IMÁGENES DE GRAY DE R-CÓDIGOS

TESIS QUE PRESENTA

ÁNGEL RAÚL GARCÍA RAMÍREZ

PARA OBTENER EL TÍTULO DE
MAESTRO EN CIENCIAS MATEMÁTICAS

ASESOR: DR. CARLOS ALBERTO LÓPEZ
ANDRADE

BENEMÉRITA UNIVERSIDAD AUTÓNOMA
DE PUEBLA
Facultad de Ciencias Físico Matemáticas
Diciembre 2019
http://www.fcfm.buap.mx/

ÁNGEL RAÚL GARCÍA RAMÍREZ : *Imágenes de Gray de R-códigos* ,
© Diciembre 2019.

E-MAIL:
argr_040890@hotmail.com

BUAP

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 el(la) C:

ÁNGEL RAÚL GARCÍA RAMÍREZ

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 5 de diciembre de 2019, con la tesis titulada:

Imágenes de Gray de R-códigos

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 5 de diciembre de 2019

DRA. PATRICIA DOMÍNGUEZ SOTO
COORDINADORA DEL POSGRADO
EN MATEMÁTICAS.

III

Ccp.Archivo.
DRA. PDS/mtrv

A Jeny:
Porqué siempre estuviste allí conmigo, porqué hemos crecido juntos y allá dónde vayamos, seguirán nuestros asuntos...

AGRADECIMIENTOS

Agradezco en primer lugar a mis sinodales, aquellos que fueron testigos del desarrollo de este trabajo y que aportaron su paciente guía y consejo para mi crecimiento profesional. Al Dr. David Villa Hernández por sus cursos al inicio de la maestría quien amplió mi conocimiento en el álgebra abstracta y me mostró la importancia de la atención al detalle. Al Dr. César Cejudo Castilla quien dedicó su valioso tiempo y sincera opinión en los foros de avance para mi reflexión personal sobre el presente manuscrito, al Dr. Iván Fernando Vilchis Montalvo por su sincera preocupación en los contenidos abordados y su honestidad, así como sus sugerencias para mejorar la exposición y defensa de esta tesis y al Dr. Carlos Guillén Galván a quien conozco desde la licenciatura, quien me dió una visión diferente de esta carrera, por su incorporación al jurado y por aceptar la lectura de mi tesis a una fecha tan cercana a su conclusión.

A mi asesor, el Dr. Carlos Alberto López Andrade quien en su tesis de doctorado colocó los cimientos que dieron origen al presente trabajo, bajo su tutela conocí la importancia del trabajo duro y constante. Siempre mostrando una gran disposición a señalarme el camino y brindarme la oportunidad de realizar este proyecto dando continuación a sus pasos, por no perder la fé en mi. Gracias.

A mis padres Mario Raúl y Soledad quiénes me han acompañado hasta esta nueva meta, en el cual espero vean recompensado su apoyo y cariño. A mis hermanas Graciela, Verónica y Monserrath las cuales al igual que yo luchan día a día para lograr sus objetivos y que ahora, como nuestros padres, construyen la senda para que mis amados sobrinos Mateo, Raúl, Leslie y Samantha alcancen sus sueños. Los amo.

A mi prometida Jeny, la mujer que apareció en mi vida cuando sentí que perdía el rumbo, que se quedó allí en mi oscuridad y con su amor, paciencia y ternura me devolvió la sonrisa, lo mejor de mi y que trajo a mi vida personas excepcionales.

A ustedes Doña Leonor, Don José, Saúl, Abel y Gabriel, quiénes abrieron las puertas de su casa y corazón para aceptarme como parte

de su familia, gracias pues sus palabras de aliento y buenos deseos me ayudaron a seguir cuando lo necesité.

A mis amigos, aquellos que estuvieron, a los que están y quiénes están por venir. Agustín R., Carlos A., Carlos J., Zuñiga G., Alexis, Arturo, Hugo Saúl, Itzel, Jerónimo, Jez, Karen G., Manuel, Rafael A., Ricardo Thaddeus, Roque, Santiago, Emmanuel N., Oscar P., Gerardo H., Gerardo M., Iván G., Yas, Aleyda T., Mireya, Brenda C. y aquellos que pudiera haber olvidado, perdonen el atropello, son tantas las memorias y *este margen tan pequeño...*

Quizás la parte de la historia que desconocen todos aquellos quienes lean estos agradecimientos es todo aquel tiempo que he pensado que no podría llegar hasta aquí, es una historia larga y llena de momentos de frustración e impaciencia, pero de igual manera todos ustedes formaron parte de ella, dejándome ver como todos con sus talentos, esfuerzos, penas y alegrías hicieron que en mi corazón creciera el deseo de verlos triunfar y en el proceso me trajeron hasta aquí, a mí, a quien desconfía de sus habilidades, gracias, en verdad, por hacerme confirmar que *el trabajo duro, tarde o temprano supera al talento.*

Finalmente, pero no por esto menos importante, agradezco al Consejo Nacional de Ciencia y Tecnología (CONACYT), por haber aceptado mi solicitud y haberme otorgado una beca en el Programa Nacional de Posgrados de Calidad (PNPC), pues ésta fue mi sustento y permitió mi dedicación a este proyecto. Gracias por apoyar a los estudiantes y permitirnos contribuir a este gran país con nuestra labor en el desarrollo de la ciencia.

INTRODUCCIÓN

La Teoría de códigos algebraicos ha utilizado a los anillos finitos de cadena [4] en los últimos años, en particular a los anillos de Galois (los cuales son una subclase de éstos cf. [3], [19]) y a las imágenes bajo la función de Gray de códigos definidos sobre éstos últimos, (cf.[8], [9] y [14]) para el estudio de códigos sobre anillos de Galois y campos finitos, teniendo como ejemplo los trabajos de Nechaev [16] y Hammons et. al. en [2] dónde demostraron que el código de Kerdock es la imágen de Gray de un código cíclico lineal extendido sobre el anillo de Galois $GR(2^2, 1) = \mathbb{Z}^4$.

Por otro lado, los anillos de Galois son extensiones únicas del anillo de clases residuales $\mathbb{Z}_{p^s} = \mathbb{Z}/p^s\mathbb{Z}$, con p y s enteros positivos y p un número primo. Suelen denotarse por $R = GR(p^s, m)$, dónde la característica del anillo es p^s y su cardinalidad p^{sm}. La representación p-ádica de los elementos de $GR(p^s, m)$ es vital en la definición de la función de Gray para códigos definidos sobre éstos anillos, y la estructura del *anillo truncado de vectores de Witt de longitud "s"* sobre el campo finito $\mathbb{F}_{p^m}$, $W_s(\mathbb{F}_{p^m})$, se vuelve imprescindible para nosotros, en la tarea de averiguar cómo se operan las μ-reducciones de las *componentes p-ádicas* de los elementos de $GR(p^s, m)$, dicho anillo truncado de vectores de Witt fue propuesto por Ernst Witt en 1936, el cual los descubrió mientras estudiaba las extensiones p-abelianas en los trabajos de A.A. Albert, Artin-Scherier y Kummar. (cf. [7],[10])

La presente tesis tiene como objetivo hallar las condiciones necesarias y suficientes para que la imágen bajo la función de Gray de un *código λ-cíclico* definido sobre un anillo de Galois de índice de nilpotencia 3 sea *cuasi-cíclica* y que la imágen bajo la función de Gray de un *código cíclico lineal* definido sobre un anillo de Galois de índice de nilpotencia 3, sea *cuasi-cíclica*.

Este manuscrito está organizado de la siguiente manera:

El Capítulo 1 está conformado por un repaso sobre las estructuras algebraicas que están involucradas en el desarrollo y culminación del objetivo de esta tesis, siendo sus primeras tres secciones un recordatorio sobre anillos de Galois, campos finitos y teoría de códigos

y destacando en su cuarta sección el Teorema 1.4.9 el cual exhibe un isomorfismo entre el *anillo truncado de vectores de Witt de longitud* s y el anillo de Galois $GR(p^s, m)$.

En el Capítulo 2 estudiamos algunas definiciones de la función de Gray para anillos de Galois comenzando con $\mathbb{Z}_4 = GR(2^2, 1)$:

$$\begin{aligned} \phi : \mathbb{Z}_4 &\to \mathbb{F}_2^2 \\ 0 \mapsto 00 \quad & 2 \mapsto 11 \\ 1 \mapsto 01 \quad & 3 \mapsto 10 \end{aligned}$$

y como se obtienen las imágenes de Gray de *códigos cuaternarios*. En la sección 2.3 se estudia la función de Gray que se utilizara en este trabajo, utilizando herramientas como el *producto de Kronecker*, una dispocisión particular de los elementos del campo finito $\mathbb{F}_{p^m}$ y tres vectores $\mathbf{c}_0, \mathbf{c}_1$ y $\mathbf{c}_2$ para este propósito:

Definición. Sea R un anillos de Galois de índice de nilpotencia 3. La función de Gray definida en R^n está dada por:

$$\begin{aligned} \Phi : R^n &\to \mathbb{F}_q^{nq^2} \\ \underline{c} &\mapsto r_0(\underline{c}) \otimes \mathbf{c}_0 + r_1(\underline{c}) \otimes \mathbf{c}_1 + r_2(\underline{c}) \otimes \mathbf{c}_2 \end{aligned}$$

con $R = GR(p^3, m)$ y $q = p^m$.

El Capítulo 3 está dedicado a los pormenores de conceptos y preeliminares que resultan necesarios para el desarrollo y comprensión de las demostraciones de los resultados centrales de este trabajo:

Teorema. Un R-código $\mathcal{C}$ de longitud n es λ-cíclico si y sólo si, su imagen bajo la función de Gray $\Phi(\mathcal{C})$ es un código cuasi-cíclico sobre $\mathbb{F}_{p^m}$ de índice p^{2m-1} y longitud np^{2m}.

Teorema. Un R-código $\mathcal{C}$ de longitud n es un código cíclico lineal si y sólo si $\Pi^{\otimes p^{2m-1}}(\Phi(C))$ es un código cuasi-cíclico de índice p^{2m-1} y longitud nq^2 sobre $\mathbb{F}_q$.

Los anteriores resultados no son nuevos, ya que en el artículo de S. Jitman y P. Udomkavanich [8] se publican resultados similares, sin embargo, el tratamiento que se le ha dado en el presente trabajo tiene como eje principal poner enfásis en el uso de herramientas alternativas como *la permutación de Nechaev*, las representaciones polinomiales de palabras-ćodigo y la manipulación de ciertas unidades especiales en los anillos de Galois mediante relaciones obtenidas a tráves del análisis del *anillo truncado de vectores de Witt de longitud* 3.

Dicho tratamiento proporciona nuevas demostraciones para estos resultados que resultarán de utilidad para el lector familiarizado con los contenidos ya mencionados y que presente interés en el estudio de los códigos definidos sobre anillos de Galois.

Finalmente, el lector encontrará dos apéndices, en el primero se concentran enunciados y definiciones que sirven como complemento para los temas abordados y en el segundo, un breve manual de algunas instrucciones del programa computacional MAGMA el cual resultó ser una herramienta extremadamente útil en la construcción de ejemplos a fin de tener una visión concreta de los teoremas que fueron el núcleo de éstos dos años de trabajo.

ÍNDICE GENERAL

1 PRELIMINARES 1
- 1.1 Campos Finitos 1
- 1.2 Anillos de Galois 3
- 1.3 Teoría de códigos 6
  - 1.3.1 Códigos sobre campos finitos 7
  - 1.3.2 Códigos cuaternarios 9
  - 1.3.3 Códigos sobre anillos de Galois 12
- 1.4 Anillo de vectores de Witt 16
  - 1.4.1 Aritmética p-ádica 30

2 LA ISOMETRIA DE GRAY 37
- 2.1 La función de Gray en $\mathbb{Z}_4$ 37
- 2.2 Imágenes de $\mathbb{Z}_4^n$-códigos 39
- 2.3 La función de Gray generalizada 42
  - 2.3.1 Producto de Kronecker 42
  - 2.3.2 Los elementos de $\mathbb{F}_q$ 43
  - 2.3.3 Dos definiciones de la función de Gray 45

3 IMÁGENES DE GRAY DE R-CÓDIGOS 53
- 3.1 Imagen de Gray de un código constacíclico 53
  - 3.1.1 Códigos constacíclicos 53
- 3.2 Imagen de Gray de un código γ-cíclico lineal 57
  - 3.2.1 Representaciones polinomiales de códigos 57
  - 3.2.2 Códigos γ-cíclicos y la permutación de Nechaev 63

A RESULTADOS COMPLEMENTARIOS 73
- A.1 Inmersión de la estructura de anillo 73
- A.2 Polinomios en varias variables 74
- A.3 Raíces p-ésimas en campos finitos 76

B MAGMA 79
- B.1 Representaciones p-ádicas 79
  - B.1.1 Polinomios Mónicos Básicos Primitivos 82
- B.2 La función de Gray 82
  - B.2.1 MAGMA en anillos de índice de nilpotencia 3 84

B.2.2 La función de Gray 86
B.3 Códigos en MAGMA 87
B.3.1 Códigos constacíclicos 87
B.3.2 Códigos cíclicos lineales 89

BIBLIOGRAFÍA 94

Índice Alfabético 95

Índice de Figuras 97

Índice de Cuadros 99

1 PRELIMINARES

En este capítulo introduciremos conceptos y resultados fundamentales concernientes a las estructuras algebraicas involucradas en el desarrollo del presente trabajo, las cuales son: los campos finitos, anillos de Galois y los códigos definidos sobre estos alfabetos.

Para estos fines, se presentará el contenido estructurado de la siguiente manera: teoría sobre campos finitos, un acercamiento a los anillos de Galois, conceptos básicos y propiedades de la teoría de códigos definidos sobre campos finitos y anillos de Galois y finalmente un desarrollo detallado de una construcción del anillo de vectores de Witt y su relación con los anillos de Galois.

En la primera parte (Campos finitos y Anillos de Galois) se han omitido las demostraciones de los resultados y se presentan a modo de resumen considerando que el lector esta familiarizado con la literatura elemental de estos tópicos, sin embargo, se pueden encontrar dichas demostraciones en [3], [11], [17], [18] y [19].

1.1 CAMPOS FINITOS

Recordemos que un *campo* es un conjunto no vacío $\mathbb{F}$ con dos operaciones binarias suma $+$ y producto $\cdot$ tales que:

- Los pares $(\mathbb{F}, +)$ y $(\mathbb{F}^*, \cdot)$ $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, son grupos abelianos con elementos neutros 0 y 1 respectivamente.

- Existe una ley distributiva del producto sobre la suma.

Además, si $\mathbb{F}$ es un conjunto finito, diremos que éste es un *campo finito*. Un subconjunto K de $\mathbb{F}$ que también es un campo, es un *subcampo* de $\mathbb{F}$ y decimos que $\mathbb{F}$ es una *extensión* del campo K. Un campo (subcampo) K que no posee subcampos distintos de sí mismo, es un *campo primo* (*subcampo primo* de $\mathbb{F}$).

Todo campo finito $\mathbb{F}$ con p^m elementos donde $m \in \mathbb{N}$, satisface las siguientes propiedades:

- La característica de $\mathbb{F}$ es un número primo p y su subcampo primo es isomorfo a $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$.
- Si $f(x) \in \mathbb{Z}_p[x]$ es irreducible con $\text{grad}(f) = m$, entonces el anillo cociente $\mathbb{Z}_p[x]/\langle f(x)\rangle$ es un campo finito con p^m elementos, en consecuencia (salvo isomorfismos) solo hay un campo finito con p^m elementos.
- Para todo $k \in \mathbb{N}$ y $u, v \in \mathbb{F}$ un campo finito de característica p: $(u+v)^{p^k} = u^{p^k} + v^{p^k}$.
- El grupo multiplicativo $\mathbb{F}^*$ formado por los elementos distintos de cero del campo, es cíclico y cualquier generador de éste es llamado *elemento primitivo*, más aún si $h(x) \in \mathbb{F}[x]$ es el polinomio mínimo[1] de dicho elemento primitivo, decimos que $h(x)$ es un *polinomio primitivo*.
- Todo subcampo K de un campo finito con p^m elementos posee p^d elementos donde d es un divisor positivo de m. De manera recíproca, para cada divisor positivo d de m existe un subcampo de $\mathbb{F}$ con exactamente p^d elementos, en consecuencia los subcampos de un campo finito forman una retícula completa respecto a la contención.
- Todo elemento $u \in \mathbb{F}$ satisface que $u^{p^m} = u$, además $\mathbb{F}$ es isomorfo al campo de descomposición del polinomio $x^{p^m} - x \in \mathbb{Z}_p[x]$.
- El campo $\mathbb{F}$ es un espacio vectorial de dimensión finita sobre su subcampo primo, de hecho, si P es el subcampo primo de $\mathbb{F}$:
$$[\mathbb{F} : P] := dim\,({}_P\mathbb{F}),$$
el entero $[\mathbb{F} : P]$ es llamado *grado de la extensión* de $\mathbb{F}$ sobre P.
- Si $f(x)$ es un polinomio irreducible en $\mathbb{Z}_p[x]$ y primitivo en $\mathbb{F}[x]$, de grad$f(x) = m$ con ω como una de sus raíces, entonces $\mathbb{F} \simeq \mathbb{Z}_p[x]/\langle f(x)\rangle$, $\beta = \{1, \omega, \omega^2, \ldots, \omega^{m-1}\}$ es una base de $\mathbb{F}$ sobre $\mathbb{Z}_p$ y denotamos $\mathbb{F} = \mathbb{Z}_p[\omega]$.
- Existe un automorfismo:
$$\begin{aligned} \sigma : \mathbb{F}_{p^m} &\to \mathbb{F}_{p^m} \\ u &\mapsto u^p, \end{aligned}$$

1 $h(x)$ es el polinomio mínimo de α si es el polinomio irreducible de menor grado tal que $h(\alpha) = 0$.

que deja fijos a los elementos de su subcampo primo, es decir, $\sigma(u) = u$ si y sólo si $u \in \mathbb{Z}_p$. σ recibe el nombre *automorfismo de Frobenius*.

- El automorfismo de Frobenius σ forma un grupo cíclico de orden m bajo la composición, el cual es llamado *grupo de Galois* de $\mathbb{F}_{p^m}$ sobre $\mathbb{F}_p$ y se denota por $Gal(\mathbb{F}_{p^m}/\mathbb{F}_p)$.

En lo sucesivo, adoptaremos la siguiente notación: $GF(p^m)$ o $\mathbb{F}_{p^m}$ para denotar a un campo finito con p^m elementos, el subcampo primo de un campo finito será denotado por $\mathbb{F}_p$ o $GF(p)$ dependiendo del contexto y si al hacer uso indistinto no hay ambigüedad también lo denotaremos por $\mathbb{Z}_p$.

1.2 ANILLOS DE GALOIS

Los anillos de Galois son extensiones únicas salvo isomorfismos del anillo de clases residuales $\mathbb{Z}_{p^s}$ con $s \in \mathbb{N}$. Una de las particularidades que hacen que estos anillos sean de interés para nuestros propósitos es la estrecha relación que guardan con los campos finitos, como el lector podrá contemplar a continuación. Los siguientes resultados pueden ser consultados así como sus demostraciones en [3] y [19].

Sean p un número primo y s un entero positivo, consideremos a $\mathbb{Z}_{p^s} = \mathbb{Z}/p^s\mathbb{Z}$ el anillo de enteros módulo p^s, $\mathbb{Z}_{p^s}[x]$ el anillo de polinomios en la indeterminada x con coeficientes en $\mathbb{Z}_{p^s}$, $\langle p1 \rangle$ el ideal principal generado por $p1$ y las funciones:

$$\begin{aligned} \mu : \mathbb{Z}_{p^s} &\to \frac{\mathbb{Z}_{p^s}}{\langle p1 \rangle} \\ a &\mapsto a + \langle p1 \rangle \end{aligned} \qquad \begin{aligned} \hat{\mu} : \mathbb{Z}_{p^s}[x] &\to \frac{\mathbb{Z}_{p^s}}{\langle p1 \rangle}[x] \\ f(x) &\mapsto \hat{\mu}(f(x)), \end{aligned}$$

donde μ es el *homomorfismo canónico* o *μ-reducción* el cual se extiende de manera natural al anillo de polinomios $\mathbb{Z}_{p^s}[x]$, aplicando μ a los coeficientes de un polinomio $f(x)$. Es fácil verificar que $\frac{\mathbb{Z}_{p^s}}{\langle p1 \rangle} \simeq \mathbb{F}_p$ y por consiguiente $\frac{\mathbb{Z}_{p^s}}{\langle p1 \rangle}[x] \simeq \mathbb{F}_p[x]$, de modo que los denotaremos de esta manera y tanto $\mu(a)$ como $\hat{\mu}(f(x))$ serán denotados de manera indistinta por $\overline{a}$ y $\overline{f}(x)$ respectivamente.

Un polinomio mónico $f(x) \in \mathbb{Z}_{p^s}[x]$ será llamado *básico irreducible* (*básico primitivo*) si $\overline{f}(x) \in \mathbb{F}_p[x]$ es irreducible (primitivo).

Un anillo finito, conmutativo R con identidad 1, es un *anillo de Galois*, si el conjunto $\mathcal{D}$ de los divisores de cero de R con el cero añadido, forman un ideal principal, el cual es generado por 0 o por $p1$. Algunas de las propiedades de un anillo de Galois que nos resultarán de suma utilidad se enlistan a continuación, cabe mencionar que abusando de la notación, denotaremos a $p1$ mediante p.

- Si R es un anillo de Galois tal que $\mathcal{D}$ es el conjunto vacío, entonces es un campo finito, de lo contrario el ideal principal $\langle p \rangle = \mathcal{D} \cup \{0\}$ es el único ideal maximal de R, es decir, R es un *anillo local*.

- El *campo residual* $RF = R/\langle p \rangle$ es isomorfo a $\mathbb{F}_{p^m}$ y la característica de R es p^s, para algunos enteros no negativos m y s, es por está razón que denotamos al anillo de Galois R mediante $GR(p^s, m)$.

- R contiene un subanillo isomorfo a $\mathbb{Z}_{p^s}$, en [3, Lema 3.2.2] se exhibe que dicho subanillo es $\{r1 : r \in \mathbb{Z}\}$, en lo sucesivo lo denotaremos por Z_{p^s} y todos sus ideales son de la forma $\langle p^k \rangle$ con $k \in \{0, 1, \ldots, s\}$ y son tales que $|\langle p^k \rangle| = p^{(s-k)m}$. Además, forman la cadena:

$$\langle 0 \rangle = \langle p^s \rangle \subsetneq \langle p^{s-1} \rangle \subsetneq \cdots \subsetneq \langle p \rangle \subsetneq \langle p^0 \rangle = \langle 1 \rangle = R,$$

  es decir, R es un *anillo finito de cadena* de índice de nilpotencia s.

- Sea $\mu_R : R \to RF$ el homomorfismo canónico entre R y su campo residual, de manera análoga a μ éste puede extenderse mediante $\hat{\mu}_R : R[x] \to RF[x]$ aplicando μ_R a los coeficientes del polinomio $f(x) \in R[x]$.

