xi]/(w(\xi))$ una clase arbitraria pero cuyo representante $h(\xi) \in GF(p)[\xi]$ es tal que $grad h(\xi) < m$, entonces $h(\xi)+\left(w(\xi)^k\right) \in \mathcal{A}$ y notemos que

$$\varphi\left(h(\xi)+\left(w(\xi)^k\right)\right) = h(\xi)+(w(\xi))\,,$$

se sigue que φ es un homomorfismo sobreyectivo de anillos.

Sea $f(\xi)+\left(w(\xi)^k\right) \in \ker(\varphi)$,

$$\begin{array}{rrcl} \Rightarrow & \varphi\left(f(\xi)+\left(w(\xi)^k\right)\right) & = & 0+(w(\xi)) \\ \Rightarrow & f(\xi)+(w(\xi)) & = & 0+(w(\xi)) \\ \Rightarrow & f(\xi) & \in & (w(\xi)) \\ \Rightarrow & f(\xi) & = & w(\xi)t(\xi) \text{ para algún } t(\xi) \in GF(p)[\xi] \\ \Rightarrow & f(\xi)+\left(w(\xi)^k\right) & = & w(\xi)t(\xi)+\left(w(\xi)^k\right) \\ \Rightarrow & f(\xi)+\left(w(\xi)^k\right) & \in & \langle w(\xi)+\left(w(\xi)^k\right)\rangle, \end{array}$$

de ahí que $\ker(\varphi) \subseteq \langle w(\xi)+\left(w(\xi)^k\right)\rangle$, y ya que $\varphi\left(w(\xi)+\left(w(\xi)^k\right)\right) = w(\xi)+(w(\xi)) = 0+\left(w(\xi)^k\right)$, entonces $w(\xi)+\left(w(\xi)^k\right) \in \ker(\varphi)$. Por lo tanto, $\ker(\varphi) = \langle w(\xi)+\left(w(\xi)^k\right)\rangle = \mathcal{M}$.

Por el Primer Teorema de Isormorfismos de Anillos tenemos que

$$\frac{\mathcal{A}}{\ker(\varphi)} \cong Im(\varphi).$$

Entonces

$$RF = \frac{\mathcal{A}}{\mathcal{M}} \cong \frac{GF(p)[\xi]}{(w(\xi))}.$$

Recordemos que $GF(p)[\xi]/(w(\xi)) \cong \mathbb{F}_{p^m}$. Por lo que $RF \cong \mathbb{F}_{p^m}$.

A partir de este momento, y haciendo uso de lo anterior, cuando se hable del campo residual del anillo $\mathcal{A}$ trabajaremos con $GF(p)[\xi]/(w(\xi))$.

Notación. Observemos que los elementos de RF son de la forma $\lambda(\xi)+(w(\xi))$, sin embargo denotaremos a los elementos de RF de la siguiente manera:

$$\lambda(\xi)+(w(\xi)) := \lambda,$$

donde $\lambda(\xi) \in GF(p)[\xi]$ y recordemos que podemos tomar a $\lambda(\xi)$ de grado menor que $m = grad(w(\xi))$.

A continuación definimos el producto escalar, "$\cdot_e$", entre elementos de $\mathcal{A}$ y RF para después probar que $\mathcal{A}$ es un espacio vectorial sobre RF.

Sean $\lambda \in GF(p)[\xi]$ y $\overline{f(\xi)} \in \mathcal{A}$ entonces

$$\lambda \cdot_e \overline{f(\xi)} := [\lambda(\xi)f(\xi)] + \left(w(\xi)^k\right) = \overline{\lambda(\xi)f(\xi)}.$$

Lema 4.2. *$\mathcal{A}$ es un espacio vectorial sobre* RF.

Sabemos que $(\mathcal{A}, +, \overline{0})$ es un grupo conmutativo. Por lo que sólo debemos probar que las siguientes propiedades se satisfacen:

i) $\forall \alpha, \beta \in RF: \forall \overline{f(\xi)} \in \mathcal{A}: \alpha \cdot_e (\beta \cdot_e \overline{f(\xi)}) = (\alpha\beta) \cdot_e \overline{f(\xi)}$,

ii) $\forall \alpha \in RF : \forall \overline{f(\xi)}, \overline{g(\xi)} \in \mathcal{A}: \alpha \cdot_e (\overline{f(\xi)} + \overline{g(\xi)}) = \alpha \cdot_e \overline{f(\xi)} + \alpha \cdot_e \overline{g(\xi)}$,

iii) $\forall \alpha, \beta \in RF: \forall \overline{f(\xi)} \in \mathcal{A}: (\alpha + \beta) \cdot_e \overline{f(\xi)} = \alpha \cdot_e \overline{f(\xi)} + \beta \cdot_e \overline{f(\xi)}$,

iv) $\exists 1 \in RF: \forall \overline{f(\xi)} \in \mathcal{A}: 1 \cdot_e \overline{f(\xi)} = \overline{f(\xi)}$.

Demostración. Sean $\alpha, \beta \in RF$ y $\overline{f(\xi)}, \overline{g(\xi)} \in \mathcal{A}$,

i) $\alpha \cdot_e (\beta \cdot_e \overline{f(\xi)}) = \alpha \cdot_e \overline{\beta(\xi)f(\xi)} = \overline{\alpha(\xi)[\beta(\xi)f(\xi)]} = \overline{[\alpha(\xi)\beta(\xi)f](\xi)} = (\alpha\beta) \cdot_e \overline{f(\xi)}$,

ii) $\alpha \cdot_e (\overline{f(\xi)} + \overline{g(\xi)}) = \alpha \cdot_e (\overline{f(\xi) + g(\xi)}) = \overline{\alpha(\xi)[f(\xi) + g(\xi)]} = \overline{\alpha(\xi)f(\xi) + \alpha(\xi)g(\xi)} = \overline{\alpha(\xi)f(\xi)} + \overline{\alpha(\xi)g(\xi)} = \alpha \cdot_e \overline{f(\xi)} + \alpha \cdot_e \overline{g(\xi)}$,

iii) $(\alpha + \beta) \cdot_e \overline{f(\xi)} = \overline{(\alpha(\xi) + \beta(\xi))f(\xi)} = \overline{\alpha(\xi)f(\xi) + \beta(\xi)f(\xi)} = \overline{\alpha(\xi)f(\xi)} + \overline{\beta(\xi)f(\xi)} = \alpha \cdot_e \overline{f(\xi)} + \beta \cdot_e \overline{f(\xi)}$,

iv) Sabemos que $1 \in RF$ donde $1 := 1 + (w(\xi))$ con $1 \in GF(p)[\xi]$, luego $1 \cdot_e \overline{f(\xi)} = \overline{1f(\xi)} = \overline{f(\xi)}$ pues $1f(\xi) = f(\xi) \in GF(p)[\xi]$.

□

Proposición 4.5. *El conjunto $\mathcal{B} = \{\overline{1}, \overline{w(\xi)}, \ldots, \overline{w^{k-1}(\xi)}\}$ es una base del espacio vectorial $\mathcal{A}$ sobre* RF.

Demostración. Sean $\lambda_0, \lambda_1, \ldots, \lambda_{k-1} \in RF$ tales que $\lambda_0 \cdot_e \overline{1} + \lambda_1 \cdot_e \overline{w(\xi)} + \cdots + \lambda_{k-1} \cdot_e \overline{w^{k-1}(\xi)} = \overline{0}$. Entonces

$$\begin{array}{rrcll}
 & \overline{\lambda_0(\xi)} + \overline{\lambda_1(\xi)w(\xi)} + \cdots + \overline{\lambda_{k-1}(\xi)w^{k-1}(\xi)} & = & \overline{0} & \\
\Rightarrow & \lambda_0(\xi) + \lambda_1(\xi)w(\xi) + \cdots + \lambda_{k-1}(\xi)w^{k-1}(\xi) & \in & \left(w(\xi)^k\right) & \\
\Rightarrow & \lambda_0(\xi) + \lambda_1(\xi)w(\xi) + \cdots + \lambda_{k-1}(\xi)w^{k-1}(\xi) & = & w(\xi)^k f(\xi) \text{ para algún } f(\xi) \in GF(p)[\xi] & \\
\Rightarrow & w(\xi)^k f(\xi) - \lambda_1(\xi)w(\xi) - \cdots - \lambda_{k-1}(\xi)w^{k-1}(\xi) & = & \lambda_0(\xi) & \\
\Rightarrow & [w(\xi)^{k-1} f(\xi) - \lambda_{k-1}(\xi)w^{k-2}(\xi) - \cdots - \lambda_1(\xi)]w(\xi) & = & \lambda_0(\xi) & (*)
\end{array}$$

Así que $w(\xi) | \lambda_0(\xi)$. Dado que $grad(\lambda_0(\xi)) < m = grad(w(\xi))$ entonces $\lambda_0(\xi) = 0$. Sustituyendo $\lambda_0(\xi)$ en $(*)$ se sigue que

$$[w(\xi)^{k-1} f(\xi) - \lambda_{k-1}(\xi)w^{k-2}(\xi) - \cdots - \lambda_1(\xi)]w(\xi) = 0.$$

Como $w(\xi) \neq 0$. Entonces

$$\begin{array}{rrcll}
 & 0 & = & w(\xi)^{k-1} f(\xi) - \lambda_{k-1}(\xi)w^{k-2}(\xi) - \cdots - \lambda_1(\xi) & \\
\Rightarrow & \lambda_1(\xi) & = & [w(\xi)^{k-2} f(\xi) - \lambda_{k-1}(\xi)w^{k-2}(\xi) - \cdots - \lambda_2(\xi)]w(\xi) & (**).
\end{array}$$

Luego $w(\xi) | \lambda_1(\xi)$. De manera análoga a como se hizo con $\lambda_0(\xi)$ tenemos que $\lambda_1(\xi) = 0$. Continuando de esta forma obtendremos que $\lambda_0(\xi) = \lambda_1(\xi) = \cdots = \lambda_{k-1}(\xi) = 0$. Así que para cada $0 \leqslant i \leqslant k-1$ se tiene que $\lambda_i := \lambda_i(\xi) + (w(\xi)) = 0 + (w(\xi)) := 0$. Por lo tanto, $\mathcal{B}$ es un conjunto linealmente independiente sobre RF.

Ahora veamos que el conjunto $\mathcal{B}$ genera a todo $\mathcal{A}$. Sea $\overline{f(\xi)} \in \mathcal{A}$, sabemos que $f(\xi) \in GF(p)[\xi]$. Además, puede ser tomado de tal forma que $grad(f(\xi)) < n = mk$. Por el algoritmo de la división existen $q_0(\xi), r_0(\xi) \in GF(p)[\xi]$ tales que

$$f(\xi) = q_0(\xi)w(\xi) + r_0(\xi) \tag{43}$$

donde $r_0(\xi) = 0$ ó $grad(r_0(\xi) < m)$. Aplicando nuevamente el algoritmo de la división a $q_0(\xi)$ y $r_0(\xi)$, tenemos que existen $q_1(\xi), r_1(\xi) \in GF(p)[\xi]$ tales que $q_0(\xi) = q_1(\xi)w(\xi) + r_1(\xi)$, donde $r_1(\xi) = 0$ ó $grad(r_1(\xi)) < m$. Sustituyendo $q_0(\xi)$ en (43) obtenemos que

$$f(\xi) = q_1(\xi)w^2(\xi) + r_1(\xi)w(\xi) + r_0(\xi).$$

Haciendo este análisis $k-2$ veces más tendremos que

$$f(\xi) = q_{k-1}(\xi)w^k(\xi) + r_{k-1}(\xi)w^{k-1}(\xi) + \cdots + r_1(\xi)w(\xi) + r_0(\xi). \tag{44}$$

Observemos que para cada $0 \leqslant i \leqslant k-1$, $grad(r_1(\xi)) < m$ ó $r_i(\xi) = 0$. Por lo que $r_i(\xi) + (w(\xi)) \in RF$ para cada $i = 0, 1 \ldots, k-1$.

De (44) se tiene que $\overline{f(\xi)} = \overline{r_{k-1}(\xi)w^{k-1}(\xi) + \cdots + r_1(\xi)w(\xi) + r_0(\xi)}$ y sea $r_i = r_i(\xi) + (w(\xi)) \in RF$. Entonces

$$f(\xi) = r_{k-1} \cdot_e \overline{w^{k-1}(\xi)} + \cdots + r_1 \cdot_e \overline{w(\xi) + r_0(\xi)}.$$

Así, $\mathcal{B}$ genera al espacio vectorial $\mathcal{A}$ sobre RF. Por lo tanto, $\mathcal{B}$ es una base de $\mathcal{A}$ sobre RF. □

De lo anterior se tiene que: para cada $\overline{f(\xi)} \in \mathcal{A}$

$$\overline{f(\xi)} = \lambda_0\overline{1} + \lambda_1\overline{w(\xi)} + \cdots + \lambda_{k-1}\overline{w^{k-1}(\xi)} \tag{45}$$

donde los $\lambda_i \in RF$ para cada $i = 0, \ldots, k-1$.

4.2 EL GRUPO DE UNIDADES DEL ANILLO $\mathcal{A}$

Sea $\overline{a(\xi)}$ en $\mathcal{A}$. Observemos que si $\overline{a(\xi)}$ es una unidad, entonces $\overline{a(\xi)} \in \mathcal{A} \setminus \mathcal{M}$, es decir, $\overline{a(\xi)} \notin \mathcal{M}$. Como podemos tomar a $a(\xi) \in GF(p)[\xi]$ de tal forma que $grad(a(\xi)) < n = mk$, entonces existe $j \in \{0, 1, \ldots, k-1\}$ tal que $mj \leqslant grad(a(\xi)) < m(j+1)$. Si $j = 0$ entonces $0 \leqslant grad(a(\xi)) < m$. Sean $\overline{s_0(\xi)} = \overline{a(\xi)}$ y $\overline{s_i(\xi)} = \overline{0}$ para cada $i \in \{1, \ldots, k-1\}$. Entonces

$$\overline{a(\xi)} = \sum_{i=0}^{k-1} \overline{w^i(\xi)}\overline{s_i(\xi)}.$$

Si $j > 0$, entonces por el Algoritmo de la División existen $q_0(\xi), r_0(\xi) \in GF(p)[\xi]$ tales que

$$a(\xi) = w^j(\xi)q_0(\xi) + r_0(\xi) \qquad \text{donde } 0 \leqslant grad(r_0(\xi)) < grad(w^j(\xi)) \text{ y } 0 \leqslant grad(q_0(\xi)) < m. \tag{46}$$

Notemos que $r_0(\xi) \neq 0$ pues $a(\xi) \notin \mathcal{M}$. Si $grad(q_0(\xi)) \geqslant m$ entonces $grad(a(\xi)) \geqslant mj + m$. Lo cual es una contradicción. Por otro lado, si $grad(r_0(\xi)) \geqslant m$ entonces, existe $j_1 \in \{1, \ldots, j-1\}$ tal que $mj_1 \leqslant grad(r_0(\xi)) < m(j_1+1)$. Así que, existen $q_1(\xi), r_1(\xi) \in GF(p)[\xi]$ tales que $r_0(\xi) = w^{j_1}(\xi)q_1(\xi) + r_1(\xi)$, donde $0 \leqslant grad(r_1(\xi)) < grad(w^{j_1}(\xi))$ y $0 \leqslant grad(q_1(\xi)) < m$. Sustituyendo $r_0(\xi)$ en (46) se tiene que

$$a(\xi) = w^j(\xi)q_0(\xi) + w^{j_1}(\xi)q_1(\xi) + r_1(\xi), \tag{47}$$

donde $0 \leqslant grad(r_1(\xi)) < grad(w^{j_1}(\xi))$ y $0 \leqslant grad(q_0(\xi)), grad(q_1(\xi)) < m$. Si $grad(r_1(\xi)) \geqslant m$ entonces, realizamos el análisis previo para $r_1(\xi)$, y así sucesivamente hasta encontrar un $r_t(\xi) \in GF(p)[\xi]$ con $1 \leqslant t \leqslant j-1$ tal que $0 \leqslant grad(r_t(\xi)) < m$ y

$$a(\xi) = w^j(\xi)q_0(\xi) + w^{j_1}(\xi)q_1(\xi) + \cdots + w^{j_t}(\xi)q_t(\xi) + r_t(\xi).$$

Además $j > j_1 > \cdots > j_t$. Más aún, se cumple que

$$a(\xi) = w^j(\xi)s_j(\xi) + w^{j-1}(\xi)s_{j-1}(\xi) + \cdots + w^2(\xi)s_2(\xi) + w(\xi)s_1(\xi) + s_0(\xi),$$

donde $s_0(\xi) = r_t(\xi)$, t de los $s_i(\xi)$ son iguales a los $q_1(\xi)$ y el resto a cero . Observemos que $r_t(\xi) \neq 0$ ya que en caso contrario, $\overline{a(\xi)}$ sería un divisor de cero, lo cual no es posible pues $\overline{a(\xi)}$ es una unidad de $\mathcal{A}$.

Con lo anterio se prueba el siguiente resultado

Proposición 4.6. *Sea $\overline{a(\xi)}$ un unidad en el anillo $\mathcal{A}$. Se tiene que*

$$\overline{a(\xi)} = \sum_{i=0}^{k-1} \overline{w^i(\xi)}\overline{s_i(\xi)} \tag{48}$$

donde para cada $i \in \{1, \ldots, k-1\}$, $\overline{s_i(\xi)} = \overline{0}$ ó $0 \leqslant grad(s_i(\xi)) < m$, además $\overline{s_0(\xi)} \neq \overline{0}$ y $0 \leqslant grad(s_0(\xi)) < m$.

Es bien sabido que el conjunto de unidades de un anillo es un grupo multiplicativo, en este caso el grupo de unidades del anillo $\mathcal{A}$ es el conjunto $\mathcal{A}^* = \mathcal{A} \setminus \mathcal{M}$ y por la Proposición 4.6 tenemos una caracterización de los elementos de $\mathcal{A}^*$ y es la siguiente:

$$\mathcal{A}^* = \left\{ \sum_{i=0}^{k-1} \overline{w^i(\xi)}\overline{s_i(\xi)} : \overline{s_0(\xi)} \neq \overline{0}, \text{ y para cada } i \in \{1, \ldots, k-1\} \ \overline{s_i(\xi)} = \overline{0} \text{ ó } 0 \leqslant grad(s_i(\xi)) < m \right\}.$$

Corolario 4.1. $|\mathcal{A}^*| = p^{m(k-1)}(p^m - 1)$.

Demostración. Por la caracterización de los elementos de $\mathcal{A}^*$ sabemos que, cuando $i \neq 0$, $s_i(\xi) \in \{f(\xi) \in GF(p)[\xi] : f(\xi) = \mathbf{f_0} + \mathbf{f_1}\xi + \cdots + \mathbf{f_{m-1}}\xi^{m-1} \text{ con } \mathbf{f_l} \in GF(p) \text{ para cada } l = 0, \ldots, m-1\} = G$. Para $i = 0$ se cumple que, $s_0(\xi) \in G \setminus \{0\}$. Observemos que $|G| = p^m$. Por el principio de la multiplicación se tiene que $|\mathcal{A}^*| = (p^m)^{k-1}(p^m - 1) = p^{m(k-1)}(p^m - 1)$. □

Observación 4.4. *Sabemos que $\mathcal{A}^* \cap \mathcal{M} = \emptyset$. Por lo que $|\mathcal{M}| = |\mathcal{A} \setminus \mathcal{A}^*|$. Así que $|\mathcal{M}| = p^{mk} - p^{m(k-1)}(p^m - 1) = p^{m(k-1)}$, es decir, $|\mathcal{M}| = p^{m(k-1)}$.*

Definimos el siguiente conjunto,

$$\overline{1} + \mathcal{M} := \{\overline{1} + \overline{m(\xi)} \,|\, \overline{m(\xi)} \in \mathcal{M}\}.$$

Es claro que $\overline{1} + \mathcal{M} \subseteq \mathcal{A}^*$. De no ser así tendremos que, existe $\overline{a(\xi)} \in \mathcal{A}$ tal que $\overline{a(\xi)} \notin \mathcal{A}^*$ y $\overline{a(\xi)} \in \overline{1} + \mathcal{M}$. Por consiguiente, existe $\overline{m(\xi)} \in \mathcal{M}$ tal que $\overline{a(\xi)} = \overline{1} + \overline{m(\xi)}$. Como $\overline{a(\xi)} \notin \mathcal{A} \setminus \mathcal{M}$, se tendrá que $\overline{a(\xi)} \in \mathcal{M}$. Entonces $\overline{a(\xi)} - \overline{m(\xi)} \in \mathcal{M}$. Por lo tanto, $\overline{1} \in \mathcal{M}$. Lo cual no es posible pues $\mathcal{M}$ es el ideal maximal de $\mathcal{A}$. Por otro lado, notemos que por la Observación 4.4 se cumple que $|\overline{1} + \mathcal{M}| = p^{m(k-1)}$.