- Para todo anillo de Galois $R = GR(p^s, m)$ existe un polinomio mónico básico irreducible $h(x)$ en $\mathbb{Z}_{p^s}[x]$ tal que $grad(h(x)) = m$ y:

$$GR(p^s, m) \simeq \frac{\mathbb{Z}_{p^s}[x]}{\langle h(x) \rangle}, \tag{1.2.1}$$

  además existe un elemento no cero $\xi \in R$ que es raíz del polinomio $h(x)$ y tal que todo elemento de $c \in R$ admite una representación única dada por:

$$c_0 + c_1\xi + \cdots + c_{m-1}\xi^{m-1} \qquad (c_k \in \mathbb{Z}_{p^s}, 0 \leq k \leq m-1). \tag{1.2.2}$$

de ahí que podemos denotar también $R = \mathbb{Z}_{p^s}[\xi]$, a esta notación se le ha dado el nombre de *representación aditiva* de los elementos del anillo de Galois.

- Si el elemento ξ en $GR(p^s, m)$ es tal que $ord(\xi) = p^m - 1$, el conjunto:
$$\mathcal{T} = \{\xi^k : 0 \leq k \leq p^m - 2\} \cup \{0\}, \tag{1.2.3}$$
recibe el nombre del *conjunto de Teichmüller* y es tal que: $\mu(\mathcal{T}) = RF$, es decir, es un conjunto de representantes del campo residual de R. Además, todo elemento $c \in GR(p^s, m)$ puede expresarse de manera única mediante:
$$c = \rho_0(c) + p\rho_1(c) + \cdots + p^{s-1}\rho_{s-1}(c), \tag{1.2.4}$$
donde $\rho_j(c) \in \mathcal{T}$ para $0 \leq j \leq s-1$. (1.2.4) recibe el nombre de *representación p-ádica* y los $\rho_j(c)$ son llamados *componentes p-ádicas*.

- Un elemento $c \in R = GR(p^s, m)$ satisface que $c \in \langle p \rangle$ si y sólo $\rho_0(c) = 0$ y $c \notin \langle p \rangle$ si y sólo si $\rho_0(c) \neq 0$, además si R^* denota el grupo de unidades del anillo entonces $R = \langle p \rangle \cup R^*$ y R^* es producto directo de un grupo cíclico de orden $p^m - 1$ y un grupo $\mathcal{G}$ de orden $p^{(s-1)m}$.

Para continuar con la revisión de los anillos de Galois, nótese que en lo sucesivo denotaremos a los homomorfismos μ_R y $\hat{\mu}_R$ mediante – como ya se hizo anteriormente para $\mathbb{Z}_{p^s}$, se heredan los conceptos de polinomios básicos irreducibles y básicos primitivos para un polinomio mónico $f(x) \in R[x]$ si $\overline{f}(x)$ es irreducible o primitivo en $\overline{R}[x] = \mathbb{F}_{p^m}[x]$; la notación aditiva (1.2.2) corresponde a un polinomio $r(x) \in \mathbb{Z}_{p^s}[x]$, pues por (1.2.1) todo elemento puede ser visto como una clase polinomial $f(x) + \langle h(x) \rangle$, en virtud de esto, $r(x)$ es un polinomio tal que $h(x) \mid [f(x) - r(x)]$ o en otras palabras $f(x) \equiv r(x) \pmod{h(x)}$. Algunos ejemplos de anillos de Galois son:

(i) $GR(p, m) = GF(p^m) = \mathbb{F}_{p^m}$

(ii) Dado el polinomio $f(x) = x^2 + 5x + 7 \in \mathbb{Z}_{2^3}[x]$, $\overline{f}(x) = x^2 + x + 1$ es primitivo en $\mathbb{F}_2[x]$, así $f(x)$ es básico primitivo y por consiguiente $\frac{\mathbb{Z}_{2^3}[x]}{\langle x^2+5x+7 \rangle} \simeq GR(2^3, 2)$.

Finalmente, consideremos que $R = \mathbb{Z}_{p^s}[\xi]$, entonces puede definirse un isomorfismo de anillos $\Theta : R \to R$ dado por:

$$\Theta(c_0 + c_1\xi + \cdots + c_{m-1}\xi^{m-1}) = c_0 + c_1\xi^{p^m} + \cdots + c_{m-1}\xi^{(m-1)p^m}, \tag{1.2.5}$$

tal que $\Theta(c) = c$, si y sólo si $c \in Z_{p^s}$, éste isomorfismo forma un grupo cíclico de orden $p^m - 1$ con la composición de funciones denotado por $\langle\Theta\rangle$ o $Gal(R/\mathbb{Z}_{p^s})$ y es llamado el *grupo de Galois* de R sobre $\mathbb{Z}_{p^s}$ y tal isomorfismo es llamado *automorfismo generalizado de Frobenuis*.

1.3 TEORÍA DE CÓDIGOS

En éste apartado, recordaremos algunos conceptos básicos de la teoría códigos sobre campos finitos y anillos de Galois.

- Cualquier conjunto finito no vacío $\mathcal{A}$ es un *alfabeto* y sus elementos reciben el nombre de *símbolos*.

- Un *código* de longitud n es un subconjunto C del producto cartesiano $\mathcal{A}^n$, los elementos de un código son llamados *palabras código* y si $|C| = M$ entonces decimos que C es un (n, M)-código sobre $\mathcal{A}$.

- Si $\mathcal{A}$ es un anillo finito, entonces un *código lineal* es un submódulo de $\mathcal{A}^n$ (visto como $\mathcal{A}$-módulo).

- Si $\mathcal{A}$ es un campo finito con p^m elementos, entonces un $[n, k]$-*código lineal* es un subespacio vectorial de $\mathcal{A}^n$ (visto como $\mathbb{F}_{p^m}$-espacio vectorial) de dimensión k.

- Un *corrimiento cíclico* es una función:

$$\begin{aligned} \overline{\sigma} : \mathcal{A}^n &\to \mathcal{A}^n \\ (a_0, \ldots, a_{n-2}, a_{n-1}) &\mapsto (a_{n-1}, a_0, \ldots, a_{n-2}) \end{aligned}$$

  y un *código cíclico* es un código C tal que $\overline{\sigma}(C) = C$.

- Dado n un entero positivo, si existen t, s enteros positivos tales que $n = st$, el vector $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$ de longitud n, puede ser escrito en t bloques de longitud s, es decir, $\underline{a} =$

$\left(a^{[1]} \mid a^{[2]} \mid \ldots \mid a^{[t]}\right)$ donde el k-ésimo bloque de longitud s estaría dado por:

$$a^{[k]} := (a_{k1}, \ldots, a_{k(s-1)}, a_{sk}).$$

- Dado un vector de longitud $n = st$, un *corrimiento cuasi-cíclico* $\sigma^{\otimes t} : \mathbb{F}^n \to \mathbb{F}^n$ es una función tal que:

$$\sigma^{\otimes t}(\underline{a}) = \left(\overline{\sigma}\left(a^{[1]}\right), \overline{\sigma}\left(a^{[2]}\right), \ldots, \overline{\sigma}\left(a^{[t]}\right)\right).$$

- El código $\mathcal{C}$ se dirá *cuasi-cíclico* de índice t y longitud st, si $\sigma^{\otimes t}(\mathcal{C}) = \mathcal{C}$.

1.3.1 Códigos sobre campos finitos

Sea $\mathbb{F}_q$ un campo finito con $q = p^m$ elementos y n un entero positivo.

- La *intersección* de dos palabras código $\underline{x} = (x_0, x_1, \ldots, x_{n-1})$ y $\underline{y} = (y_0, y_1, \ldots, y_{n-1})$ en $\mathbb{F}_2^n$, es el vector:

$$\underline{x} \cap \underline{y} = (x_0 y_0, x_1 y_1, \ldots, x_{n-1} y_{n-1}).$$

- El *peso de Hamming* de una palabra código $\underline{x} \in \mathbb{F}_q^n$, denotado por $w_H(\underline{x})$ se define como:

$$w_H(\underline{x}) := \left|\{0 \leq j \leq n-1 \mid x_j \neq 0\}\right|.$$

- La *distancia de Hamming* entre dos palabras código $\underline{x}, \underline{y}$ la denotaremos por $d_H(\underline{x}, \underline{y})$ está dado por:

$$w_H(\underline{x} - \underline{y}).$$

- Si C es un código sobre $\mathbb{F}_q$, la *distancia mínima de Hamming* es:

$$\begin{aligned} d_C &= \text{mín}\{d_H(\underline{x}, \underline{y}) \mid \underline{x}, \underline{y} \in C \text{ y } \underline{x} \neq \underline{y}\} \\ &= \text{mín}\{w_H(\underline{x} - \underline{y}) \mid \underline{x}, \underline{y} \in C \text{ y } \underline{x} \neq \underline{y}\} \end{aligned}$$

  Si C es un código lineal de longitud n, dimensión k y distancia mínima d decimos que C es un $[n, k, d]$-código lineal.

- La distancia mínima de un $[n,k]$-código lineal es de suma importancia en la teoría de códigos detectores-correctores de errores, uno de los resultados más relevantes respecto a este parámetro se enuncia a continuación.

Teorema 1.3.1 ([12] Teorema 3.9, pág. 16)**.** *Un $[n,k,d]$-código lineal, puede corregir $\left[\frac{1}{2}(d-1)\right]$*[2] *o menos errores.*

Ejemplo 1.3.2.

- El *código de repetición binario* de longitud $n \geq 1$, es un $[n,1,n]$-código lineal sobre $\mathbb{F}_2$ dado por:

$$Rep(n) := \{(0,0,\ldots,0),(1,1,\ldots,1)\}$$

- Los códigos de Hamming son de suma importancia en la teoría de códigos, unos de los más famosos es el $[7,4,3]$-código lineal binario de Hamming $\mathcal{H}_3$ o *código simplex*.

$$\begin{aligned}\mathcal{H}_3 = \{&(0000000),(1000011),(1100110),(0100101),(0110011),\\ &(1110000),(1010101),(0010110),(0011001),(1011010),\\ &(1111111),(0111100),(0101010),(1101001),(1001100),(0001111)\}\end{aligned}$$

La dimensión de $\mathcal{H}_3$ es 4 puesto que coincide con el núcleo de la matriz:

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

esta matriz, es llamada *matriz de chequeo de paridad*, en [12] se abordan con mayor profundidad el estudio de estos códigos y las matrices asociadas a éstos.

- El código $C_2 = \{(00|00),(10|01),(01|10),(11|11)\}$ es un $[4,2]$-código lineal sobre $\mathbb{F}_2$. Hemos separado a cada palabra código de C en $t = 2$ bloques formados por $s = 2$ símbolos así, aplicando $\sigma^{\otimes 2}$ tenemos que:

$$\begin{aligned}\sigma^{\otimes 2}(00|00) &= (\overline{\sigma}(00)\overline{\sigma}(00)) = (0000)\\ \sigma^{\otimes 2}(10|01) &= (\overline{\sigma}(10)\overline{\sigma}(01)) = (0110)\\ \sigma^{\otimes 2}(01|10) &= (\overline{\sigma}(01)\overline{\sigma}(10)) = (1001)\\ \sigma^{\otimes 2}(11|11) &= (\overline{\sigma}(11)\overline{\sigma}(11)) = (1111),\end{aligned}$$

por consiguiente, $\sigma^{\otimes 2}(C) = C$, y en consecuencia, C es un código cuasi-cíclico de índice 2 y longitud 4.

2 Aquí $[\frac{1}{2}(d-1)]$ denota al máximo entero menor o igual que $\frac{1}{2}(d-1)$.

- Un ejemplo muy famoso de códigos sobre $\mathbb{F}_2$, son los famosos *códigos de Reed-Müller*, dichos códigos poseen diversas construcciones, como la construcción $(u|u+v)$ de Plotkin o mediante el uso de *polinomios Booleanos* (cf. [15] y [17]).

  Dados m un entero positivo y r un entero no negativo tal que $r \leq m$, un código de Reed-Müller denotado por $\mathcal{R}(r,m)$ es un $[2^m, r, 2^{m-r}]$- código lineal y si $r \neq m$ todas las palabras de $\mathcal{R}(r,m)$ tienen peso par.

$$\begin{aligned}\mathcal{R}(1,3) := \{&00000000, 11111111, 00001111, 00110011, 01010101, 00111100,\\ &01011010, 01100110, 01101001, 11110000, 11001100, 10101010,\\ &11000011, 10100101, 10011001, 10010110\}\end{aligned}$$

1.3.2 Códigos cuaternarios

Definición 1.3.3. (i) Decimos que un código C es *cuaternario* si su alfabeto es $\mathbb{Z}_4$ o $\mathbb{F}_{2^2}$, y diremos que es *cuaternario lineal* si es un $\mathbb{Z}_4$-módulo, o bien un $\mathbb{F}_2$-espacio vectorial respectivamente.

(ii) El *peso de Lee* en $\mathbb{Z}_4$ lo denotamos $w_L(x)$ y está dado por:

$$\begin{aligned} w_L : \mathbb{Z}_4 &\to \mathbb{Z} \\ 0 \mapsto 0 \quad & 2 \mapsto 2 \\ 1 \mapsto 1 \quad & 3 \mapsto 1 \end{aligned} \tag{1.3.1}$$

(iii) Para cada $k \in \{1,2,3\}$, si $\underline{x} \in \mathbb{Z}_4^n$ definimos:

$$w_k(\underline{x}) := |\{0 \leq j \leq n-1 \mid x_j = k\}| \tag{1.3.2}$$

(iv) El peso y la distancia de Lee en $\mathbb{Z}_4^n$ son respectivamente:

$$\mathbf{w}_L(\underline{x}) := \sum_{j=0}^{n-1} w_L(x_j) \tag{1.3.3}$$

$$\mathbf{d}_L(\underline{x}, \underline{y}) := \sum_{j=0}^{n-1} w_L(x_j - y_j) \tag{1.3.4}$$

Observación 1.3.4. La *distancia de Lee* sólo puede calcularse en códigos cuaternarios lineales, más aún el concepto de *distancia mínima* se extiende a la distancia de Lee de manera usual:

$$\delta_C := \text{mín}\{w_L(\underline{c}) \in C \mid \underline{c} \neq \underline{0}\}.$$

Lema 1.3.5. *Sean* $\underline{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{Z}_4^n$, $\underline{y} = (y_0, \ldots, y_{n-1}), \underline{z} = (z_0, \ldots, z_{n-1}) \in \mathbb{F}_2^n$. *Entonces:*

(i) $\mathbf{w}_L(\underline{x}) = w_1(\underline{x}) + 2w_2(\underline{x}) + w_3(\underline{x})$.

(ii) $w_H(\underline{y} + \underline{z}) = w_H(\underline{y}) + w_H(\underline{z}) - 2w_H(\underline{y} \cap \underline{z})$

(iii) Si denotamos mediante $(\underline{y}, \underline{z}) \in \mathbb{F}_2^{2n}$ *a la concatenación de* $\underline{y}$ *y* $\underline{z}$ *se consigue que:*

$$w_H(\underline{y}, \underline{z}) = w_H(\underline{y}) + w_H(\underline{z})$$

Demostración. (i) Veamos que en $\mathbb{Z}_4$: $w_L(x_i) = w_1(x_i) + 2w_2(x_i) + w_3(x_i)$, para esto observe la Figura 1.

x	$w_1(x)$	$w_2(x)$	$w_3(x)$	$w_1(x) + 2w_2(x) + w_3(x)$	$w_L(x)$
0	0	0	0	0	0
1	1	0	0	1	1
2	0	1	0	2	2
3	0	0	1	1	1

Figura 1.: Peso de Lee en $\mathbb{Z}_4$.

Por otro lado, aplicando (1.3.3):

$$\begin{aligned}
\mathbf{w}_L(\underline{x}) &= \sum_{i=0}^{n-1} \mathbf{w}_L(x_i) \\
&= \sum_{i=0}^{n-1} \left[w_1(x_i) + 2w_2(x_i) + w_3(x_i) \right] \\
&= \sum_{i=0}^{n-1} w_1(x_i) + 2\sum_{i=0}^{n-1} w_2(x_i) + \sum_{i=0}^{n-1} w_3(x_i) \\
&= w_1(\underline{x}) + 2w_2(\underline{x}) + w_3(\underline{x}).
\end{aligned}$$

(ii) Sean $w_H(\underline{y}) = p$ y $w_H(\underline{z}) = q$, supóngase, sin pérdida de generalidad que, $0 \leq p \leq q \leq n$. Si $0 = p = q$ entonces $\underline{y} = \underline{0} = \underline{z}$ y el resultado es trivialmente cierto. Si $0 = p < q$ entonces $\underline{y} = \underline{0}$, $\underline{y} + \underline{z} = \underline{z}$ y $\underline{y} \cap \underline{z} = \underline{0}$ y el resultado se sigue nuevamente. Ahora, si $0 < p \leq q$ y $w_H(\underline{y} \cap \underline{z}) = r$ entonces ambas palabras-código coinciden en r componentes, así que al sumar $\underline{y}$ con $\underline{z}$ el vector resultante tiene r ceros y por consiguiente hay $(p - r)$ coordenadas con $1's$ que son aportados por $\underline{y}$ y $(q - r)$ coordenadas con $1's$ aportados por $\underline{z}$, luego:

$$\begin{aligned}
w_H(\underline{y} + \underline{z}) &= (p - r) + (q - r) \\
&= p + q - 2r \\
&= w_H(\underline{y}) + w_H(\underline{y}) - 2w_H(\underline{y} \cap \underline{z}).
\end{aligned}$$

(iii) Notemos que:

$$(\underline{y}, \underline{z}) = (\underline{y}, \underline{0}) + (\underline{0}, \underline{z}).$$

El resultado se sigue trivialmente de (ii). □

Ejemplo 1.3.6. • El código

$$C_1 = \{(0000), (1111), (2222), (3333), (0202), (1313), (2020), (3131)\}$$

es un código cuaternario cíclico lineal de longitud 4, así que aplicando el Lema 1.3.5, podemos hallar el peso de Lee de cada palabra código.

$\underline{c}$	$w_1(\underline{c})$	$w_2(\underline{c})$	$w_3(\underline{c})$	$\mathbf{w}_L(\underline{c})$
(0000)	0	0	0	0
(1111)	4	0	0	4
(2222)	0	4	0	8
(3333)	0	0	4	4
(0202)	0	2	0	4
(1313)	2	0	2	4
(2020)	0	2	0	4
(3131)	2	0	2	4

luego, como C_1 es un código lineal, se sigue que la distancia mínima de Lee δ_{C_1} es 4.

- Un código cuaternario puede estar determinado por una matriz como en el Ejemplo 1.3.2. Sea

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

el código C_2 resulta de las filas de G, es decir, $G = \langle (02), (20) \rangle$ de ahí que:

$$C_2 = \{(00), (20), (02), (22)\}$$

y los pesos de Lee de sus palabras código son:

$\underline{c}$	$\mathbf{w}_L(\underline{c})$	$\underline{c}$	$\mathbf{w}_L(\underline{c})$
(00)	0	(02)	2
(20)	2	(22)	4

De ahí que C_2 es un $[2, 2]$- código cíclico lineal con distancia mínima 2.

1.3.3 Códigos sobre anillos de Galois

Sea $R = GR(p^s, m)$ donde p es un número primo y s, m son enteros positivos. Como se ha mencionado antes, R es un anillo finito de cadena de índice de nilpotencia s, es decir la cadena:

$$(0) \subset (p^{s-1}) \subset \cdots \subset (p^2) \subset (p) \subset (1) = R \tag{1.3.5}$$

enlista y ordena a todos los ideales de R, haciendo uso de estose introduce la siguiente:

Definición 1.3.7. Sea $R = GR(p^s, m)$, se define (ver [6]):

(i) El *peso homogéneo* en R como:

$$w_{hom}(c) = \begin{cases} (p^m - 1)p^{m(s-2)} & \text{si } c \in R \setminus (p^{s-1}) \\ p^{m(s-1)} & \text{si } c \in (p^{s-1}) \setminus (0) \\ 0 & \text{si } c = 0. \end{cases} \tag{1.3.6}$$

(ii) La *distancia homogénea* en R:

$$d_{hom}(c, d) = w_{hom}(c - d). \tag{1.3.7}$$

(iii) El peso homogéneo de $\underline{c}$ en un R-código C:

$$\mathbf{w}_{hom}(\underline{c}) = \sum_{i=0}^{n-1} w_{hom}(c_i). \tag{1.3.8}$$

(iv) La distancia homogénea entre dos palabras código $\underline{c}$ y $\underline{d}$ de un R-código C:

$$\mathbf{d}_{hom}(\underline{c}, \underline{d}) = \sum_{i=0}^{n-1} d_{hom}(c_i, d_i) \tag{1.3.9}$$

El peso homogéno y la distancia homogénea definidos en este apartado resultan herramientas de gran utilidad en el estudio de los códigos definidos sobre *anillos finitos de cadena* en general, por dicho motivo al ser los anillos de Galois pertenecientes a esta familia analizaremos sus propiedades. (cf. [4],[6])

Lema 1.3.8. *Para cada $c, d \in R$:*

(i) $w_{hom}(c) \geq 0$.

(ii) $w_{hom}(c) = 0$ *si y sólo si* $c = 0$.

(iii) $w_{hom}(c) = w_{hom}(-c)$.

(iv) $w_{hom}(c+d) \leq w_{hom}(c) + w_{hom}(d)$.

Demostración. (i) y (ii) son inmediatas de (1.3.6).

(iii) Si $c = 0$ entonces $-c = 0$ y se tiene el resultado. Por otro lado si $c \neq 0$ y $c \in (p^{s-1})$, como éste es un ideal entonces es un subgrupo aditivo de $(R, +)$, luego $-c \in (p^{s-1})$ y nuevamente se tiene el resultado. Si por el contrario $c \notin (p^{s-1})$ entonces éste es una unidad, luego existe $u \in R$ tal que $cu = 1$, pero tenemos que $(-c)(-u) = cu = 1$, es decir $-c$ es también una unidad y así se confirma que para todo $c \in R$:

$$w_{hom}(c) = w_{hom}(-c).$$

(iv) Tenemos los siguientes casos:

CASO 1: $(c = d = 0)$. Aquí es claro que:

$$w_{hom}(c+d) = w_{hom}(c) = w_{hom}(c) + 0 = w_{hom}(c) + w_{hom}(d).$$

CASO 2: $(c = 0$ o $d = 0)$. Sin pérdida de generalidad, supongamos que $c \neq 0$.

$$w_{hom}(c+d) = w_{hom}(c) = w_{hom}(c) + 0 = w_{hom}(c) + w_{hom}(d).$$

CASO 3: $(c \neq 0, d \neq 0)$. Tenemos tres subcasos:

SUBCASO 1: $(c, d \in (p^{s-1}))$. Si esto ocurre, entonces $c + d \in (p^{s-1})$ pues éste es un ideal, así:

$$w_{hom}(c+d) = p^{m(s-1)} < p^{m(s-1)} + p^{m(s-1)} = w_{hom}(c) + w_{hom}(d).$$

SUBCASO 2: $(c, d \notin (p^{s-1}))$. Puede ocurrir que $c + d = 0$, $c + d \notin (p^{s-1})$ o por otro lado que $c + d \in (p^{s-1})$, en el primer caso es trivial, para el segundo se sigue que:

$$\begin{aligned} w_{hom}(c+d) &= (p^m - 1)p^{m(s-2)} \\ &< (p^m - 1)p^{m(s-2)} + (p^m - 1)p^{m(s-2)} \\ &= w_{hom}(c) + w_{hom}(d). \end{aligned}$$

Mientras que en el tercer caso consideremos que:

$$\begin{aligned} 2 &\leq p^m \\ 2 + p^m &\leq 2p^m \\ p^m &\leq 2(p^m - 1) \\ p^{m(s-1)} &\leq 2(p^m - 1)p^{m(s-2)} \\ w_{hom}(c+d) &\leq w_{hom}(c) + w_{hom(d)}. \end{aligned}$$

SUBCASO 3: ($c \in (p^{s-1}), d \notin (p^{s-1})$). Puede suceder que $c + d \in (p^{s-1})$, o bien, $c + d \notin (p^{s-1})$. Si ocurre lo primero, como $(p^m - 1)p^{m(s-2)} \geq 0$ entonces:

$$\begin{aligned} w_{hom}(c+d) &= p^{m(s-1)} \\ &\leq p^{m(s-1)} + (p^m - 1)p^{m(s-2)} \\ &= w_{hom}(c) + w_{hom}(d). \end{aligned}$$

Si ocurre lo segundo, notemos que también $p^{m(s-1)} \geq 0$ y así:

$$\begin{aligned} w_{hom}(c+d) &= (p^m - 1)p^{m(s-2)} \\ &\leq p^{m(s-1)} + (p^m - 1)p^{m(s-2)} \\ &= w_{hom}(c) + w_{hom}(d). \end{aligned}$$

Por lo tanto, para todos $c, d \in R$:

$$w_{hom}(c+d) \leq w_{hom}(c) + w_{hom}(d).$$

□

Corolario 1.3.9. *(i) Para todo $n \geq 1$. $(R^n, \mathbf{d}_{hom})$ es un espacio métrico.*

(ii) Para todo $c \in R$ y $u \in R^*$: $w_{hom}(c) = w_{hom}(uc)$.

Demostración. (i) Por el Lema 1.3.8, d_{hom} satiface los axiomas de una métrica, luego también lo hace $\mathbf{d}_{hom}$ por ser ésta una extensión de d_{hom}.

(ii) Tenemos cuatro casos:

CASO 1: ($c = 0$) Entonces para todo $u \in R^*$: $uc = 0$ así $w_{hom}(c) = 0 = w_{hom}(uc)$.

CASO 2: ($c \in R^*$) Sea $u \in R^*$, luego $uc \in R^*$ y es claro que $w_{hom}(c) = w_{hom}(uc)$.

CASO 3: ($c \in (p^k)$, $1 \leq k \leq s-2$) Dado que $u \in R^*$ y como cada (p^k) es un ideal distinto de (p^{s-1}) es claro que $uc \in (p^k) \neq (p^{s-1})$ y se tiene la afirmación.

CASO 4: ($c \in (p^{(s-1)}) \setminus (0)$). Como éste es un ideal entonces $uc \in (p^{s-1}) \setminus (0)$ para cualquier $u \in R^*$ de dónde se sigue el resultado.

□

Para finalizar la sección apliquemos algunos de estos conceptos en el anillo de Galois $R = GR(p^3, m)$. Como ya mencionamos R es tal que:

- Todos sus ideales son:
$$(0) \subset (p^2) \subset (p) \subset R$$
- Existe un elemento $\xi \neq 0$ de orden $p^m - 1$, tal que para todo $c \in R$:
$$c = \rho_0(c) + p\rho_1(c) + p^2\rho_2(c)$$
donde $\rho_k(c) \in \mathcal{T} = \{0, 1, \xi, \ldots \xi^{p^m-2}\}$, su representación p-ádica.
- El grupo de unidades de R, es un grupo abeliano multiplicativo de cardinalidad $(p^m - 1)p^{2m}$.
- El peso homogéneo en R es:
$$w_{hom}(c) = \begin{cases} (p^m - 1)p^m & \text{si } c \in R \setminus (p^2) \\ p^{2m} & \text{si } c \in (p^2) \setminus (0) \\ 0 & \text{si } c = 0 \end{cases}$$

Ejemplo 1.3.10. Sean $p = 2$, $m = 3$, $n = 3$ entonces:
$$R \simeq \frac{\mathbb{Z}_8[x]}{(x^3 + x + 1)}.$$
Los elementos del anillo son *clases de equivalencia* de polinomios de grado a lo más dos con coeficientes en $\mathbb{Z}_8$, así que usaremos unicamente a los representantes de dichas clases como los elementos de R, es decir:
$$R := \left\{ a_0 + a_1 x + a_2 x^2 \mid a_k \in \mathbb{Z}_8,\ (0 \leq k \leq 2) \right\}.$$
El siguiente conjunto C es un $(3, 6)$-código sobre $GR(2^3, 3)$:
$$C := \left\{ (2x, x, x^2), (5x^2, 2x, x), (5x, 5x^2, 2x), (2x, 5x, 5x^2), (x^2, 2x, 5x), (x, x^2, 2w) \right\}.$$
El peso homogéneo de los elementos de $GR(2^3, 3)$ está dado por:
$$w_{hom}(c) = \begin{cases} 56 & \text{si } c \in R \setminus (4) \\ 64 & \text{si } c \in (4) \setminus (0) \\ 0 & \text{si } c = 0 \end{cases}$$
y la siguiente tabla exhibe el peso homógeneo de cada palabra código de C.

$\underline{c}$	$w_{hom}(\underline{c})$	$\underline{c}$	$w_{hom}(\underline{c})$
$(2x, x, x^2)$	168	$(2x, 5x, 5x^2)$	168
$(5x^2, 2x, x)$	168	$(x^2, 2x, 5x)$	168
$(5x, 5x^2, 2x)$	168	$(x, x^2, 2x)$	168

1.4 ANILLO DE VECTORES DE WITT

En esta sección analizaremos la construcción del anillo de vectores de Witt y el isomorfismo entre el anillo truncado de vectores de Witt y el anillo de Galois $GR(p^s, m)$. Dicho análisis se encuentra basado en [5], [7] y [10].

Consideremos $\mathcal{Q} = \mathbb{Q}[x_i, y_j, z_k]$ con $i, j, k \in \mathbb{N} \cup \{0\}$ y $\mathcal{Q}^{\mathbb{N}}$ el anillo de las sucesiones infinitas $a = (a_\nu) = (a_0, a_1, \ldots, a_{n-1}, \ldots)$ tales que $a_\nu \in \mathcal{Q}$ para $\nu \in \mathbb{N} \cup \{0\}$ dotado de las operaciones suma y producto componente a componente y los elementos $(0) = (0, 0, \ldots, 0, \ldots)$ y $(1) = (1, 1, \ldots, 1 \ldots)$, como los neutros de éstas operaciones respectivamente.

Dotaremos a $\mathcal{Q}^{\mathbb{N}}$ de dos nuevas operaciones *suma* y *producto*. Así, dada una sucesión $a \in \mathcal{Q}^{\mathbb{N}}$ y p un número primo, definimos:

$$\begin{aligned} P : \mathcal{Q}^{\mathbb{N}} &\to \mathcal{Q}^{\mathbb{N}} \\ a &\mapsto P(a) := (a_0^p, a_1^p, \ldots, a_{n-1}^p, \ldots), \end{aligned}$$

y para cada $\nu \in \mathbb{N} \cup \{0\}$ las relaciones:

$$a^{(0)} = a_0 \quad \text{y} \quad a^{(\nu+1)} = (P(a))^{(\nu)} + p^{\nu+1} a_{\nu+1}. \tag{1.4.1}$$

Es fácil ver que de (1.4.1):

$$\begin{aligned} a^{(1)} &= a_0^p + p a_1 \\ a^{(2)} &= a_0^{p^2} + p a_1^p + p^2 a_2 \\ \vdots \quad &\vdots \qquad\qquad \vdots \\ a^{(\nu)} &= a_0^{p^\nu} + p a_1^{p^{\nu-1}} + \cdots + p^{\nu-1} a_{\nu-1}^p + p^\nu a_\nu. \end{aligned}$$

Con todo esto, definimos las funciones:

$$\begin{aligned} \phi : \mathcal{Q}^{\mathbb{N}} &\to \mathcal{Q}^{\mathbb{N}} \\ a &\mapsto \phi(a) := (a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots), \\ \psi : \mathcal{Q}^{\mathbb{N}} &\to \mathcal{Q}^{\mathbb{N}} \\ b &\mapsto \psi(b) := (c_0, c_1, \ldots, c_{n-1}, \ldots), \end{aligned}$$

donde:

$$\begin{aligned} c_0 &= b_0 \\ c_1 &= \frac{1}{p}\left(b_1 - c_0^p\right) \\ c_2 &= \frac{1}{p^2}\left(b_2 - c_0^{p^2} - pc_1^p\right) \\ &\vdots \\ c_{\nu-1} &= \frac{1}{p^{\nu-1}}\left(b_{\nu-1} - c_0^{p^{\nu-1}} - pc_1^{p^{\nu-2}} - \cdots - p^{\nu-2}c_{\nu-2}^p\right). \end{aligned} \tag{1.4.2}$$

El siguiente lema nos muestra la estrecha relación entre las funciones ϕ y ψ.

Lema 1.4.1. *La función ϕ es una biyección y $\phi^{-1} = \psi$.*

Demostración. Sea $a = (a_0, a_1, \ldots, a_{n-1}, \ldots) \in \mathcal{Q}^{\mathbb{N}}$, entonces:

$$\begin{aligned} \psi\phi(a) &= \psi(a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots) \\ &= \psi(a_0, a_0^p + pa_1, \ldots, a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-2}a_{n-2}^p + p^{n-1}a_{n-1}, \ldots) \\ &= (c_0, c_1, \ldots, c_{n-1}, \ldots). \end{aligned}$$

Demostraremos por inducción que $c_i = a_i$ para $i \in \{0, 1, \ldots\}$.

Si $i = 0$ se sigue de (1.4.1) que $c_0 = a_0$. Ahora supongamos que para cada $i < n-1$, $c_i = a_i$ entonces por (1.4.2):

$$\begin{aligned} c_{n-1} &= \frac{1}{p^{n-1}}\left(a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-2}a_{n-2}^p + p^{n-1}a_{n-1} - c_0^{p^{n-1}} - pc_1^{p^{n-2}} - \cdots - p^{n-2}c_{n-2}^p\right) \\ &= \frac{1}{p^{n-1}}\left(a_0^{p^{n-1}} + pa_1^{p^{n-2}} + \cdots + p^{n-2}a_{n-2}^p + p^{n-1}a_{n-1} - a_0^{p^{n-1}} - pa_1^{p^{n-2}} - \cdots - p^{n-2}a_{n-2}^p\right) \\ &= \frac{1}{p^{n-1}}\left(p^{n-1}a_{n-1}\right) = a_{n-1}, \end{aligned}$$

de ahí que: $\psi\phi(a) = (c_0, c_1, \ldots, c_{n-1}, \ldots) = a$. Por otro lado, sea $b = (b_0, b_1, \ldots, b_{n-1}, \ldots)$. Entonces:

$$\phi\psi\,(b) = \phi\,(c_0, c_1, \ldots, c_{n-1} \ldots) = \left(c^{(0)}, c^{(1)}, \ldots, c^{(n-1)}\right).$$

Nuevamente mediante inducción probaremos que $c^{(i)} = b_i$ para cada $i \in \{0, 1, \ldots\}$, como se dijo antes, por (1.4.1) se tiene que $c_0 = b_0$. Si

suponemos que para $i < n-1$, $c^{(i)} = b_i$ y sustituimos a c_{n-1} según (1.4.2) tenemos que:

$$\begin{aligned}
c^{(n-1)} &= c_0^{p^{n-1}} + pc_1^{p^{n-2}} + \cdots + p^{n-2}c_{n-2}^{p} \\
&\quad + p^{n-1}\left(\tfrac{1}{p^{n-1}}\left(b_{n-1} - c_0^{p^{n-1}} - pc_1^{p^{n-2}} - \cdots - p^{n-2}c_{n-2}^{p}\right)\right) \\
&= \cancel{c_0^{p^{n-1}}} + \cancel{pc_1^{p^{n-2}}} + \cdots + \cancel{p^{n-2}c_{n-2}^{p}} + b_{n-1} - \cancel{c_0^{p^{n-1}}} - \cancel{pc_1^{p^{n-2}}} - \cdots - \cancel{p^{n-2}c_{n-2}^{p}} \\
&= b_{n-1}
\end{aligned}$$

de lo anterior, se concluye que $\psi\phi(b) = (b_0, b_1, \ldots, b_{n-1}, \ldots) = b$, y se sigue el resultado. □

Dado que la función ϕ, resulta ser una biyección en $\mathcal{Q}^{\mathbb{N}}$, podemos inducir una nueva estructura de anillo, mediante la definición de nuevas operaciones suma y producto, como lo haremos en la siguiente proposición. Si el lector desea revisar una demostración detallada de esta afirmación puede consultar el Teorema A.1.1.

Proposición 1.4.2. *Dados $a, b \in \mathcal{Q}^{\mathbb{N}}$ definimos:*

$$\begin{aligned}
a \oplus b &:= \psi\left(\phi(a) + \phi(b)\right) \\
a \odot b &:= \psi\left(\phi(a) \cdot \phi(b)\right)
\end{aligned}$$

*entonces $(\mathcal{Q}^{\mathbb{N}}, \oplus, \odot)$ es un anillo conmutativo con identidad $(1, 0, \ldots, 0, \ldots)$, neutro de la suma $(0, 0, \ldots, 0, \ldots)$ al cual llamaremos **anillo de vectores de Witt**, lo denotaremos por $W(\mathcal{Q})$, y sus elementos neutro de la suma e identidad se denotarán por $\mathbf{0}$ y $\mathbf{1}$ respectivamente.*

Nótemos que por la Proposición 1.4.2 y la biyectividad de ϕ:

$$\begin{aligned}
\phi(a \oplus b) &= \phi(a) + \phi(b) \\
\phi(a \odot b) &= \phi(a)\phi(b).
\end{aligned}$$

Ahora, de la definición de ϕ, si $c = a \oplus b$ y $d = a \odot b$ entonces:

$$\begin{aligned}
(c^{(0)}, c^{(1)}, \ldots, c^{(n-1)}, \ldots) &= (a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots) + (b^{(0)}, b^{(1)}, \ldots, b^{(n-1)}, \ldots), \\
(d^{(0)}, d^{(1)}, \ldots, d^{(n-1)}, \ldots) &= (a^{(0)}, a^{(1)}, \ldots, a^{(n-1)}, \ldots) \cdot (b^{(0)}, b^{(1)}, \ldots, b^{(n-1)}, \ldots),
\end{aligned}$$

por consiguiente para cada $\nu \geq 0$:

$$\begin{aligned}
(a \oplus b)^{(\nu)} &= a^{(\nu)} + b^{(\nu)} \\
(a \odot b)^{(\nu)} &= a^{(\nu)} b^{(\nu)}.
\end{aligned} \tag{1.4.3}$$

Lema 1.4.3. *Sean $m \geq 1$, $0 \leq i, j, k \leq n-1$, $a = (a_\nu), b = (b_\nu)$ tales que $a_\nu, b_\nu \in \mathbb{Z}[x_i, y_j]$ con $0 \leq \nu \leq m-1$. Entonces:*

$$a_\nu \equiv b_\nu \pmod{p^m} \qquad (0 \leq \nu \leq k)$$

si y sólo si:

$$a^{(\nu)} \equiv b^{(\nu)} \pmod{p^{m+\nu}} \qquad (0 \leq \nu \leq k).$$

Demostración. Ya que $\mathbb{Z} \subset \mathbb{Q}$, tenemos que $a, b \in W(\mathcal{Q})$ y así haremos inducción sobre $k \geq 0$.

Para $k = 0$ tenemos que $a^{(0)} = a_0$ y $b^{(0)} = b_0$ entonces $a_0 \equiv b_0 \pmod{p^m}$ si y sólo si $a^{(0)} \equiv b^{(0)} \pmod{p^{m+0}}$.

De (1.4.1) tenemos que para $k > 0$:

$$\begin{aligned} a^{(k)} &= (P(a))^{(k-1)} + p^k a_k \\ b^{(k)} &= (P(b))^{(k-1)} + p^k b_k, \end{aligned} \tag{1.4.4}$$

y supongamos que el resultado es válido para $\nu \leq k-1$. Es claro que:

$$a_k \equiv b_k \pmod{p^m} \text{ si y sólo si } p^k a_k \equiv p^k b_k \pmod{p^{m+k}}. \tag{1.4.5}$$

Entonces resulta suficiente demostrar que bajo la hipótesis inductiva:

$$(P(a))^{(k-1)} \equiv (P(b))^{(k-1)} \pmod{p^{m+k}},$$

para llegar al resultado. En efecto si $a_\nu \equiv b_\nu \pmod{p^m}$ tenemos que:

$$\begin{aligned} a_\nu &= l p^m + b_\nu \\ (a_\nu)^p &= (l p^m + b_\nu)^p \\ &= l^p p^{mp} + \sum_{i=1}^{p-1} \tbinom{p}{i} (l p^m)^i (b_\nu)^{p-i} + (b_\nu)^p \end{aligned}$$

dado que $p \mid \binom{p}{i}$ para $1 \leq i \leq p$ se sigue que:

$$\begin{aligned} a_\nu^p - b_\nu^p &= l^p p^{mp} + p^{m+1} \sum_{i=1}^{p-1} t_i l^i p^{m(i-1)} (b_\nu)^{p-i} \\ &= p^{m+1} \left[l^p p^{m(p-1)-1} + \sum_{i=1}^{p-1} t_i l^i p^{m(i-1)} (b_\nu)^{p-i} \right] \end{aligned}$$

donde $t_i = \frac{1}{p}\binom{p}{i}$, para $1 \leq i \leq p-1$, por consiguiente, $a_\nu^p \equiv b_\nu^p \pmod{p^{m+1}}$ y esto se sigue para $0 \leq \nu \leq k-1$. Por otro lado, como

$P(a) = (a_0^p, a_1^p, \ldots, a_{n-1}^p, \ldots)$ y $P(b) = (b_0^p, b_1^p, \ldots, b_{n-1}^p, \ldots)$ entonces por lo anterior si denotamos $P(a)_\nu = a_\nu^p$ y $P(b)_\nu = b_\nu^p$ entonces:

$$P(a)_\nu \equiv P(b)_\nu \pmod{p^{m+1}}$$

y por hipótesis inductiva, esto equivale a:

$$P(a)^{(\nu)} \equiv P(b)^{(\nu)} \pmod{p^{m+1+\nu}} \qquad (0 \leq \nu \leq k-1)$$

en particular para $\nu = k-1$ tenemos que $P(a)^{(k-1)} \equiv P(b)^{(k-1)}$ (mód p^{m+k}) como queríamos y así sumando lo anterior con (1.4.5): $P(a)^{(k-1)} + p^k a_k \equiv P(b)^{(k-1)} + p^k b_k$ (mód p^{m+k}) y combinando con (1.4.4)

$$a_k \equiv b_k \pmod{p^m} \Leftrightarrow a^{(k)} \equiv b^{(k)} \pmod{p^{m+k}} \qquad (0 \leq \nu \leq k)$$

□

Con los resultados anteriores estamos listos para el siguiente:

Teorema 1.4.4. *Sean $a, b \in W(\mathcal{Q})$. Si $a \circ b$ representa: $a \oplus b$ o $a \odot b$ y $a \hat{\circ} b$ $a + b$ o $a \cdot b$ respectivamente, entonces $(a \circ b)_\nu = f_\nu(a_i, b_j)$ donde $f_\nu(x_i, y_j)$ es un polinomio con coeficientes enteros y término constante 0 en las variables x_i, y_j donde $0 \leq i, j \leq \nu$.*

Demostración. Por definición, $(a \circ b)_\nu = f_\nu(a_i, b_j)$ donde el polinomio $f_\nu(x_i, y_j) \in \mathbb{Q}[x_i, y_j]$, luego resta demostrar por inducción sobre $\nu \geq 0$ que $f_\nu(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$. Si $\nu = 0$, es evidente que $(a \circ b)_0 = a_0 \hat{\circ} b_0$ luego si tomamos $f_0(x_i, y_j) = x_i \hat{\circ} y_j \in \mathbb{Z}[x_i, y_j]$ tenemos el resultado.

Supongamos que el resultado es válido para $(a \circ b)_k$ con $0 \leq k \leq \nu - 1$ y consideremos (1.4.1), entonces:

$$p^\nu (a \circ b)_\nu = (a \circ b)^{(\nu)} - (P(a \circ b))^{(\nu-1)}. \tag{1.4.6}$$

Por hipótesis inductiva, si $0 \leq k \leq \nu - 1$, $(a \circ b)_k$ corresponde a algún polinomio $f_k(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$ así, por el Corolario A.2.5 tenemos que $(a \circ b)_k^p$ corresponde a algún polinomio $\hat{f}_k(x_i^p, y_j^p) = \hat{f}(P(x_i), P(y_j))$ (mód p), por consiguiente:

$$P(a \circ b)_k \equiv (P(a) \circ P(b))_k \pmod{p} \qquad (0 \leq k \leq \nu - 1),$$

y así, por el Lema 1.4.3, esto equivale a:

$$(P(a \circ b))^{(\nu-1)} \equiv (P(a) \circ P(b))^{(\nu-1)} \pmod{p^\nu}. \tag{1.4.7}$$

De (1.4.1) se sigue que $a^{(\nu)} \equiv (P(a))^{(\nu-1)}$ (mód p^ν) y $b^{(\nu)} \equiv (P(b))^{(\nu-1)}$ (mód p^ν) luego por (1.4.3):

$$\begin{aligned}(a \circ b)^{(\nu)} = a^{(\nu)} \hat{\circ}\, b^{(\nu)} &\equiv (P(a))^{(\nu-1)} \hat{\circ} (P(b))^{(\nu-1)} \pmod{p^\nu} \\ &\equiv (P(a) \circ P(b))^{(\nu-1)} \pmod{p^\nu}.\end{aligned} \tag{1.4.8}$$

Combinando (1.4.7) y (1.4.8) tenemos que p^ν es un factor de la diferencia de los polinomios que corresponden a $(a \circ b)^{(\nu)}$ y $(P(a \circ b))^{(\nu-1)}$, se sigue de (1.4.6) que $(a \circ b)_\nu$ está asociado a un polinomio $g_\nu(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$ módulo p como queríamos demostrar. □

En virtud del teorema anterior para $(a_\nu), (b_\nu) \in W(\mathcal{Q})$ denotaremos en lo sucesivo:

$$\begin{aligned}(a \oplus b)_\nu &= s_\nu(a_0, a_1, \ldots, a_{\nu-1}, b_0, b_1, \ldots, b_{\nu-1}) = s_\nu(a_i, b_j) \\ (a \odot b)_\nu &= m_\nu(a_0, a_1, \ldots, a_{\nu-1}, b_0, b_1, \ldots, b_{\nu-1}) = m_\nu(a_i, b_j),\end{aligned} \tag{1.4.9}$$

donde $s_\nu, m_\nu \in \mathbb{Z}[x_i, y_j]$ para $\nu \geq 0$.