Proposición 4.7. *El conjunto $\overline{1} + \mathcal{M}$ es un subgrupo del grupo de unidades del anillo $\mathcal{A}$.*

Demostración. Sean $\overline{a(\xi)}, \overline{b(\xi)} \in \overline{1} + \mathcal{M}$, entonces existen $\overline{m_1(\xi)}, \overline{m_2(\xi)} \in \mathcal{M}$ tales que $\overline{a(\xi)} = \overline{1} + \overline{m_1(\xi)}$ y $\overline{b(\xi)} = \overline{1} + \overline{m_2(\xi)}$.

i) $\overline{a(\xi)b(\xi)} = [\overline{1} + \overline{m_1(\xi)}][\overline{1} + \overline{m_2(\xi)}] = \overline{1} + \overline{m_1(\xi)} + \overline{m_2(\xi)} + \overline{m_1(\xi)m_2(\xi)} = \overline{1} + \overline{m_3(\xi)}$, donde $\overline{m_3(\xi)} = \overline{m_1(\xi)} + \overline{m_2(\xi)} + \overline{m_1(\xi)m_2(\xi)} \in \mathcal{M}$, pues $\mathcal{M}$ es un ideal en $\mathcal{A}$. Por lo que $\overline{a(\xi)b(\xi)} \in \overline{1} + \mathcal{M}$.

ii) Dado que $\overline{0} \in \mathcal{M}$ y $\overline{1} = \overline{1} + \overline{0}$, entonces $\overline{1} \in \overline{1} + \mathcal{M}$.

iii) Veamos que $(\overline{a(\xi)})^{-1} \in \overline{1} + \mathcal{M}$. Ya que $\overline{a(\xi)} \in \overline{1} + \mathcal{M} \subseteq \mathcal{A}^*$, entonces $(\overline{a(\xi)})^{-1} \in \mathcal{A}^*$. Además $\overline{a(\xi)}(\overline{a(\xi)})^{-1} = \overline{1}$. Sustituyendo $\overline{a(\xi)}$, se cumple que $\left[\overline{1} + \overline{m_1(\xi)}\right](\overline{a(\xi)})^{-1} = \overline{1}$. Distribuyendo el producto y despejando $(\overline{a(\xi)})^{-1}$ obtenemos que, $(\overline{a(\xi)})^{-1} = \overline{1} - \overline{m_1(\xi)}(\overline{a(\xi)})^{-1} = \overline{1} + \overline{m'(\xi)}$ con $\overline{m'(\xi)} = -\overline{m_1(\xi)}(\overline{a(\xi)})^{-1} \in \mathcal{M}$, pues $\overline{m_1(\xi)} \in \mathcal{M}$ y $\mathcal{M}$ es ideal. Así, $(\overline{a(\xi)})^{-1} = \overline{1} + \overline{m'(\xi)} \in \overline{1} + \mathcal{M}$.

□

EL resultado que a continuación se enuncia nos permite afirmar que existe un subgrupo de $\mathcal{A}^*$, dígamos H, de cardinalidad $p^m - 1$. Sin embargo omitimos su prueba, la cual puede consultarse en la referencia indicada.

Proposición 4.8. *[Roto3, Proposición 2.78,Pág. 90] Si G es un grupo finito abeliano y d es un divisor de $|G|$, entonces G contiene un subgrupo de orden d.*

Observación 4.5. *Sea H un subgrupo de $\mathcal{A}^*$ tal que $|H| = p^m - 1$. Tenemos que $\left[\overline{1} + \mathcal{M}\right] \cap H = \{\overline{1}\}$, ya que $\left[\overline{1} + \mathcal{M}\right]$ está formado por todos los elementos de $\mathcal{A}^*$ que tienen orden p^i con $0 \leqslant i \leqslant m(k-1)$. Si suponemos que existe $\overline{a(\xi)} \in \left[\overline{1} + \mathcal{M}\right] \cap H$ tal que $\overline{a(\xi)} \neq \overline{1}$ entonces, $\circ(\overline{a(\xi)}) = p^i$ para algún $i \in \{1, \ldots, m(k-1)\}$, es decir, $p | \circ(\overline{a(\xi)})$. Por otro lado, como $\overline{a(\xi)} \in H$, entonces $\circ(\overline{a(\xi)}) | |H|$, es decir, $\circ(\overline{a(\xi)}) | p^m - 1$. Luego $p | p^m - 1$. Aí que, existe $t \in \mathbb{Z}$ tal que $p^m - 1 = tp$. De ahí que $p|1$. Lo cual es una contradcción. Por lo que, en efecto, $\left[\overline{1} + \mathcal{M}\right] \cap H = \{\overline{1}\}$.*

Los siguientes resultados de la Teoría de Grupos nos permiten poder afirmar una serie de propiedades sobre $\mathcal{A}^*$. Las pruebas de estas proposiciones se omiten. Sin embargo sus demostraciones se pueden consultar en las citas correspondientes.

Proposición 4.9. *[Hun74, Cap. II, Proposición 4.8] Si H y K son subgrupos de un grupo G, entonces $[H : H \cap K] \leqslant [G : K]$. Si $[G : K]$ es finito, entonces $[H : H \cap K] = [G : K]$ si y sólo si $G = KH$.*

Proposición 4.10. *[Roto3, Proposición 2.80, pág. 91] Si G es un grupo que contiene subgrupos normales H y K con $H \cap K = \{1\}$ y $HK = G$, entonces $G \cong H \times K$.*

Sea H como en la Observación 4.5. Sabemos que $\left[\overline{1} + \mathcal{M}\right]$ y H son subgrupos de $\mathcal{A}^*$. Además $|\overline{1} + \mathcal{M}| = p^{m(k-1)}$, $|H| = p^m - 1$ y $|\mathcal{A}^*| = p^{m(k-1)}(p^m - 1)$. Entonces $[\mathcal{A}^* : \overline{1} + \mathcal{M}] = |\mathcal{A}^*|/|\overline{1} + \mathcal{M}| = p^m - 1$, es decir, $[\mathcal{A}^* : \overline{1} + \mathcal{M}]$ es finito. Dado que $H \cap [\overline{1} + \mathcal{M}] = \{\overline{1}\}$, se sigue que $[H : H \cap [\overline{1} + \mathcal{M}]] = |H| = p^m - 1$. Así, por la Proposicón 4.9, se tiene que

$$\mathcal{A}^* = \left[\overline{1} + \mathcal{M}\right] H. \tag{49}$$

Por la Proposición 4.10 tenemos que

$$\mathcal{A}^* \cong \left[\overline{1} + \mathcal{M}\right] \times H. \tag{50}$$

En [McD74] se prueba el siguiente resultado:

Teorema 4.1. *[McD74, Teorema XVIII.2, pág. 355]*

$$\mathcal{R}^* \cong \left[\overline{1} + \mathcal{M}\right] \times K^*.$$

Donde K^* denota del grupo mutiplicativo del campo residual del anillo R.

Así que

$$\mathcal{A}^* \cong \left[\overline{1} + \mathcal{M}\right] \times RF^*. \tag{51}$$

Dado que $\overline{1} + \mathcal{M}, H, RF^*$ son grupos abelianos finitos, entonces por el Teorema de Walker (c.f. [Wal56]) se cumple que $H \cong RF^*$. De ahí que H es un grupo cíclico.

Por lo tanto, $\mathcal{A}^*$ es el producto directo de dos grupos, $G_{PRC} = H$ y $G_{PRA} = \overline{1} + \mathcal{M}$, donde G_{PRC} es un grupo cíclico de orden $p^m - 1$ y G_{PRA} es un grupo abeliano de orden $p^{m(k-1)}$,

$$\mathcal{A}^* \cong G_{PRC} \times G_{PRA}.$$

Por lo anterior y (49), cualquier unidad del anillo $\mathcal{A}$ se puede escribir como el prodoucto de dos elementos, uno tomado de G_{PRC} y el otro de G_{PRA}. Es decir, sea $\overline{a(\xi)} \in \mathcal{A}^*$, entonces existen $\overline{b(\xi)} \in G_{PRC}$ y $\overline{c(\xi)} \in G_{PRA}$ tales que

$$\overline{a(\xi)} = \overline{b(\xi)c(\xi)}.$$

Lema 4.3. *El conjunto $F = G_{PRC} \cup \{\overline{0}\}$ es un campo.*

Demostración. Dado que G_{PRC} es un subgrupo de $\mathcal{A}^*$, entonces $(F^*, \cdot)$ es un grupo abeliano. Además, dado que $F \subseteq \mathcal{A}$ se cumple que para cada $\overline{f(\xi)} \in F$, $\overline{f(\xi)}\overline{0} = \overline{0}$. Resta probar que $(F, +)$ es un grupo

conmutativo. Para ello primero veamos que la suma es cerrada en F. Sean $\overline{a(\xi)}, \overline{b(\xi)} \in F$. Entonces $\overline{a(\xi)}, \overline{b(\xi)} \in \mathcal{A}$, el cual es un anillo de característica p. Por lo que

$$\begin{aligned} & \left(\overline{a(\xi)} + \overline{b(\xi)}\right)^p &=& \overline{a(\xi)}^p + \overline{b(\xi)}^p \\ \Rightarrow \quad & \left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^2} &=& \left[\overline{a(\xi)}^p + \overline{b(\xi)}^p\right]^p \\ & &=& \overline{a(\xi)}^{p^2} + \overline{b(\xi)}^{p^2}. \end{aligned}$$

Siguiendo de esta manera tenemos que

$$\left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m} = \overline{a(\xi)}^{p^m} + \overline{b(\xi)}^{p^m}.$$

Dado que $\overline{a(\xi)}, \overline{b(\xi)} \in F = G_{PRC} \cup \{\overline{0}\}$, se tiene que $\overline{a(\xi)}^{p^m} = \overline{a(\xi)}$ y $\overline{b(\xi)}^{p^m} = \overline{b(\xi)}$, pues $|G_{PRC}| = p^m - 1$ y $\overline{0}^{p^m} = \overline{0}$. Entonces

$$\begin{aligned} \overline{a(\xi)} + \overline{b(\xi)} &= \left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m} \\ \Rightarrow \quad \overline{0} &= \left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m} - \left(\overline{a(\xi)} + \overline{b(\xi)}\right) \\ \Rightarrow \quad \overline{0} &= \left[\overline{a(\xi)} + \overline{b(\xi)}\right]\left[\left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m-1} - \overline{1}\right]. \end{aligned}$$

Supongamos que $\overline{a(\xi)}+\overline{b(\xi)} \neq \overline{0}$ y $\left(\overline{a(\xi)}+\overline{b(\xi)}\right)^{p^m-1} - \overline{1} \neq \overline{0}$. Entonces $\overline{a(\xi)}+\overline{b(\xi)}$, $\left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m-1} - \overline{1} \in \mathcal{M}$, ya que $\mathcal{M} = \langle\overline{w(\xi)}\rangle$ contiene a todos los divisores de cero del anillo. Luego, por la Proposición 4.4 se tiene que, existen $\overline{u(\xi)}, \overline{v(\xi)} \in \mathcal{A}^*$ y $i_1, i_2 \in \{1, 2, \ldots, k-1\}$ tales que $\overline{a(\xi)} + \overline{b(\xi)} = \overline{w(\xi)}^{i_1}\overline{u(\xi)}$ y $\left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m-1} - \overline{1} = \overline{w(\xi)}^{i_2}\overline{v(\xi)}$. Entonces

$$\begin{aligned} \overline{w(\xi)}^{i_2}\overline{v(\xi)} &= \left[\overline{w(\xi)}^{i_1}\overline{u(\xi)}\right]^{p^m-1} - \overline{1}, \\ \Rightarrow \quad \overline{1} &= \left[\overline{w(\xi)}^{i_1}\overline{u(\xi)}\right]^{p^m-1} - \overline{w(\xi)}^{i_2}\overline{v(\xi)}, \\ \Rightarrow \quad \overline{1} &= \overline{w(\xi)}\left[\overline{w(\xi)}^{i_1(p^m-1)-1}\overline{u(\xi)}^{p^m-1} - \overline{w(\xi)}^{i_2-1}\overline{v(\xi)}\right]. \end{aligned}$$

De ahí que $\overline{w(\xi)}$ es una unidad en $\mathcal{A}$. Lo cual no es posible, pues $\overline{w(\xi)}$ es un divisor de cero. Por lo tanto, sólo ocurre uno de los siguientes casos: $(\overline{a(\xi)} + \overline{b(\xi)} = \overline{0}$ ó $\left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m-1} - \overline{1} = \overline{0}$.

Si ocurre el primero, es decir, $\overline{a(\xi)} + \overline{b(\xi)} = \overline{0}$, entonces $\overline{a(\xi)} + \overline{b(\xi)} \in F$. Lo cual queríamos probar. En caso de que ocurra el segundo, $\left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m-1} - \overline{1} = \overline{0}$, se tiene que

$$\begin{aligned} \overline{1} &= \left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m-1}, \\ \Rightarrow \quad \overline{1} &= \left(\overline{a(\xi)} + \overline{b(\xi)}\right)\left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m-2}, \\ \Rightarrow \quad \left(\overline{a(\xi)} + \overline{b(\xi)}\right) &\in \mathcal{A}^*. \end{aligned}$$

Entonces, existen $\overline{c(\xi)} \in G_{PRC}$ y $\overline{d(\xi)} \in G_{PRA}$ tales que

$$\overline{a(\xi)} + \overline{b(\xi)} = \overline{c(\xi)d(\xi)}. \tag{52}$$

Como $\overline{c(\xi)} \in G_{PRC}$, se tiene que $\overline{c(\xi)}^{p^m-1} = \overline{1}$ (pues $|G_{PRC}| = p^m - 1$). Luego

$$\begin{aligned} \overline{1} &= \left(\overline{a(\xi)} + \overline{b(\xi)}\right)^{p^m-1} \\ &= \left(\overline{c(\xi)d(\xi)}\right)^{p^m-1} \\ &= \overline{c(\xi)}^{p^m-1}\overline{d(\xi)}^{p^m-1} \\ &= \overline{d(\xi)}^{p^m-1}. \end{aligned}$$

De ahí que $\overline{1} = \overline{d(\xi)}^{p^m-1}$. Entonces $\circ(\overline{d(\xi)})$ divide a $p^m - 1$. Recordemos que $\overline{d(\xi)} \in G_{PRA}$ y $|G_{PRA}| = p^{m(k-1)}$. Así que $\circ(\overline{d(\xi)}) = p^i$ para algún $i \in \{0, 1, \ldots, m(k-1)\}$. Luego p^i divide a $p^m - 1$. Lo cual sólo ocurre cuando $i = 0$. Así que $\circ(\overline{d(\xi)}) = p^0 = 1$. Por lo que, $\overline{d(\xi)} = \overline{1}$. Entonces de (52) se sigue que $\overline{a(\xi)} + \overline{b(\xi)} = \overline{c(\xi)} \in G_{PRC} \subseteq F$. Por lo tanto la suma es cerrada en F. Ya que $F \subseteq \mathcal{A}$ se tiene que F es asociativo y conmutativo bajo la suma. Además se cumplen las propiedades de distributividad. Notemos que $\overline{0}$ es el neutro aditivo en F. Por lo que solo falta probar que para cada $\overline{f(\xi)} \in F$, su inverso aditivo, $-\overline{f(\xi)}$, se encuentra en F. Probemos la siguiente afirmación.

Afirmación. Para todo $p \in \mathbb{Z}$, con p primo, se cumple que $-\overline{1} \in G_{PRC}$.

En efecto, si $p = 2$, tenemos que $1 \equiv -1 \mod p$. Como $\overline{1} \in G_{PRC}$ entonces $-\overline{1} = \overline{-1} = \overline{1} \in G_{PRC} \subseteq F$. Si $p \neq 2$, se tiene que $p^m - 1$ es par para cada $m \in \mathbb{Z}$. Además, siempre se cumple que $\circ(-1) = 2$ en $GF(p)$. Más aún, cuando tomamos $\overline{-1} \in \mathcal{A}$, se tiene que $\circ(\overline{-1}) = 2$. Por otro lado, ya que $\overline{-1}$ es una unidad se sigue que, $\overline{-1} \in G_{PRC}$ ó $\overline{-1} \in G_{PRA}$. Si $\overline{-1} \in G_{PRA}$ entonces, $\circ(\overline{-1}) | p^{m(k-1)}$, donde $p^{m(k-1)} = |G_{PRA}|$. Lo cual no es posible pues $p^{m(k-1)}$ es impar. Así que $\overline{-1} \in G_{PRC}$. Sea $\overline{f(\xi)} \in F$, como $-\overline{1} \in G_{PRC} \subseteq F$, y F es cerrada bajo productos, se tiene que $-\overline{1}\overline{f(\xi)} = -\overline{f(\xi)} \in F$, donde $-\overline{f(\xi)}$ es tal que $-\overline{f(\xi)} + \overline{f(\xi)} = \overline{0}$. Por lo tanto, $(F, +)$ es un grupo conmutativo. Así que F es un campo. □

Observación 4.6. *Dado que* $F = G_{PRC} \cup \{\overline{0}\}$ *con* $G_{PRC} = H$ *y* $H \cap [\overline{1} + \mathcal{M}] = \{\overline{1}\}$ *(por Observación 4.5) entonces* $F \cap [\overline{1} + \mathcal{M}] = \{\overline{1}\}$ *pues además* H *y* $[\overline{1} + \mathcal{M}]$ *son subgrupos de* $\mathcal{A}^*$.

Notemos que el conjunto F es, además, un subanillo del anillo $\mathcal{A}$ y $|F| = p^m$, pues $F = G_{PRC} \cup \{\overline{0}\}$ y $|G_{PRC}| = p^m - 1$.

Corolario 4.2. $F \cong RF$.

Demostración. Recordemos que $RF = GF(p)[\xi]/(w(\xi))$, donde $w(\xi) \in GF(p)[\xi]$ es un polinomio mónico irreducible de grado m. Por lo que $RF \cong \mathbb{F}_{p^m}$. Como $|F| = p^m$, entonces $F \cong \mathbb{F}_{p^m}$. Así que $F \cong RF$. □

A continuación daremos otra representación del anillo $\mathcal{A}$ haciendo uso de su subanillo $F = G_{PRC} \cup \{\overline{0}\}$. El cual es también un subespacio de $\mathcal{A}$ sobre RF ya que $F \cong RF$ y RF es un RF− espacio vectorial. Así que F es un RF−subespacio vectorial de $\mathcal{A}$. Ya sabemos, por (45), que para cada $\overline{f(\xi)} \in \mathcal{A}$ existen $\lambda_0, \lambda_1, \ldots, \lambda_{k-1} \in RF$ tales que

$$\overline{f(\xi)} = \lambda_0\overline{1} + \lambda_1\overline{w(\xi)} + \cdots + \lambda_{k-1}\overline{w^{k-1}(\xi)}.$$

Dado que $F \cong RF$ entonces, para cada $\lambda_i \in RF$ podemos encontrar un único $\overline{a_i(\xi)} \in F$ tal que

$$\overline{f(\xi)} = \overline{a_0(\xi)}\overline{1} + \overline{a_1(\xi)w(\xi)} + \cdots + \overline{a_{k-1}(\xi)}\overline{w^{k-1}(\xi)}. \tag{53}$$

De manera más general podemos escribir a $\overline{f(\xi)}$ de la siguiente forma

$$\overline{f(\xi)} = F + \overline{w(\xi)}F + \cdots + \overline{w^{k-1}(\xi)}F. \tag{54}$$

A la representación (53) la denotaremos como la *representación base ideal*.

Ejemplo 4.1. *Sea* $w(\xi) = 1 + \xi + \xi^3 \in GF(2)[\xi]$, $w(\xi)$ *es un polinomio irreducible. Construimos el anillo de clases*

$$\mathcal{A} = \frac{GF(2)[\xi]}{(w^2(\xi))}.$$

Observemos que $w^2(\xi) = 1 + \xi^2 + \xi^6$. *Por lo que, se tienen las siguiente relaciones sobre* $GF(2)[\xi]$

$$\begin{aligned} \xi^2(1 + \xi^4) &\equiv 1 \quad \mod w^2(\xi) \\ 1 + \xi^2 &\equiv \xi^6 \quad \mod w^2(\xi). \end{aligned}$$

Sea $a(\xi) = \xi^2$. *Se puede observar que* $\overline{a(\xi)}$ *es una unidad en* $\mathcal{A}$. *Más aún,* $\circ(\overline{a(\xi)}) = 7$. *Por lo que,* $G_{PRC} = \{\overline{a(\xi)}, \ldots, \overline{a(\xi)}^7\}$. *Por otro lado, los divisores de cero en el anillo son de la forma* $\overline{w(\xi)a_u(\xi)}$, *donde* $\overline{a_u(\xi)} \in \mathcal{A}^*$, *esto por la Proposición 4.4. Dado que los divisores de cero son los elementos del maximal y* $|\mathcal{M}| = 8$ *se puede verificar que*

$$\mathcal{M} = \left\{\overline{0}, \overline{w(\xi)a(\xi)}, \ldots, \overline{w(\xi)a^7(\xi)}\right\}.$$

Ejemplo 4.2. *Consideramos el anillo* $\mathcal{A} = \dfrac{GF(2)[\xi]}{(w^2(\xi))}$, *donde* $w(\xi) = 1 + \xi + \xi^2 \in GF(2)[\xi]$ *es un polinomio irreducible. Mostraremos las tres representaciones que tienen los elementos del anillo* $\mathcal{A}$. *Primero notemos que* $w^2(\xi) = 1 + \xi^2 + \xi^4$. *Por lo que* $\mathcal{A} = \{\overline{a(\xi)} | a(\xi) \in GF(2)[\xi] \text{ y } grad(a(\xi)) < 4\}$. *De manera similar a como se trabajó en el Ejemplo 4.1 obtenemos que* $G_{PRC} = \{\overline{1}, \overline{\xi^2}, \overline{1+\xi^2}\}$. *Sea* $\delta = \overline{\xi^2}$, *notemos que* $\delta^2 = \overline{\xi^2+1}$ *y* $\delta^3 = \overline{1}$. *Así que* $F = \{\overline{0}, \overline{1}, \overline{\xi^2}, \overline{1+\xi^2}\}$. *Para fines prácticos, a los elementos del campo* F *los denotaremos sin la barra que denota a la clase. Por lo que,*

$$F = \{0, 1, \delta, \delta^2\}.$$

Por otro lado, tenemos que el campo residual de $\mathcal{A}$ *es*

$$RF = \{[0], [1], [\xi], [1+\xi]\}.$$

Para este ejemplo usaremos la notacion $[a]$ *para denotar a los elementos del* RF.