Sea A un anillo conmutativo con identidad 1_A, dado que $\mathbb{Z} \subseteq \mathbb{Q}$ es claro que $\mathbb{Z}[x_i, y_j, z_k] \subseteq \mathbb{Q}[x_i, y_j, z_k]$, así puede ser sumergido en el anillo de polinomios $A[X_i, Y_j, Z_k]$ mediante:

$$\begin{aligned}\lambda : \mathbb{Z}[x_i, y_j, z_k] &\to A[X_i, Y_j, Z_k] \\ n &\mapsto n1_A \qquad (n \in \mathbb{Z}) \\ x_i &\mapsto X_i \\ y_j &\mapsto Y_j \\ z_k &\mapsto Z_k.\end{aligned}$$

Dado un polinomio $f(x_i, y_j, z_k) \in \mathbb{Z}[x_i, y_j, z_k]$ denotemos por $\hat{f}(X_i, Y_j, Z_k)$ a $\lambda\left(f(x_i, y_j, z_k)\right)$. Por otro lado, a la luz del Teorema 1.4.4, las operaciones $\oplus$, $\odot$ son cerradas al tomar $a, b \in \mathbb{Z}[x_i, y_j, z_k]^{\mathbb{N}}$ y $\mathbf{0}, \mathbf{1} \in \mathbb{Z}[x_i, y_j, z_k]^{\mathbb{N}}$, es decir, éste es un subanillo de $W(\mathcal{Q})$ que denotaremos por $W(\mathbb{Z})$. Ahora consideremos los conjuntos de sucesiones infinitas: $A^{\mathbb{N}}$ y $(\lambda(\mathbb{Z}[x_i, y_j, z_k]))^{\mathbb{N}}$, entonces $\lambda : \mathbb{Z}[x_i, y_j, z_k] \to \lambda(\mathbb{Z}[x_i, y_j, z_k])$, es un homomorfismo de anillos sobreyectivo y puede ser extendido de manera natural como sigue:

$$\begin{aligned}\Lambda : W(\mathbb{Z}) &\to \mathcal{A} = (\lambda(\mathbb{Z}[x_i, y_j, z_k]))^{\mathbb{N}} \\ (f_\nu(x_i, y_j, z_k)) &\mapsto (\hat{f}_\nu(X_i, Y_j, Z_k)).\end{aligned} \tag{1.4.10}$$

Nuevamente, por el Teorema 1.4.4 dadas dos sucesiones $a, b \in W(\mathbb{Z})$ existen polinomios con coeficientes enteros s_ν, m_ν que satisfacen (1.4.9), así tenemos la siguiente:

Definición 1.4.5. Dados dos elementos $r = (r_\nu), t = (t_\nu) \in \mathcal{R}$ definimos la suma y el producto de éstos como las sucesiones $r \oplus t = ((r+t)_\nu)$ y $r \odot t = ((rt)_\nu)$ tales que:

$$\begin{aligned} (r+t)_\nu &= \Lambda(s_\nu(x_i, y_j)) = \hat{s}_\nu(r_i, t_j) \\ (rt)_\nu &= \Lambda(m_\nu(x_i, y_j)) = \hat{m}_\nu(r_i, t_j), \end{aligned} \tag{1.4.11}$$

para cada $\nu \geq 0$.

Veamos que en efecto mediante las operaciones definidas antes, se puede dotar de una estructura de anillo a $\mathcal{A}$:

Teorema 1.4.6. *$\mathcal{A}$ con las operaciones $\oplus$ y $\odot$ es un anillo conmutativo con identidad $(1_A, 0_A, \ldots, 0_A, \ldots)$ y neutro de la suma $(0_A, 0_A, \ldots, 0_A, \ldots)$.*

Demostración. Sean $X = (X_0, X_1, \ldots, X_{n-1}, \ldots), Y = (Y_0, Y_1, \ldots, Y_{n-1}, \ldots)$ y $Z = (Z_0, Z_1, \ldots, Z_{n-1}, \ldots) \in \mathcal{A}$, entonces como Λ es sobreyectiva existen a saber: $x = (x_0, x_1, \ldots, x_{n-1}, \ldots)$, $y = (y_0, y_1, \ldots, y_{n-1}, \ldots)$ y $z = (z_1, z_2, \ldots, z_{n-1}, \ldots) \in \mathbb{Z}^{\mathbb{N}}$ tales que $\Lambda(x) = X$, $\Lambda(y) = Y$ y $\Lambda(z) = Z$. Luego, por (1.4.11):

$$\begin{aligned} (X+Y)_\nu &= (\hat{s}_\nu(X_i, Y_j)) = \Lambda(s_\nu(x \oplus y)_\nu) \\ (XY)_\nu &= (\hat{m}_\nu(x_i, y_j)) = \Lambda(m_\nu(x \odot y)_\nu) \end{aligned}$$

y esto se cumple para cada $\nu \geq 0$, entonces:

$$\begin{aligned} \Lambda(x) \oplus \Lambda(y) &= X \oplus Y = \Lambda(x \oplus y) \\ \Lambda(x) \odot \Lambda(y) &= X \odot Y = \Lambda(x \odot y) \end{aligned}$$

es decir, Λ preserva las operaciones entre $W(\mathbb{Z})$ y $\mathcal{A}$, en otras palabras Λ es un homomorfismo de anillos, luego por el primer teorema de isomorfismos:

$$\mathcal{A} \simeq \frac{W(\mathbb{Z})}{\ker(\Lambda)}$$

Finalmente, dado que los elementos $(1, 0, \ldots, 0, \ldots)$ y $(0, 0, \ldots, 0, \ldots)$ son la identidad y el neutro de la suma en $W(\mathcal{Q})$ (y por consiguiente en $W(\mathbb{Z})$) respectivamente, se sigue que: $\Lambda(\mathbf{1}) = (1_A, 0_A, \ldots, 0_A, \ldots)$ y $\Lambda(\mathbf{0}) = (0_A, 0_A, \ldots, 0_A, \ldots)$ son la identidad y el neutro de la suma en $\mathcal{A}$ respectivamente. □

El teorema anterior establece un hecho importante, puesto que nos ha bastado con hallar una *copia* del anillo de polinomios en varias indeterminadas (x_i, y_j, z_k) con coeficientes en $\mathbb{Z}$ para poder extender la estructura del anillo de vectores de Witt $W(\mathcal{Q})$ al conjunto de

sucesiones infinitas $\mathcal{A}$, esto resulta muy útil dado que si $\mathcal{A} = \mathbb{F}_{p^m}$ las condiciones se satisfacen de manera inmediata y nos acerca a nuestro objetivo.

Es importante reconocer la diferencia al usar $\mathbb{Z}[x_i, y_j, z_k]^{\mathbb{N}}$ y $W(\mathbb{N})$ pues el primero hace referencia a las sucesiones con las operaciones usuales de suma y producto, mientras que el segundo nos debe indicar que estamos usando la estructura inducida mediante $\oplus$ y $\odot$. El siguiente corolario es el paso final en la construcción del anillo truncado de vectores de Witt.

Corolario 1.4.7. *Sean*

$$\begin{aligned} W_{(s)}(A) &= \{(r_\nu) \in W(A) : r_\nu = 0_A, \nu \geq s\}, \\ W_s(A) &= \{(r_0, r_1, \ldots, r_{s-1}) : r_i \in A, 0 \leq i \leq s-1\}, \end{aligned}$$

y la función:

$$\begin{aligned} \tau : W_{(s)}(A) &\to W_s(A) \\ (r_\nu) &\mapsto (r_0, r_1, \ldots, r_{s-1}). \end{aligned} \tag{1.4.12}$$

Si definimos la suma $\oplus_s$ y el producto $\odot_s$ en $W_s(A)$ mediante:

$$\begin{aligned} (r_0, r_1, \ldots, r_{s-1}) \oplus_s (t_0, t_1, \ldots, t_{s-1}) &= \tau(r \oplus t), \\ (r_0, r_1, \ldots, r_{s-1}) \odot_s (t_0, t_1, \ldots, t_{s-1}) &= \tau(r \odot t). \end{aligned} \tag{1.4.13}$$

Entonces $(W_s(A), \oplus_s, \odot_s)$ es un anillo conmutativo con elemento identidad $(1_A, 0_A, \ldots, 0_A)$ y neutro de la suma $(0_A, 0_A, \ldots, 0_A)$.

Demostración. Por la Definición 1.4.5 y el Teorema 1.4.4, $W_{(s)}(A)$ es un subanillo de $W(A)$ y no resulta difícil notar que τ es una biyección entre $W_{(s)}(A)$ y $W_s(A)$; de ahí se sigue el resultado. □

Hasta aquí hemos analizado la construcción del anillo de vectores de Witt y su generalización en anillos conmutativos con identidad. En adelante, denotaremos únicamente por 0 y 1 a los elementos 0_A y 1_A respectivamente en los anillos conmutativos con identidad y diremos solamente "anillo(s) conmutativos" para referirnos a éstos. Asimismo denotaremos simplemente por $+_s$ y $\cdot_s$ a las operaciones $\oplus_s$ y $\odot_s$.

Definición 1.4.8. Sea A un anillo conmutativo. Los anillos conmutativos $(W(A), \oplus, \odot)$ y $(W_s(A), +_s, \cdot_s)$ asociados a A, reciben el nombre de: *anillo generalizado de vectores de Witt* y *anillo truncado de vectores de Witt de longitud s* respectivamente.

A continuación estudiaremos el isomorfismo entre el anillo truncado de vectores de Witt y los anillos de Galois.

Teorema 1.4.9. *El anillo truncado de vectores de Witt de longitud s, $W_s(\mathbb{F}_{p^m})$ es isomorfo al anillo de Galois $GR(p^s, m)$ mediante la función:*

$$\Gamma : GR(p^s, m) \to W_s(\mathbb{F}_{p^m})$$
$$c = \rho_0(c) + \rho_1(c)p + \cdots + \rho_{s-1}(c)p^{s-1} \mapsto \left(r_0(c), r_1(c)^p, \ldots, r_{s-1}(c)^{p^{s-1}}\right)$$

donde $\rho_i(c) \in \mathcal{T}$, $(0 \leq i \leq s-1)$ son las componentes p-ádicas del elemento $c \in GR(p^s, m)$ como en (1.2.4) y $r_i(c) = \overline{\rho_i}(c)$ la μ_R-reducción de las componentes p-ádicas.

Demostración. Sean $c, d \in GR(p^s, m)$ dados por $c = \rho_0(c) + \rho_1(c)p + \cdots + \rho_{s-1}(c)p^{s-1}$ y $d = \rho_0(d) + \rho_1(d)p + \cdots + \rho_{s-1}(d)p^{s-1}$, luego:

$$c + d = (\rho_0(c) + \rho_0(d)) + (\rho_1(c) + \rho_1(d))p + \cdots + (\rho_{s-1}(c) + \rho_{s-1}(d))p^{s-1} \tag{1.4.14}$$

notemos que en (1.4.14) no necesariamente $\rho_i(c) + \rho_i(d) \in \mathcal{T}$, sin embargo también:

$$c + d = u = \rho_0(u) + \rho_1(u)p + \cdots + \rho_{s-1}(u)p^{s-1} \tag{1.4.15}$$

donde $\rho_i(u) \in \mathcal{T}$. Denotemos por simplicidad:

$$\rho_i(c) = c_i,\ \rho_i(d) = d_i,\ \rho_i(u) = u_i,\ r_i(c) = \overline{c}_i,\ r_i(d) = \overline{d}_i \text{ y } r_i(u) = \overline{u}_i.$$

Usando lo anterior veamos que $\Gamma(c) +_s \Gamma(d) = \Gamma(u) = \Gamma(c + d)$. En efecto, si denotamos $v = (\overline{v}_0, \ldots, \overline{v}_{s-1}) = \Gamma(c) +_s \Gamma(d)$, por el Corolario 1.4.7, tenemos que:

$$\overline{v}_l = \tau((r + t)_l) = \tau(\hat{s}_l(\overline{c}_i^{p^i}, \overline{d}_j^{p^j})) := \overline{s}_l(\overline{c}_i^{p^i}, \overline{d}_j^{p^j}),$$

por otro lado, dado que $\Gamma(u) = (\overline{u}_0, \ldots, \overline{u}_{s-1}^{p^{s-1}})$ resulta suficiente demostrar que para toda $l \in \{0, 1, \ldots, s-1\}$: $u_l^{p^l} \equiv v_l \pmod{p}$. Para ver esto hagamos inducción sobre l. Igualando las ecuaciones (1.4.14), (1.4.15) y aplicando la μ-redución de ambos lados tenemos que: $\overline{u}_0 = \overline{c}_0 + \overline{d}_0$, es decir, $u_0 \equiv c_0 + d_0 \pmod{p}$, pero $\overline{v}_0 = \overline{s}_0(\overline{c}_i^{p^i}, \overline{d}_i^{p^i}) = \overline{c}_0 + \overline{d}_0$, entonces:

$$u_0^{p^0} \equiv v_0 \pmod{p}.$$

Ahora, supongamos que $u_i^{p^i} \equiv v_i \pmod{p}$ para $0 \leq i \leq l-1$. Entonces, de la ecuación (1.4.3) tenemos que:

$$v^{(l)} = (\Gamma(c))^{(l)} + (\Gamma(d))^{(l)}$$

o de manera equivalente:

$$v_0^{p^l} + pv_1^{p^{l-1}} + \cdots + p^l v_l = \left[\bar{c}_0^{p^l} + \bar{d}_0^{p^l}\right] + p\left[(\bar{c}_1^p)^{p^{l-1}} + \left(\bar{d}_1^p\right)^{p^{l-1}}\right] + \cdots + p^l\left[\bar{c}_l^{p^l} + \bar{d}_l^{p^l}\right]$$

$$p^l v_l = \sum_{i=0}^{l} p^i \left[\left(\bar{c}_i^{p^i}\right)^{p^{l-i}} + \left(\bar{d}_i^{p^i}\right)^{p^{l-i}}\right] - \sum_{i=0}^{l-1} p^i v_i^{p^{l-i}}. \tag{1.4.16}$$

Por definición, $v_l = \bar{s}_l(\bar{c}_i^{p^i}, \bar{d}_i^{p^i})$ donde $s_l(x_i, y_j) \in \mathbb{Z}[x_i, y_j]$, de ahí que la expresión en el lado derecho de (1.4.16) es divisible por p^l. Ahora, igualando nuevamente (1.4.14), (1.4.15) y tomando $0 \leq l \leq s-1$, se tiene:

$$u_0 + pu_1 + \cdots + p^l u_l \equiv (c_0 + d_0) + p(u_1 + d_1) + \cdots + p^l(c_l + d_l) \pmod{p^{l+1}}.$$

Notemos que cada sumando $p^i u_i$ esta en su *representación aditiva*, luego podemos aplicar el automorfismo generalizado de Frobenius Θ a ambos lados de la congruencia y tras hacer esto de manera sucesiva llegamos a:

$$\Theta^l(u_0 + pu_1 + \cdots + p^l u_l) \equiv \Theta^l((c_0 + d_0) + p(u_1 + d_1) + \cdots + p^l(c_l + d_l)) \pmod{p^{l+1}}.$$

Dado que $p^i 1$ pertenece al subanillo de $GR(p^s, m)$ isomorfo a $\mathbb{Z}_{p^s}$, entonces $\Theta^l(p^i 1) = p^i 1$ y ya que $u_i, c_i, d_i \in \mathcal{T} = \langle \xi \rangle \cup \{0\}$ entonces cada uno de éstos son de la forma ξ^j para algún $j \in \{0, 1, \ldots, p^m - 1\}$ o bien son cero, pero $\Theta^l(\xi^j) = (\Theta^l(\xi))^j = (\xi^{p^l})^j = (\xi^j)^{p^l}$, en consecuencia $\Theta^l(c_i) = c_i^{p^l}$ análogamente para d_i y u_i con $i \in \{0, 1, \ldots, l\}$, de ahí que:

$$u_0^{p^l} + pu_1^{p^l} + \cdots + p^l u_l^{p^l} \equiv (c_0^{p^l} + d_0^{p^l}) + p(u_1^{p^l} + d_1^{p^l}) + \cdots + p^l(c_l^{p^l} + d_l^{p^l}) \pmod{p^{l+1}}$$

$$p^l u_l^{p^l} \equiv \sum_{i=0}^{l} p^i \left[c_i^{p^l} + d_i^{p^l}\right] - \sum_{i=0}^{l-1} p^i u_i^{p^l} \pmod{p^{l+1}},$$

dado que $p^l = p^i(p^{l-i})$, entonces $c_i^{p^l} = \left(c_i^{p^i}\right)^{p^{l-i}}$, análogamente para d^{p^l} y $u_i^{p^l}$, además por hipótesis inductiva tenemos que $u_i^{p^i} \equiv v_i \pmod{p}$ entonces:

$$p^l u_l^{p^l} \equiv \sum_{i=0}^{l} p^i \left[\left(c_i^{p^i}\right)^{p^{l-i}} + \left(d_i^{p^i}\right)^{p^{l-i}}\right] - \sum_{i=0}^{l-1} p^i v_i^{p^{l-i}} \pmod{p^{l+1}}, \tag{1.4.17}$$

ahora, una comparación del lado derecho de (1.4.17) con el lado derecho de (1.4.16) nos lleva a que podemos dividir la congruencia por p^l, concluyendo que:

$$u_l^{p^l} \equiv v_l \pmod{p},$$

y por lo tanto $\Gamma(c+d) = \Gamma(c) +_s \Gamma(d)$, de una manera similar se llega a que $\Gamma(cd) = \Gamma(c) \cdot_s \Gamma(d)$. Para ver la inyectividad de Γ sea $c \in \ker \Gamma$ entonces:

$$(\overline{c}_0, \overline{c}_i^p, \ldots, \overline{c}_{s-1}^{p^{s-1}}) = \Gamma(c) = (0, 0, \ldots, 0),$$

nótese que para toda $i \in \{0, 1 \ldots, s-1\} : 0 = \overline{c}_i^{p^i} = \sigma^i(\overline{c}_i)$ dónde σ es el automorfismo de Frobenius, luego se sigue que $\overline{c}_i = 0$ pero esto implica que c_i es un divisor de cero de $GR(p^s, m)$ o bien es cero, sin embargo dado que $c_i \in \mathcal{T} = \langle \xi \rangle \cup \{0\}$ y $\xi \neq 0$, es claro que $c_i = 0$ para toda $i \in \{0, 1, \ldots, s-1\}$ concluimos así que Γ es inyectiva. Finalmente dado que los elementos de $W_s(\mathbb{F}_{p^m})$ son vectores de longitud s, es decir, $v = (v_0, v_1, \ldots, v_{s-1})$ y $v \in \mathbb{F}_{p^m}$, entonces es claro que $\left|W_s(\mathbb{F}_{p^m})\right| = p^{sm} = |GR(p^s, m)|$, luego Γ es biyectiva y por lo tanto un isomorfismo. □

En lo sucesivo, cada vez que sea conveniente denotaremos los polinomios relativos a la suma y producto de Witt $s_\nu(x_i, y_j)$ y $m_\nu(x_i, y_j)$ solamente por s_ν y m_ν para $\nu \geq 0$, también denotaremos la suma y producto en $(W_s(R), +_s, \cdot_s)$ mediante el símbolo de suma usual y la notación multiplicativa, es decir, si $u, v \in W_s(R)$ entonces $u +_s v = u + v$, $u \cdot_s v = uv$ y cada vez que esto no cause ambigüedad denotaremos $\overline{u}$ solo por u.

Ejemplo 1.4.10. (i) Sean $p = 2, s = 2, m = 1$ entonces por el teorema anterior $W_2(\mathbb{F}_2)$ es isomorfo a $GR(2^2, 1) = \mathbb{Z}_4$ y tenemos que:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Figura 2.: Tabla de Cayley $(\mathbb{Z}_4, +)$

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Figura 3.: Tabla de Cayley $(\mathbb{Z}_4, \cdot)$

Luego, para el anillo $W_2(\mathbb{F}_2) = \{(0,0), (1,0), (0,1), (1,1)\}$, dados $(u_0, u_1), (v_0, v_1) \in W_2(\mathbb{F}_2)$ tenemos $(u_0, u_1) + (v_0, v_1) = (s_0, s_1)$ y $(u_0, u_1)(v_0, v_1) = (m_0, m_1)$ donde $s_0 = u_0 + v_0$ y $m_0 = u_0 v_0$.

Podemos hallar s_1 y m_1 de (1.4.3) como sigue:

$$\begin{aligned}
s_0^2 + 2s_1 &= u_0^2 + 2u_1 + v_0^2 + 2v_1 \\
s_1 &= u_1 + v_1 + \tfrac{1}{2}\left[u_0^2 + v_0^2 - s_0^2\right] \\
s_1 &= u_1 + v_1 + \tfrac{1}{2}\left[u_0^2 + v_0^2 - (u_0 + v_0)^2\right] \\
s_1 &= u_1 + v_1 + \tfrac{1}{2}\left[u_0^2 + v_0^2 - (u_0^2 + 2u_0v_0 + v_0^2)\right] \\
s_1 &= u_1 + v_1 - u_0v_0
\end{aligned}$$

$$\begin{aligned}
m_0^2 + 2m_1 &= (u_0^2 + 2u_1)(v_0^2 + 2v_1) \\
2m_1 &= u_0^2v_0^2 + 2(u_0^2v_1 + v_0^2u_1) + 4u_1v_1 - m_0^2 \\
m_1 &= u_0^2v_1 + v_0^2u_1 + 2u_1v_1 + \tfrac{1}{2}\left[u_0^2v_0^2 - m_0^2\right] \\
m_1 &= u_0^2v_1 + v_0^2u_1 + 2u_1v_1 + \tfrac{1}{2}\left[u_0^2v_0^2 - (u_0v_0)^2\right] \\
m_1 &= u_0^2v_1 + v_0^2u_1 + 2u_1v_1,
\end{aligned}$$

considere que s_1, m_1 son polinomios con coeficientes enteros de los cuales al aplicar reducción módulo $p = 2$ se consiguen los polinomios s_1 y m_1, así las reglas para la suma y producto en $W_2(\mathbb{F}_2)$ están dadas por:

$$\begin{aligned}
(u_0, u_1) + (v_0, v_1) &= (u_0 + v_0,\ u_1 + v_1 - u_0v_0), \\
(u_0, u_1)(v_0, v_1) &= (u_0v_0,\ u_0^2v_1 + v_0^2u_1)
\end{aligned} \tag{1.4.18}$$

y las tablas de Cayley para estas operaciones son:

$+_2$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,0)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,0)$	$(1,0)$	$(0,1)$

Figura 4.: Tabla de Cayley para $(W_2(\mathbb{F}_2), +)$

$\cdot_2$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,0)$

Figura 5.: Tabla de Cayley para $(W_2(\mathbb{F}_2), \cdot)$

(ii) En general, para $(u_0, u_1), (v_0, v_1) \in W_2(\mathbb{F}_{p^m})$ tenemos que $(u_0, u_1) + (v_0, v_1) = (s_0, s_1)$ y $(u_0, u_1)(v_0, v_1) = (m_0, m_1)$ donde $s_0 = u_0 + v_0$ y $m_0 = u_0 v_0$ así:

$$\begin{aligned}
s_0^p + ps_1 &= u_0^p + 2u_1 + v_0^p + pv_1 \\
s_1 &= u_1 + v_1 + \tfrac{1}{p}\left[u_0^p + v_0^p - s_0^p\right] \\
s_1 &= u_1 + v_1 + \tfrac{1}{p}\left[u_0^p + v_0^p - (u_0 + v_0)^p\right] \\
s_1 &= u_1 + v_1 + \tfrac{1}{p}\left[u_0^p + v_0^p - \left(u_0^p + \sum_{i=1}^{p-1} \tbinom{p}{i} u_0^{p-i} v_0^i + v_0^p\right)\right] \\
s_1 &= u_1 + v_1 - \tfrac{1}{p}\sum_{i=1}^{p-1} \tbinom{p}{i} u_0^{p-i} v_0^i,
\end{aligned}$$

$$\begin{aligned}
m_0^p + pm_1 &= (u_0^p + pu_1)(v_0^p + pv_1) \\
pm_1 &= u_0^p v_0^p + p(u_0^p v_1 + v_0^p u_1) + p^2 u_1 v_1 - m_0^p \\
m_1 &= u_0^p v_1 + v_0^p u_1 + pu_1 v_1 + \tfrac{1}{p}\left[u_0^p v_0^p - m_0^p\right] \\
m_1 &= u_0^p v_1 + v_0^p u_1 + pu_1 v_1 + \tfrac{1}{p}\left[u_0^p v_0^p - (u_0 v_0)^p\right] \\
m_1 &= u_0^p v_1 + v_0^p u_1 + pu_1 v_1,
\end{aligned}$$

por consiguiente:

$$\begin{aligned}
(u_0, u_1) + (v_0, v_1) &= (u_0 + v_0, u_1 + v_1 - h(u_0, v_0)) \\
(u_0, u_1)(v_0, v_1) &= (u_0 v_0, u_0^p v_1 + v_0^p u_1),
\end{aligned}$$

donde:

$$h(u_0, v_0) = \sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} u_0^{p-i} v_0^i.$$

(iii) $p = 2, s = 3, m \in \mathbb{N}$. Dado que $p = 2$ podemos retomar las expresiones de (i) para s_i, m_i con $i = 0, 1$. Ahora, para calcular s_2 y m_2 tenemos que:

$$s_0^4 + 2s_1^2 + 4s_2 = u_0^4 + v_0^4 + 2(u_1^2 + v_1^2) + 4(u_2 + v_2),$$

$$m_0^4 + 2m_1^2 + 4m_2^4 = (u_0^4 + 2u_1^2 + 4u_2)(v_0^4 + 2v_1^2 + 4v_2),$$

procediendo como antes, es decir, realizando las operaciones de las expresiones anteriores en $\mathbb{Q}[u_i, v_j]$ y finalmente aplicando reducción módulo $p = 2$ obtenemos las expresiones:

$$\begin{aligned}
s_2 &= u_2 + v_2 - h_1(u_0, u_1, v_0, v_1), \\
m_2 &= u_1 v_1 \left[u_1 v_1 - (u_0 v_0)^2\right] + u_0^4 v_2 + v_0^4 u_2,
\end{aligned}$$

de ahí que:

$$\begin{aligned}(u_0,u_1,u_2)+(v_0,v_1,v_2) &= (u_0+v_0, u_1+v_1-u_0v_0, u_2+v_2-h_1(u_0,u_1,v_0,v_1))\\ (u_0,u_1,u_2)(v_0,v_1,v_2) &= (u_0v_0, u_0^2v_1+v_0^2u_1, u_1v_1[u_1v_1-(u_0v_0)^2]+u_0^4v_2+v_0^4u_2)\end{aligned} \tag{1.4.19}$$

donde: $h_1(u_0,u_1,v_0,v_1) = u_1v_1+(u_1+v_1)u_0v_0-(u_0^3v_0+v_0^3u_0)$.

(iv) $p=3, s=3, m\in\mathbb{N}$. Ahora, usando (ii) con los parámetros actuales, podemos obtener las fórmulas para s_i y m_i con $i=0,1$ así:

$$\begin{aligned}s_0 &= u_0+v_0\\ s_1 &= u_1+v_1-(u_0^2v_0+u_0v_0^2)\end{aligned}$$

$$\begin{aligned}m_0 &= u_0v_0\\ m_1 &= u_0^3v_1+u_1v_0^3\end{aligned}$$

luego, aplicando:

$$s_0^9+3s_1^3+9s_2 = u_0^9+v_0^9+3(u_1^3+v_1^3)+9(u_2+v_2),$$

$$m_0^9+3m_1^3+9m_2 = (u_0^9+3u_1^3+9u_2)(v_0^9+3v_1^3+9v_2),$$

y tras realizar las operaciones y reduciendo módulo $p=3$:

$$\begin{aligned}s_2 = u_2+v_2 &+ 2u_0^8v_0+2u_0^7v_0^2+2u_0^5v_0^4+2u_0^4u_1v_0^2+2u_0^4v_0^5\\ &+ u_0^3u_1v_0^3+u_0^3v_0^3v_1+u_0^2u_1^2v_0+2u_0^2u_1v_0^4+2u_0^2u_1v_0v_1\\ &+ 2u_0^2v_0^7+2u_0^2v_0^4v_1+u_0^2v_0v_1^2+u_0u_1^2v_0^2+2u_0u_1v_0^2v_1\\ &+ 2u_0v_0^8+u_0v_0^2v_1^2+2u_1^2v_1+2u_1v_1^2+2u_0^4v_0^2v_1\end{aligned}$$

$$m_2 = u_0^9v_2+2u_0^6u_1v_0^3v_1^2+2u_0^3u_1^2v_0^6v_1+u_1^3v_1^3+u_2v_0^9.$$

Con lo cual obtenemos que:

$$\begin{aligned}(u_0,u_1,u_2)+(v_0,v_1,v_2) &= (u_0+v_0, u_1+v_1-[u_0^2v_0+u_0v_0^2],\\ &\qquad u_2+v_2-h_1(u_0,u_1,v_0,v_1))\\ (u_0,u_1,u_2)(v_0,v_1,v_2) &= (u_0v_0, u_0^3v_1+u_1v_0^3,\\ &\qquad u_0^9v_2+u_2v_0^9+l_1(u_0,u_1,v_0,v_1)).\end{aligned}$$

donde $h_1(u_0,u_1,v_0,v_1)$ se obtiene de s_2 sustrayendo u_2+v_2 y $l_1(u_0,u_1,v_0,v_1)$ se obtiene de m_2 sustrayendo $u_0^9v_2+u_2v_0^9$.

Como puede observarse, entre mayor sea la longitud de los elementos de $W_s(\mathbb{F}_{p^m})$, las expresiones para la suma y producto involucran una serie de cálculos cada vez más extensa y por ende difícil de recordar. Sin embargo, podemos observar un patrón en la suma el cual se exhibe a continuación:

Lema 1.4.11. *Sean $r = (r_0, r_1, \ldots, r_{s-1}), t = (t_0, t_1, \ldots, t_{s-1}) \in W_s(\mathbb{F}_{p^m})$. Entonces:*

$$(r +_s t)_\nu = r_\nu + t_\nu - h_{\nu-1}(r_i, t_j), \tag{1.4.20}$$

donde $0 \leq i, j \leq \nu - 1$ y $h_l(x_i, y_j)$ es un polinomio con coeficientes enteros y término constante cero (respecto a todas sus variables) donde $0 \leq \nu \leq s - 1$ y $0 \leq l \leq \nu - 1$.

Demostración. Por (1.4.3) tenemos que $(r +_s t)^{(\nu)} = r^{(\nu)} + s^{(\nu)}$ y expandiendo (1.4.1) obtenemos la igualdad y abusando de la notación denotamos por s_k a $s_k(r_i, t_j)$:

$$\begin{aligned} s_0^{p^\nu} + ps_1^{p^{\nu-1}} + \cdots + p^{\nu-1}s_{\nu-1}^p + p^\nu s_\nu &= \left(r_0^{p^\nu} + pr_1^{\nu-1} + \cdots + p^{\nu-1}r_{\nu-1}^p + p^\nu r_\nu\right) \\ &= \quad + \left(t_0^{p^\nu} + pt_1^{\nu-1} + \cdots + p^{\nu-1}t_{\nu-1}^p + p^\nu t_\nu\right), \end{aligned}$$

despejando $p^\nu s_\nu$ obtenemos que:

$$\begin{aligned} p^\nu s_\nu &= p^\nu(r_\nu + t_\nu) + \sum_{k=0}^{\nu-1} p^k \left(r_k^{p^{\nu-k}} + t_k^{p^{\nu-k}}\right) - \sum_{k=0}^{\nu-1} p^k s_k^{p^{\nu-k}} \\ &= p^\nu(r_\nu + t_\nu) + \sum_{k=0}^{\nu-1} p^k \left(r_k^{p^{\nu-k}} + t_k^{p^{\nu-k}} - s_k^{p^{\nu-k}}\right). \end{aligned} \tag{1.4.21}$$

De lo anterior, nombremos $h_{\nu-1}(r_i, t_j)$ al segundo término en el lado derecho de (1.4.21) y dividiendo por p^ν ambos lados de dicha ecuación, se obtiene (1.4.20). Las propiedades del polinomio $h_l(x_i, y_j)$ se siguen del Teorema 1.4.4. □

1.4.1 Aritmética p-ádica

En esta última sección, aplicaremos los resultados obtenidos sobre el anillo de vectores de Witt, para poder determinar las μ-reducciones de las componentes p-ádicas de la suma de dos elementos arbitrarios y del producto de un elemento y un tipo particular de unidad en los anillos de Galois $GR(p^3, m)$.

Dados dos elementos $c, d \in R$ con sus representaciones p-ádicas:

$$\begin{aligned} c &= \rho_0(c) + p\rho_1(c) + p^2\rho_2(c) \\ d &= \rho_0(d) + p\rho_1(d) + p^2\rho_2(d) \end{aligned}$$

usando Γ del Teorema 1.4.9 tenemos que:

$$\Gamma(c) = \left(r_0(c), r_1(c)^p, r_2(c)^{p^2}\right)$$
$$\Gamma(d) = \left(r_0(d), r_1(d)^p, r_2(d)^{p^2}\right)$$

por otro lado, consideremos la representación p-ádica de $c+d$:

$$c+d = \rho_0(c+d) + p\rho_1(c+d) + p^2\rho_2(c+d)$$

y por consiguiente:

$$\Gamma(c+d) = \left(r_0(c+d), r_1(c+d)^p, r_2(c+d)^{p^2}\right),$$

por el Lema 1.4.11 tenemos que:

$$\begin{aligned} r_0(c+d) &= r_0(c) + r_0(d) \\ r_1(c+d)^p &= r_1(c)^p + r_1(d)^p - h_0(r_0(c), r_1(c)) \\ r_2(c+d)^{p^2} &= r_2(c)^{p^2} + r_2(d)^{p^2} - h_1\left(r_i(c)^{p^i}, r_j(d)^{p^j}\right) \end{aligned}$$

por lo tanto, de la Definición A.3.2 tenemos que:

$$\begin{aligned} r_0(c+d) &= r_0(c) + r_0(d) \\ r_1(c+d) &= [r_1(c)^p + r_1(d)^p - h_0(r_0(c), r_1(c))]^{1/p} \\ r_2(c+d) &= \left[r_2(c)^{p^2} + r_2(d)^{p^2} - h_1\left(r_i(c)^{p^i}, r_j(d)^{p^j}\right)\right]^{1/p^2} \qquad (0 \le i, j \le 1) \end{aligned} \tag{1.4.22}$$

El conjunto de ecuaciones (1.4.22) resume las μ-reducciones de las componentes p-ádicas de la suma de dos elementos en $GR(p^3, m)$.

Un resultado que resultará de utilidad más adelante es el siguiente:

Teorema 1.4.12. *Sea $c \in R$. Entonces:*

$$r_j(p^k c) = \begin{cases} r_{j-k}(c) & k \le j \le 2 \\ 0 & c.o.c. \end{cases} \tag{1.4.23}$$

para $0 \le k \le 2$.

Demostración. Sea $c \in R$ con representación p-ádica: $c = \rho_0(c) + p\rho_1(c) + p^2\rho_2(c)$ entonces:

$$\begin{aligned} p^k c &= p^k\left(\rho_0(c) + p\rho_1(c) + p^2\rho_2(c)\right) \\ &= p^k\rho_0(c) + p^{k+1}\rho_1(c) + p^{k+2}\rho_2(c) \end{aligned}$$

Si $k = 1$ es claro que: $pc = p\rho_0(c) + p^2\rho_1(c)$ y dado que $\rho_0(c), \rho_1(c) \in \mathcal{T}$, se sigue de la unicidad de la representación p-ádica que:

$$\rho_0(pc) = 0, \rho_1(pc) = \rho_0(c) \text{ y } \rho_2(pc) = \rho_1(c) \tag{1.4.24}$$

Por otro lado, si $k = 2$ tenemos que: $p^2c = p^2\rho_0(c)$ y dado que $\rho_0(c) \in \mathcal{T}$, entonces:

$$\rho_0(pc) = \rho_1(pc) = 0 \text{ y } \rho_2(pc) = \rho_0(c). \tag{1.4.25}$$

Finalmente, aplicado la μ-reducción a las expresiones (1.4.24) y (1.4.25) se tiene el resultado. □

Como ya se ha mencionado antes, un anillo de Galois es un anillo *local* de ahí que los elementos de la forma $1 + \pi$ con $\pi \in (p)$[3] son todos unidades, nosotros enfocaremos nuestra atención a aquellas unidades de la forma $\lambda = 1 + p^k N'$ tales que $N' \in \mathcal{T}$ y a saber existen dos tipos de éstas:

TIPO 1: $\rho_0(\lambda) = 1, \rho_1(\lambda) = N'$ y $\rho_2(\lambda) = 0$

TIPO 2: $\rho_0(\lambda) = 1, \rho_1(\lambda) = 0$ y $\rho_2(\lambda) = N'$,

luego, al aplicar Γ a éstas obtenemos:

$$\begin{aligned} \Gamma(1 + pN') &= (1, n'^p, 0) \\ \Gamma(1 + p^2N') &= (1, 0, n'^{p^2}), \end{aligned} \tag{1.4.26}$$

donde $n' = \mu(N')$. Haciendo uso de esto hallaremos las expresiones para la μ-reducción del producto de un elemento $c \in R$ y las unidades de tipo 1 y 2. En (ii) del Ejemplo 1.4.10 obtuvimos las expresiones para m_0 y m_1 de un vector (m_0, m_1, m_2) asociado al producto de dos vectores de Witt. Ahora, utilizaremos dichas expresiones y la siguiente expresión para hallar m_2:

$$m_0^{p^2} + pm_1^p + p^2m_2 = (u_0^{p^2} + pu_1^p + p^2u_2)(v_0^{p^2} + pv_1^p + p^2v_2) \tag{1.4.27}$$

Desarrollando (1.4.27) y sustituyendo m_0 y m_1 ahí:

$$\begin{aligned} p^2m_2 = &\cancel{\left(u_0^{p^2}v_0^{p^2} - (u_0v_0)^{p^2}\right)} + p\left(u_0^{p^2}v_1^p + v_0^{p^2}u_1^p - (u_0^pv_1 + v_0^pu_1 + pu_1v_1)^p\right) \\ &+ p^2\left[u_0^{p^2}v_2 + u_1^pv_1^p + v_0^{p^2}u_2\right] + p^3\mathbf{T}, \end{aligned} \tag{1.4.28}$$

hasta aquí, $\mathbf{T}$ representa a todos los términos que tienen al factor p^3 en común, así tras dividir por p^2 y aplicar reducción módulo p este factor se desvanece. Denotemos por $f(u_0, u_1, v_0, v_1)$ al desarrollo de la expresión restante que está acompañada por el factor p entonces:

3 Pues éste resulta ser su ideal maximal.

$$
\begin{aligned}
f(u_0,u_1,v_0,v_1) &= \Big(u_0^{p^2}v_1^p + v_0^{p^2}u_1^p - (u_0^pv_1+v_0^pu_1)^p \\
&\qquad - \sum_{j=1}^{p}\tbinom{p}{j}(u_0^pv_1+v_0^pu_1)^{p-j}(pu_1v_1)^j\Big) \\
&= -\left(\sum_{j=1}^{p-1}\tbinom{p}{j}(u_0^pv_1)^{p-j}(v_0^pu_1)^j + \sum_{j=1}^{p}\tbinom{p}{j}(u_0^pv_1+v_0^pu_1)^{p-j}(pu_1v_1)^j\right) \\
&= -\left(p\sum_{j=1}^{p-1}\frac{\binom{p}{j}}{p}(u_0^pv_1)^{p-j}(v_0^pu_1)^j + p^2\sum_{j=1}^{p}\frac{\binom{p}{j}}{p}(u_0^pv_1+v_0^pu_1)^{p-j}p^{j-1}(u_1v_1)^j\right).
\end{aligned}
$$

Para abreviar denotaremos:

$$
\begin{aligned}
\theta_1(u_i,v_k) &= \sum_{j=1}^{p-1}\frac{\binom{p}{j}}{p}(u_0^pv_1)^{p-j}(v_0^pu_1)^j \\
\theta_2(u_i,v_k) &= \sum_{j=1}^{p}\frac{\binom{p}{j}}{p}(u_0^pv_1+v_0^pu_1)^{p-j}p^{j-1}(u_1v_1)^j
\end{aligned}
\tag{1.4.29}
$$

sustituyendo (1.4.29) en (1.4.28):

$$
\begin{aligned}
p^2m_2 &= p(p\theta_1(u_i,v_k)+p^2\theta_2(u_i,v_k)) + p^2\left[u_0^{p^2}v_2 + u_1^pv_1^p + v_0^{p^2}u_2\right] + p^3\mathbf{T} \\
\Rightarrow p^2m_2 &= p^2\left[\theta_1(u_i,v_k) + u_0^{p^2}v_2 + u_1^pv_1^p + v_0^{p^2}u_2\right] + p^3(\mathbf{T}+\theta_2(u_i,v_k)) \\
\Rightarrow m_2 &= \left[\theta_1(u_i,v_k) + u_0^{p^2}v_2 + u_1^pv_1^p + v_0^{p^2}u_2\right] + p(\mathbf{T}+\theta_2(u_i,v_k)).
\end{aligned}
$$

Finalmente, basta aplicar reducción módulo p y sustituir $m_2 = r_2(w)^{p^2}$, $u_i = r_i(c)^{p^i}$ y $v_k = r_k(\lambda)^{p^k}$ llegamos a los siguientes casos:

CASO 1: Supongamos que $\Gamma(\lambda) = (1, n'^p, 0)$ entonces $v_0 = 1$, $v_1 = n'^p$, $v_2 = 0$, así:

$$
\begin{aligned}
\theta_1\left(r_i(c)^{p^i}, r_k(\lambda)^{p^k}\right) &= \sum_{j=1}^{p-1}\frac{\binom{p}{j}}{p}\left(r_0(c)^pn'^p\right)^{p-j}\left(r_1(c)^p\right)^j \\
&= \sum_{j=1}^{p-1}\frac{\binom{p}{j}}{p}\left(r_0(c)n'\right)^{p(p-j)}\left(r_1(c)\right)^{pj}.
\end{aligned}
$$

Continuando con la sustitución:

$$
\begin{aligned}
r_2(w)^{p^2} &= \theta_1\left(r_i(c)^{p^i}, r_k(\lambda)^{p^k}\right) + \left[r_0(c)^{p^2}(0) + r_1(c)^{p^2}n'^{p^2} + r_2(c)^{p^2}\right] \\
&= \theta_1\left(r_i(c)^{p^i}, r_k(\lambda)^{p^k}\right) + \left[r_1(c)n' + r_2(c)\right]^{p^2}.
\end{aligned}
$$

De ahi que si λ es una unidad de tipo 1:

$$
\begin{aligned}
r_0(\lambda c) &= r_0(c) \\
r_1(\lambda c) &= n'r_0(c) + r_1(c) \\
r_2(\lambda c) &= n'r_1(c) + r_2(c) + \left[\theta_1\Big(r_i(c)^{p^i}, r_k(c)^{p^k}\Big)\right]^{1/p^2}
\end{aligned}
\tag{1.4.30}
$$

CASO 2: Si $\Gamma(\lambda) = (1, 0, n'^{p^2})$ entonces $v_0 = 1$, $v_1 = 0$, $v_2 = n'^{p^2}$ y se sigue de (1.4.29) que $\theta_1(r_i(c)^{p^i}, r_k(\lambda)^{p^k}) = 0$ y de ahí tenemos:

$$\begin{aligned} r_2(w)^{p^2} &= \left[r_0(c)^{p^2}(n')^{p^2} + r_1(c)^{p^2}(0)^{p^2} + (1)r_2(c)^{p^2}\right] \\ &= \left[r_0(c)n' + r_2(c)\right]^{p^2}. \end{aligned}$$

Luego, si λ es una unidad de tipo 2:

$$\begin{aligned} r_0(\lambda c) &= r_0(c) \\ r_1(\lambda c) &= r_1(c) \\ r_2(\lambda c) &= n' r_0(c) + r_2(c). \end{aligned} \tag{1.4.31}$$

Con las ecuaciones (1.4.30) y (1.4.31) hemos alcanzado el objetivo de esta última sección.

Ejemplo 1.4.13. Sean $p = 2$, $m = 2$ entonces:

$$GR(p^3, m) = GR(8, 2) \simeq \frac{\mathbb{Z}_8[x]}{(x^2 + x + 1)}.$$

Considere los elementos $c = 2x + 7$ y $d = 7x + 4$ y su suma $c + d := x + 3$ con representaciones 2-ádicas:

$$\begin{aligned} 2x + 7 &= 1 + 2(7x + 7) + 2^2(x) \\ 7x + 4 &= w + 2(x) + 2^2(7x + 7) \\ x + 3 &= (7x + 7) + 2(x) + 2^2(1). \end{aligned}$$

Por otro lado, sea $\alpha = \overline{x}$ una raíz primitiva de la unidad, entonces:

$$\begin{aligned} \Gamma(2x + 7) &= (1, (\alpha + 1)^2, \alpha^4) = (1, \alpha^2 + 1, \alpha) = (1, \alpha, \alpha) \\ \Gamma(7x + 4) &= (\alpha, \alpha^2, (\alpha + 1)^4) = (\alpha, \alpha^2, \alpha + 1) = (\alpha, \alpha^2, \alpha^2), \end{aligned}$$

como en (ii) y (iii) del Ejemplo 1.4.10, para $p = 2$ y $s = 3$:

$$\begin{aligned} h_0(u_0, v_0) &= u_0 v_0 \\ h_1(u_0, u_1, v_0, v_1) &= u_1 v_1 + (u_1 + v_1)u_0 v_0 - (u_0^3 v_0 + v_0^3 u_0). \end{aligned}$$

tenemos que:

$$\begin{aligned} h_0(1, \alpha) &= \alpha \\ h_1(1, \alpha^2, \alpha, \alpha^4) &= \alpha^3 + (\alpha + \alpha^2)\alpha - (\alpha + \alpha^3) = \alpha^2 + \alpha + 1 = 0. \end{aligned}$$

entonces, por (1.4.22):

$$(r_0(x + 3), r_1(x + 3), r_2(x + 3)) := \left(\alpha + 1, \left[\alpha^2 + (\alpha^2)^2 - \alpha\right]^{1/2}, \left[\alpha^4 + \alpha^8 - 0\right]^{1/4}\right)$$

$$
\begin{aligned}
&= \left(\alpha+1, [\alpha^2+\alpha-\alpha]^{1/2}, [\alpha+\alpha+1]^{1/4}\right) \\
&= (\alpha+1, \alpha, 1).
\end{aligned}
$$

corroborando (1.4.30). Además, para $\lambda = 1 - 2^2 = -3 \equiv 5 \pmod 8$ se tiene que:

$$\lambda(2x+7) = 10x + 35 \equiv 2x + 3 \pmod 8.$$

Como $2x+7 = 1 + 2(7x+7) + 2^2(x)$ y $\lambda(2x+7) = 2x+3 = 1 + 2(7x+7) + 2^2(7x+7)$ entonces tenemos que:

$$
\begin{aligned}
r_0(\lambda(2x+7)) &= r_0(2x+3) = 1 = r_0(2x+7) \\
r_1(\lambda(2x+7)) &= r_1(2x+3) = \theta + 1 = r_1(2x+7) \\
r_2(\lambda(2x+7)) &= r_2(2x+3) = \theta + 1 = r_2(2x+7) + r_0(2x+7),
\end{aligned}
$$

tal como se afirma en (1.4.31).