Sabemos que existe un isomorfismo entre F *y* RF, *dicho isomorfismo tiene la siguiente regla de correpondencia:* $\delta \longrightarrow [\xi + 1]$ *y* $\delta^2 \longrightarrow [\xi]$. *Notemos que este isomorfismo coincide con el que se crea cuando restringimos al homomorfismo sobreyectivo natural* $\mu\colon \mathcal{R} \longrightarrow RF$ *al conjunto* F.

En (40) tenemos la representación estándar, la cual está dada sobre el campo $GF(2)$ *respecto la base* $\mathcal{B}_1 = \{\overline{1}, \overline{\xi}, \overline{\xi^2}, \overline{\xi^3}\}$. *Es fácil obtener la respresentación de cada elemento de* $\mathcal{A}$. *Basta con fijarnos en los escalares que acompañan a las potencias de* ξ. *Por ejemplo, sea* $\overline{a(\xi)} = \overline{1 + \xi + \xi^2 + \xi^3}$, *tenemos que los representantes de* $\overline{a(\xi)}$ *son* $(1, 1, 1, 1)$, *así que escribiremos* $\overline{a(\xi)} = (1, 1, 1, 1)$.

La segunda representación se muestra en (45). Esta representación está dada respecto la base $\mathcal{B}_2 = \{\overline{1}, \overline{w(\xi)}\}$ *sobre* RF. *El algoritmo para obtener los representantes está dado en la prueba de la Proposición 4.5 y se ejemplificará para un elemento de* $\mathcal{A}$. *Sea* $\overline{a(\xi)} = \overline{1 + \xi + \xi^2 + \xi^3}$, *tenemos que* $a(\xi) \in GF(2)[\xi]$. *Aplicando el algoritmo de la división obtenemos* $q_0(\xi) = \xi, r_0(\xi) = 1 \in GF(2)[\xi]$ *tales que*

$$a(\xi) = q_0(\xi)w(\xi) + r_0(\xi) \text{ es decir } a(\xi) = r_0(\xi) + q_0(\xi)w(\xi).$$

Notemos que $[q_0(\xi)], [r_0(\xi)] \in RF$. *Por lo que, hemos obtenido una representación para* $\overline{a(\xi)}$ *y sus representantes son* $([r_0], [q_0]) = ([1], [\xi])$. *Haciendo abuso de notación diremos que* $\overline{a(\xi)} = ([1], [\xi])$.

La tercer representación de los elementos de $\mathcal{A}$ *está enunciada en (53). Esta representación al igual que la segunda, está dada respecto de la base* $\mathcal{B}_2$ *pero los represetantes son tomados en* $F \subset R$. *Para obtener la representación de los elementos de* $\mathcal{R}$ *primero encontraremos la representación de* $\overline{\xi}, \overline{\xi^2}$ *y* $\overline{\xi^3}$. *Notemos que las representaciones de* $\overline{0}$ *y* $\overline{1}$ *son* $(0, 0)$ *y* $(1, 0)$ *respectivamente. Para conseguir la representación de* $\overline{\xi}$ *haremos uso del isomorfismo que existe entre* F *y* RF, *el cual es igual a* $\mu|_F$. *Observemos que* $\mu(\overline{(\xi)}) = \xi + (w(\xi)) = [\xi]$. *Ya sabemos que existen únicos* $a, b \in F$ *tales que* $\overline{\xi} = a \cdot \overline{1} + b \cdot \overline{w(\xi)}$. *Entonces* $\mu(\overline{\xi}) = \mu(a \cdot \overline{1} + b \cdot \overline{w(\xi)}) = \mu(a)$, *es decir,* $[\xi] = \mu(a)$ *donde* $a \in F$. *Así que* $\mu(a) = \mu|_F(a)$. *Como* $\mu|_F$ *es un isomorfismo entre* F *y* RF *entonces existe el isomorfismo inverso, dígamos* $\lambda\colon RF \longrightarrow F$ *tal que* $\lambda([\xi]) = \overline{\delta^2}$. *Por lo que* $\delta^2 = a$. *Aí,* $\overline{\xi} = \delta^2 \cdot \overline{1} + b \cdot \overline{w(\xi)}$. *Luego,* $\overline{\xi} = \overline{1 + \xi^2} + b \cdot \overline{w(\xi)}$. *Por ende,* $\overline{\xi^2 + \xi + 1} = b \cdot \overline{w(\xi)}$, *es decir,* $\overline{w(\xi)} = b \cdot \overline{w(\xi)}$. *Entonces* $(\overline{1+b})\overline{w(\xi)} = \overline{0}$. *De ahí que* $\overline{1+b} = \overline{0}$ *ó* $\overline{1+b}$ *es un divisor de cero. En cualquier caso se cumple que* $\overline{1+b} \in \mathcal{M}$. *Por lo que, existe* $\overline{b_1} \in \mathcal{M}$ *tal que* $\overline{b} = \overline{1} + \overline{b_1}$, *esto implica que* $b \in [\overline{1} + \mathcal{M}]$, *además* $b \in F$, *donde* $F = G_{PRC} \cup \{\overline{0}\}$. *Por la Observación 4.6 se tiene que* $F \cap [\overline{1} + \mathcal{M}] = \{\overline{1}\}$. *Entonces* $b \in F \cap [\overline{1} + \mathcal{M}] = \{\overline{1}\}$. *Así* $b = 1$. *Por lo tanto*

$$\overline{\xi} = \delta^2 \cdot \overline{1} + 1 \cdot \overline{w(\xi)} = (\delta^2, 1).$$

La representación de $\overline{\xi^2}$ *se obtiene de manera simple pues recordemos que* $\delta = \overline{\xi^2} \in F$. *Así que*

$$\overline{\xi^2} = \delta \cdot \overline{1} + 0 \cdot \overline{w(\xi)} = (\delta, 0).$$

Para obtener la representación de $\overline{\xi^3}$ *notemos que* $\overline{\xi^3} = \overline{\xi\xi^2}$, *así que multplicando las representaciones de* $\overline{\xi}$ *y* $\overline{\xi^2}$, *obtenemos que* $\overline{\xi^3} = \delta^3 \cdot \overline{1} + \delta \cdot \overline{w(\xi)}$. *Como* $\delta^3 = 1$, *se tiene que:*

$$\overline{\xi^3} = 1 \cdot \overline{1} + \delta \cdot \overline{w(\xi)} = (1, \delta).$$

Las representaciones de los demás elementos de $\mathcal{R}$ *se obtienen sumando las representaciones de los que ya tenemos. Por ejemplo, sea* $\overline{a(\xi)} = \overline{1 + \xi + \xi^2 + \xi^3} \in \mathcal{R}$, *entonces*

ó bien

$$
\begin{aligned}
\overline{a(\xi)} = {} & 1 && \cdot\overline{1}+ && 0 && \cdot\overline{w(\xi)}+ \\
& \delta^2 && \cdot\overline{1}+ && 1 && \cdot\overline{w(\xi)}+ \\
& \delta && \cdot\overline{1}+ && 0 && \cdot\overline{w(\xi)}+ \\
& 1 && \cdot\overline{1}+ && \delta && \cdot\overline{w(\xi)} \\
= {} & (\delta+\delta^2) && \cdot\overline{1}+ && (1+\delta) && \cdot\overline{w(\xi)} \\
= {} & (\overline{\xi^2+1+\xi^2}) && \cdot\overline{1}+ && (\overline{1+\xi^2}) && \cdot\overline{w(\xi)} \\
\overline{a(\xi)} = {} & 1 && \cdot\overline{1}+ && \delta^2 && \cdot\overline{w(\xi)}
\end{aligned}
\qquad
\begin{aligned}
\overline{a(\xi)} = {} & (1,0)+ \\
& (\delta^2,1)+ \\
& (\delta,0)+ \\
& (1,\delta) \\
= {} & (\delta+\delta^2,1+\delta) \\
\overline{a(\xi)} = {} & (1,\delta^2).
\end{aligned}
$$

Este último procedimiento se puede llevar a cabo puesto que F *es un campo.*

En la siguiente tabla se enlistan los 16 elementos de $\mathcal{A}$ *con sus tres representaciones.*

Base :	$\left\{\overline{1},\overline{\xi},\overline{\xi^2},\overline{\xi^3}\right\}$	$\left\{\overline{1},\overline{w(\xi)}\right\}$	
Campo :	GF(2)	RF	F
Elementos de $\mathcal{A}$	Representaciones		
$\overline{0}$	$(0,0,0,0)$	([0] , [0])	(0 , 0)
$\overline{1}$	$(1,0,0,0)$	([1] , [0])	(1 , 0)
$\overline{\xi}$	$(0,1,0,0)$	([ξ] , [0])	(δ^2, 1)
$\overline{\xi^2}$	$(0,0,1,0)$	([1 + ξ], [1])	(δ , 0)
$\overline{\xi^3}$	$(0,0,0,1)$	([1] ,[1 + ξ])	(1 , δ)
$\overline{1+\xi}$	$(1,1,0,0)$	([1 + ξ], [0])	(δ , 1)
$\overline{1+\xi^2}$	$(1,0,1,0)$	([ξ] , [1])	(δ^2, 0)
$\overline{1+\xi^3}$	$(1,0,0,1)$	([0] ,[1 + ξ])	(0 , δ)
$\overline{\xi+\xi^2}$	$(0,1,1,0)$	([1] , [1])	(1 , 1)
$\overline{\xi+\xi^3}$	$(0,1,0,1)$	([1 + ξ],[1 + ξ])	(δ ,δ^2)
$\overline{\xi^2+\xi^3}$	$(0,0,1,1)$	([ξ] , [ξ])	(δ^2, δ)
$\overline{1+\xi+\xi^2}$	$(1,1,1,0)$	([0] , [1])	(0 , 1)
$\overline{1+\xi+\xi^3}$	$(1,1,0,1)$	([ξ] ,[1 + ξ])	(δ^2,δ^2)
$\overline{1+\xi^2+\xi^3}$	$(1,0,1,1)$	([1 + ξ], [ξ])	(δ , δ)
$\overline{\xi+\xi^2+\xi^3}$	$(0,1,1,1)$	([0] , [ξ])	(0 ,δ^2)
$\overline{1+\xi+\xi^2+\xi^3}$	$(1,1,1,1)$	([1] , [ξ])	(1 ,δ^2)

Tabla 2: Representaciones de los elementos de $\mathcal{A}$

Observación 4.7. *Obtener a través de estos procedimientos los representantes de los elementos del anillo* $\mathcal{A}$ *es posible gracias a las propiedades que este anillo posee. Sin embargo, para anillos diferentes a los abordados en este capítulo, encontrar las representaciones de sus elementos no siempre es una tarea fácil y se suele requerir del apoyo de algún software.*

4.3 EXTENSIONES DE GALOIS DEL ANILLO $\mathcal{A}$

En esta sección a los elementos del anillo $\mathcal{A}$ los denotaremos de la siguiente manera, $a := \overline{a(\xi)} \in \mathcal{A}$.

El método para construir anillos de Galois a partir del anillo $\mathcal{A}$ es similar a la construcción de anillos de Galois sobre $\mathbb{Z}_{p^k}$. Recordemos que existe un homomorfismo sobreyectivo natural que envía a los elementos del anillo $\mathcal{A}$ a su campo residual, RF, y dado que RF es isomorfo a F, el cual es un campo contenido en $\mathcal{A}$, entonces existe un homomorfismo sobreyectivo de $\mathcal{A}$ en F, dígamos μ, este homomorfismo se puede extender a la reducción polinomial $\hat{\mu}\colon \mathcal{A}[x] \to F[x]$ de la siguiente forma:

$$f(x) = \sum_{i=0}^{r} a_i x^i \xrightarrow{\hat{\mu}} \sum_{i=0}^{r} \mu(a_i) x^i.$$

Un polinomio $H(x) \in \mathcal{A}[x]$ es un *básico irreducible* si $\hat{\mu}(H(x))$ es irreducible en $F[x]$ y es *mónico* si su coeficiente principal es 1.

Definición 4.3. *El anillo de Galois de $\mathcal{A}$ denotado como $GR(\mathcal{A}, r)$ está definido como*

$$\frac{\mathcal{A}[x]}{(H(x))},$$

donde $H(x)$ es un polinomio mónico básico irreducible de grado r sobre $\mathcal{A}$.

El polinomio mónico básico irreducible de grado r sobre $\mathcal{A}$ se puede obtener de un polinomio mónico irreducible sobre RF, el cual es isomorfo a $GF(p^m)$, a través de un "levantamiento". El truco es considerar un polinomio mónico irreducible sobre F en lugar de tomarlo en RF. Como F es un subanillo de $\mathcal{A}$, cualquier polinomio irreducible sobre el subanillo es básico irreducible sobre el anillo. Así, el levantamiento se puede obtener definiendo una función φ de $GF(p^m)$ a F, la cual nos dará un polinomio mónico básico irreducible sobre $\mathcal{A}$ a partir de un polinomio mónico irreducible sobre $GF(p^m)$.

En el siguiente ejemplo se ilustra el procedimiento para obtener un polinomio básico irreducible a tráves de un "levantamiento".

Ejemplo 4.3. *Tomemos el anillo $\mathcal{A}$ que se abordó en el Ejemplo 4.2.*

$$\mathcal{A} = \frac{GF(2)[\xi]}{(w^2(\xi))}$$

donde $w(\xi) = 1 + \xi + \xi^2$, y recordemos que $F = \{0, 1, \xi^2, 1 + \xi^2\}$ es isomorfo a $GF(4) = \{0, 1, \beta, 1 + \beta\}$. El polinomio $f(x) = \beta + \beta^2 x + x^2 + x^3$ es irreducible sobre $GF(4)$ donde $\beta^3 = 1$ y $\beta^2 = 1 + \beta$. Definimos la función $\varphi : GF(4) \longrightarrow F$ donde $\beta \xrightarrow{\varphi} \xi^2$. Esta función aplicada a los coeficientes del poliomio $h(x)$ nos da el polinomio $H(x) = \xi^2 + (1 + \xi^2)x + x^2 + x^3$, el cual es un polinomio irreducible sobre F y básico irreducible sobre $\mathcal{A}$. Con el polinomio $H(x) \in \mathcal{A}[x]$ podemos construir el anillo de Galois

$$GR(\mathcal{A}, 3) = \frac{\mathcal{A}[x]}{(H(x))}.$$

4.4 LA LINEALIDAD DE LA FUNCIÓN DE GRAY

En el Capítulo 2 se habló de la función de Gray tomando anillos de Galois de índice de nilpotencia 2 (los cuales también son anillos finitos de cadena). En el se abordaron las propiedades más importantes de dicha función, entre ellas el hecho de que la función de Gray no es lineal sobre este tipo de anillos ($GR(p^2, m)$). Sin embargo cuando tomamos un anillo cociente de la forma $\mathcal{A} = GF(p)[\xi]/(w^2(\xi))$ con $w(\xi) \in GF(p)[\xi]$ irreducible (observemos que $\mathcal{A}$ es un caso particular de los anillos estudiados en este capítulo), la función de Gray definida sobre $\mathcal{A}^n$, con $n \in \mathbb{N}$, resulta ser lineal.

Ya sabemos que en los anillos de la forma $GF(p)[\xi]/(w^k(\xi))$ cada elemeto tiene tres representaciones diferentes, cada una de ellas sobre diferentes campos y bases, esto para cualquier p primo y k entero positivo. En particular, y para esta sección consideraremos $k = 2$. Así que nuestro anillo será

$$\mathcal{A} = \frac{GF(p)[\xi]}{(w^2(\xi))},$$

donde $w(\xi) \in GF(p)[\xi]$ es un polinomio mónico irreducible de grado m. A los elementos del anillo $\mathcal{A}$ los denotaremos de la siguiente manera: $a := \overline{a(\xi)} \in \mathcal{A}$. Por otro lado, a los elementos del campo F contenido en $\mathcal{A}$ los representaremos como a continuación se muestra: $F = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{p^m-2}\}$. Recordemos que F es isomorfo al campo residual del anillo $\mathcal{A}$, y cada elemento del anillo $\mathcal{A}$ tiene una única representación respecto a la base $\mathcal{B} = \{1, w\}$ sobre F. Es decir, para cada $a \in \mathcal{A}$ existen únicos $\rho_0(a), \rho_1(a) \in F$ tales que

$$a = \rho_0(a) + w\rho_1(a).$$

Observación 4.8. *i) Sean* $a, b \in \mathcal{A}$*, sabemos que existen únicos* $\rho_0(a), \rho_0(b), \rho_0(a+b), \rho_1(a), \rho_1(b), \rho_1(a+b) \in \mathsf{F}$ *tales que* $a = \rho_0(a) + w\rho_1(a)$*,* $b = \rho_0(b) + w\rho_1(b)$ *y* $a+b = \rho_0(a+b) + w\rho_1(a+b)$*, pero* $a + b = \rho_0(a) + \rho_0(b) + w(\rho_1(a) + \rho_1(b))$*, donde* $\rho_0(a) + \rho_0(b), \rho_1(a) + \rho_1(b) \in \mathsf{F}$ *y como* $\rho_0(a+b)$*, y* $\rho_1(a+b)$ *son únicos, entonces* $\rho_0(a+b) = \rho_0(a) + \rho_0(b)$ *y* $\rho_1(a+b) = \rho_1(a) + \rho_1(b)$*.*

ii) Sean $\beta \in \mathsf{F}$ *y* $a \in \mathcal{A}$*, notemos que la representación de* β *es* $\beta = \beta + w0$ *y como sabemos, existen* $\rho_0(a), \rho_0(\beta a), \rho_1(a), \rho_1(\beta a) \in \mathsf{F}$ *tales que* $a = \rho_0(a) + w\rho_1(a)$ *y* $\beta a = \rho_0(\beta a) + w\rho_1(\beta a)$*, pero* $\beta a = \beta\rho_0(a) + w\beta\rho_1(a)$ *donde* $\beta\rho_0(a), \beta\rho_1(a) \in \mathsf{F}$*. Por lo que,* $\rho_0(\beta a) = \beta\rho_0(a)$ *y* $\rho_1(\beta a) = \beta\rho_1(a)$*.*

Sea $n \in \mathbb{N}$, tomamos $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{A}^n$, sabemos que para cada $i = 0, 1, \ldots, n-1$ existen $\rho_0(a_i), \rho_1(a_i) \in \mathsf{F}$ únicos tales que $a_i = \rho_0(a_i) + w\rho_1(a_i)$. Tomando $\rho_j(\mathbf{A}) = (\rho_j(a_0), \rho_j(a_1), \ldots, \rho_j(a_{n-1}))$ para $j = 0, 1$, entonces $\mathbf{A} = \rho_0(\mathbf{A}) + w\rho_1(\mathbf{A}))$. Observemos que $\rho_0(\mathbf{A}), \rho_1(\mathbf{A}) \in \mathsf{F}^n$ son únicos ya que $\rho_0(a_i)$ y $\rho_1(a_i)$ son únicos para cada $i \in \{0, 1, \ldots, n-1\}$ y además las propiedades expuestas en la Observación 4.8 se pueden extender a $\mathcal{A}^n$, de manera que para cada $\mathbf{A}, \mathbf{B} \in \mathcal{A}^n$ y $\beta \in \mathsf{F}$ se cumplen:

i) $\rho_0(\mathbf{A} + \mathbf{B}) = \rho_0(\mathbf{A}) + \rho_0(\mathbf{B})$ y $\rho_1(\mathbf{A} + \mathbf{B}) = \rho_1(\mathbf{A}) + \rho_1(\mathbf{B})$

ii) $\rho_0(\beta\mathbf{A}) = \beta\rho_0(\mathbf{A})$ y $\rho_1(\beta\mathbf{A}) = \beta\rho_1(\mathbf{A})$

Para definir la fución de Gray sobre $\mathcal{R}^n$ donde $\mathcal{R} = \mathrm{GR}(p^2, m)$ (Capítulo 2), hicimos uso de la expasión p-ádica de los elementos del anillo $\mathcal{R}$ y del campo residual de dicho anillo. Sin embargo, para definir esta función sobre el anillo $\mathcal{A}$ usaremos la representación de los elementos respecto la base ideal sobre el campo F, además usaremos este campo en lugar del campo residual, lo cual es posible dado que son isomorfos. Sean $\mathbf{C_0} \in \mathsf{F}^q$ el vector que enlista a todos los elementos del campo F y $\mathbf{C_1} \in \mathsf{F}^q$ el vector cuyas entradas son todas iguales a 1, ambos de longitud $q = p^m$, definimos la *función de Gray* sobre $\mathcal{A}^n$ de la siguiente manera:

$$\begin{array}{rccl} \Phi\colon & \mathcal{A}^n & \longrightarrow & \mathsf{F}^{nq} \\ & \mathbf{A} & \longmapsto & \mathbf{C_0} \otimes \rho_0(\mathbf{A}) + \mathbf{C_1} \otimes \rho_1(\mathbf{A}) \end{array} \tag{55}$$

con $\mathbf{A} = (a_0, a_1, \ldots, a_{n-1}) \in \mathcal{A}^n$ y "$\otimes$" el producto de Kronecker definido como en (11), pero sobre $\mathcal{A}^n$. Observemos que las propiedades enunciadas en el Lema 2.1 también se satisfacen sobre $\mathcal{A}^n$.