2 LA ISOMETRIA DE GRAY

2.1 LA FUNCIÓN DE GRAY EN $\mathbb{Z}_4$

En este capítulo estudiaremos la función de Gray, iniciando con los códigos cuaternarios y mostrando que es una isometría entre $\mathbb{Z}_4$ y $\mathbb{F}_2^{2n}$, y posteriormente revisaremos la generalización de dicho resultado en anillos de Galois de índice de nilpotencia 3. A lo largo de esta sección , denotaremos según nos sea conveniente a los vectores $(x_0, x_1, \ldots, x_{n-1})$ mediante la concatenación de sus componentes, es decir: $(x_0, x_1, \ldots, x_{n-1}) = (x_0 x_1 \cdots x_{n-1})$.

Definición 2.1.1. La *función de Gray* para $\mathbb{Z}_4$ se define por:

$$\begin{aligned} \phi : \mathbb{Z}_4 &\to \mathbb{F}_2^2 \\ 0 \mapsto 00 \quad & 2 \mapsto 11 \\ 1 \mapsto 01 \quad & 3 \mapsto 10 \end{aligned} \tag{2.1.1}$$

De (2.1.1), la función de Gray es claramente una biyección entre $\mathbb{Z}_4$ y $\mathbb{F}_2^2$, sin embargo no es un homomorfismo de anillos, esto es fácil de notar dado que $\phi(0) = (00) \neq (11) = (10) + (01) = \phi(3) + \phi(1)$ pero $1 + 3 = 0$ en $\mathbb{Z}_4$.

Lema 2.1.2. *Sean $x, y \in \mathbb{Z}_4$ entonces $w_L(x) = (w_H \circ \phi)(x)$ y $d_L(x,y) = (d_H \circ \psi)(x,y)$ donde la función $\psi \colon \mathbb{Z}_4^2 \to \left(\mathbb{F}_2^2\right)^2$ es tal que $(x,y) \mapsto (\phi(x), \phi(y))$, donde $w_L(\cdot)$ y $w_H(\cdot)$ son los pesos de Lee y Hamming respectivamente.*

Demostración. Comparando las columnas de las siguientes tablas se consiguen ambas afirmaciones: □

x	$\phi(x)$	$(w_H(\phi(x))$	$w_L(x)$
0	(00)	0	0
1	(01)	1	1
2	(11)	2	2
3	(10)	1	1

Figura 6.: Comparación de w_L y $w_H \circ \psi$

(x,y)	$\psi(x,y)$	$(d_H(\psi((x,y)))$	$d_L(x,y)$
(00)	00 00	0	0
(01)	00 01	1	1
(02)	00 11	2	2
(03)	00 10	1	1
(10)	01 00	1	1
(11)	01 01	0	0
(12)	01 11	1	1
(13)	01 10	2	2
(20)	11 00	2	2
(21)	11 01	1	1
(22)	11 11	0	0
(23)	11 10	1	1
(30)	10 00	1	1
(31)	10 01	2	2
(32)	10 11	1	1
(33)	10 10	0	0

Figura 7.: Comparación entre d_L y $d_H \circ \psi$

Observación 2.1.3. Por el Lema 2.1.2 tenemos que para cualesquiera $x, y \in \mathbb{Z}_4$:

$$w_L(x) = w_H(\phi(x))$$
$$d_L(x,y) = d_H(\phi(x), \phi(y)).$$

Hasta aquí siguiendo a [18], hemos demostrado que la función de Gray es una isometría entre $\mathbb{Z}_4$ y $\mathbb{F}_2^2$, por otro lado, consideremos la representación 2-ádica de los elementos de $\mathbb{Z}_4 = GR(2^2, 1)$, es decir:

$$x = \rho_0(x) + 2\rho_1(x) \text{ donde } \rho_0(x), \rho_1(x) \in \tau = \{0,1\}. \tag{2.1.2}$$

y denotemos por $r_i(x) = \mu(\rho_i(x)) \in RF \simeq \mathbb{F}_2$ con $i = 0, 1$.

Definición 2.1.4. Sea $x = \rho_0(x) + 2\rho_1(x)$ la representación $2-$ádica de $x \in \mathbb{Z}_4$. Definimos las funciones $\alpha, \beta, \gamma : \mathbb{Z}_4 \to \mathbb{F}_2$ mediante:

$$\alpha(x) = r_0(x)$$
$$\beta(x) = r_1(x)$$
$$\gamma(x) = \alpha(x) + \beta(x).$$

Observación 2.1.5. En base a la definición anterior se construye la siguiente tabla para las funciones α, β y γ.

x	$\rho_0(x)+2\rho_1(x)$	$\alpha(x)$	$\beta(x)$	$\gamma(x)$
0	$0+(2)(0)$	0	0	0
1	$1+(2)(0)$	1	0	1
2	$0+(2)(1)$	0	1	1
3	$1+(2)(1)$	1	1	0

Figura 8.: Imágenes de α, β, γ sobre $\mathbb{Z}_4$

Corolario 2.1.6. *Sean α, β y γ como en la Definición 2.1.4, entonces α es un homomorfismo de grupos aditivos entre $\mathbb{Z}_4$ y $\mathbb{F}_2$ mientras que β y γ no lo son. Sin embargo, para toda $x \in \mathbb{Z}_4$ se cumple la relación: $(\alpha+\beta+\gamma) \equiv 0 \pmod 2$.*

Demostración. Sean $x, y \in \mathbb{Z}_4$ entonces $x = \rho_0(x) + 2\rho_1(x)$ y $y = \rho_0(y) + 2\rho_1(y)$ donde se tiene que: $\rho_i(x), \rho_i(y) \in \{0,1\}$ para $i = 0,1$. Entonces $x + y = (\rho_0(x) + \rho_0(y)) + 2(\rho_1(x) + \rho_1(y))$ así:

$$\begin{aligned}\alpha(x+y) &= \mu(\rho_0(x)+\rho_0(y)) \\ &= \mu(\rho_0(x)) + \mu(\rho_0(y)) \\ &= r_0(x) + r_0(y) = \alpha(x) + \alpha(y)\end{aligned}$$

por consiguiente, α es un homomorfismo de grupos aditivos. Por otro lado, dado que $1 = 1 + (2)(0)$ y $2 = 0 + (2)(1)$ sin embargo $\beta(2) = \gamma(2) = \mu(1) = 1 \neq 0$ mientras que $0 = \mu(0) + \mu(0) = \beta(1) + \beta(1) = \gamma(1) + \gamma(1)$, es decir, β y γ no son homomorfismos de grupos aditivos. Finalmente, como $\mathrm{Car}(\mathbb{F}_2) = 2$, entonces para todo $c \in \mathbb{F}_2$ tenemos que $2c = 0$, luego para toda $x \in \mathbb{Z}_4$ se tiene que:

$$\begin{aligned}(\alpha+\beta+\gamma)(x) &= \alpha(x) + \beta(x) + \gamma(x) \\ &= \alpha(x) + \beta(x) + \alpha(x) + \beta(x) \\ &= 2(\alpha(x) + \beta(x)) = 0\end{aligned}$$

□

Antes de continuar, definimos la función $L : \mathbb{Z}_4 \to \mathbb{F}_2^2$ tal que $L(x) = (\beta(x), \gamma(x))$, es fácil ver de la Figura 8 que $L = \phi$, es decir:

$$\phi(x) = (\beta(x), \gamma(x)) \qquad (x \in \mathbb{Z}_4) \tag{2.1.3}$$

2.2 IMÁGENES DE $\mathbb{Z}_4^n$-CÓDIGOS

En esta sección haremos uso de los resultados vistos antes para analizar a la función de Gray de una manera más general, y más aún, demostrar que esta es, de hecho, una isometría, para esto, extenderemos de manera natural a las funciones α, β, γ y ϕ mediante:

Definición 2.2.1. Sean α, β, γ como en la Definición 2.1.4, ϕ la función de Gray en $\mathbb{Z}_4$ y $n \geq 2$ un entero positivo. Para $\underline{x} = (x_0, x_1, \ldots, x_n) \in \mathbb{Z}_4^n$ definimos:

$$\begin{aligned}
&\tilde{\alpha} : \mathbb{Z}_4^n \to \mathbb{F}_2^n \text{ con } \tilde{\alpha}(\underline{x}) = (\alpha(x_0), \alpha(x_1), \ldots, \alpha(x_{n-1})) \\
&\tilde{\beta} : \mathbb{Z}_4^n \to \mathbb{F}_2^n \text{ con } \tilde{\beta}(\underline{x}) = (\beta(x_0), \beta(x_1), \ldots, \beta(x_{n-1})) \\
&\tilde{\gamma} : \mathbb{Z}_4^n \to \mathbb{F}_2^n \text{ con } \tilde{\gamma}(\underline{x}) = (\gamma(x_0), \gamma(x_1), \ldots, \gamma(x_{n-1})) \\
&\overline{\phi} : \mathbb{Z}_4^n \to \mathbb{F}_2^{2n} \text{ con } \overline{\phi}(\underline{x}) = (\tilde{\beta}(\underline{x}), \tilde{\gamma}(\underline{x}))
\end{aligned}$$

Observación 2.2.2. $\overline{\phi}(\underline{x})$ es un vector con $2n$ componentes, sin embargo, considerando la ecuación (2.1.3), podemos denotar:

$$\overline{\phi}(\underline{x}) = (\phi(x_0), \phi(x_1), \cdots, \phi(x_{n-1})), \tag{2.2.1}$$

donde $\phi(x_i) = (\beta(x_i), \gamma(x_i))$ para $i = 1, 2, \ldots, n-1$. Dado que $\phi(x_i) \in \mathbb{F}_2^2$, la expresión (2.2.1) está bien definida puesto que los espacios vectoriales $\mathbb{F}_2^{2n}$ y $\left(\mathbb{F}_2^2\right)^n$ son isomorfos.

Lema 2.2.3. *$\overline{\phi}$ es una biyección entre $\mathbb{Z}_4^n$ y $\mathbb{F}_2^{2n}$.*

Demostración. Es claro, viendo la Figura 8 que las funciones β y γ son sobreyectivas, en consecuencia $\tilde{\beta}$ y $\tilde{\gamma}$ lo son y por consiguiente $\overline{\phi}$ es sobreyectiva. Por otro lado, dados $\underline{x}, \underline{y} \in \mathbb{Z}_4^n$ tales que $\overline{\phi}(\underline{x}) = \overline{\phi}(\underline{y})$, entonces, $(\tilde{\beta}(\underline{x}), \tilde{\gamma}(\underline{x})) = (\tilde{\beta}(\underline{y}), \tilde{\gamma}(\underline{y}))$, luego por la Definición 2.2.1 tenemos que:

$$\begin{aligned}
\tilde{\beta}(\underline{x}) &= \tilde{\beta}(\underline{y}) \\
(\beta(x_0), \beta(x_1), \ldots, \beta(x_{n-1})) &= (\beta(y_0), \beta(y_1), \ldots, \beta(y_{n-1}))
\end{aligned}$$

y

$$\begin{aligned}
\tilde{\gamma}(\underline{x}) &= \tilde{\gamma}(\underline{y}) \\
(\gamma(x_0), \gamma(x_1), \ldots, \gamma(x_{n-1})) &= (\gamma(y_0), \gamma(y_1), \ldots, \gamma(y_{n-1}))
\end{aligned}$$

esto implica que para cada $i = 0, 1, \ldots, n-1$, $\beta(x_i) = \beta(y_i)$ y $\gamma(x_i) = \gamma(y_i)$, entonces de la Observación 2.2.2, $\phi(x_i) = \phi(y_i)$ y como ϕ es inyectiva (2.1.1); $x_i = y_i$ para toda $i = 0, 2, \ldots, n-1$, luego $\underline{x} = \underline{y}$ y así $\overline{\phi}$ es inyectiva. □

El lema anterior nos dice que dados $n \in \mathbb{N}$ y un vector $\underline{x} \in \mathbb{Z}_4^n$ existe una única $2n$*-ada binaria* que corresponde a dicho $\underline{x}$, en vista de esto nombraremos a ésta la **imagen binaria** de $\underline{x}$ bajo $\overline{\phi}$.

A continuación, presentamos un resultado relacionado a la función de Gray, y aunque nos restringiremos al caso de $\mathbb{Z}_4^n$, dicho resultado se demostrará para cualquier $\mathbb{Z}_{p^2}^n$ más adelante.

Teorema 2.2.4. *$\overline{\phi}$ es una isometría que preserva el peso entre $(\mathbb{Z}_4^n, \tilde{w}_L)$ y $\left(\mathbb{F}_2^{2n}, \tilde{w}_H\right)$.*

Demostración. Veamos en primer lugar que $\overline{\phi}$ preserva el peso entre $(\mathbb{Z}_4^n, \tilde{w}_L)$ y $(\mathbb{F}_2^{2n}, \tilde{w}_H)$. Para esto sean $\underline{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_4^n$ y $w_1(\cdot)$ como en (1.3.2) de la Definición 1.3.3 entonces:

$$\begin{aligned}
\tilde{w}_H\left(\overline{\phi}(\underline{x})\right) &= w_H((\tilde{\beta}(\underline{x}), \tilde{\gamma}(\underline{x}))) \\
&= w_H\left(\tilde{\beta}(\underline{x})\right) + w_H\left(\tilde{\gamma}(\underline{x})\right) \\
&= \sum_{i=1}^{n} w_1(\beta(x_i)) + \sum_{i=1}^{n} w_1(\gamma(x_i)) \\
&= \sum_{i=1}^{n} [w_1(\beta(x_i)) + w_1(\gamma(x_i))] \\
&= \sum_{i=1}^{n} w_H(\beta(x_i), \gamma(x_i)) \\
&= \sum_{i=1}^{n} w_H(\phi(x_i)) = \sum_{i=1}^{n} w_L(x_i) = \tilde{w}_L(\underline{x})
\end{aligned}$$

Ahora, para ver que es una isometría sean $\underline{x}, \underline{y} \in \mathbb{Z}_4^n$ entonces:

$$\begin{aligned}
d_H\left(\overline{\phi}(\underline{x}), \overline{\phi}(\underline{y})\right) &= w_H\left(\overline{\phi}(\underline{x}) - \overline{\phi}(\underline{y})\right) \\
&= w_H\left[(\tilde{\beta}(\underline{x}), \tilde{\gamma}(\underline{x})) - (\tilde{\beta}(\underline{y}), \tilde{\gamma}(\underline{y}))\right] \\
&= w_H\left[(\tilde{\beta}(\underline{x}) - \tilde{\beta}(\underline{y}), \tilde{\gamma}(\underline{x}) - \tilde{\gamma}(\underline{y}))\right] \\
&= \sum_{i=1}^{n} [w_1(\beta(x_i) - \beta(y_i))] + \sum_{i=1}^{n} [w_1(\gamma(x_i) - \gamma(y_i))] \\
&= \sum_{i=1}^{n} [w_1(\beta(x_i) - \beta(y_i)) + w_1(\gamma(x_i) - \gamma(y_i))] \\
&= \sum_{i=1}^{n} w_H[(\beta(x_i) - \beta(y_i), \gamma(x_i) - \gamma(y_i))] \\
&= \sum_{i=1}^{n} w_H[(\beta(x_i), \gamma(x_i)) - (\beta(y_i), \gamma(y_i))] \\
&= \sum_{i=1}^{n} w_H(\phi(x_i) - \phi(y_i)) \\
&= \sum_{i=1}^{n} d_H(\phi(x_i), \phi(y_i)) \\
&= \sum_{i=1}^{n} d_H(\psi(x_i, y_i)) \qquad \text{(por el Lema 2.1.2)} \\
&= \sum_{i=1}^{n} d_L(x_i, y_i) \\
&= \sum_{i=1}^{n} w_L(x_i - y_i) = \tilde{w}_L(\underline{x} - \underline{y}) = d_L(\underline{x}, \underline{y})
\end{aligned}$$

□

2.3 LA FUNCIÓN DE GRAY GENERALIZADA

En esta sección presentamos una versión general de la función de Gray (cf. [4]) además, en lo sucesivo, $\langle * \rangle_k$ representará que el elemento o símbolo, se repite k-veces en un vector.

2.3.1 Producto de Kronecker

Definición 2.3.1. Sean R un anillo conmutativo con identidad, n, m enteros positivos y dos vectores $u = (u_0, u_1, \ldots, u_{n-1}) \in R^n$, $v = (v_0, v_1, \ldots, v_{m-1}) \in R^m$, el *producto de Kronecker expandido de derecha a izquierda* de u y v está definido por:

$$u \otimes v = (u_0 v, u_1 v, \ldots, u_{n-1} v) \in R^{mn}, \tag{2.3.1}$$

donde, $u_j v = (u_j v_0, u_j v_1, \ldots, u_j v_{m-1}) \in R^m$ para $0 \leq j \leq n$.

Observación 2.3.2. (i) De manera similar a (2.3.1) se define el *producto de Kronecker expandido de izquierda a derecha* mediante:

$$u \otimes v = (u v_0, u v_1, \ldots, u v_{m-1}).$$

(ii) El producto de Kronecker no es conmutativo en general.

Dados $u = (1, 0), v = (0, 1) \in R^2$ se sigue que:

$$\begin{aligned} u \otimes v &= (1v, 0v) = (1 \cdot 0, 1 \cdot 1, 0 \cdot 0, 0 \cdot 1) = (0, 1, 0, 0), \\ v \otimes u &= (0u, 1u) = (0 \cdot 1, 0 \cdot 0, 1 \cdot 1, 1 \cdot 0) = (0, 0, 1, 0), \end{aligned}$$

es decir, $u \otimes v \neq v \otimes u$.

(iii) Las propiedades del producto de Kronecker son las siguientes:

$$\begin{aligned} u \otimes (v + w) &= (u \otimes v) + (u \otimes w), \\ (u + v) \otimes w &= (u \otimes w) + (v \otimes w), \\ \lambda(v \otimes w) &= (\lambda u) \otimes v = u \otimes (\lambda w), \end{aligned}$$

donde $u \in R^n$, $v \in R^m$, $w \in R^l$, $n, m, l \in \mathbb{N}$ y $\lambda \in R$.

(iv) Si u está dado por bloques:

$$u = \left(u^{[1]} \mid u^{[2]} \mid \cdots \mid u^{[r]} \right)$$

entonces:

$$u \otimes v = (u^{(1)} \otimes v \mid u^{(2)} \otimes v \mid \cdots \mid u^{(r)} \otimes v)$$

2.3.2 Los elementos de $\mathbb{F}_q$

El propósito de este apartado será introducir una forma muy particular de ordenar los elementos del campo finito como en [13] y [14].

Sean $\mathbb{F}_q$ un campo finito con $q = p^m$ elementos y ω un generador del grupo de unidades $\mathbb{F}^*$, es decir ω es un elemento primitivo y consideremos:

$$\beta := \{1, \omega, \omega^2, \ldots, \omega^{m-1}\}, \tag{2.3.2}$$

una base para $\mathbb{F}_q$ visto como un $\mathbb{F}_p$-espacio vectorial, tal como se menciono en la Sección 1.1. Por otro lado, sea $\mathbb{Z}_{p^m} = \mathbb{Z}/p^m\mathbb{Z}$, y dado un elemento $h \in \mathbb{Z}_{p^m}$, éste puede expresarse de la siguiente manera:

$$h = h_0 + h_1 p + h_2 p^2 + \cdots + h_{m-1} p^{m-1}, \tag{2.3.3}$$

donde: $0 \leq h_j \leq p-1$ y $0 \leq j \leq m-1$.

Haciendo uso de (2.3.2) y (2.3.3) podemos definir una biyección:

$$\begin{gathered} \mathbb{Z}_{p^m} \to \mathbb{F}_q \\ h = h_0 + h_1 + \cdots + h_{m-1} p^{m-1} \mapsto \omega_h = h_0 + h_1 \omega + \cdots + h_{m-1} \omega^{m-1}. \end{gathered} \tag{2.3.4}$$

Luego, usando el orden de los enteros representantes de las clases de $\mathbb{Z}_{p^m}$ podemos ordenar el campo finito $\mathbb{F}_q$:

$$\mathbb{F}_q = \{\omega_0, \omega_1, \ldots, \omega_{p^m-1}\}. \tag{2.3.5}$$

Ejemplo 2.3.3. Considere $p = 2$, $m = 3$. Sabemos que el campo finito $\mathbb{F}_8$ puede ser ordenado mediante las potencias de un elemento primitivo ω:

$$\mathbb{F}_8 := \{0, 1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$$

Pero usando la biyección (2.3.4) entre $\mathbb{Z}_8$ y $\mathbb{F}_8$ tenemos que:

$$\begin{aligned}
0 + (0)2 + (0)4 = 0 &\mapsto \omega_0 = 0 \\
1 + (0)2 + (0)4 = 1 &\mapsto \omega_1 = 1 \\
0 + (1)2 + (0)4 = 2 &\mapsto \omega_2 = \omega \\
1 + (1)2 + (0)4 = 3 &\mapsto \omega_3 = 1 + \omega \\
0 + (0)2 + (1)4 = 4 &\mapsto \omega_4 = \omega^2 \\
1 + (0)2 + (1)4 = 5 &\mapsto \omega_5 = 1 + \omega^2 \\
0 + (1)2 + (1)4 = 6 &\mapsto \omega_6 = \omega + \omega^2 \\
1 + (1)2 + (1)4 = 7 &\mapsto \omega_7 = 1 + \omega + \omega^2.
\end{aligned}$$

Ahora, tomando el polinomio mínimo de ω dado por $m(x) = x^3 + x + 1$ tenemos que:

$$\omega^3 = \omega + 1$$

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

de ahí que, tras ordenar como en (2.3.5) y comparar tenemos que:

$$\mathbb{F}_8 = \{\omega_0, \omega_1, \omega_2, \omega_3, \omega_4, \omega_5, \omega_6, \omega_7\} = \{0, 1, \omega, \omega^3, \omega^2, \omega^6, \omega^4, \omega^5\}.$$

Con este ejemplo podemos ver que los elementos de un campo finito admiten más de un orden, ya sea basados en las potencias de un elemento primitivo o usando (2.3.5).

Lema 2.3.4. *Considere a $\mathbb{F}_q$ como en (2.3.5) y sean $0 \leq i \leq p^{m-1}$, $0 \leq j, k \leq p-1$. Entonces:*

$$\omega_{ip} + k = \omega_{ip+k}, \tag{2.3.6}$$

$$\omega_{ip+j} + k = \omega_{ip+(j+k)_p} \tag{2.3.7}$$

donde $(*)_p$ denota la reducción módulo p.

Demostración. Sea $0 \leq i \leq p^{m-1}$ entonces:

$$ip = 0 + h_1 p + \cdots + h_{m-1} p^{m-1},$$

para algunos, $h_j \in \{0, 1, \ldots, p-1\}$ y $j \in \{1, \ldots, m-1\}$. Entonces es claro que si $j, k \in \{0, 1, \ldots, p-1\}$, $(j+k)_p \in \{0, 1, \ldots, p-1\}$ y así:

$$\begin{aligned}
ip + k &= k + h_1 p + \cdots + h_{m-1} p^{m-1}, \\
ip + (j+k)_p &= (j+k)_p + h_1 p + \cdots + h_{m-1} p^{m-1}.
\end{aligned}$$

Ahora, consideremos los elementos $\omega_{ip}, \omega_{ip+j} \in \mathbb{F}_q$, por la biyección (2.3.4) tenemos:

$$\begin{aligned}
\omega_{ip} &= h_1 \omega + \cdots + h_{m-1} \omega^{m-1} \\
\Rightarrow \omega_{ip} + k &= k + h_1 \omega + \cdots + h_{m-1} \omega^{m-1},
\end{aligned}$$

mientras que:

$$\begin{aligned}
\omega_{ip+k} &= k + h_1 \omega + \cdots + h_{m-1} \omega^{m-1} \\
\Rightarrow \omega_{ip+j} + k &= \left(j + h_1 \omega + \cdots + h_{m-1} \omega^{m-1}\right) + k \\
&= (j+k)_p + h_1 \omega + \cdots + h_{m-1} \omega^{m-1}.
\end{aligned}$$

una rápida comparación de las expresiones anteriores nos lleva a la conclusión. □

Dado $\mathbb{F}_q$ con el orden (2.3.5) definimos como en [13] los vectores:

$$\Omega_i = \left(\omega_{ip}, \omega_{ip+1}, \ldots, \omega_{ip+(p-1)}\right) \tag{2.3.8}$$

para $0 \leq i \leq p^{m-1} - 1$. En realidad, estos vectores son *bloques* de longitud p y serán de utilidad al definir la función de Gray.

Ejemplo 2.3.5. Continuando con el Ejemplo 2.3.3, para $\mathbb{F}_8$, los bloques de longitud p son:

$$\begin{aligned}
\Omega_0 &= (\omega_0, \omega_1) = (0, 1) \\
\Omega_1 &= (\omega_2, \omega_3) = (\omega, \omega^3) = (\omega, \omega + 1) \\
\Omega_2 &= (\omega_4, \omega_5) = (\omega^2, \omega^6) = (\omega^2, \omega^2 + 1) \\
\Omega_3 &= (\omega_6, \omega_7) = (\omega^4, \omega^5) = (\omega^2 + \omega, \omega^2 + \omega + 1).
\end{aligned}$$

2.3.3 Dos definiciones de la función de Gray

En este apartado, supondremos que el producto de Kronecker está siendo expandido de izquierda a derecha.

Definición 2.3.6. Sea $\mathbb{F}_q$ el campo finito con $q = p^m$ y los vectores $u, v \in \mathbb{F}_q^q$:

$$u = \left(\Omega_0, \ldots, \Omega_i, \ldots, \Omega_{p^m-1}\right) \tag{2.3.9}$$

$$v = \underbrace{(1, \ldots, 1, \ldots, 1)}_{q-veces} \tag{2.3.10}$$

definimos los vectores en $\mathbb{F}_q^{q^2}$:

$$\begin{aligned}
\mathbf{c}_0 &= u \otimes v \\
\mathbf{c}_1 &= v \otimes u \\
\mathbf{c}_2 &= v \otimes v
\end{aligned} \tag{2.3.11}$$

Es claro que el vector u enlista a todos los elementos de $\mathbb{F}_q$ y v consta de la unidad en sus q-entradas como se hace en [4]. Con estos vectores podemos definir la función de Gray en de forma general para nuestros propósitos. Sean $R = GR(p^3, m)$, n un entero positivo y dado un elemento $\underline{c} \in R^n$ denotaremos para $0 \leq i \leq 2$:

$$r_i(\underline{c}) = (r_i(c_0), r_i(c_1), \ldots, r_i(c_{n-1}))$$

donde $r_i(c_j)$ es como en el Teorema 1.4.9 (pág. 19), entonces:

Definición 2.3.7. La función de Gray está dada por:

$$\begin{aligned}
\Phi : R^n &\to \mathbb{F}_q^{nq^2} \\
\underline{c} &\mapsto r_0(\underline{c}) \otimes \mathbf{c}_0 + r_1(\underline{c}) \otimes \mathbf{c}_1 + r_2(\underline{c}) \otimes \mathbf{c}_2
\end{aligned} \tag{2.3.12}$$

donde $q = p^m$.

Observación 2.3.8. En [8], se define de manera general la función de Gray para anillos finitos de cadena, sin embargo tomando el caso particular para anillos finitos de cadena de índice de nilpotencia 3 tenemos lo que sigue:

Sean $0 \leq i, j \leq p^m - 1$, $r_0(\underline{c}), r_1(\underline{c}), r_2(\underline{c})$ las μ-reducciones de las componentes p-ádicas de un elemento y considerando el orden (2.3.5) en $\mathbb{F}_q$ $\underline{c} \in R^n$ entonces:

$$\Phi(\underline{c}) = (b_0, b_1 \ldots, b_{p^{q-1}}) \tag{2.3.13}$$

donde:

$$b_{iq+j} = \omega_j r_0(\underline{c}) + \omega_i r_1(\underline{c}) + r_2(\underline{c})$$

Podemos apreciar que la versatilidad al definir la función de Gray en distintas maneras, no afecta el orden supuesto en (2.3.5), lo cual resalta la importancia del mismo.

Proposición 2.3.9. *Las expresiones* (2.3.12) *y* (2.3.13) *para la función de Gray son equivalentes.*

Demostración. Demostraremos que los bloques de longitud nq correspondientes entre ambas expresiones coinciden.

En efecto, tomemos el k-ésimo bloque de longitud nq en (2.3.13) esto es:

$$B_k := (b_{kq}, \ldots, b_{kq+j}, \ldots, b_{kq+(q-1)})$$

dado que cada b_l es de longitud n. Desarrollando esto:

$$\begin{aligned}
B_k &= (\omega_0 r_0(\underline{c}) + \omega_k r_1(\underline{c}) + r_2(\underline{c}), \ldots, \omega_j r_0(\underline{c}) + \omega_k r_1(\underline{c}) + r_2(\underline{c}), \ldots, \\
&\qquad \omega_{q-1} r_0(\underline{c}) + \omega_k r_1(\underline{c}) + r_2(\underline{c})) \\
&= (\omega_0 r_0(\underline{c}), \ldots, \omega_j r_0(\underline{c}), \ldots, \omega_{q-1} r_0(\underline{c})) + (\omega_k r_1(\underline{c}), \ldots, \omega_k r_1(\underline{c}), \ldots, \omega_k r_1(\underline{c})) + \\
&\qquad (r_2(\underline{c}), \ldots, r_2(\underline{c}), \ldots, r_2(\underline{c})) \\
&= r_0(\underline{c}) \otimes (\omega_0, \ldots, \omega_j, \ldots, \omega_{p^m-1}) + r_1(\underline{c}) \otimes (\omega_k, \ldots, \omega_k, \ldots, \omega_k) + \\
&\qquad r_2(\underline{c}) \otimes (1, \ldots, 1, \ldots, 1) \\
&= r_0(\underline{c}) \otimes u + r_1(\underline{c}) \otimes (\omega_k v) + r_2(\underline{c}) \otimes v.
\end{aligned} \tag{2.3.14}$$

Por otro lado, analizando los vectores $\mathbf{c}_0, \mathbf{c}_1$ y $\mathbf{c}_2$ tenemos que:

$$\begin{aligned}
\mathbf{c}_0 &= u \otimes (1, \ldots, 1, \ldots, 1) \\
\mathbf{c}_1 &= v \otimes (\omega_0, \ldots, \omega_k, \ldots, \omega_{p^m-1}) \\
\mathbf{c}_2 &= v \otimes (1, \ldots, 1, \ldots, 1)
\end{aligned} \tag{2.3.15}$$

por (iv) de la Observación 2.3.2 el k-ésimo bloque de longitud q de cada vector está dado por:

$$\mathbf{c}_0^{[k]} = u, \quad \mathbf{c}_1^{[k]} = w_k v, \quad \mathbf{c}_2^{[k]} = v \tag{2.3.16}$$

de ahí que el k-ésimo bloque de longitud nq de $\phi(\underline{c})$, denotado por $\phi(\underline{c})^{[k]}$ está dado por:

$$\Phi(\underline{c})^{[k]} = r_0(\underline{c}) \otimes u + r_1(\underline{c}) \otimes (\omega_k v) + r_2(\underline{c}) \otimes v, \tag{2.3.17}$$

una comparación de (2.3.14) y (2.3.17) prueba la afirmación. □

Para alcanzar el propósito de entender la importancia de la función de Gray, veamos un resultado auxiliar de gran ayuda:

Proposición 2.3.10. *Sean $\underline{c}, \underline{d} \in R^n$. Entonces:*

$$\Phi(p^2\underline{c}) = (r_0(\underline{c}), \ldots, r_0(\underline{c}), \ldots, r_0(\underline{c})), \tag{2.3.18}$$

$$\Phi(\underline{d} + p^2\underline{c}) = \Phi(\underline{d}) + \phi(p^2\underline{c}). \tag{2.3.19}$$

Demostración. Por el Teorema 1.4.12 tenemos que:

$$r_0(p^2\underline{c}) = \underline{0}, \quad r_1(p^2\underline{c}) = \underline{0}, \quad r_2(p^2\underline{c}) = r_2(\underline{c}) \tag{2.3.20}$$

entonces:

$$\begin{aligned}
\Phi(p^2\underline{c}) &= r_0(p^2\underline{c}) \otimes \mathbf{c}_0 + r_1(p^2\underline{c}) \otimes \mathbf{c}_1 + r_2(p^2\underline{c}) \otimes \mathbf{c}_2 \\
&= \underline{0} \otimes \mathbf{c}_0 + \underline{0} \otimes \mathbf{c}_1 + r_0(\underline{c}) \otimes \mathbf{c}_2 \\
&= r_0(\underline{c}) \otimes (1, \ldots, 1 \ldots, 1) \\
&= (r_0(\underline{c}), \ldots, r_0(\underline{c}), \ldots, r_0(\underline{c})).
\end{aligned}$$

Por otro lado, por las ecuaciones (1.4.22), y (2.3.20), para cada $0 \leq i \leq n$:

$$\begin{aligned}
r_0(d_i + p^2c_i) &= r_0(d_i) \\
r_1(d_i + p^2c_i) &= [r_1(d_i)^p - h_0(r_0(d_i), 0)]^{1/p} \\
r_2(d_i + p^2c_i) &= \left[r_2(d_i)^{p^2} + r_0(c_i)^{p^2} - h_1(r_0(d_i), r_1(d_i)^p, 0, 0)\right]^{1/p^2}
\end{aligned}$$

dado que los polinomios h_0, h_1 son polinomios con término constante cero y están formados por los productos cruzados entonces éstos se anulan en este caso y así:

$$\begin{aligned}
\Phi(\underline{d} + p^2\underline{c}) &= r_0(\underline{d} + p^2\underline{c}) \otimes \mathbf{c}_0 + r_1(\underline{d} + p^2\underline{c}) \otimes \mathbf{c}_1 + r_2(\underline{d} + p^2\underline{c}) \otimes \mathbf{c}_2 \\
&= r_0(\underline{d}) \otimes \mathbf{c}_0 + r_1(\underline{d}) \otimes \mathbf{c}_1 + [r_2(\underline{d}) + r_0(\underline{c})] \otimes \mathbf{c}_2 \\
&= r_0(\underline{d}) \otimes \mathbf{c}_0 + r_1(\underline{d}) \otimes \mathbf{c}_1 + r_2(\underline{d}) \otimes \mathbf{c}_2 + r_0(\underline{c}) \otimes \mathbf{c}_2 \\
&= \Phi(\underline{d}) + \Phi(p^2\underline{c}).
\end{aligned}$$

□

Como se mencionó al inicio de éste capítulo, el siguiente resultado una propiedad importante de la función de Gray para la teoría de códigos sobre anillos finitos de cadena.

Teorema 2.3.11. *La función de Gray es una isometría inyectiva preservadora de peso entre* $(R^n, \mathbf{d}_{hom})$ *y* $(\mathbb{F}_q^{nq^2}, \mathbf{d}_H)$.

Demostración. Sean $\underline{c}, \underline{d} \in R^n$ tales que $\Phi(\underline{c}) = \Phi(\underline{c})$, por la ecuación (2.3.17), el k-ésimo bloque de longitud nq de la diferencia $\Phi(\underline{c}) - \Phi(\underline{d})$ está dado por:

$$(r_0(\underline{c}) - r_0(\underline{d})) \otimes u + (r_1(\underline{c}) - r_1(\underline{d})) \otimes \langle \omega_k \rangle_q + (r_2(\underline{c}) - r_2(\underline{d})) \otimes v = \langle 0 \rangle_{nq}.$$

Luego, el i-ésimo bloque de longitud np es:

$$(r_0(\underline{c}) - r_0(\underline{d})) \otimes \Omega_i + (r_1(\underline{c}) - r_1(\underline{d})) \otimes \langle \omega_k \rangle_p + (r_2(\underline{c}) - r_2(\underline{d})) \otimes \langle 1 \rangle_p = \langle 0 \rangle_{np},$$

y su j-ésima componente es:

$$(r_0(\underline{c}) - r_0(\underline{d}))\, \omega_{ip+j} + (r_1(\underline{c}) - r_1(\underline{d}))\, \omega_k + (r_2(\underline{c}) - r_2(\underline{d})) = 0.$$

Como ω es un elemento primitivo entonces $\omega_{ip+j}, \omega_k, 1$ son linealmente independientes, de ahí que: $r_t(\underline{c}) = r_t(\underline{d})$ con $0 \leq t \leq 2$, y así para cada $l \in \{0, 1, \ldots, n-1\}$:

$$\Gamma(c_l) = (r_0(c_l), r_1(c_l)^p, r_0(c_l)^{p^2}) = (r_0(d_l), r_1(d_l)^p, r_0(d_l)^{p^2}) = \Gamma(d_l).$$

y como Γ es un isomorfismo, se sigue que $c_l = d_l$ y se concluye que $\underline{c} = \underline{d}$, es decir, Φ es inyectiva.

Para ver que Φ es una isometría basta con mostrar que $w_{hom}(c_l - d_l) = w_H(\Phi(c_l) - \Phi(d_l))$ para $0 \leq l \leq n-1$ con $c_l \neq d_l$, podemos considerar los siguientes casos:

CASO 1: $c_l - d_l \in (p^2) \setminus \{0\}$ entonces existe $e_l \in R$ tal que $c_l - d_l = p^2 e_l$ luego tenemos que $c_l = p^2 e_l + d_l$ y así por la Proposición 2.3.10 tenemos que:

$$\begin{aligned} \Phi(c_l) &= \Phi(d_l + p^2 e_l) \\ &= \Phi(d_l) + \Phi(p^2 e_l) \end{aligned}$$

de ahí que $\Phi(c_l) - \Phi(d_l) = \Phi(p^2 e_l)$ y se tiene que:

$$w_H(\Phi(c_l) - \Phi(d_l)) = w_H(\Phi(p^2 e_l)) = w_H(\langle r_0(e_l) \rangle_{q^2}). \tag{2.3.21}$$

Notemos que si $r_0(e_l) = 0$ entonces $r_t(c_l) = r_t(d_l)$, con $0 \leq t \leq 2$, (cf. Teorema 1.4.12), pero esto implica que $c_l = d_l$ lo cual no puede ocurrir, de ahí que $r_0(e_l) \neq 0$ y en consecuencia:

$$w_H(\Phi(c_i) - \Phi(d_i)) = q^2 = p^{2m} = w_{hom}(c_i - d_i).$$

CASO 2: $c_l - d_l \in R \setminus (p^2)$, en este caso tenemos que $c_l - d_l$ puede ser una unidad o bien pertenece a (p), en cualquier caso tenemos que:

$$c_l = d_l + p^k e_l \qquad (k = 0, 1).$$

Para determinar el valor de $w_H(\Phi(c_l) - \Phi(d_l))$ basta con hallar las componentes que son cero, así viendo a la función de Gray como en (2.3.13), estudiemos la expresión:

$$\omega_l(r_0(p^k e_l)) + \omega_j(r_1(p^k e_l)) + (r_2(p^k e_l)) = 0 \in \mathbb{F}_q. \tag{2.3.22}$$

Por el Teorema 1.4.12 tenemos que si $k \leq t \leq 2$ entonces $r_t(p^k e_l) \neq 0$, es decir que al menos $r_1(p^k e_l), r_2(p^k e_l) \neq 0$, en (2.3.22), de ahí que:

$$\omega_j = -\Big(\omega_l(r_0(p^k e_l)) + r_2(p^k e_l)\Big)\Big(r_1(p^k e_l)\Big)^{-1}$$

debido a que para $0 \leq i \leq 2$, los términos $r_i(p^k e_l)$ están determinados de manera única (puesto que las componentes p-ádicas lo están) y $\omega_l \in \mathbb{F}_{p^m}$, es claro que hay p^m soluciones diferentes para (2.3.22) (al menos una por cada valor de ω_l), por consiguiente:

$$w_H(\Phi(c_l) - \Phi(d_l)) = p^{2m} - p^m = p^m(p^m - 1) = w_{hom}(c_l - d_l). \tag{2.3.23}$$

Finalmente, observemos que:

$$\begin{aligned} \mathbf{w}_{hom}(\underline{c}) &= \mathbf{d}_{hom}(\Phi(\underline{c}), \Phi(\underline{0})) \\ &= d_H(\Phi(\underline{c}), \underline{0}) = w_H(\Phi(\underline{c})), \end{aligned}$$

lo cual demuestra que la función de Gray preserva el peso. □

Ejemplo 2.3.12. (i) Considere el código C definido sobre el anillo de Galois $GR(2^3, 3)$ como en el Ejemplo 1.3.10, tomemos dos palabras-código de C y calculemos sus imágenenes de Gray, por el Ejemplo 2.3.3 tenemos que: $u = (\Omega_0 \mid \Omega_1 \mid \Omega_2 \mid \Omega_3)$ y además $v = (\langle 1\rangle_2 \mid \langle 1\rangle_2 \mid \langle 1\rangle_2 \mid \langle 1\rangle_2)$, de ahí que:

$$\begin{aligned} \mathbf{c}_0 &= (\langle u\rangle_2 \mid \langle u\rangle_2 \mid \langle u\rangle_2 \mid \langle u\rangle_2) \\ \mathbf{c}_1 &= (\langle \Omega_0\rangle_8 \mid \langle \Omega_1\rangle_8) \mid \langle \Omega_2\rangle_8 \mid \langle \Omega_3\rangle_8) \\ \mathbf{c}_2 &= (\langle v\rangle_2 \mid \langle v\rangle_2 \mid \langle v\rangle_2 \mid \langle v\rangle_2), \end{aligned} \tag{2.3.24}$$

$\Phi((2x, x, x^2))$

$\Big(0000\omega\omega^2 \mid 0\omega^2\omega^3 0\omega^4\omega^5 \mid 0\omega^3\omega^4 01\omega \mid 0\omega^5\omega^6 0\omega^6 1 \mid \omega 00\omega\omega\omega^2 \mid \omega\omega^2\omega^3\omega\omega^4\omega^5 \mid$

$\omega\omega^3\omega^4\omega 1\omega \mid \omega\omega^5\omega^6\omega\omega^6 1 \mid \omega^2 00\omega^2\omega\omega^2 \mid \omega^2\omega^2\omega^3\omega^2\omega^4\omega^5 \mid \omega^2\omega^3\omega^4\omega^2 1\omega \mid$

$\omega^2\omega^5\omega^6\omega^2\omega^6 1 \mid \omega^4 00\omega^4\omega\omega^2 \mid \omega^4\omega^2\omega^3\omega^4\omega^4\omega^5 \mid \omega^4\omega^3\omega^4\omega^4 1\omega \mid \omega^4\omega^5\omega^6\omega^4\omega^6 1 \mid$

$\omega^3 00\omega^3\omega\omega^2 \mid \omega^3\omega^2\omega^3\omega^3\omega^4\omega^5 \mid \omega^3\omega^3\omega^4\omega^3 1\omega \mid \omega^3\omega^5\omega^6\omega^3\omega^6 1 \mid 1001\omega\omega^2 \mid$
$1\omega^2\omega^3 1\omega^4\omega^5 \mid 1\omega^3\omega^4 11\omega \mid 1\omega^5\omega^6 1\omega^6 1 \mid \omega^5 00\omega^5\omega\omega^2 \mid \omega^5\omega^2\omega^3\omega^5\omega^4\omega^5 \mid$
$\omega^5\omega^3\omega^4\omega^5 1\omega \mid \omega^5\omega^5\omega^6\omega^5\omega^6 1 \mid \omega^6 00\omega^6\omega\omega^2 \mid \omega^6\omega^2\omega^3\omega^6\omega^4\omega^5 \mid$
$\omega^6\omega^3\omega^4\omega^6 1\omega \mid \omega^6\omega^5\omega^6\omega^6\omega^6 1\Big)$

$\Phi((5x^2, 2x, x))$
$\Big(\omega^2 0000\omega \mid \omega^5 0\omega^2\omega^3 0\omega^4 \mid \omega 0\omega^3\omega^4 01 \mid 10\omega^5\omega^6 0\omega^6 \mid \omega^2\omega 00\omega\omega \mid \omega^5\omega\omega^2\omega^3\omega\omega^4 \mid$
$\omega\omega\omega^3\omega^4\omega 1 \mid 1\omega\omega^5\omega^6\omega\omega^6 \mid \omega^2\omega^2 00\omega^2\omega \mid \omega^5\omega^2\omega^2\omega^3\omega^2\omega^4 \mid \omega\omega^2\omega^3\omega^4\omega^2 1 \mid$
$1\omega^2\omega^5\omega^6\omega^2\omega^6 \mid \omega^2\omega^4 00\omega^4\omega \mid \omega^5\omega^4\omega^2\omega^3\omega^4\omega^4 \mid \omega\omega^4\omega^3\omega^4\omega^4 1 \mid 1\omega^4\omega^5\omega^6\omega^4\omega^6 \mid$
$\omega^2\omega^3 00\omega^3\omega \mid \omega^5\omega^3\omega^2\omega^3\omega^3\omega^4 \mid \omega\omega^3\omega^3\omega^4\omega^3 1 \mid 1\omega^3\omega^5\omega^6\omega^3\omega^6 \mid \omega^2 1001\omega \mid$
$\omega^5 1\omega^2\omega^3 1\omega^4 \mid \omega 1\omega^3\omega^4 11 \mid 11\omega^5\omega^6 1\omega^6 \mid \omega^2\omega^5 00\omega^5\omega \mid \omega^5\omega^5\omega^2\omega^3\omega^5\omega^4 \mid$
$\omega\omega^5\omega^3\omega^4\omega^5 1 \mid 1\omega^5\omega^5\omega^6\omega^5\omega^6 \mid \omega^2\omega^6 00\omega^6\omega \mid \omega^5\omega^6\omega^2\omega^3\omega^6\omega^4 \mid \omega\omega^6\omega^3\omega^4\omega^6 1 \mid$
$1\omega^6\omega^5\omega^6\omega^6\omega^6\ \Big)$

En este ejemplo, puede notarse como fácilmente el tamaño de las palabras código se "dispara" cuando se utiliza la función de Gray sobre anillos de Galois de índice de nilpotencia 3, más aún si calculamos el peso de Hamming de cada palabra código, podemos observar que es 168 puesto que ambas palabras tienen 24 ceros, si buscamos en la tabla de pesos del Ejemplo 1.3.10 podemos ver que las palabras código de donde provienen poseen peso 168.