Observación 4.9. $\mathcal{A}^n$ *y* F^n *son* F*— espacios vectoriales.*

Sean $\mathbf{A}, \mathbf{B} \in \mathcal{A}^n$ y $\beta \in \mathsf{F}$, sabemos que existen únicos $\rho_0(\mathbf{A}), \rho_1(\mathbf{A}), \rho_0(\mathbf{B}), \rho_1(\mathbf{B}) \in \mathsf{F}^n$ tales que $\mathbf{A} = \rho_0(\mathbf{A}) + w\rho_1(\mathbf{A}))$ y $\mathbf{B} = \rho_0(\mathbf{B}) + w\rho_1(\mathbf{B}))$. Entonces, por las propiedades el producto de Kronecker

$$\begin{aligned} \Phi(\mathbf{A} + \beta\mathbf{B}) &= \mathbf{C_0} \otimes \rho_0(\mathbf{A} + \beta\mathbf{B}) + \mathbf{C_1} \otimes \rho_1(\mathbf{A} + \beta\mathbf{B}) \\ &= \mathbf{C_0} \otimes (\rho_0(\mathbf{A}) + \beta\rho_0(\mathbf{B})) + \mathbf{C_1} \otimes (\rho_1(\mathbf{A}) + \beta\rho_1(\mathbf{B})) \\ &= (\mathbf{C_0} \otimes \rho_0(\mathbf{A})) + (\mathbf{C_0} \otimes \beta\rho_0(\mathbf{B})) + (\mathbf{C_1} \otimes \rho_1(\mathbf{A})) + (\mathbf{C_1} \otimes \beta\rho_1(\mathbf{B})) \\ &= (\mathbf{C_0} \otimes \rho_0(\mathbf{A}) + \mathbf{C_1} \otimes \rho_1(\mathbf{A})) + \beta(\mathbf{C_0} \otimes \rho_0(\mathbf{B})) + \beta(\mathbf{C_1} \otimes \rho_1(\mathbf{B})) \\ &= (\mathbf{C_0} \otimes \rho_0(\mathbf{A}) + \mathbf{C_1} \otimes \rho_1(\mathbf{A})) + \beta(\mathbf{C_0} \otimes \rho_0(\mathbf{B}) + \mathbf{C_1} \otimes \rho_1(\mathbf{B})) \\ &= \Phi(\mathbf{A}) + \beta\Phi(\mathbf{B}). \end{aligned}$$

Por lo que, la función de Gray definida sobre $\mathcal{A}^n$ es F—lineal.

De ahÃ que, si $\mathcal{C}$ es un $\mathcal{A}$—código cíclico lineal de longitud n, con n coprimo con la característica del campo residual F, entonces $\Phi(\mathcal{C})$ es un F—código lineal.

5 MAGMA

Magma es un software diseñado para realizar cálculos en álgebra, teoría de números, geometría algebraica y combinatoria (algebraica). Posee de un entorno matemático riguroso que permite al usuario definir y operar con estructuras comos lo son grupos, anillos, campos, códigos, módulos y muchas otras (c.f. [BCP97], [BCFS08]).

En este capítulo mostraremos algunos de los cálculos que se hicieron en MAGMA. Mostraremos los algoritmos que se implementaron. Además describiremos algunos que el software posee y que fueron de gran apoyo. A lo largo de este apartado encontraremos ejemplos de implementación de los comandos, los cuales estarán precedidos de por el símbolo >, y el resultado de su evaluación se mostrará dentro de un recuadro.

Si se desea saber más sobre algunas funciones empleadas se puede consultar el manual de usuario a través del siguiente link:

https://magma.maths.usyd.edu.au/magma/handbook/

Algunos de los ejemplos que se muestan en este capítulo se pueden realizar en la calculadora que MAGMA porporciona a través de su página. Dicha calculadora tiene un límite de operaciones pero puede ser un primer acercamiento al software. Se puede acceder a ella a través del siguiente enlace:

http://magma.maths.usyd.edu.au/calc/

5.1 ANILLOS DE GALOIS

MAGMA posee varias funciones que nos permiten construir anillos de Galois. Una de ellas es a partir de un número primo p y dos enteros positivos a y d, con los cuales se construye el anillo $GR(p^a, d)$ a través del comando "`GaloisRing(p,a,d)`". Sin embargo podemos sustituir a "`d`", por un polinomio"`f`" que es mónico sobre $\mathbb{Z}$ e irreducible módulo p. En este trabajo el comando que se usó fue "`GaloisRing(p,a,f)`", el cual construye el anillo de Galois $GR(p^a, m) = \mathbb{Z}_{p^a}[x]/\langle f(x)\rangle$, con $grad(f(x)) = m$. En el siguiente ejemplo se muestra como se usa este comando. Lo primero que hacemos es definir el anillo de polinomios $\mathbb{Z}[x]$, después damos un polinomio $f(x) \in \mathbb{Z}[x]$ tal que $f(x)$ es mónico y además es irreducible módulo p ($f(x)$ visto como un polinomio sobre $\mathbb{Z}_{p^a}$ es mónico básico irreducible).

Ejemplo 5.1.

```
> Z:=IntegerRing();
> PZ<x>:=PolynomialRing(Z);
> p:=3;
> a:=2;
> f:= x^3 + 2*x + 1;

> GR:=GaloisRing(p,a,f);
> GR;
```

```
GaloisRing(3, 2, x^3 + 2*x + 1)
```

Sin embargo, obtener polinomios con estas propiedades no es fácil, y MAGMA no posee una función que nos permita obtener polinomios mónicos básicos primitivos sobre un anillo $\mathbb{Z}/p^a\mathbb{Z}$. Lo que si tiene es una función que nos proporciona todos los polinomios irreducibles de grado d sobre un campo finito $F = \mathbb{F}_q$, la cual es "`AllIrreduciblePolynomials(F,d)`". Además, la función "`IsPrimitive(f)`" nos permite saber si el polinomio f, cuyos coeficientes están en un campo finito, es primitivo o no lo es. Ambas funciones se muestran en el siguiente ejemplo.

Ejemplo 5.2. *Primero obtendremos todos los polinomios irreducibles de grado* d *sobre el campo* $\mathbb{F}_p$.

```
> p:=3;
> a:=1;
> d:=3;
> GF<u>:=FiniteField(p^a);
> PGF<t>:=PolynomialRing(GF);

> AllIrreduciblePolynomials(GF,d);
```

```
{
   t^3 + 2*t + 1,
   t^3 + 2*t^2 + 2*t + 2,
   t^3 + t^2 + t + 2,
   t^3 + 2*t + 2,
   t^3 + t^2 + 2,
   t^3 + 2*t^2 + t + 1,
   t^3 + t^2 + 2*t + 1,
   t^3 + 2*t^2 + 1
}
```

Ahora veremos cuales de estos polinomios son primitivos.

```
> IsPrimitive( t^3 + 2*t + 1 );
> IsPrimitive( t^3 + 2*t^2 + 2*t + 2 );
> IsPrimitive( t^3 + t^2 + t + 2 );
> IsPrimitive( t^3 + 2*t + 2 );
> IsPrimitive( t^3 + t^2 + 2 );
> IsPrimitive( t^3 + 2*t^2 + t + 1 );
> IsPrimitive( t^3 + t^2 + 2*t + 1 );
> IsPrimitive( t^3 + 2*t^2 + 1 );
```

```
true
false
false
false
false
true
true
true
```

Por lo tanto los polinomios primitivos de grado 3 *sobre* $\mathbb{F}_3$ *son* $t^3 + 2t + 1$, $t^3 + 2t^2 + t + 1$, $t^3 + t^2 + 2t + 1$, $t^3 + 2t^2 + 1$.

Siguiendo el procedimiento del Ejemplo 5.2, podemos obtener todos los polinomios primitivos de grado d sobre el campo finito $\mathbb{F}_{p^a}$. Sin embargo, en la práctica puede resultar tedioso hacer este procedimiento, ya que cuando cambiamos los valores p, a y d, el número de polinomios irreducibles que obtenemos aumenta. Es por ello que con ayuda del lenguaje de programación que MAGMA posee

pudimos implementar una función que nos permitirá obtener de manera explícita todos los polinomios primitivos de grado d sobre un campo finito.

Algoritmo 1: Polinomios primitivos de grado d sobre un campo F

```
> AllPrimitivePolynomials:=function(F,d)
    PF<t>:=PolynomialRing(F);
    IP:=AllIrreduciblePolynomials(F,d);
    PrimitivePolynomials:={};
    for h in IP do
      if IsPrimitive(h) eq true then
        Include(~PrimitivePolynomials,h);
      end if;
    end for;
    return PrimitivePolynomials;
  end function;
```

Nota 5.1. *Este algoritmo debe de escribirse al principio de nuestra hoja de trabajo y únicamente en aquellas hojas donde sea requerido, como se muestra en el ejemplo.*

Ejemplo 5.3.

```
> AllPrimitivePolynomials:=function(F,d)
    PF<t>:=PolynomialRing(F);
    IP:=AllIrreduciblePolynomials(F,d);
    PrimitivePolynomials:={};
    for h in IP do
      if IsPrimitive(h) eq true then
        Include(~PrimitivePolynomials,h);
      end if;
    end for;
    return PrimitivePolynomials;
  end function;
> p:=3;
> a:=1;
> d:=3;
> GF<u>:=GaloisField(p^a);
> AllPrimitivePolynomials(GF,d);
```

```
{
   t^3 + 2*t + 1,
   t^3 + 2*t^2 + t + 1,
   t^3 + t^2 + 2*t + 1,
   t^3 + 2*t^2 + 1
}
```

Nota 5.2. *Si en el ejemplo anterior cambiamos los valores de* p, a *y* d *la función se ejecutará de manera adecuada.*

Con las funciones que tenemos podemos obtener todos los polinomios primitivos de cierto grado sobre un campo finito. Sin embargo, para la construcción de los anillos de Galois que usamos en esta tesis, fue necesario tener polinomios mónicos básicos primitivos sobre anillos de la forma $\mathbb{Z}/p^2\mathbb{Z}$, pues recordemos que trabajamos con anillos de Galois de índice de nilpotencia 2. Es por ello que la siguiente

función que implementamos en MAGMA nos da polinomios mónicos básicos primitivos con coeficientes sobre $\mathbb{Z}/p^2\mathbb{Z}$ de cierto grado.

Algoritmo 2: Polinomios básicos primitvos de grado d sobre un anillo $\mathbb{Z}_{p^2}$

```
> BasicPrimitivePolynomials:=function(p,d)
    PZ<x>:=PolynomialRing(IntegerRing());
    PZz<z>:=PolynomialRing(IntegerRing(p^2));
    BasicPrimitivePolynomials:={};
    for a in AllPrimitivePolynomials(GaloisField(p),d) do
      Include(~BasicPrimitivePolynomials, PZz!(PZ!a));
    end for;
    return BasicPrimitivePolynomials;
  end function;
```

Lo que hace esta función es obtener todos los polinomios primitivos sobre el campo residual del anillo $\mathbb{Z}/p^2\mathbb{Z}$, el cual es $\mathbb{F}_p$, y posteriormente los incrusta en el anillo $\mathbb{Z}/p^2\mathbb{Z}$, a través de la inclusión $\mathbb{F}_p[x] \hookrightarrow \mathbb{Z}_{p^2}[x]$. Observemos que el Algoritmo 2 depende del Algoritmo 1, por lo que cuando se desee usarlo será necesario escribir previamente el Algoritmo 1, tal como se muestra en el siguiente ejemplo.

Ejemplo 5.4.

```
> AllPrimitivePolynomials:=function(F,d)
    PF<t>:=PolynomialRing(F);
    IP:=AllIrreduciblePolynomials(F,d);
    PrimitivePolynomials:={};
    for h in IP do
      if IsPrimitive(h) eq true then
        Include(~PrimitivePolynomials,h);
      end if;
    end for;
    return PrimitivePolynomials;
  end function;
> BasicPrimitivePolynomials:=function(p,d)
    PZ<x>:=PolynomialRing(IntegerRing());
    PZz<z>:=PolynomialRing(IntegerRing(p^2));
    BasicPrimitivePolynomials:={};
    for a in AllPrimitivePolynomials(GaloisField(p),d) do
      Include(~BasicPrimitivePolynomials, PZz!(PZ!a));
    end for;
  return BasicPrimitivePolynomials;
  end function;
> p:=3;
> d:=3;
> BasicPrimitivePolynomials(p,d);
```

```
    {
       z^3 + 2*z + 1,
       z^3 + 2*z^2 + z + 1,
       z^3 + z^2 + 2*z + 1,
       z^3 + 2*z^2 + 1
    }
```

Nota 5.3. *Esta función (*BasicPrimitivePolynomials*) no nos proporciona todos los polinomios básicos primitivos sobre $\mathbb{Z}/p^2\mathbb{Z}$, sólo algunos de ellos.*

Una vez obtenidos algunos polinomios mónicos básicos primitivos podemos construir un anillo de Galois. No olvidemos que para poder construir un anillo de Galois en MAGMA es necesario que los coeficientes del polinomio que utilicemos estén sobre el anillo de los enteros. Para ello basta que usemos la función "`R!f`", la cual incrusta al elemento `f` en el anillo `R`, en nuestro caso `R` será el anillo $\mathbb{Z}[x]$ y `f` el polinomio que usaremos para construir nuestro anillo $GR(p^2, f)$.

Ejemplo 5.5.

```
> p:=3;
> PZz<z>:=PolynomialRing(IntegerRing(p^2));
> PZ<x>:=PolynomialRing(IntegerRing());
> f:=z^3 + 2*z + 1;
> PZ!f;
```

```
x^3 + 2*x + 1
```

Nota 5.4. *En adelante, en la mayoria de los ejemplos que se presenten en este capítulo sólo emplearemos la función que se acaba de mencionar sin escribir todo el algoritmo. Sin embargo, si se desea hacer uso de estas funciones es necseario escribirlas justo como se desarrollaron previamente (en los Algoritmos), así como se mostró en los Ejemplos 5.3 y 5.4.*

5.1.1 Representación p−ádica

Sabemos que los elementos de un anillo de Galois tienen su representación p−ádica, esta representación resulta importante en la implementación de la función de Gray. A pesar de que `MAGMA` no tiene una función que calcule esta representación, es posible implementarla. Para ello es necesario tener el conjunto de Teichmüller del anillo de Galois sobre el cual estamos trabajando, el cual lo obtendremos de la siguiente manera:

Algoritmo 3: Conjunto de Teichmüller

```
> Teichmuller:=function(R)
    RF<w>:=ResidueField(R);
    T:={R!a :a in RF};
    return T;
  end function;
```

Nota 5.5. `R` *puede ser cualquier anillo de Galois.*

Ejemplo 5.6.

```
> PZ<x>:=PolynomialRing(IntegerRing());
> Zf:=x^3 + 2*x + 1;
> p:=3;
> GR<u>:=GaloisRing(p^2,Zf);
> Teichmuller(GR);
```

```
{ 0, 2, u + 2, u^2 + 2, 2*u^2 + 2, 2*u + 2, u^2 + u + 1, 2*u^2 + u + 1, u^2 +
  2*u, 2*u^2 + 2*u, u^2 + u + 2, 2*u^2 + u + 2, u^2 + 2*u + 1, 2*u^2 + 2*u +
  1, u, 2*u, u^2 + 2*u + 2, u^2, 2*u^2 + 2*u + 2, 2*u^2, u + 1, 2*u + 1, u^2 +
  1, 2*u^2 + 1, u^2 + u, 2*u^2 + u, 1 }
```

La función para obtener las representaciones $p-$ádicas de los elementos de un anillo de Galois requerirá dos datos: el elemento del cual se desea obtener su repesentación, `a`, y el anillo al que pertenece, `R`. Es recomendable que este último sea citado previamente.

Algoritmo 4: Representación $p-$ádica

```
> pAdicRepresentation:=function(a,R)
    d:=Degree(R);
    p:=Characteristic(ResidueField(R));
     RF<w>:=ResidueField(R);
    T:={R!a :a in RF};
    for x,y in T do
      z:=x+p*y;
      if z eq a then
        r:=<x,y>;
      end if;
    end for;
    return r;
  end function;
```

La función nos dará una dupla formada por elementos del Teichmüller, cuyas entradas corresponden a los elementos que conforman la representación $p-$ádica de a.

Ejemplo 5.7.

```
> PZ<x>:=PolynomialRing(IntegerRing());
> Zf:=x^3 + 2*x + 1;
> p:=3;
> GR<u>:=GaloisRing(p^2,Zf);
> a:=8*u^2 + u;
> pAdicRepresentation(a,GR);
```

```
    <2*u^2 + u, 2*u^2>
```

Los dos valores que obtenemos son elementos del Teichmüller, y satisfacen la igualdad $a = 8u^2 + 4u + 6 + p(3u^2 + 8u + 1)$ *con* $p = 3$. *Ambas afirmaciones pueden comprobarse si en la misma hoja de trabajo colocamos lo siguiente:*

```
> Teichmuller:=function(R)
    RF<w>:=ResidueField(R);
    T:={R!a :a in RF};
    return T;
  end function;
> 2*u^2 + u in T;
> 2*u^2 in T;
> (2*u^2 + u) + p*(2*u^2);
```

```
    true
    true

    8*u^2 + u
```

Observación 5.1. *La función* `pAdicRepresentation` *sólo funciona para anillos de Galois de índice de nilpotencia 2.*

5.1.2 Campo Residual

Para obtener el campo residual de un anillo de Galois, MAGMA tiene una función que nos lo proporciona, "`ResidueField(R)`", donde `R` es el anillo del cual se desea obtener el campo residual. Además podemos construir el homomorfismo sobreyectivo canónico, $\mu : R \to RF$, con RF el campo residual de R, mediante el comando "`Coercion(D,C)`", donde `D` y `C` son el anillo R y su campo residual RF , respectivamente.

Ejemplo 5.8.

```
> PZ<x>:=PolynomialRing(IntegerRing());
> Zf:=x^3 + 2*x + 1;
> p:=3;
> GR<u>:=GaloisRing(p^2,Zf);
> RF<w>:=ResidueField(GR);
> Mu:=Coercion(GR,RF);
> Mu(1);
> Mu(u);
> Mu(8);
> Mu(7*u^2 + 8*u + 1);
```

```
1
w
2
w^18
```

Nota 5.6. MAGMA *nos proporciona a los elementos del campo como potencias del elemento primitivo, por lo que las imágenes de los elementos del anillo bajo la función* μ *siempre se verán como potencias del elemento primitivo del campo.*

5.1.3 Factorización

En MAGMA existe una función que nos permite factorizar polinomios con coeficientes sobre cierto tipo de anillos, dicha función es "`Factorization(f)`". Nos proporciona los polinomios que son factores de `f` y la multiplicidad de cada uno de ellos. La factorización que nos da está formada por polinomios mónicos irreducibles. Sin embargo, si deseamos emplear está función para polinomios sobre anillos de Galois no tendremos éxito. Es por ello que hemos implemetado una función que nos permitirá factorizar un polinomio sobre este tipo de anillos. Dicha función nos proporcionará una $n-$ada, cada entrada estará formada por una dupla donde el primer elemento será un factor de `g` y el segundo la multiplicidad de este, así que n corresponde al número de factores distintos que forman la factorización de g. Esta función sólo trabaja de manera adecuada con polinomios mónicos; si `g` no lo es, la función arrojará el mensaje "`El polinomio no es monico`".

Algoritmo 5: Factorización sobre Anillos de Galois

```
> FactorizationOverGR:=function(g,R)
    f:=g;
    PR<z>:=PolynomialRing(R);
    if LeadingCoefficient(f) eq 1 then
      d:=Degree(f);
      F:=[];
      repeat
        for i in [2..d] do
          h:=[Random(R): l in [1..i]];
          t:=PR!h;
          if t eq 0 then
            t:=0;
          else
            if LeadingCoefficient(t) eq 1 then
              r:=f mod t;
              if r eq 0 then
                if t eq 1 then
                  t:=1;
                else
                  Include(~F,t);
                  f:=ExactQuotient(f,t);
                end if;
              end if;
            end if;
          end if;
        end for;
      until f eq 1;
      MF:=[];
      h:=F[1];
      i:=2;
      repeat
        h:=h*F[i];
        i:=i+1;
      until i eq (#F+1);
      t:=ExactQuotient(g,h);
      i:=1;
      repeat
        m:=1;
        repeat
          if IsDivisibleBy(t,F[i]) eq true then
            t:=ExactQuotient(t,F[i]);
            m:=m+1;
          else
            m:=1;
          end if;
        until IsDivisibleBy(t,F[i]) eq false;
        M:=<F[i], m>;
        Include(~MF,M);
        i:=i+1;
      until i eq (#F+1);
    else
      T:="Ingrese un polinomio monico";
    end if;
    return MF;
  end function;
```

Nota 5.7. *La función mostrada en el Algoritmo 5 no nos proporciona una factorización única, ya que para poder hablar de la unicidad de esta se debe cumplir con las condiciones que propone el Teorema de Factorización Única para anillos de Galois, el cual nos dice que los factores deben ser polinomios mónicos primarios y coprimos por pares (c.f. [Wan03, Teorema 14.21]).*

Ejemplo 5.9.

```
> PZ<x>:=PolynomialRing(IntegerRing());
> Zf:=x^2 + x + 2;
> p:=3;
> GR<u>:=GaloisRing(p^2,Zf);
> PGR<z>:=PolynomialRing(GR);
> f:=z^5-1;
> FactorizationOverGR(f,GR);
```

```
[
  <z + 8, 1>,
  <z^2 + (4*u + 7)*z + 1, 1>,
  <z^2 + (5*u + 3)*z + 1, 1>
]
```

Ahora veremos como se comporta la función `FactorizationOverGR` *con un polinomio cuyo coeficiente principal es distinto de uno.*

```
> g:=(2*u)*z^3+(3*u+7)*z^2 +u*z+1;
> FactorizationOverGR(g,GR);
```

```
Ingrese un polinomio monico
```

A continuación se muestran las dos posibles factorizaciones que se pueden tener de un polinomio sobre el mismo anillo GR.

```
> h:=z^4+z^2;
> H1:=FactorizationOverGR(h,GR);
> H1;
```

```
[
  <z + 3*u + 6, 1>,
  <z + 5*u + 7, 1>,
  <z + 6*u + 3, 1>,
  <z + 4*u + 2, 1>
]
```

Al evaluar la función `FactorizationOverGR` *en el polinomio* h *y el anillo* GR *por segunda vez, la factorización que nos proporcionó fue la siguiente:*

```
> h:=z^4+z^2;
> H2:=FactorizationOverGR(h,GR);
> H2;
```

```
[
  <z + 4*u + 2, 1>,
  <z + 5*u + 7, 1>,
  <z, 2>
]
```

A pesar de que no sabemos si la factorización que nos proporciona la función `FactorizacionOverGR` es única bajo las condiciones debidas, en algunos casos podemos averiguarlo con los siguientes dos algoritmos. El primero nos permite saber si dado un conjunto de polinomios, sus elementos son coprimos por pares, de serlo la función nos dará el valor "`True`", en caso contrario la respuesta será "`False`".

Algoritmo 6: Polinomios coprimos sobre un Anillo de Galois

```
> AreCoprimesOverGR:=function(S,R)
    RF<w>:=ResidueField(R);
    PRF<t>:=PolynomialRing(RF);
    Si:="True";
    No:="False";
    H:=[];
    i:=1;
   repeat
      h:=PRF!S[i];
      Append(~H,h);
      i:=i+1;
    until i eq (#S +1);
    j:=1;
    repeat
      k:=j+1;
      repeat
        a:=GCD(H[j],H[k]) eq 1;
        if  a eq false then
          Coprimes:=No;
          break;
        else
          Coprimes:=Si;
        end if;
        k:=k+1;
      until k eq (#H+1);
      if Coprimes eq No then
        break;
      else
        j:=j+1;
      end if;
    until j eq #H;
    return  Coprimes;
  end function;
```

Nota 5.8. `S` *es un conjunto de polinomios introducido en un entorno de sucesión y* `R` *es el anillo de Galois sobre el cual se encuentran sus coeficientes.*

En el Ejemplo 5.9, obtuvimos dos factorizaciones distintas del polinomio $h(x) = z^4 + z^2$, en el siguiente ejemplo aplicaremos la función `AreCoprimesOverGR` a los polinomios de ambas factorizaciones. Recordemos que la función `FactorizationOverGR` nos proporciona $n-$adas, formadas por duplas, de

las cuales la primer entrada es un divisor de $h(x)$, es por eso que en el siguiente ejemplo primero agrupamos a los polinomios de la factorización en un entorno de sucesión.

Ejemplo 5.10.

```
> S:= [ w[1] : w in H1];
//S es el conjunto formado solo por los polinomios de H1
> S;
> AreCoprimesOverGR(S,GR);
```

```
[
  z + 3*u + 6,
  z + 5*u + 7,
  z + 6*u + 3,
  z + 4*u + 2
]

False
```

```
> T:= [ w[1] : w in H2];
//T es el conjunto formado solo por los polinomios de H2
> T;
> AreCoprimesOverGR(T,GR);
```

```
[
  z + 4*u + 2,
  z + 5*u + 7,
  z
]

True
```

Podemos ver que los elementos de la primer factorización no son coprimos por pares pero si lo son los de la segunda factorización.

La segunda función nos muestra cuando un polinomio es primario, si el polinomio cumple con las características que esta función verifica, entonces nos mostrará al polinomio acompañado con el mensaje "`True`". Sin embargo, el que un polinomio no cumpla con las propiedades que analiza el algoritmo no significa que no sea primario (c.f. [Wan03, Lema 14.18]), ya que el algoritmo carece de argumentos para poder afirmar cuando no lo es. Es por eso que en caso de que el polinomio no cumpla con las propiedades que analiza la función, esta nos mostrará al polinomio junto con el mensaje "`Indeterminate`".

Algoritmo 7: Polinomios Primarios

```
> IsPrimary:=function(f,R);
    PRF<t>:=PolynomialRing(ResidueField(R));
    h:=PRF!f;
    H:=Factorization(h);
    S:=[ w[1] : w in H];
    a:=#S eq 1;
    if a eq true then
      if IsIrreducible(S[1]) eq true then
        b:="True";
      else
        b:="Indeterminate" ;
      end if;
    else
      b:="Indeterminate";
    end if;
    return f,b;
  end function;
```

En el siguiente ejemplo a los polinomios de los conjuntos `S` y `T` del Ejemplo 5.10 les aplicaremos la función `IsPrimary`, recordando que dicha función requiere de dos argumentos, un polinomio y el anillo sobre el cual se encuentran sus coeficientes.

Ejemplo 5.11.

```
> for f in S do
    IsPrimary(f,GR);
  end  for;
```

```
z + 3*u + 6
True

z + 5*u + 7
True

z + 6*u + 3

True
z + 4*u + 2
True
```

```
> for f in T do
    IsPrimary(f,GR);
  end  for;
```

```
z + 4*u + 2
True

z + 5*u + 7
True

z
True
```

Es claro que los elementos de los dos conjuntos, S y T, son primarios.

Nota 5.9. *Los Ejemplos 5.10 y 5.11 son complementos del Ejemplo 5.9, y previo a usar las funciones* `IsPrimary` *y* `AreCoprimesOverGR` *es necesario que en la hoja de trabajo se escriban los algoritmos completos.*

Observación 5.2. *De los Ejemplos 5.9, 5.10 y 5.11 podemos deducir que la segunda factorización del polinomio* $h(z) = z^4 + z^2$ *que se proporcionó en el Ejemplo 5.9 es la factorización que cumple con las condiciones del Teorema de Factorización Única ([Wano3, Teorema 14.21]), pues los polinomios que la conforman son mónicos, primarios y coprimos por pares, por lo que es la única factorización que cumplirá estas características.*

5.2 FUNCIÓN DE GRAY

La función de Gray no está implementada en `MAGMA`, pero puede ser programada con ayuda de algunas funciones que existen y otras mas que se desarrollaron en la Sección 5.1

Es importante mencionar que la función de Gray y demás algoritmos que se muestran en esta sección fueron implementados primero para anillos de índice de nilpotencia 3 (c.f.[GR19, Apéndice B `MAGMA`]). Con base en los resultados que se muestran en [GR19] hemos podido implementar las funciones que a continuación se abordarán y se les ha dado una presentación un tanto distinta, de manera que puediese ser más fácil trabajar con ellas.

Recordemos que la función de Gray va del $\mathcal{R}$−módulo $\mathcal{R}^n$, al $\mathbb{F}_q$−espacio vectorial $\mathbb{F}_q^{qn}$, tal como se muestra en (14), y para poder implementarla necesitamos extender algunas funciones para anillos de Galois, vistas en la Sección 5.1, al $\mathcal{R}$−módulo $\mathcal{R}^n$. En particular la mostrada en el Algoritmo 4 y la función "`Coercion(GR,RF)`" que se mostró en el Ejemplo 5.8.

La función mostrada en el Algoritmo 4 calcula la representación p−ádica de cualquier elemento del anillo de Galois $\mathcal{R} = GR(p^2, m)$. Lo que necesitamos ahora es obtener "la representación p−ádica" de cualquier elemento del $\mathcal{R}$−módulo $\mathcal{R}^n$, es decir: sea $\mathbf{A} \in \mathcal{R}^n$ debemos encontrar dos n−adas del conjunto $\mathcal{T}^n$, $\rho_0(\mathbf{A}), \rho_1(\mathbf{A})$, con $\mathcal{T}$ el conjunto de Teichmüller del anillo $\mathcal{R}$, tales que $\mathbf{A} = \rho_0(\mathbf{A}) + p\rho_1(\mathbf{A})$. En el Capítulo 2 se menciona que $\rho_i(\mathbf{A}) = (\rho_i(a_0), \rho_i(a_1), \ldots, \rho_i(a_{n-1}))$ para $i = 0, 1$, por lo que podemos basarnos en el Algoritmo 4 para obtener las compenentes p−ádicas de $\mathbf{A}$.

Algoritmo 8: Extensión de la representación p−ádica

```
> pAdicRepresentationExtension:=function(A,R)
    d:=Degree(R);
    p:=Characteristic(ResidueField(R));
    T:={R!a :a in ResidueField(R)};
    P0:=[];
    P1:=[];
    i:=1;
    repeat
      for x,y in T do
        if (x+p*y) eq A[i] then
          Append(~P0,x);
          Append(~P1,y);
        end if;
      end for;
      i:=i+1;
    until i eq (#A+1);
    return <P0,P1>;
  end function;
```

En el siguiente ejemplo se omite el desarrollo de la función `pAdicRepresentationExtension`, escrito en el Algoritmo 8, pero en la practica es necesario escribirlo, prefrentemente antes de realizar los cálculo.

Ejemplo 5.12. *Construimos el anillo de Galois y tomamos un elemento de* GR^n *con* $n = 5$*, y a este elemento le aplicamos la función* `pAdicRepresentationExtension`.

```
> PZ<x>:=PolynomialRing(IntegerRing());
> p:=3;
> Zf:=x^2+x+2;
> GR<u>:=GaloisRing(p^2,Zf);
> A:=[ u + 5, 6*u + 6, u + 2, u + 7, 8*u + 1 ];
> pAdicRepresentationExtension(A,GR);
```

```
    <[ u + 2, 0, u + 2, u + 1, 2*u + 1 ], [ 1, 2*u + 2, 0, 2, 2*u ]>
```

El resultado es una dupla de n*—adas, las cuales son las componentes de la represenctación* p*—ádica de* $\mathbf{A}$*, así que* $\rho_0(\mathbf{A}) = (u+2, 0, u+2, u+1, 2u+1)$*,* $\rho_1(\mathbf{A}) = (1, 2u+2, 0, 2, 2u)$ *y* $\mathbf{A} = \rho_0(\mathbf{A}) + p\rho_1(\mathbf{A})$.

En la Sección 5.1 se mostró como obtener el campo residual de un anillo de Galois y como construir el homomorfismo canónico μ. En el siguiente Algoritmo se aplicará el homomorfismo μ a cada entrada del elemento `A`, el cual es una n—ada sobre el anillo de Galois `GR`.

Algoritmo 9: Extensión del homomorfismo μ

```
> MuGRModule:=function(A,R)
    RF<w>:=ResidueField(R);
    Mu:=Coercion(R,RF);
    MuA:=[];
    i:=1;
    repeat
      Append(~MuA,Mu(A[i]));
      i:=i+1;
    until i eq (#A+1);
    return MuA;
  end function;
```

Observación 5.3. *Como se mencionó antes,* `MAGMA` *proporciona a los elementos del campo residual como potencias del elemento primitivo, en este caso, asignamos a* `w` *como el elemento primitivo del campo residual.*

Ejemplo 5.13.

```
> PZ<x>:=PolynomialRing(IntegerRing());
> Zf:=x^2 + x + 2;
> p:=3;
> GR<u>:=GaloisRing(p^2,Zf);
> A:=[u + 5, 6*u + 6, u + 2, u + 7, 8*u + 1];
> MuGRModule(A,GR);
```

```
    [ w^6, 0, w^6, w^7, w^2 ]
```

La función de Gray involucra al Producto de Kronecker, nosotros en particular trabajamos con el produco de Kronecker extendido de derecha a izquierda, justo como se definió en (11), y nuestro software posee una función que realiza este producto. Dicha función es "`KroneckerProduct(A,B)`" donde `A` y `B` deben ser matrices, por ello, cuando se proporcione la función de Gray se podrán ver algunos elementos metidos en un ambiente de matrices.

Antes de proporcionar el Algoritmo de la función de Gray es importante recordar que haremos uso de la función "pAdicRepresentationExtension", mostrada en el Algoritmo 8, así que dicho algoritmo debe ser escrito antes de la función de Gray.

Algoritmo 10: Función de Gray

```
> GrayMap:=function(A,R)
       RF<w>:=ResidueField(R);
       q:=#RF;
       A:=Eltseq(A);
       n:=#A;
       F:=[s: s in RF];
       Exclude(~F,0);
       Exclude(~F,1);
       C:=[Matrix(RF,1,q,[0,1]cat[a:a in F]),Matrix(RF,1,q,[1 : i in [1..q]])];
       Rep:=pAdicRepresentationExtension(A,R);
       GM:=Matrix(RF,1,q*n,[0:i in [1..(q*n)]]);
       j:=1;
       repeat
         Rj:=Matrix(RF,[Rep[j]]);
         KP:=KroneckerProduct(C[j],Rj);
         GM:= GM+KP;
         j:=j+1;
       until j eq (#Rep+1);
       return Vector(q*n,Eltseq(GM));
     end function;
```

Observación 5.4. *Los vectores* $\mathbf{c_0}$ *y* $\mathbf{c_1}$ *están dados por los comandos* `Matrix(RF,1,q,[0,1]cat[w^a:a in [1..(q-2)]])` *y* `Matrix(RF,1,q,[1 : i in [1..q]])`*, respectivamente.*

Ejemplo 5.14.

```
> PZ<x>:=PolynomialRing(IntegerRing());
> Zf:=x^2 + x + 2;
> p:=3;
> GR<u>:=GaloisRing(p^2,Zf);
> A:=[u + 5, 6*u + 6, u + 2, u + 7, 8*u + 1];
> GrayMap(A,GR);
```

```
(w^2 w^3 w^5 w^6 1 0 w^3 2 w^5 w^3 2 w^3 1 w w^5 w^3 w^3 w^2 w^3 0 1 w^3 0 0 w^2
 w^6 w^3 w^7 1 w w w^3 w^6 w^7 w^6 w^5 w^3 w^3 2 2 w^7 w^3 w w^2 w^7)
```

Recordemos que la función de Gray va de $\mathcal{R}^n$ *a* $\mathbb{F}_q^{qn}$*. En nuestro ejemplo* $\mathcal{R} = \mathrm{GR}(3^2, 2)$ *y* $n = 5$*, así que el campo residual del anillo es* $\mathbb{F}_{3^2}$ *y por tanto la longitud de la imagen de los elemento de* $\mathcal{R}^5$ *es* 45*.*

5.2.1 Permutación de Nechaev

Se implementó la permutación de Nechaev para un estudio más completo de las imágenes de Gray de los códigos con los que trabajamos. En el siguiente algoritmo se proporciona la permutación de Nechaev sobre el conjunto $\{0, 1, \ldots, pn-1\}$, donde p es un primo y n es un entero positivo coprimo con

p. Además menciona cual es el inverso de n módulo p, el cual es necesario para obtener la permutación (Definición 2.3).

Algoritmo 11: Permutación de Nechaev

```
> NechaevPermutation:=procedure(p,n);
    if IsPrime(p) eq true then
      if GCD(p,n) eq 1 then
        //Calculo del inverso de n modulo p
        for k in [1..p-1] do
          y:=k*n mod p;
          if y eq 1 then
            q:=k mod p;
          end if;
        end for;
        "El inverso de",n,"modulo",p,"es n'=",q;

        "Permutacion de Nechaev en el conjunto {0,1,...,",n*p-1,"}";
        for x in [0..n*p-1] do
          for u in [0..p-1] do
            if x in [n*u..n*(u+1)-1] then
              x,"--->",(n*(q*x -u mod p)+x) mod (n*p);
            end if;
          end for;
        end for;
      else
        p," y",n,"no son coprimos";
      end if;
    else
      p,"no es primo";
    end if;
  end procedure;
```

El algoritmo nos muestra de manera ilustrativa la permutación de Nechaev y en caso de que p no sea primo ó n y p no sean coprimos nos lo mostrará.

Ejemplo 5.15.

```
> NechaevPermutation(3,2);
```

```
El inverso de 2 modulo 3 es n'= 2
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 5
2 ---> 2
3 ---> 1
4 ---> 4
5 ---> 3
```

A continuación se ingresa un valor de p *que no es primo.*

```
> NechaevPermutation(4,3);
```

```
4 no es primo
```

Ahora mostramos como trabaja la función cuando p *y* n *no son coprimos.*

```
> NechaevPermutation(3,6);
```

```
  3  y 6 no son coprimos
```

La función mostrada en el siguiente Algoritmo nos proporciona el valor de un entero x, con $x \in \{0, 1, \ldots, pn - 1\}$, bajo la permutación de Nechaev. Además, es necesario ingresar los parámetros p y n de la permutación.

Algoritmo 12: Función π (Permutación de Nechaev)

```
> Pi:=function(p,n,x)
    for k in [1..p-1] do
      if (k*n mod p) eq 1 then
        q:=k mod p;
      end if;
    end for;
    for u in [0..p-1] do
      if x in [n*u..n*(u+1)-1] then
        return (n*(q*x -u mod p)+x) mod (n*p);
      end if;
    end for;
  end function;
```

Nota 5.10. *A diferencia de la función* `NechaevPermutation`*, la que se menciona en el Algoritmo 12 no muestra si algún argumento es erróneo, pues eso haría que los procesos en los que se emplea esa función se vuelvan más lentos. Por ello se le pide al lector que sea cuidadoso con los argumentos que inserta, verificando que cumplan las características pertinentes.*

Ejemplo 5.16.

```
> Pi(3,2,1);
```

```
  5
```

Se puede comprobar, consultando el Ejemplo 5.15 que en efecto $\pi(1) = 5$.

En la Definición 2.3 se menciona a la permutación global de Nechaev y se define sobre $\mathbb{F}_q^{nq}$ con $q = p^m$. Con base en la definición obtendremos la permutación global de Nechaev para cualquier $nq-$ada, cuyos elementos no necesariamente deben estar en el campo $\mathbb{F}_q$.

Algoritmo 13: Permutación global de Nechaev, Π

```
> PI:=function(p,m,A);
    A:=Eltseq(A);
    n:=#A div (p^m);
    N:=[];
    k:=0;
    l:=(n*(p^m)) div (p^(m-1));
    while k lt p^(m-1) do
      c:=[A[(k*l+1)+Pi(p,n,j mod l)]: j in [k*l..((k+1)*l-1)]];
      Append(~N,c);
      k:=k+1;
    end while;
    return Vector(p^m*n,Eltseq(&cat N));
  end function;
```

Observación 5.5. *i) La función* `PI` *requiere de tres argumentos: los primero dos son enteros positivos* p *y* m*, con* p *primo, el tercero es un "vector" cuya longitud debe ser* np^m*, además* n *debe ser coprimo con* p*.*

ii) Antes de ingresar esta función es necesario escribir el Algoritmo 11 puesto que la función `Pi` *lo requiere.*

Ejemplo 5.17. *Recordemos que la permutación de Nechaev divide al "vector" en* $p^{(m-1)}$ *bloques de longitud* np *y aplica la permutación de Nechaev a la posición de cada entrada del bloque. Para ilustrar este proceso, nuestro elemento* `A` *será un vector en bloques cuyas entradas serán las mismas.*

```
> p:=3;
> m:=2;
> A:=[10,11,12,13,14,15,10,11,12,13,14,15,10,11,12,13,14,15];
> PI(p,m,A);
```

```
(10 15 12 11 14 13 10 15 12 11 14 13 10 15 12 11 14 13)
```

Como podemos ver, `PI` *realiza el mismo proceso en cada bloque, lo que hace es permutar las entradas del bloque mediante la función* `Pi`*. Hagamos el proceso de manera detenida: Tomemos la entrada* a_1 *de* A*, que es* 11*, lo que hace la función* `PI` *es calcular el valor de* `Pi(p,n,1)`*, en este caso* `Pi(p,n,1)=5`*, así que la entrada* a_5 *toma la posición de* a_1*, es decir en el lugar de* 11 *se coloca el* 15*, y dado que* `Pi(p,n,3)=1`*, entonces* 11 *toma el lugar de* 13*, este proceso se realiza en cada entrada y se repite en cada bloque.*

5.3 TEORÍA DE CÓDIGOS

En el apartado "Coding Theory" del manual de MAGMA, se pueden encontrar diversas funciones ya establecidas para la construcción de códigos sobre diferentes estructuras algebraicas, además de funciones que nos permiten saber propiedades de los mismos. En particular, dicho apartado tiene dos secciones que son de especial interés pues nos dan las herramientas para construir códigos sobre anillos de Galois y poder estudiar sus imágenes bajo la función de Gray, estas secciones son: "Linear Codes Over Finite Fields" y "Linear Codes Over Finite Rings".

A continuación se mostrarán la funciones mas relevantes para la construción y estudio de nuestros códigos.

Recordemos que nosotros trabajamos con códigos cíclicos lineales sobre anillos de Galois, así que la función que usaremos para construir estos códigos es "`CyclicCode(n,g)`", donde `n` es la longitud

del código y g es su polinomio generador. No obstante, si se revisa la sección "Linear Codes Over Finite Rings" del manual, se encontrarán otros comandos que nos permiten construir códigos lineales y cíclicos lineales.

Ejemplo 5.18. *Primero construimos el anillo de Galois,* $GR = (p^2, f)$*, sobre el cual vamos a trabajar. Además, damos la longitud del código,* $n \in \mathbb{N}$ *con* $(n, p) = 1$ *y proporcionamos un polinomio generador,* $g(z) \in GR[z]$*.*

```
> PZ<x>:=PolynomialRing(IntegerRing());
> Zf:=x^3 + x^2 + 1;
> p:=2;
> GR<u>:=GaloisRing(p^2,Zf);
> PGR<z>:=PolynomialRing(GR);
> g:=z^2+z+3;
> n:=3;
> C:=CyclicCode(n,g);
> C;
```

```
(3, 4096, 1) Cyclic Linear Code over GaloisRing(2, 2, x^3 + x^2 + 1)
Generator matrix:
[1 1 1]
[0 2 0]
[0 0 2]
```

Podemos ver que con la función `CyclicCode` *obtenemos el* $[3, 4096, 1]$*—código cíclico lineal* $\mathcal{C}$*, donde* 3 *es la longitud del código,* 4096 *su cardinalidad y* 1 *la distancia mínima de Hamming. Además nos proporciona la matriz generadora del código.*

Existe un comando que muestra si un código es cíclico, dicho comando es `IsCyclic(C)`, nos regresará el mensaje "`true`" si y sólo si, el código es cíclico.

En los ejemplos que se abordarán en la Sección 5.4 estudiaremos las imágenes bajo la función de Gray de algunos códigos cíclicos lineales sobre anillos de Galois. Nos enfocaremos en saber si sus imágenes son lineales y cíclicas. Las imágenes de la función de Gray estarán en un $\mathbb{F}$—espacio vectorial, donde $\mathbb{F}$ es isomorfo al campo residual del anillo de Galois. Con dichas imágenes construiremos un código lineal usando la función "`LinearCode<F,m |V>`", donde `F` es un campo, `m` es la longitud de las palabras-código, y `V` es un conjunto de vectores sobre `F`. Lo que esta función nos proporciona es un $[l, k, d]$—código lineal, donde `l` es la longitud de sus palabrabras-código, `k` la dimensión del código como subespacio vectorial de $\mathbb{F}^l$ y `d` es la distancia mínima de Hamming del código. El código que nos muestra es generado por los elementos del conjunto `V`. Está claro que `V` está contenido en dicho código y además, si la cardinalidad del código es igual a la del conjunto `V` entonces el conjunto `V` es el código lineal que se nos proporciona.

5.4 CÓDIGOS CÍCLICOS LINEALES Y SUS IMÁGENES DE GRAY

En está sección se exhibirán los códigos que fueron estudiados y con los cuales se descartó poder probar que las imágenes bajo la función de Gray de $\mathcal{R}$—códigos cíclicos lineales son cíclicas. En cada código se realizó el mismo proceso:

i) Escribir todos los Algoritmos que sean necesarios (Algoritmos 3,8, 9, 10,11,12,13).

ii) Generar el anillo de Galois, $\mathcal{R} = GR(p^2, m)$.

iii) Obtener el campo residual del anillo $RF = \mathbb{F}_{p^m}$.

iv) Construir los anillos de polinomios $\mathcal{R}[z]$ y $\mathbb{F}_{p^m}[t]$.

v) Obtener el conjunto de Teichmüller, $\mathcal{T}$, del anillo $\mathcal{R}$.

vi) Construir el código $\mathcal{C}$ de longitud n, con $(p, n) = 1$, a través del polinomio $G(z) = B(z) + p$, donde $B(z)$ es tal que $z^n - 1 = B(z)C(z)$ y $B(z)$ coprimo con $C(z)$.

vii) Aplicar la Función de Gray, Φ, a los elementos de $\mathcal{C}$, formando el conjunto $\Phi(\mathcal{C})$.

viii) Construir el código $\mathcal{E}$, $\mathbb{F}_{p^m}$−lineal de longitud np^m generado por los elemento de $\Phi(\mathcal{C})$.

ix) Verificar que el código $\mathcal{E}$ tenga la misma cardinalidad que $\Phi(\mathcal{C})$, de ser así, $\Phi(\mathcal{C}) = \mathcal{E}$ por lo que $\Phi(\mathcal{C})$ es lineal.

x) Evaluar la función `IsCyclic()` en el código $\mathcal{E}$ para saber si es cíclico.

xi) Aplicar la permutación global de Nechaev a los elementos del código $\mathcal{E}$.

xii) Repetir los pasos viii) al x) para saber si el conjunto $\Pi(\mathcal{E})$ es lineal y cíclico.

El polinomio que se requiere en ii) se obtuvo de manera previa con el Algoritmo 2, y el polinomio que se necesita para construir el código (vi)) surge de factorizar el polinomio $z^n - 1$, dicha factorización se realizó con el Algoritmo 5 previamente, por lo que no se muestran en el desarrollo de los códigos.

Código 1. *El anillo de Galois sobre el que construiremos este código es:* $\mathcal{R} = GR(5, 2, 1)$*, es decir,* $\mathcal{R} \cong \mathbb{Z}/5^2\mathbb{Z}$*. Observemos que* $\mathcal{R}$ *sigue siendo un anillo de Galois de índice de nilpotencia* 2*. Las imágenes de códigos cíclicos lineales sobre este tipo de anillos,* $\mathcal{R} = \mathbb{Z}/p^2\mathbb{Z}$*, ya han sido estudiadas por Sang Ling y J. T. Blackford. Ellos prueban que las imágenes de códigos cuyo generador es de la forma* $B(z) + p$ *son lineales (c.f [LBo2, Teorema 4.13]), por lo que para el* $[3, 3125, 1]$*−código cíclico lineal su imagen bajo la función de Gray es cíclica lineal. Sin embargo este código se construyo para comprobar que las funciones implementadas en el software, como la Función de Gray y la permutación de Nechaev, trabajan de manera adecuada.*

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller
> Teichmuller:=function(R)
    RF<w>:=ResidueField(R);
    T:={R!a :a in RF};
    return T;
  end function;
```

```
//Extension de la representacion p-adica de n-adas
> pAdicRepresentationExtension:=function(A,R)
    d:=Degree(R);
    p:=Characteristic(ResidueField(R));
    T:={R!a :a in ResidueField(R)};
    P0:=[];
    P1:=[];
    i:=1;
    repeat
      for x,y in T do
        if (x+p*y) eq A[i] then
          Append(~P0,x);
          Append(~P1,y);
        end if;
      end for;
      i:=i+1;
    until i eq (#A+1);
    return <P0,P1>;
  end function;
```

```
//Funcion de Gray
> GrayMap:=function(A,R)
    RF<w>:=ResidueField(R);
    q:=#RF;
    A:=Eltseq(A);
    n:=#A;
    F:=[s: s in RF];
    Exclude(~F,0);
    Exclude(~F,1);
    C:=[Matrix(RF,1,q,[0,1]cat[a:a in F]),Matrix(RF,1,q,[1 : i in [1..q]])];
    Rep:=pAdicRepresentationExtension(A,R);
    GM:=Matrix(RF,1,q*n,[0:i in [1..(q*n)]]);
    j:=1;
    repeat
      Rj:=Matrix(RF,[Rep[j]]);
      KP:=KroneckerProduct(C[j],Rj);
      GM:= GM+KP;
      j:=j+1;
    until j eq (#Rep+1);
    return Vector(q*n,Eltseq(GM));
  end function;
```

```
//Permutacion de Nechaev
> NechaevPermutation:=procedure(p,n);
    if IsPrime(p) eq true then
      if GCD(p,n) eq 1 then
        //Calculo del inverso de n modulo p
        for k in [1..p-1] do
          y:=k*n mod p;
          if y eq 1 then
            q:=k mod p;
          end if;
        end for;
        "El inverso de",n,"modulo",p,"es n'=",q;
        "Permutacion de Nechaev en el conjunto {0,1,...,",n*p-1,"}";
        for x in [0..n*p-1] do
          for u in [0..p-1] do
            if x in [n*u..n*(u+1)-1] then
              x,"--->",(n*(q*x -u mod p)+x) mod (n*p);
            end if;
          end for;
        end for;
      else
        p," y",n,"no son coprimos";
      end if;
    else
      p,"no es primo";
    end if;
  end procedure;
```

```
//Funcion Pi de la permutacion de Nechaev
> Pi:=function(p,n,x)
    for k in [1..p-1] do
```

```
      if (k*n mod p) eq 1 then
        q:=k mod p;
      end if;
    end for;
    for u in [0..p-1] do
      if x in [n*u..n*(u+1)-1] then
        return (n*(q*x -u mod p)+x) mod (n*p);
      end if;
    end for;
  end function;
```

```
//Permutacion global de Nechaev
> PI:=function(p,m,A);
    A:=Eltseq(A);
    n:=#A div (p^m);
    N:=[];
    k:=0;
    l:=(n*(p^m)) div (p^(m-1));
    while k lt p^(m-1) do
      c:=[A[(k*l+1)+Pi(p,n,j mod l)]: j in [k*l..((k+1)*l-1)]];
      Append(~N,c);
      k:=k+1;
    end while;
    return Vector(p^m*n,Eltseq(&cat N));
  end function;
```

---

ii) Construcción del anillo $\mathcal{R} = \mathrm{GR}(5, 2, 1)$.

```
//Anillo de Galois

> P<x>:=PolynomialRing(IntegerRing());
> p:=5;
> m:=1;
> GR<u>:=GaloisRing(p,2,m);
> GR;
```

```
GaloisRing(5, 2, 1)
```

iii) Construcción del campo residual.

```
//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;
```

```
Finite field of size 5
```

iv) Construcción de los anillos de polinomios.

```
//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;
```

```
Univariate Polynomial Ring in z over GaloisRing(5, 2, 1)

Univariate Polynomial Ring in t over GF(5)
```

v) Construcción del conjunto de Teichmüller.

```
//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
Conjunto de Teichmuller: { 0, 1, 2, 3, 4 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Construccion del codigo C de longitud n

> B:=z-1;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo: G(z)= z + 4

Longitud del codigo: n= 3

(3, 3125, 1) Cyclic Linear Code over GaloisRing(5, 2, 1)
Generator matrix:
[1 0 4]
[0 1 4]
[0 0 5]
```

vii) Aplicación de la función de Gray a los elementos del código $\mathcal{C}$.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];
```

viii) y ix) Construcción del código generado por las imágenes de Gray del código $\mathcal{C}$.

```
//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;
```

```
[15, 5, 5] Cyclic Linear Code over GF(5)
Generator matrix:
[1 0 0 0 0 1 4 0 2 3 0 3 2 0 4]
[0 1 0 0 0 1 0 4 2 0 3 3 0 2 4]
[0 0 1 0 0 1 0 0 1 0 0 1 0 0 1]
[0 0 0 1 0 4 2 0 3 3 0 2 4 0 1]
[0 0 0 0 1 4 0 2 3 0 3 2 0 4 1]

true

true
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. De ahí que $\Phi(\mathcal{C})$ es un código lineal, más aún, $\Phi(\mathcal{C})$ es cíclico.

El inciso x) se omite, ya que al generar el código $\mathcal{E}$ con los elementos de $\Phi(\mathcal{C})$, MAGMA nos muestra las características de dicho código, entre ellas que el código es lineal.

Calculamos la permutación de Nechaev en los parámetros $p = 5$ y $n = 3$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 5 es n'= 2
Permutacion de Nechaev en el conjunto {0,1,..., 14 }
0 ---> 0
1 ---> 7
2 ---> 14
3 ---> 3
4 ---> 10
5 ---> 2
6 ---> 6
7 ---> 13
8 ---> 5
9 ---> 9
10 ---> 1
11 ---> 8
12 ---> 12
13 ---> 4
14 ---> 11
```

xi) Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$–lineal $\mathcal{E}$ y repetimos los pasos viii) y ix) para el conjunto $\Pi(\mathcal{E})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE
```

```
[15, 5, 5] Cyclic Linear Code over GF(5)
Generator matrix:
[1 0 0 0 0 1 4 0 2 3 0 3 2 0 4]
[0 1 0 0 0 1 0 4 2 0 3 3 0 2 4]
[0 0 1 0 0 1 0 0 1 0 0 1 0 0 1]
[0 0 0 1 0 4 2 0 3 3 0 2 4 0 1]
[0 0 0 0 1 4 0 2 3 0 3 2 0 4 1]

true

true
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$, $\mathcal{H}$, está contenido en el conjunto $\Pi(\mathcal{E})$, por lo que $\Pi(\mathcal{E})$ es un código lineal. De manera análoga a como se mostró en los incisos viii) y ix) para el código $\mathcal{E}$, tenemos que $\mathcal{H} = \Pi(\mathcal{E})$ es un código cíclico, por lo que no es necesario realizar el inciso x).

Conclusión. *El conjunto de las imágenes de Gray del $[3, 3125, 1]$—código cíclico lineal forman un $[15, 5, 5]$—código cíclico lineal de longitud 15, tal como debía ser.*

Código 2. *Este código se costruyó con el mismo propósito que el Código 1, mostrar que las funciones implementadas en MAGMA trabajan de manera adecuada.*

El anillo de Galois sobre el que construiremos este código es: $\mathcal{R} = \mathrm{GR}(5, 2, 1)$, es decir, $\mathcal{R} \cong \mathbb{Z}/5^2\mathbb{Z}$, por lo que para el $[3, 625, 1]$—código cíclico lineal su imagen bajo la función de Gray es cíclica lineal.

En este código se omite el desarrollo de los Algoritmos 3, 8, 10, 11, 12, y 13, sólo se comentarán las funciones donde deben ir desarrolladas, sin embargo, en la práctica es necesario escribir los algoritmos completos.

Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas

//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

Construcción del anillo $\mathcal{R} = \mathrm{GR}(5,2,1)$ y de su campo residual.

```
//Anillo de Galois

> P<x>:=PolynomialRing(IntegerRing());
> p:=5;
> m:=1;
> GR<u>:=GaloisRing(p,2,m);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;
```

```
   GaloisRing(5, 2, 1)

   Finite field of size 5
```

Construcción de los anillos de polinomios y obetención del conjunto de Teichmuüller.

```
//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
Univariate Polynomial Ring in z over GaloisRing(5, 2, 1)

Univariate Polynomial Ring in t over GF(5)

Conjunto de Teichmuller: { 0, 1, 2, 3, 4 }
```

Construcción del código $\mathcal{C}$.

```
//Construccion del codigo C de longitud n

> B:=z^2+z+1;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo G(z)= z^2 + z + 6

Longitud del codigo n= 3

(3, 625, 1) Cyclic Linear Code over GaloisRing(5, 2, 1)
Generator matrix:
[1 1 1]
[0 5 0]
[0 0 5]
```

Evaluación de la función de Gray en los elementos del código $\mathcal{C}$ y obtención del código generado por las imágenes.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;
```

```
[15, 4, 5] Cyclic Linear Code over GF(5)
Generator matrix:
[1 0 0 0 4 4 4 3 3 3 2 2 2 1 1]
[0 1 0 0 1 0 0 1 0 0 1 0 0 1 0]
[0 0 1 0 0 1 0 0 1 0 0 1 0 0 1]
[0 0 0 1 1 1 2 2 2 3 3 3 4 4 4]

true

true
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. Además el código $\mathcal{E}$ es cíclico.

Calculamos la permutación de Nechaev en los parámetros $p = 5$ y $n = 3$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 5 es n'= 2
Permutacion de Nechaev en el conjunto {0,1,..., 14 }
0 ---> 0
1 ---> 7
2 ---> 14
3 ---> 3
4 ---> 10
5 ---> 2
6 ---> 6
7 ---> 13
8 ---> 5
9 ---> 9
10 ---> 1
11 ---> 8
12 ---> 12
13 ---> 4
14 ---> 11
```

Aplicación de la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$−lineal $\mathcal{E}$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE
```

```
[15, 4, 5] Cyclic Linear Code over GF(5)
Generator matrix:
[1 0 0 0 4 4 4 3 3 3 2 2 2 1 1]
[0 1 0 0 1 0 0 1 0 0 1 0 0 1 0]
[0 0 1 0 0 1 0 0 1 0 0 1 0 0 1]
[0 0 0 1 1 1 2 2 2 3 3 3 4 4 4]

true

true
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$, $\mathcal{H}$, está contenido en el conjunto $\Pi(\mathcal{E})$, por lo que $\Pi(\mathcal{E})$ es un código lineal. además se muestra que $\mathcal{H} = \Pi(\mathcal{E})$ es un código cíclico.

Conclusión. *El conjunto de las imágenes de Gray del $[3, 625, 1]$−código cíclico lineal forman un $[15, 4, 5]$−código cíclico lineal de longitud 15, tal como debía ser.*

A partir de este punto, los códigos que se presentan son sobre anillos de Galois de la forma $GR = (p, 2, f)$, con f un polinomio mónico básico primitivo tal que $grad(f) = m \geqslant 2$.

En los códigos siguientes realizaremos un calculo más, ya que fue importante para poder esclarecer la Proposición 3.1, la cual afirma que el ideal $\langle p + I \rangle \subset \langle B(z) + p + I \rangle$. Lo que haremos será preguntar al software si la $n-$ada $P = (p, 0, 0, \ldots, 0)$ es un elemento del código. De ser así, cuando pasamos todo al anillo de clases polinomiales $\mathcal{R}_n$ tendremos que la clase polinomial $p + I$ es un elemento del ideal $\langle B(z) + p + I \rangle$ y por lo tanto la Proposición 3.1 se cumple.

Código 3. *Construcción del* $[3, 256, 1]-$*código cíclico lineal con polinomio generador* $G(z) = z^2 + z + 3$*, sobre el anillo* $\mathcal{R} = GR(2, 2, 2)$.

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller
> Teichmuller:=function(R)
    RF<w>:=ResidueField(R);
    T:={R!a :a in RF};
    return T;
  end function;
```

```
//Extension de la representacion p-adica de n-adas
> pAdicRepresentationExtension:=function(A,R)
    d:=Degree(R);
    p:=Characteristic(ResidueField(R));
    T:={R!a :a in ResidueField(R)};
    P0:=[];
    P1:=[];
    i:=1;
    repeat
      for x,y in T do
        if (x+p*y) eq A[i] then
          Append(~P0,x);
          Append(~P1,y);
        end if;
      end for;
      i:=i+1;
    until i eq (#A+1);
    return <P0,P1>;
  end function;
```

```
//Funcion de Gray
> GrayMap:=function(A,R)
    RF<w>:=ResidueField(R);
    q:=#RF;
    A:=Eltseq(A);
    n:=#A;
    F:=[s: s in RF];
    Exclude(~F,0);
    Exclude(~F,1);
    C:=[Matrix(RF,1,q,[0,1]cat[a:a in F]),Matrix(RF,1,q,[1 : i in [1..q]])];
    Rep:=pAdicRepresentationExtension(A,R);
    GM:=Matrix(RF,1,q*n,[0:i in [1..(q*n)]]);
    j:=1;
    repeat
```

```
      Rj:=Matrix(RF,[Rep[j]]);
      KP:=KroneckerProduct(C[j],Rj);
      GM:= GM+KP;
      j:=j+1;
    until j eq (#Rep+1);
    return Vector(q*n,Eltseq(GM));
  end function;
```

```
//Permutacion de Nechaev
> NechaevPermutation:=procedure(p,n);
    if IsPrime(p) eq true then
      if GCD(p,n) eq 1 then
        //Calculo del inverso de n modulo p
        for k in [1..p-1] do
          y:=k*n mod p;
          if y eq 1 then
            q:=k mod p;
          end if;
        end for;
        "El inverso de",n,"modulo",p,"es n'=",q;
        "Permutacion de Nechaev en el conjunto {0,1,...,",n*p-1,"}";
        for x in [0..n*p-1] do
          for u in [0..p-1] do
            if x in [n*u..n*(u+1)-1] then
              x,"--->",(n*(q*x -u mod p)+x) mod (n*p);
            end if;
          end for;
        end for;
      else
        p," y",n,"no son coprimos";
      end if;
    else
      p,"no es primo";
    end if;
  end procedure;
```

```
//Funcion Pi de la permutacion de Nechaev
> Pi:=function(p,n,x)
    for k in [1..p-1] do
      if (k*n mod p) eq 1 then
        q:=k mod p;
      end if;
    end for;
    for u in [0..p-1] do
      if x in [n*u..n*(u+1)-1] then
        return (n*(q*x -u mod p)+x) mod (n*p);
      end if;
    end for;
  end function;
```

```
//Permutacion global de Nechaev
> PI:=function(p,m,A);
    A:=Eltseq(A);
```

```
    n:=#A div (p^m);
    N:=[];
    k:=0;
    l:=(n*(p^m)) div (p^(m-1));
    while k lt p^(m-1) do
      c:=[A[(k*l+1)+Pi(p,n,j mod l)]: j in [k*l..((k+1)*l-1)]];
      Append(~N,c);
      k:=k+1;
    end while;
    return Vector(p^m*n,Eltseq(&cat N));
  end function;
```

ii) Construcción del anillo $\mathcal{R} = \mathrm{GR}(2,2,2)$.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
> p:=2;
> Zf:=x^2+x+1;
> m:=2;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;
```

```
GaloisRing(2, 2, x^2 + x + 1)
```

iii) Construcción del campo residual.

```
//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;
```

```
Finite field of size 2^2
```

iv) Construcción de los anillos de polinomios.

```
//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;
```

```
Univariate Polynomial Ring in z over GaloisRing(2, 2, x^2 + x + 1)

Univariate Polynomial Ring in t over GF(2^2)
```

v) Construcción del conjunto de Teichmüller.

```
//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
    Conjunto de Teichmuller: { 0, 1, u, u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z^2+z+1;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
    Polinomio generador del codigo: G(z)= z^2 + z + 3

    Longitud del codigo: n= 3

    (3, 256, 1) Cyclic Linear Code over GaloisRing(2, 2, x^2 + x + 1)
    Generator matrix:
    [1 1 1]
    [0 2 0]
    [0 0 2]
```

vii) Aplicación de la función de Gray a los elementos del código $\mathcal{C}$.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];
```

viii) y ix) Construcción del código generado por las imágenes de Gray del código $\mathcal{C}$.

```
//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;
```

```
[12, 4, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   1   1 w^2   w   w   w w^2 w^2]
[  0   1   0   0   1   0   0   1   0   0   1   0]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   1   1   w   w   w w^2 w^2 w^2]

true
true
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. De ahí que $\Phi(\mathcal{C})$ es un código lineal.

---

x) Se verifica si el código lineal $\mathcal{E}$ es cíclico.

```
//Funcion IsCyclic

> IsCyclic(E);
```

```
false
```

Calculamos la permutación de Nechaev en los parámetros $p = 2$ y $n = 3$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 2 es n'= 1
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 4
2 ---> 2
3 ---> 3
4 ---> 1
5 ---> 5
```

xi) Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$−lineal $\mathcal{E}$ y repetimos los pasos viii),ix) para el conjunto $\Pi(\mathcal{E})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE
```

```
[12, 4, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   1   1 w^2   w   w   w w^2 w^2]
[  0   1   0   0   1   0   0   1   0   0   1   0]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   1   1   w   w   w w^2 w^2 w^2]

true

true
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ *está contenido en el conjunto* $\Pi(\mathcal{E})$*, por lo que* $\Pi(\mathcal{E})$ *es un código lineal.*

---

x) Se verifica si el código $\mathcal{H} = \Pi(\mathcal{E})$ *es cíclico*

```
//Se aplica la funcion IsCyclic

> IsCyclic(H);
```

```
false
```

Elemento $(p, 0, 0)$

```
//Elemento (p,0,0) en C

> P:=Vector(GR,[p,0,0]);
> P in  C;
```

```
true
```

Conclusión. *El conjunto de las imágenes de Gray del* $[3, 256, 1]$*—código cíclico lineal forma un* $[12, 4, 4]$*—código cuasi-cíclico lineal de longitud* 12*, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la* n*—ada* $(2, 0, 0)$ *es un elemento del código.*

En los siguientes códigos se omitirá el desarrollo del inciso i), pues se emplean los mismos Algoritmos para cada código, sin embargo en la práctica es necesario agregarlos. El desarrollo de los siguientes códigos empezará en el inciso ii), con la creación del anillo de Galois.

Código 4. *Construcción del* $[3, 1024, 1]$*—código cíclico lineal con polinomio generador* $G(z) = z + u + 3$*, sobre el anillo* $\mathcal{R} = GR(2, 2, 2)$*.*

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas

//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

ii),iii),iv),v) Construcción del anillo de Galois, su campo residual, los anillos de polinomios y el conjunto de Teichmüller.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
> p:=2;
> Zf:=x^2+x+1;
> m:=2;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;

//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
GaloisRing(2, 2, x^2 + x + 1)

Finite field of size 2^2

Univariate Polynomial Ring in z over GaloisRing(2, 2, x^2 + x + 1)

Univariate Polynomial Ring in t over GF(2^2)

Conjunto de Teichmuller: { 0, 1, u, u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z + u + 1;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo: G(z)= z + u + 3

Longitud del codigo: n= 3

(3, 1024, 1) Cyclic Linear Code over GaloisRing(2, 2, x^2 + x + 1)
Generator matrix:
[    1     0 u + 1]
[    0     1     u]
[    0     0     2]
```

vii),viii), ix), x). Evaluación de la función de Gray, construcción del código generado por $\Phi(\mathcal{C})$. Confirmación sobre la no cíclicidad de $\Phi(\mathcal{C})$.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;

//Funcion IsCyclic

> IsCyclic(E);
```

```
[12, 5, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   0 w^2 w^2   0   1   w   0   w]
[  0   1   0   0   0   w   0 w^2 w^2   0   w   1]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   0 w^2   w   0   1 w^2   0   w]
[  0   0   0   0   1   w   0   w w^2   0 w^2   1]

true

true

false
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. De ahí que $\Phi(\mathcal{C})$ es un código lineal, además $\Phi(\mathcal{C})$ no es cíclico.

Calculamos la permutación de Nechaev en los parámetros $p = 2$ y $n = 3$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 2 es n'= 1
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 4
2 ---> 2
3 ---> 3
4 ---> 1
5 ---> 5
```

xi). Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$−lineal $\mathcal{E}$ y repetimos los pasos viii),ix) y x) para el conjunto $\mathcal{E} = \Pi(\mathcal{C})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE

//PI(E) no es ciclico

> IsCyclic(H);
```

```
[12, 5, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   0 w^2 w^2   0   1   w   0   w]
[  0   1   0   0   0   w   0 w^2 w^2   0   w   1]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   0 w^2   w   0   1 w^2   0   w]
[  0   0   0   0   1   w   0   w w^2   0 w^2   1]

true

true

false
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ está contenido en el conjunto $\Pi(\mathcal{E})$, por lo que $\Pi(\mathcal{E})$ es un código lineal pero no cíclico.

$(p,0,0)$ *en* $\mathcal{C}$.

```
//Elemento (p,0,0) en C

> P:=Vector(GR,[p,0,0]);
> P in  C;
```

```
true
```

Conclusión. *El conjunto de las imágenes de Gray del* $[3, 1024, 1]$*—código cíclico lineal forma un* $[12, 5, 4]$*—código cuasi-cíclico lineal de longitud* 12*, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la* $\mathfrak{n}$*—ada* $(2, 0, 0)$ *es un elemento del código.*

Código 5. *Construcción del* $[3, 1024, 1]$*—código cíclico lineal con polinomio generador* $G(z) = z + 3u + 2$*, sobre el anillo* $\mathcal{R} = GR(2, 2, 2)$*.*

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas

//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

ii),iii),iv),v). Construcción del anillo de Galois, su campo residual, los anillos de polinomios y el conjunto de Teichmüller.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
> p:=2;
> Zf:=x^2+x+1;
> m:=2;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;

//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
GaloisRing(2, 2, x^2 + x + 1)

Finite field of size 2^2

Univariate Polynomial Ring in z over GaloisRing(2, 2, x^2 + x + 1)

Univariate Polynomial Ring in t over GF(2^2)

Conjunto de Teichmuller: { 0, 1, u, u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z + 3*u;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo: G(z)= z + 3*u + 2

Longitud del codigo: n= 3

(3, 1024, 1) Cyclic Linear Code over GaloisRing(2, 2, x^2 + x + 1)
Generator matrix:
[    1     0     u]
[    0     1 u + 1]
[    0     0     2]
```

vii),viii), ix), x). Evaluación de la función de Gray, construcción del código generado por $\Phi(\mathcal{C})$. Confirmación sobre la no cíclicidad de $\Phi(\mathcal{C})$.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;

//Funcion IsCyclic
```

```
> IsCyclic(E);
```

```
[12, 5, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   0   w w^2   0 w^2   w   0   1]
[  0   1   0   0   0 w^2   0 w^2   1   0   w   w]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   0   w   w   0 w^2 w^2   0   1]
[  0   0   0   0   1 w^2   0   w   1   0 w^2   w]

true

true

false
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. De ahí que $\Phi(\mathcal{C})$ es un código lineal, además $\Phi(\mathcal{C})$ no es cíclico.

Calculamos la permutación de Nechaev en los parámetros $\mathfrak{p} = 2$ y $\mathfrak{n} = 3$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 2 es n'= 1
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 4
2 ---> 2
3 ---> 3
4 ---> 1
5 ---> 5
```

xi). Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{\mathfrak{p}^{\mathfrak{m}}}$—lineal $\mathcal{E}$ y repetimos los pasos viii),ix) y x) para el conjunto $\mathcal{E} = \Pi(\mathcal{C})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE

//PI(E) no es ciclico

> IsCyclic(H);
```

```
[12, 5, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   0   w w^2   0 w^2   w   0   1]
[  0   1   0   0   0 w^2   0 w^2   1   0   w   w]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   0   w   w   0 w^2 w^2   0   1]
[  0   0   0   0   1 w^2   0   w   1   0 w^2   w]

true

true

false
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ está contenido en el conjunto $\Pi(\mathcal{E})$, por lo que $\Pi(\mathcal{E})$ es un código lineal pero no cíclico.

$(p, 0, 0)$ *en* $\mathcal{C}$.

```
//Elemento (p,0,0) en C

> P:=Vector(GR,[p,0,0]);
> P in  C;
```

```
true
```

Conclusión. *El conjunto de las imágenes de Gray del $[3, 1024, 1]$—código cíclico lineal forma un $[12, 5, 4]$—código cuasi-cíclico lineal de longitud 12, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la n—ada $(2, 0, 0)$ es un elemento del código.*

Código 6. *Construcción del $[3, 1024, 1]$—código cíclico lineal con polinomio generador $G(z) = z + 1$, sobre el anillo $\mathcal{R} = GR(2, 2, 2)$.*

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas

//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

ii),iii),iv),v). Construcción del anillo de Galois, su campo residual, los anillos de polinomios y el conjunto de Teichmüller.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
```

```
> p:=2;
> Zf:=x^2+x+1;
> m:=2;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;

//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
GaloisRing(2, 2, x^2 + x + 1)

Finite field of size 2^2

Univariate Polynomial Ring in z over GaloisRing(2, 2, x^2 + x + 1)

Univariate Polynomial Ring in t over GF(2^2)

Conjunto de Teichmuller: { 0, 1, u, u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z + 1;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo: G(z)= z + 1

Longitud del codigo: n= 3

(3, 1024, 1) Cyclic Linear Code over GaloisRing(2, 2, x^2 + x + 1)
Generator matrix:
[1 0 1]
[0 1 1]
[0 0 2]
```

vii),viii), ix), x). Evaluación de la función de Gray, construcción del código generado por $\Phi(\mathcal{C})$*. Confirmación sobre la no cíclicidad de* $\Phi(\mathcal{C})$*.*

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;

//Funcion IsCyclic

> IsCyclic(E);
```

```
[12, 5, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   0   1 w^2   0   w   w   0 w^2]
[  0   1   0   0   0   1   0 w^2   w   0   w w^2]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   0   1   w   0   w w^2   0 w^2]
[  0   0   0   0   1   1   0   w   w   0 w^2 w^2]

true

true

false
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$*, está contenido en* $\Phi(\mathcal{C})$ *y ambos conjuntos tienen la misma cardinalidad, por lo que* $\mathcal{E} = \Phi(\mathcal{C})$*. De ahí que* $\Phi(\mathcal{C})$ *es un código lineal, además* $\Phi(\mathcal{C})$ *no es cíclico.*

Calculamos la permutación de Nechaev en los parámetros $p = 2$ *y* $n = 3$*.*

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 2 es n'= 1
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 4
2 ---> 2
3 ---> 3
4 ---> 1
5 ---> 5
```

xi). Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$−lineal $\mathcal{E}$ y repetimos los pasos viii),ix) y x) para el conjunto $\mathcal{E} = \Pi(\mathcal{C})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE

//PI(E) no es ciclico

> IsCyclic(H);
```

```
[12, 5, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   0   1 w^2   0   w   w   0 w^2]
[  0   1   0   0   0   1   0 w^2   w   0   w w^2]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   0   1   w   0   w w^2   0 w^2]
[  0   0   0   0   1   1   0   w   w   0 w^2 w^2]

true

true

false
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ está contenido en el conjunto $\Pi(\mathcal{E})$, por lo que $\Pi(\mathcal{E})$ es un código lineal pero no cíclico.

$(p,0,0)$ en $\mathcal{C}$.

```
//Elemento (p,0,0) en C

> P:=Vector(GR,[p,0,0]);
> P in  C;
```

```
    true
```

Conclusión. *El conjunto de las imágenes de Gray del* $[3, 1024, 1]$*—código cíclico lineal forma un* $[12, 5, 4]$*—código cuasi-cíclico lineal de longitud* 12*, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la* $\mathfrak{n}$*—ada* $(2, 0, 0)$ *es un elemento del código.*

Código 7. *Construcción del* $[3, 256, 1]$*—código cíclico lineal con polinomio generador* $G(z) = z^2 + (3u + 3)z + u + 2$*, sobre el anillo* $\mathcal{R} = GR(2, 2, 2)$*.*

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas

//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

ii),iii),iv),v). Construcción del anillo de Galois, su campo residual, los anillos de polinomios y el conjunto de Teichmüller.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
> p:=2;
> Zf:=x^2+x+1;
> m:=2;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;

//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
GaloisRing(2, 2, x^2 + x + 1)

Finite field of size 2^2

Univariate Polynomial Ring in z over GaloisRing(2, 2, x^2 + x + 1)

Univariate Polynomial Ring in t over GF(2^2)

Conjunto de Teichmuller: { 0, 1, u, u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z^2 + (3*u + 3)*z + u;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
   Polinomio generador del codigo: G(z)= z^2 + (3*u + 3)*z + u + 2

   Longitud del codigo: n= 3

   (3, 256, 1) Cyclic Linear Code over GaloisRing(2, 2, x^2 + x + 1)
   Generator matrix:
   [    1     u u + 1]
   [    0     2     0]
   [    0     0     2]
```

vii),viii), ix), x). Evaluación de la función de Gray, construcción del código generado por $\Phi(\mathcal{C})$. Confirmación sobre la no cíclicidad de $\Phi(\mathcal{C})$.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;

//Funcion IsCyclic
```

```
> IsCyclic(E);
```

```
[12, 4, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   w w^2 w^2 w^2   1   w   1   w]
[  0   1   0   0   1   0   0   1   0   0   1   0]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   w w^2   w w^2   1 w^2   1   w]

true

true

false
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. De ahí que $\Phi(\mathcal{C})$ es un código lineal, además $\Phi(\mathcal{C})$ no es cíclico.

Calculamos la permutación de Nechaev en los parámetros $p = 2$ y $n = 3$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 2 es n'= 1
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 4
2 ---> 2
3 ---> 3
4 ---> 1
5 ---> 5
```

xi). Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$−lineal $\mathcal{E}$ y repetimos los pasos viii),ix) y x) para el conjunto $\mathcal{E} = \Pi(\mathcal{C})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE

//PI(E) no es ciclico

> IsCyclic(H);
```

```
[12, 4, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0   w w^2 w^2 w^2   1   w   1   w]
[  0   1   0   0   1   0   0   1   0   0   1   0]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1   w w^2   w w^2   1 w^2   1   w]

true

true

false
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ *está contenido en el conjunto* $\Pi(\mathcal{E})$*, por lo que* $\Pi(\mathcal{E})$ *es un código lineal pero no cíclico.*

$(p, 0, 0)$ *en* $\mathcal{C}$*.*

```
//Elemento (p,0,0) en C

> P:=Vector(GR,[p,0,0]);
> P in  C;
```

```
true
```

Conclusión. *El conjunto de las imágenes de Gray del* $[3, 256, 1]$*—código cíclico lineal forma un* $[12, 4, 4]$*—código cuasi-cíclico lineal de longitud* 12*, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la* n*—ada* $(2, 0, 0)$ *es un elemento del código.*

Código 8. *Construcción del* $[3, 256, 1]$*—código cíclico lineal con polinomio generador* $G(z) = z^2 + uz + 3u + 1$*, sobre el anillo* $\mathcal{R} = GR(2, 2, 2)$*.*

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas

//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

ii),iii),iv),v). Construcción del anillo de Galois, su campo residual, los anillos de polinomios y el conjunto de Teichmüller.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
> p:=2;
```

```
> Zf:=x^2+x+1;
> m:=2;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;

//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
GaloisRing(2, 2, x^2 + x + 1)

Finite field of size 2^2

Univariate Polynomial Ring in z over GaloisRing(2, 2, x^2 + x + 1)

Univariate Polynomial Ring in t over GF(2^2)

Conjunto de Teichmuller: { 0, 1, u, u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z^2 + u*z + 3*u + 3;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo: G(z)= z^2 + u*z + 3*u + 1

Longitud del codigo: n= 3

(3, 256, 1) Cyclic Linear Code over GaloisRing(2, 2, x^2 + x + 1)
Generator matrix:
[    1 u + 1     u]
[    0     2     0]
[    0     0     2]
```

vii),viii), ix), x). Evaluación de la función de Gray, construcción del código generado por $\Phi(\mathcal{C})$. Confirmación sobre la no cíclicidad de $\Phi(\mathcal{C})$.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;

//Funcion IsCyclic

> IsCyclic(E);
```

```
[12, 4, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0 w^2   w w^2   1 w^2   w   w   1]
[  0   1   0   0   1   0   0   1   0   0   1   0]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1 w^2   w   w   1 w^2 w^2   w   1]
true
true
false
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. De ahí que $\Phi(\mathcal{C})$ es un código lineal, además $\Phi(\mathcal{C})$ no es cíclico.

Calculamos la permutación de Nechaev en los parámetros $p = 2$ y $n = 3$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 2 es n'= 1
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 4
2 ---> 2
3 ---> 3
4 ---> 1
5 ---> 5
```

xi). Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$—lineal $\mathcal{E}$ y repetimos los pasos viii),ix) y x) para el conjunto $\mathcal{E} = \Pi(\mathcal{C})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];
```

```
//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE

//PI(E) no es ciclico

> IsCyclic(H);
```

```
[12, 4, 4] Quasicyclic of degree 2 Linear Code over GF(2^2)
Generator matrix:
[  1   0   0   0 w^2   w w^2   1 w^2   w   w   1]
[  0   1   0   0   1   0   0   1   0   0   1   0]
[  0   0   1   0   0   1   0   0   1   0   0   1]
[  0   0   0   1 w^2   w   w   1 w^2 w^2   w   1]

true

true

false
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ *está contenido en el conjunto* $\Pi(\mathcal{E})$*, por lo que* $\Pi(\mathcal{E})$ *es un código lineal pero no cíclico.*

$(p, 0, 0)$ *en* $\mathcal{C}$*.*

```
//Elemento (p,0,0) en C

> P:=Vector(GR,[p,0,0]);
> P in  C;
```

```
true
```

Conclusión. *El conjunto de las imágenes de Gray del* $[3, 256, 1]$*—código cíclico lineal forma un* $[12, 4, 4]$*—código cuasi-cíclico lineal de longitud* 12*, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la* n*—ada* $(2, 0, 0)$ *es un elemento del código.*

Código 9. *Construcción del* $[2, 729, 1]$*—código cíclico lineal con polinomio generador* $G(z) = z + 4$*, sobre el anillo* $\mathcal{R} = GR(3, 2, 2)$*.*

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas
```

```
//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

ii),iii),iv),v). Construcción del anillo de Galois, su campo residual, los anillos de polinomios y el conjunto de Teichmüller.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
> p:=3;
> Zf:=x^2+4*x+8;
> m:=2;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;

//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
GaloisRing(3, 2, x^2 + 4*x + 8)

Finite field of size 3^2

Univariate Polynomial Ring in z over GaloisRing(3, 2, x^2 + 4*x + 8)

Univariate Polynomial Ring in t over GF(3^2)

Conjunto de Teichmuller: { u + 2, 0, 1, 2, 2*u, 2*u + 1, u, 2*u + 2, u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z+1;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;
```

```
> n:=2;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo: G(z)= z + 4

Longitud del codigo: n= 2

(2, 729, 1) Cyclic Linear Code over GaloisRing(3, 2, x^2 + 4*x + 8)
Generator matrix:
[1 1]
[0 3]
```

vii),viii), ix), x). Evaluación de la función de Gray, construcción del código generado por $\Phi(\mathcal{C})$*. Confirmación sobre la no cíclicidad de* $\Phi(\mathcal{C})$*.*

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;

//Funcion IsCyclic

> IsCyclic(E);
```

```
[18, 3, 9] Linear Code over GF(3^2)
Generator matrix:
[  1   0   0   2 w^2 w^5   w w^6 w^6 w^7   2   1 w^7   w w^3 w^2 w^5 w^3]
[  0   1   0   1   0   1   0   1   0   1   0   1   0   1   0   1   0  1]
[  0   0   1   1   w   w w^2 w^2 w^3 w^3   2   2 w^5 w^5 w^6 w^6 w^7 w^7]

true

true

false
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$*, está contenido en* $\Phi(\mathcal{C})$ *y ambos conjuntos tienen la misma cardinalidad, por lo que* $\mathcal{E} = \Phi(\mathcal{C})$*. De ahí que* $\Phi(\mathcal{C})$ *es un código lineal, además* $\Phi(\mathcal{C})$ *no es cíclico.*

Calculamos la permutación de Nechaev en los parámetros $p = 3$ *y* $n = 2$*.*

```
> NechaevPermutation(p,n);
```

```
El inverso de 2 modulo 3 es n'= 2
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 5
2 ---> 2
3 ---> 1
4 ---> 4
5 ---> 3
```

xi). Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$−lineal $\mathcal{E}$ y repetimos los pasos viii),ix) y x) para el conjunto $\mathcal{E} = \Pi(\mathcal{C})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE

//PI(E) no es ciclico

> IsCyclic(H);
```

```
[18, 3, 9] Linear Code over GF(3^2)
Generator matrix:
[  1   0   0   w w^2 w^6   w w^7 w^6 w^3   2 w^2 w^7   2 w^3 w^5 w^5 1]
[  0   1   0   1   0   1   0   1   0   1   0   1   0   1   0   1   0  1]
[  0   0   1 w^5   w w^2 w^2 w^3 w^3 w^7   2 w^6 w^5   1 w^6   w w^7 2]

true

true

false
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ está contenido en el conjunto $\Pi(\mathcal{E})$, por lo que $\Pi(\mathcal{E})$ es un código lineal pero no cíclico.

$(p, 0)$ *en* $\mathcal{C}$.

```
//Elemento (p,0) en C

> P:=Vector(GR,[p,0]);
> P in  C;
```

```
true
```

Conclusión. *El conjunto de las imágenes de Gray del* $[2,729,1]$*—código cíclico lineal forma un* $[18,3,9]$*—código lineal de longitud* 18*, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la* n*—ada* $(3,0)$ *es un elemento del código.*

Código 10. *Construcción del* $[2,729,1]$*—código cíclico lineal con polinomio generador* $G(z) = z+2$*, sobre el anillo* $\mathcal{R} = GR(3,2,2)$*.*

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas

//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

ii),iii),iv),v). Construcción del anillo de Galois, su campo residual, los anillos de polinomios y el conjunto de Teichmüller.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
> p:=3;
> Zf:=x^2+4*x+8;
> m:=2;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;

//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
GaloisRing(3, 2, x^2 + 4*x + 8)

Finite field of size 3^2

Univariate Polynomial Ring in z over GaloisRing(3, 2, x^2 + 4*x + 8)

Univariate Polynomial Ring in t over GF(3^2)

Conjunto de Teichmuller: { u + 2, 0, 1, 2, 2*u, 2*u + 1, u, 2*u + 2, u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z-1;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=2;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo: G(z)= z + 2

Longitud del codigo: n= 2

(2, 729, 1) Cyclic Linear Code over GaloisRing(3, 2, x^2 + 4*x + 8)
Generator matrix:
[1 2]
[0 3]
```

vii),viii), ix), x). Evaluación de la función de Gray, construcción del código generado por $\Phi(\mathcal{C})$. Confirmación sobre la no cíclicidad de $\Phi(\mathcal{C})$.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;

//Funcion IsCyclic

> IsCyclic(E);
```

```
[18, 3, 9] Linear Code over GF(3^2)
Generator matrix:
[  1   0   0   1 w^2   w   w w^2 w^6 w^3   2   2 w^7 w^5 w^3 w^6 w^5 w^7]
[  0   1   0   1   0   1   0   1   0   1   0   1   0   1   0   1   0   1]
[  0   0   1   2   w w^5 w^2 w^6 w^3 w^7   2   1 w^5   w w^6 w^2 w^7 w^3]

true

true

false
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. De ahí que $\Phi(\mathcal{C})$ es un código lineal, además $\Phi(\mathcal{C})$ no es cíclico.

Calculamos la permutación de Nechaev en los parámetros $p = 3$ y $n = 2$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 2 modulo 3 es n'= 2
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 5
2 ---> 2
3 ---> 1
4 ---> 4
5 ---> 3
```

xi). Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$—lineal $\mathcal{E}$ y repetimos los pasos viii),ix) y x) para el conjunto $\mathcal{E} = \Pi(\mathcal{C})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE

//PI(E) no es ciclico

> IsCyclic(H);
```

```
[18, 3, 9] Linear Code over GF(3^2)
Generator matrix:
[  1   0   0 w^5 w^2 w^2   w w^3 w^6 w^7   2 w^6 w^7   1 w^3   w w^5 2]
[  0   1   0   1   0   1   0   1   0   1   0   1   0   1   0   1   0 1]
[  0   0   1   w   w w^6 w^2 w^7 w^3 w^3   2 w^2 w^5   2 w^6 w^5 w^7 1]

true

true

false
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ *está contenido en el conjunto* $\Pi(\mathcal{E})$*, por lo que* $\Pi(\mathcal{E})$ *es un código lineal pero no cíclico.*

$(p, 0)$ *en* $\mathcal{C}$.

```
//Elemento (p,0) en C

> P:=Vector(GR,[p,0]);
> P in  C;
```

```
true
```

Conclusión. *El conjunto de las imágenes de Gray del* $(2, 729, 1)$*—código cíclico lineal forma un* $(18, 3, 9)$*—código lineal de longitud* 18*, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la* n*—ada* $(3, 0)$ *es un elemento del código.*

Código 11. *Construcción del* $[3, 4096, 1]$*—código cíclico lineal con polinomio generador* $G(z) = z^2 + z + 3$*, sobre el anillo* $\mathcal{R} = GR(2, 2, 3)$.

i) Se insertan los Algoritmos que se requieren.

```
//Conjunto de Teichmuller

//Extension de la representacion p-adica de n-adas

//Funcion de Gray

//Permutacion de Nechaev

//Funcion Pi de la permutacion de Nechaev

//Permutacion global de Nechaev
```

ii),iii),iv),v). Construcción del anillo de Galois, su campo residual, los anillos de polinomios y el conjunto de Teichmüller.

```
//Anillo de Galois GR

> P<x>:=PolynomialRing(IntegerRing());
> p:=2;
> Zf:=x^3+2*x^2+x+3;
```

```
> m:=3;
> GR<u>:=GaloisRing(p,2,Zf);
> GR;

//Campo residual del anillo GR

> RF<w>:=ResidueField(GR);
> RF;

//Anillos de Polinomios

> PGR<z>:=PolynomialRing(GR);
> PGR;
> PRF<t>:=PolynomialRing(RF);
> PRF;

//Conjunto de Teichmuller del anillo GR

> T:=Teichmuller(GR);
"Conjunto de Teichmuller:",T;
```

```
GaloisRing(2, 2, x^3 + 2*x^2 + x + 3)

Finite field of size 2^3

Univariate Polynomial Ring in z over GaloisRing(2, 2, x^3 + 2*x^2 + x + 3)

Univariate Polynomial Ring in t over GF(2^3)

Conjunto de Teichmuller: { 0, 1, u, u^2, u + 1, u^2 + 1, u^2 + u, u^2 + u + 1 }
```

vi) Construcción del código $\mathcal{C}$.

```
//Codigo C de longitud n

> B:=z^2 + z + 1;
> G:=B+p;
"Polinomio generador del codigo: G(z)=",G;

> n:=3;
"Longitud del codigo: n=",n;

> C:=CyclicCode(n,G);
> C;
```

```
Polinomio generador del codigo: G(z)= z^2 + z + 3

Longitud del codigo: n= 3

(3, 4096, 1) Cyclic Linear Code over GaloisRing(2, 2, x^3 + 2*x^2 + x + 3)
Generator matrix:
[1 1 1]
[0 2 0]
[0 0 2]
```

vii),viii), ix), x). Evaluación de la función de Gray, construcción del código generado por $\Phi(\mathcal{C})$. Confirmación sobre la no cíclicidad de $\Phi(\mathcal{C})$.

```
//Se aplica la funcion de Gray a los elementos de C

> GMC:=[GrayMap(c,GR):c in C];

//Construccion del codigo generado por los elementos de GMC

> E:=LinearCode<RF,n*p^m|GMC>;
> E;

//Se verifica que el conj GMC esta contenido en el codigo E

> Q:=[e : e in E];
> Q subset GMC;
> #Q eq #GMC;

//Funcion IsCyclic

> IsCyclic(E);
```

```
[24, 4, 8] Linear Code over GF(2^3)
Generator matrix:
[1 0 0 0 1 1 w^3 w w w^6 w^2 w^2 w w^3 w^3 w^5 w^4 w^4 w^4 w^5 w^5 w^2 w^6 w^6]
[0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0]
[0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1]
[0 0 0 1 1 1 w w w w^2 w^2 w^2 w^3 w^3 w^3 w^4 w^4 w^4 w^5 w^5 w^5 w^6 w^6 w^6]

true

true

false
```

El código lineal generado por las imágenes de Gray, $\mathcal{E}$, está contenido en $\Phi(\mathcal{C})$ y ambos conjuntos tienen la misma cardinalidad, por lo que $\mathcal{E} = \Phi(\mathcal{C})$. De ahí que $\Phi(\mathcal{C})$ es un código lineal, además $\Phi(\mathcal{C})$ no es cíclico.

Calculamos la permutación de Nechaev en los parámetros $p = 2$ y $n = 3$.

```
> NechaevPermutation(p,n);
```

```
El inverso de 3 modulo 2 es n'= 1
Permutacion de Nechaev en el conjunto {0,1,..., 5 }
0 ---> 0
1 ---> 4
2 ---> 2
3 ---> 3
4 ---> 1
5 ---> 5
```

xi). Aplicamos la Permutación Global de Nechaev a los elementos de código $\mathbb{F}_{p^m}$−lineal $\mathcal{E}$ y repetimos los pasos viii),ix) y x) para el conjunto $\mathcal{E} = \Pi(\mathcal{C})$.

```
//Aplicamos la funcion PI a los elementos del codigo E

> PIE:=[PI(p,m,e):e in E];

//Se genera el codigo lineal con el conjunto PIE

> H:=LinearCode<RF,n*p^m| PIE>;
> H;

//Comprobamos que PI(E) sea el codigo lineal H

> S:=[h : h in H];
> #PIE eq #H;
> S subset PIE

//PI(E) no es ciclico

> IsCyclic(H);
```

```
[24, 4, 8] Linear Code over GF(2^3)
Generator matrix:
[1 0 0 0 1 1 w^3 w^6 w w^6 w^3 w^2 w w^5 w^3 w^5 w w^4 w^4 w^2 w^5 w^2 w^4 w^6]
[0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0]
[0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1]
[0 0 0 1 1 1 w w^6 w w^2 w^3 w^2 w^3 w^5 w^3 w^4 w w^4 w^5 w^2 w^5 w^6 w^4 w^6]

true

true

false
```

Podemos ver que el código lineal generado por el conjunto $\Pi(\mathcal{E})$ está contenido en el conjunto $\Pi(\mathcal{E})$, por lo que $\Pi(\mathcal{E})$ es un código lineal pero no cíclico.

$(p, 0, 0)$ *en* $\mathcal{C}$.

```
//Elemento (p,0,0) en C

> P:=Vector(GR,[p,0,0]);
> P in  C;
```

```
true
```

Conclusión. *El conjunto de las imágenes de Gray del* $[3, 4096, 1]$*—código cíclico lineal forma un* $[24, 4, 8]$*—código lineal de longitud* 18*, dicho código no es cíclico y su imagen bajo la permutación de Nechaev tampoco lo es. Por otro lado la* n*—ada* $(2, 0, 0)$ *es un elemento del código.*

5.4.1 Resumen

A continuación se muestran los códigos que se implementaron y los resultados que se obtuvieron.

Sean $p = 2$ y $f(x) = x^2 + x + 1 \in (\mathbb{Z}/2^2\mathbb{Z})[x]$ polinomio mónico básico primitivo de grado $m = 2$,

$$\mathcal{R} = \mathcal{GR}(2^2, 2) := \frac{(\mathbb{Z}/4\mathbb{Z})[x]}{\langle f(x)\rangle},$$

$n = 3$ y $A(z), B(z), C(z) \in \mathcal{R}[z]$ tales que $A(z)B(z)C(z) = z^n - 1$.

$\mathcal{R}$–**cód. cíclico,** $\mathcal{C}$			$\mathbb{F}_4$**-cód.** $\Phi(\mathcal{C})$		
Referencia	$\mathcal{C}$	**Generador**	**Cíclico**	**Lineal**	**Observaciones**
C 3	$[3, 256, 1]$	$z^2 + z + 3$	F	V	$[12, 4, 4]$-cuasicíclico
C 4	$[3, 1024, 1]$	$z + u + 3$	F	V	$[12, 5, 4]$ —cuasicíclico
C 5	$[3, 1024, 1]$	$z + 3u + 2$	F	V	$[12, 5, 4]$-cuasicíclico
C 6	$[3, 1024, 1]$	$z + 1$	F	V	$[12, 5, 4]$ —cuasicíclico
C 7	$[3, 256, 1]$	$z^2 + (3u + 3)z + (u + 2)$	F	V	$[12, 4, 4]$-cuasicíclico
C 8	$[3, 256, 1]$	$z^2 + uz + (3u + 1)$	F	V	$[12, 4, 4]$ —cuasicíclico

Tabla 3: Códigos sobre el anillo $GR(2^2, 2)$ de longitud 3.

Sean $p = 2$ y $f(x) = x^3 + 2x^2 + x + 3 \in (\mathbb{Z}/2^2\mathbb{Z})[x]$ polinomio mónico básico primitivo de grado $m = 3$,

$$\mathcal{R} = \mathcal{GR}(2^2, 3) := \frac{(\mathbb{Z}/2^2\mathbb{Z})x]}{\langle f(x)\rangle},$$

$n = 3$ y $A(z), B(z), C(z) \in \mathcal{R}[s]$ tales que $A(z)B(z)C(z) = z^n - 1$.

$\mathcal{R}$–**cód. cíclico,** $\mathcal{C}$			$\mathbb{F}_8$**-cód.** $\Phi(\mathcal{C})$		
Referencia	$\mathcal{C}$	**Generador**	**Cíclico**	**Lineal**	**Observaciones**
C 11	$[3, 4096, 1]$	$z^2 + z + 3$	F	V	$[24, 4, 8]$-lineal

Tabla 4: Códigos sobre el anillo $GR(2^2, 3)$ de longitud 3.

Sean $p = 3$ y $f(x) = x^2 + 4x + 8 \in (\mathbb{Z}/3^2\mathbb{Z})[x]$ polinomio mónico básico primitivo de grado $m = 2$,

$$\mathcal{R} = \mathcal{GR}(3^2, 2) := \frac{(\mathbb{Z}/3^2\mathbb{Z})[x]}{\langle f(x)\rangle},$$

$n = 2$ y $A(z), B(z), C(z) \in R[z]$ tales que $A(z)B(z)C(z) = z^n - 1$.

$\mathcal{R}$–**cód. cíclico,** $\mathcal{C}$			$\mathbb{F}_9$**-cód.** $\Phi(\mathcal{C})$		
Referencia	$\mathcal{C}$	**Generador**	**Cíclico**	**Lineal**	**Observaciones**
C 9	$[2, 729, 1]$	$z + 4$	F	V	$[18, 3, 9]$-lineal
C 10	$[2, 729, 1]$	$z + 2$	F	V	$[18, 3, 9]$ —lineal

Tabla 5: Códigos sobre el anillo $GR(3^2, 2)$ de longitud 2.

BIBLIOGRAFÍA

[AM69] M. F. Atiyah and I. G. MacDonal, *Introduction to commutative algebra*, first edition ed., Addison-Wesley Publishing Company, Inc., 1969.

[BCFS08] W. Bosma, J. Cannon, C. Fieker, and A. Steel, *Handbook of magma functions*, (versión 2.14-15) [software] ed., May 2008.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993).

[BF02] G. Bini and F. Flamini, *Finite conmutative rings and their applications*, first ed., Springer Science+Business Media, 2002.

[CS95] A. R. Calderbank and N. J. A. Sloane, *Modular and p-adic cyclic codes*, Des., Codes and Cryptogr. **6** (1995), 21–35.

[DLP04] H. Q. Dinh and S. R. López-Permouth, *Cyclic and negacyclic codes over finite chain rings*, IEEE Trans. Inform. Theory **50** (2004), no. 8, 1728–1744.

[GR17] A. R. García-Ramírez, *Anillos de Galois*, Tesis de licenciatura, Facultad de Ciencias Físico Matemáticas, BUAP, 2017.

[GR19] ———, *Imágenes de Gray de* R*-códigos*, Tesis de maestría, Facultad de Ciencias Físico Matemáticas, BUAP, 2019.

[GRLAVHon] A. R. García-Ramírez, C. A. López-Andrade, y D. Villa-Hernández, *Imágenes de Gray de códigos consta-cíclicos sobre anillos de Galois* R *de índice de nilpotencia 3*, Rev. Integr. Temas Mat. (aceptado para su publicación).

[GS99] M. Greferath and S. E. Schmidt, *Gray isometries for finite chain rings and a nonlinear ternary* $(36, 3^{12}, 15)$ *code*, IEEE Trans. Inform. Theory **45** (1999), 2522–2524.

[HKC+94] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of kerdock, preparata, goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.

[Hun74] T. W. Hungerford, *Algebra*, Springer-Verlag, 1974.

[Jac89] N. Jacobson, *Basic algebra II*, second ed., W. H. Freeman and company, 1989.

[KLP97] P. Kanwar and S. R. López-Permouth, *Cyclic codes over the integers modulo* p^m, Finite Fields and Their Applications 3 (1997), no. 4, 334–352.

[LA13] C. A. López-Andrade, *Imágenes de Gray de códigos sobre anillos de Galois*, Tesis de doctorado, Dep. de Matemáticas, UAM-Iztapalapa, 2013.

[LATR11] C. A. López-Andrade and H. Tapia-Recillas, *On the linearity and quasi-cyclicity of the Gray image of codes over a Galois ring*, Groups, Algebras and Applications, CONM/537, AMS, (2011), 255–268.

[LATR12] ———, *On the cyclicity of the Gray image of a class of linear cyclic codes over a finite chain ring*, International Journal of Pure and Applied Mathematics **80** (2012), no. 2, 181–190.

[LB02] S. Ling and J. T. Blackford, $\mathbb{Z}_{p^{k+1}}$*-linear codes*, IEEE Trans. Inform. Theory **48** (2002), no. 9, 2592–2605.

[MA78] F. J. MacWilliams and N. J. A.Sloane, *The theory of error-correcting codes*, The Netherlands: North Holland, 1978.

[McD74] B. R. McDonald, *Finite rings with identity*, Marcel Dekker Inc., 1974.

[Ple89] V. Pless, *Introduction to the theory of error-correcting codes*, Wiley-Interscience, 1989.

[PQ96] V. S. Pless and Z. Qian, *Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **42** (1996), no. 5, 1594–1600.

[Rot03] J. J. Rotman, *Advanced modern algebra*, 2nd printing ed., Prentice Hall., 2003.

[US98] P. Udaya and M. U. Siddiqi, *Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings*, IEEE, Trans. Inform. Theory **44** (1998), no. 4, 1492–1503.

[Wal56] E. A. Walker, *Cancellation in direct sums of groups*, Proceedings of the American Mathematical Society **7** (1956), no. 5, 898–902.

[Wan03] Z.-X. Wan, *Lectures on finite fields and Galois rings*, World Scientific Pub. Co. Inc., 2003.

[Wol99] J. Wolfmann, *Negacyclic and cyclic codes over $\mathbb{Z}_4$*, IEEE, Trans. Inform. Theory **45** (1999), no. 7, 2527–2532.

[Wol01] ———, *Binary images of cyclic codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory **47** (2001), no. 5.

ÍNDICE ALFABÉTICO

ÍNDICE DE ALGORITMOS