(ii) Ahora, en este caso consideremos el anillo de Galois $GR(2^3, 2)$ y apliquemos el Teorema 2.3.11 a un par de palabras código de longitud 3 en este anillo. Así $u = (\Omega_0 \mid \Omega_1)$, $v = (\langle 1\rangle_2 \mid \langle 1\rangle_2)$ luego:

$$\begin{aligned}
\mathbf{c}_0 &= (01\omega\omega^2 \mid 01\omega\omega^2 \mid 01\omega\omega^2 \mid 01\omega\omega^2)\\
\mathbf{c}_1 &= (0000 \mid 1111 \mid \omega\omega\omega\omega \mid \omega^2\omega^2\omega^2\omega^2)\\
\mathbf{c}_2 &= (1111 \mid 1111 \mid 1111 \mid 1111)
\end{aligned}$$

en consecuencia:

$\Phi((1, 3, x))$
$\big(00011\omega \mid \omega\omega\omega^2\omega^2\omega^2 1 \mid 01010\omega \mid \omega\omega^2\omega^2\omega^2\omega 1 \mid$
$0\omega 01\omega^2\omega \mid \omega 0\omega^2\omega^2 11 \mid 0\omega^2 01\omega\omega \mid \omega 1\omega^2\omega^2 01\big)$
$\Phi((5x, 1, 3))$
$\big(\omega 00011 \mid 1\omega\omega\omega^2\omega^2\omega^2 \mid \omega 01010 \mid 1\omega\omega^2\omega^2\omega^2\omega \mid$
$\omega 0\omega 01\omega^2 \mid 1\omega 0\omega^2\omega^2 1 \mid \omega 0\omega^2 01\omega \mid 1\omega 1\omega^2\omega^2 0\big)\,.$

Por otro lado, tenemos que:

$$w_{hom}(c) = \begin{cases} 12 & c \in R \setminus (4) \\ 16 & c \in (4) \setminus \{0\} \\ 0 & c = 0. \end{cases}$$

además:

$$w_{hom}\left((1,3,x)-(5x,1,3)\right)=w_{hom}((3x+1,2,x+5))=12+12+12=36.$$

Ahora, calculando en $\mathbb{F}_4^{48}$:

$$\begin{aligned}&\Phi((1,3,x))-\Phi((5x,1,3))\\&\left(\omega 0010\omega^2 \mid \omega^2 0100\omega \mid \omega 1111\omega \mid \omega^2 1001\omega^2 \mid\right.\\&\left.\omega\omega\omega 1\omega 1 \mid \omega^2\omega\omega^2 0\omega 0 \mid \omega\omega^2\omega^2 1\omega^2 0 \mid \omega^2\omega^2\omega 0\omega^2 1\right),\end{aligned}$$

como puede observarse, hay 12 entradas iguales a cero en la diferencia de $\Phi((1,3,x))-\Phi((5x,1,3))$, de ahí que:

$$w_H\left(\Phi((1,3,x))-\Phi((5x,1,3))\right)=48-12=36=w_{hom}((1,3,x)-(5x,1,3)).$$

3 IMÁGENES DE GRAY DE R-CÓDIGOS

3.1 IMAGEN DE GRAY DE UN CÓDIGO CONSTACÍCLICO

En este último capítulo estudiaremos dos familias de códigos definidos sobre anillos de Galois y su relación con códigos sobre campos finitos a tráves de sus imágenes de Gray, por esta razón en lo sucesivo $R = GR(p^3, m)$, $\mathcal{T}$ es el conjunto de Teichmüller de R, C denotará a un código definido sobre R^n y $(n, p) = 1$.

3.1.1 Códigos constacíclicos

Definición 3.1.1. Sea $\lambda = 1 - p^2 = 1 + N'p^2$, donde $N' \in \mathcal{T}$ es un elemento tal que $\mu(N') = -1$. Un corrimiento λ-cíclico o constacíclico es una función dada por:

$$\begin{aligned} \nu_\lambda : R^n &\to R^n \\ (c_0, \ldots, c_{n-2}, c_{n-1}) &\mapsto (\lambda c_{n-1}, c_0, \ldots, c_{n-2}). \end{aligned}$$

Un código C es llamado *constacíclico* o *λ-cíclico* si y sólo si $\nu_\lambda(C) \subseteq C$.

Ejemplo 3.1.2. (i) El código C dado en el Ejemplo 1.3.10 es un código λ-cíclico en el anillo $GR(2^3, 3)$ con $\lambda = 1 - 2^2 \equiv 5 \pmod{2^3}$, de longitud $n = 3$:

$$C := \left\{ (2x, x, x^2), (5x^2, 2x, x), (5x, 5x^2, 2x), (2x, 5x, 5x^2), (x^2, 2x, 5x), (x, x^2, 2x) \right\},$$

hemos resaltado el producto de λ con cada componente de los elementos de C. Ahora, dado que que $5^2 \equiv 1 \pmod{2^3}$ es claro que $\lambda^2 = 1$ y más aún el producto de λ con 2 no altera a éste, es decir, $5(2) \equiv 2 \pmod{2^3}$.

Aquí hemos considerado a la palabra código $(2x, x, x^2)$ como el *generador*[1] del código, sin embargo como es de esperarse, puede partirse de cualquiera de ellas y al aplicar ν_λ se recupera el código.

(ii) Considere $R = GR(3^3, 2)$ y $n = 4$. Entonces $\lambda = 1 - 3^2 \equiv 19 \pmod{3^3}$ y considere las palabras código: $(6, 6, 6, 6)$, $(6x, 6, 6, 6)$ y

1 Se usa esté término en paralelismo al generador de un grupo cíclico.

$(x,6,6,6)$, dado que $19(6) \equiv 6 \pmod{3^3}$ tenemos los siguientes resultados:

$$\begin{aligned} \nu_\lambda((6,6,6,6)) &= (6,6,6,6) \\ \nu_\lambda((6x,6,6,6)) &= (6,6x,6,6) \\ \nu_\lambda((x,6,6,6)) &= (6,x,6,6). \end{aligned}$$

Como podemos apreciar, el primer vector no se altera bajo ν_λ puesto que ninguna entrada lo hace, mientras que el segundo y el tercero muestran un "corrimiento" de sus componentes, si continuaramos aplicando ν_λ a éstos obtendríamos respectivamente:

$$\begin{aligned} C_1 &= \{(6x,6,6,6),(6,6x,6,6),(6,6,6x,6),(6,6,6,6x)\} \\ C_2 &= \{(x,6,6,6),(6,x,6,6),(6,6,x,6),(6,6,6,x),(19x,6,6,6),(6,19x,6,6), \\ &\quad (6,6,19x,6),(6,6,6,19x),(10x,6,6,6),(6,10x,6,6),(6,6,10x,6),(6,6,6,10x)\}. \end{aligned}$$

La diferencia entre la cantidad de elementos al aplicar de manera sucesiva ν_λ se sustenta en que 6 no es afectado por la acción de λ, pero es interesante notar que basta con que un elemento no tenga como factor a 6 y genera 12 imágenes distintas lo cual resulta del producto de la longitud del vector y el orden de λ.

El Ejemplo 3.1.2 tiene como objetivo exhibir una manera de construir códigos constacíclicos y reconocer particularidades del comportamiento de los elementos del anillo R. Sin embargo, nuestro objetivo en esta sección es mostrar la relación de un código constacíclico sobre R y un código definido sobre el campo residual $\mathbb{F}_{p^m}$.

Proposición 3.1.3. *Sea $\sigma^{\otimes p^{2m-1}}$ como en la Sección 1.3.3 y Φ la función de Gray. Entonces:*

$$\Phi \circ \nu_\lambda = \sigma^{\otimes p^{2m-1}} \circ \Phi \tag{3.1.1}$$

Demostración. Sea $A = (a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in R^n$ y denotemos por $B = (b_0, b_1, \ldots, b_{n-1}) = \nu_\lambda(A)$, entonces:

$$\begin{aligned} b_0 &= \lambda a_{n-1} \\ b_j &= a_{j-1} \qquad (1 \leq j \leq n-2), \end{aligned}$$

así de (1.4.30) tenemos:

$$\begin{aligned} r_0(B) &= (r_0(a_{n-1}), r_0(a_0), \ldots, r_0(a_{n-2})) \\ r_1(B) &= (r_1(a_{n-1}), r_1(a_0), \ldots, r_1(a_{n-2})) \\ r_2(B) &= (r_2(a_{n-1}) - r_0(a_{n-1}), r_2(a_0), \ldots, r_2(a_{n-2})). \end{aligned}$$

Ahora por (2.3.16) el k-ésimo bloque de longitud np^m de $\Phi(B)$ es:

$$\begin{aligned} \Phi(B)^{[k]} &= r_0(B) \otimes u + r_1(B) \otimes \langle \omega_k \rangle_{p^m} + r_2(B) \otimes v \\ &= r_0(B) \otimes (\Omega_0, \ldots, \Omega_i, \ldots, \Omega_{p^m-1}) + r_1(B) \otimes (\langle \omega_k \rangle_p, \ldots, \langle \omega_k \rangle_p, \ldots, \langle \omega_k \rangle_p) + \\ &\quad r_2(B) \otimes (\langle 1 \rangle_p, \ldots, \langle 1 \rangle_p, \ldots, \langle 1 \rangle_p), \end{aligned}$$

así podemos extraer el i-ésimo bloque de longitud np de $\Phi(B)$ y lo denotaremos por $\mathcal{B}_i$

$$\mathcal{B}_i = r_0(B) \otimes \Omega_i + r_1(B) \otimes \langle \omega_k \rangle_p + r_2(B) \otimes \langle 1 \rangle_p, \tag{3.1.2}$$

procediendo como antes y expandiendo los productos tenemos que:

$$\begin{aligned}\mathcal{B}_i = &(r_0(a_{n-1}), r_0(a_0), \ldots, r_0(a_{n-2})) \otimes (\omega ip, \ldots, \omega_{ip+j}, \ldots, \omega_{ip+(p-1)}) \\ &+ (r_1(a_{n-1}), r_1(a_0), \ldots, r_1(a_{n-2})) \otimes (\omega_k, \ldots, \omega_k, \ldots, \omega_k) \\ &+ (r_2(a_{n-1}) - r_0(a_{n-1}), r_2(a_0), \ldots, r_2(a_{n-2})) \otimes (1, \ldots, 1, \ldots, 1),\end{aligned}$$

tras realizar los productos, podemos estudiar el j-ésimo bloque de longitud n de $\mathcal{B}_i$ el cual denotaremos por $\mathcal{B}_{ij}$ es decir:

$$\begin{aligned}\mathcal{B}_{ij} = &\left(r_0(a_{n-1})\omega_{ip+j}, r_0(a_0)\omega_{ip+j}, \ldots, r_0(a_{n-2})\omega_{ip+j}\right) + (r_1(a_{n-1})\omega_k, r_1(a_0)\omega_k, \ldots, r_1(a_{n-2})\omega_k) \\ &+ (r_2(a_{n-1}) - r_0(a_{n-1}), r_2(a_0), \ldots, r_2(a_{n-2})).\end{aligned}$$

Notemos que la primera componente de $\mathcal{B}_{ij}$ es:

$$\begin{aligned}(\mathcal{B}_{ij})_0 = &\quad r_0(a_{n-1})\omega_{ip+j} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) - r_0(a_{n-1}) \\ = &\quad r_0(a_{n-1})\left(\omega_{ip+j} + (p-1)\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \\ = &\quad r_0(a_{n-1})\left(\omega_{ip+(j+p-1)_p}\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \\ = &\quad r_0(a_{n-1})\left(\omega_{ip+(j-1)}\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}),\end{aligned}$$

luego, se sigue que:

$$(\mathcal{B}_{ij})_0 = \quad r_0(a_{n-1})\left(\omega_{ip+(j-1)}\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \tag{3.1.3}$$

$$(\mathcal{B}_{ij})_k = \quad r_0(a_{k-1})\omega_{ip+j} + r_1(a_{k-1})\omega_k + r_2(a_{k-1}) \qquad (1 \leq k \leq n-1) \tag{3.1.4}$$

Por otro lado, aplicando la función de Gray a A nos lleva a:

$$\Phi(A) = r_0(A) \otimes c_0 + r_1(A) \otimes c_1 + r_2(A) \otimes c_2.$$

Procediendo como antes analizaremos el i-ésimo bloque de longitud np de $\Phi(A)$ así:

$$\mathcal{A}_i = r_0(A) \otimes \Omega_i + r_1(A) \otimes \langle \omega_k \rangle_p + r_2(A) \otimes \langle 1 \rangle_p,$$

expandiendo los productos de Kronecker de $\mathcal{A}_i$, podemos escribir dicho bloque como una matriz de dimensiones $n \times p$ es decir:

$$\mathcal{A}_i = \begin{pmatrix} r_0(a_0)\omega_{ip} + r_1(a_0)\omega_k + r_2(a_0) & \cdots & r_0(a_{n-1})\omega_k + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \\ \vdots & \cdots & \vdots \\ r_0(a_0)\omega_{ip+j} + r_1(a_0)\omega_k + r_2(a_0) & \cdots & r_0(a_{n-1})\omega_{ip+j} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \\ \vdots & \cdots & \vdots \\ r_0(a_0)\omega_{ip+(p-1)} + r_1(a_0)\omega_k + r_2(a_0) & \cdots & r_0(a_{n-1})\omega_{ip+(p-1)} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \end{pmatrix}$$

Observemos que al aplicar el corrimiento cíclico $\overline{\sigma}$ (cf. Sección 1.3) en este bloque:

$$\overline{\sigma}(\mathcal{A}_i) = \begin{pmatrix} r_0(a_{n-1})\omega_{ip+(p-1)} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) & \cdots & r_0(a_{n-2})\omega_{ip} + r_1(a_{n-2})\omega_k + r_2(a_{n-2}) \\ \vdots & \cdots & \vdots \\ r_0(a_{n-1})\omega_{ip+(j-1)} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) & \cdots & r_0(a_{n-2})\omega_{ip+j} + r_1(a_{n-2})\omega_k + r_2(a_{n-2}) \\ \vdots & \cdots & \vdots \\ r_0(a_{n-1})\omega_{ip+(p-2)} + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) & \cdots & r_0(a_{n-2})\omega_{ip+(p-1)} + r_1(a_{n-2})\omega_k + r_2(a_{n-2}) \end{pmatrix}$$

Así tenemos las siguientes relaciones para cada componente de $\mathcal{A}_i$:

$$(\mathcal{A}_{ij})_0 = r_0(a_{n-1})\left(\omega_{ip+(j-1)}\right) + r_1(a_{n-1})\omega_k + r_2(a_{n-1}) \tag{3.1.5}$$

$$(\mathcal{A}_{ij})_k = r_0(a_{k-1})\omega_{ip+j} + r_1(a_{k-1})\omega_k + r_2(a_{k-1}) \qquad (1 \leq k \leq n-1). \tag{3.1.6}$$

Una comparación por pares de (3.1.3) con (3.1.5) y (3.1.4) con (3.1.6) nos permite la igualdad:

$$\mathcal{B}_i = \overline{\sigma}(\mathcal{A}_i) \qquad (0 \leq i \leq p^{m-1} - 1)$$

y dado que:

$$\begin{aligned} \Phi(\nu_\lambda(A)) = \Phi(B) &= \left(\mathcal{B}_0 \mid \cdots \mid \mathcal{B}_i \mid \cdots \mid \mathcal{B}_{p^{m-1}-1}\right) \\ &= \left(\overline{\sigma}(\mathcal{A}_0) \mid \cdots \mid \overline{\sigma}(\mathcal{A}_i) \mid \cdots \mid \overline{\sigma}(\mathcal{A}_{p^{m-1}-1})\right) \\ &= \overline{\sigma}^{\otimes p^{2m-1}}(\Phi(A)), \end{aligned} \tag{3.1.7}$$

se sigue el enunciado de la proposición. □

Esta proposición nos permite enunciar el resultado principal de está sección:

Teorema 3.1.4. *Un R-código $\mathcal{C}$ de longitud n es λ-cíclico si y sólo si, su imagen bajo la función de Gray $\Phi(\mathcal{C})$ es un código cuasi-cíclico sobre $\mathbb{F}_{p^m}$ de índice p^{2m-1} y longitud np^{2m}.*

Demostración. Sea $\mathcal{C}$ un R-código tal que $\Phi(\mathcal{C})$ es un código cuasi-cíclico de índice p^{2m-1} y longitud np^{2m}, entonces por definición: $\Phi(\mathcal{C}) = \sigma^{\otimes p^{2m-1}}(\Phi(\mathcal{C}))$ usando la Proposición 3.1.3: $\Phi(\mathcal{C}) = \Phi(\nu_\lambda(\mathcal{C}))$, y de la inyectividad de Φ, $\mathcal{C} = \nu_\lambda(\mathcal{C})$. El recíproco de esta afirmación se sigue de manera análoga. □

Ejemplo 3.1.5. En (i) y (ii) del Ejemplo 2.3.12 se muestran ejemplos de códigos λ-cíclicos y sus imágenes bajo la función de Gray, en particular

para (ii) se observa que: $R = GR(2^3, 2)$ y $n = 3$, de ahí que $\lambda = 1 - 2^2 \equiv 5 \pmod{2^3}$, además $\nu_\lambda((1,3,x)) = (5x, 1, 3)$ y en consecuencia:

$$\begin{aligned}
&\Phi((1,3,x))\\
&(00011\omega \mid \omega\omega\omega^2\omega^2\omega^2 1 \mid 01010\omega \mid \omega\omega^2\omega^2\omega^2\omega 1 \mid 0\omega 01\omega^2\omega \mid \omega 0\omega^2\omega^2 11 \mid\\
&\quad 0\omega^2 01\omega\omega \mid \omega 1\omega^2\omega^2 01)\\
&\Phi((5x,1,3))\\
&(\omega 00011 \mid 1\omega\omega\omega^2\omega^2\omega^2 \mid \omega 01010 \mid 1\omega\omega^2\omega^2\omega^2\omega \mid \omega 0\omega 01\omega^2 \mid 1\omega 0\omega^2\omega^2 1 \mid\\
&\omega 0\omega^2 01\omega \mid 1\omega 1\omega^2\omega^2 0)\,.
\end{aligned}$$

Exhibimos las imágenes bajo la función de Gray cuasi-cíclicas de dos palabras código de un código constacíclico.

3.2 IMAGEN DE GRAY DE UN CÓDIGO γ-CÍCLICO LINEAL

En esta sección estudiaremos una permutación de los elementos del conjunto $\{0, 1, \ldots, np-1\}$, la permutación de Nechaev (cf.[6]), una extensión de ésta y cómo se relaciona con los códigos cíclicos lineales.

3.2.1 Representaciones polinomiales de códigos

Sean p un número primo, n un entero positivo coprimo con p, $n' \in \{1, \ldots, p-1\}$ el inverso módulo p de n, es decir: $nn' \equiv 1 \pmod{p}$ y un elemento $N' \in \mathcal{T}$ tal que $\mu(N') = n'$. Tomaremos las unidades en el anillo de Galois $GR(p^s, m)$:

$$\begin{aligned}
\gamma &:= 1 + N'p^2,\\
\lambda &:= 1 - p^2,
\end{aligned} \tag{3.2.1}$$

bajo la condición que $\lambda\gamma = 1$ y sólo cuando así suceda.

Ejemplo 3.2.1. Consideremos el anillo de Galois $GR(5^3, 2)$, entonces por (3.2.1) $\lambda = 1 - 5^2 = 101$ y el conjunto de Teichmuller:

$$\begin{aligned}
\mathcal{T} = \{&0, x, 36x+68, 114x+73, 52x+2, 124x+36, 57, 57x, 52x+1, 123x+36,\\
&89x+114, 68x+52, 124, 124x, 89x+57, 11x+52, 73x+123, x+89, 68, 68x,\\
&73x+124, 2x+89, 36x+11, 57x+73, 1\}\,.
\end{aligned}$$

Dado $n = 6$ es tal que $(6,5) = 1$, entonces tomando $n' = 1$ se sigue que $nn' = 6 \equiv 1 \pmod{5}$, y tomando $N' = 1 \in \mathcal{T}$ se satisface que $\mu(N') = \mu(1) = 1 = n'$ y así por (3.2.1) tenemos que: $\gamma = 1 + N'p^2 = 1 + (1)(25) = 26$, ya con esto podemos verificar que:

$$\lambda\gamma = (101)(26) \equiv 1 \pmod{5^3}.$$

Sin embargo, esto no ocurre siempre, pues dado $n = 2$ y $n' = 3$ entonces $nn' = 6 \equiv 1 \pmod 5$ y tomando $N' = 68 \in \mathcal{T}$ tenemos $\mu(68) = 3 = n'$, $\gamma = 1 + N'p^2 = 1 + (68)(25) = 76 \pmod{5^3}$ pero:

$$\lambda\gamma = (101)(76) \equiv 1 \pmod{5^3}.$$

Lema 3.2.2. *Sean $\gamma, \lambda \in R$ tales que $\lambda\gamma = 1$ y $k \geq 1$ un entero. Entonces:*

$$\begin{aligned} r_0(\gamma^k) &= 1 \\ r_1(\gamma^k) &= 0 \\ r_2(\gamma^k) &= kn'. \end{aligned}$$

Demostración. Como γ es una unidad de la forma $1 + N'p^2$ con $N' \in \mathcal{T}$ entonces por el isomorfismo Γ tenemos que:

$$\Gamma(\gamma) := (1, 0, n'^{p^2}),$$

luego, por las ecuaciones (1.4.30), para cada $c \in R$:

$$\begin{aligned} r_0(\gamma c) &= r_0(c) \\ r_1(\gamma c) &= r_1(c) \\ r_2(\gamma c) &= n' r_0(c) + r_2(c). \end{aligned}$$

Hagamos inducción sobre k. Para $k = 1$:

$$\begin{aligned} r_0(\gamma) &= 1 & & r_0(\gamma) = 1 \\ r_1(\gamma)^p &= 0 & \Rightarrow \quad & r_1(\gamma) = 0 \\ r_2(\gamma)^{p^2} &= n'^{p^2} & & r_2(\gamma) = 1n'. \end{aligned}$$

Supongamos que si $l(k$ entonces $r_0(\gamma^l) = 1, r_1(\gamma^l) = 0$ y $r_2(\gamma^l) = ln'$ y como $\gamma^k = \gamma\gamma^{k-1}$ se sigue que:

$$\begin{aligned} r_0(\gamma\gamma^{k-1}) &= r_0(\gamma^{k-1}) = 1 \\ r_1(\gamma\gamma^{k-1}) &= r_1(\gamma^{k-1}) = 0 \\ r_2(\gamma\gamma^{k-1}) &= n' r_0(\gamma^{k-1}) + r_2(\gamma^{k-1}) = 1n' + (k-1)n' = kn'. \end{aligned}$$

como queríamos. □

En particular, para $k = n$; $r_0(\gamma^n) = 1, r_1(\gamma^n) = 0$ y $r_2(\gamma^n) = 1$, ahora para cualquier $a \in R$, usando el isomorfismo Γ se sigue que:

$$\begin{aligned} \Gamma(a) &= \left(r_0(a), r_1(a)^p, r_2(a)^{p^2}\right) \\ \Gamma(\gamma^k) &= \left(1, 0, (kn')^{p^2}\right) \end{aligned}$$

Realizando las operaciones en $W_3(\mathbb{F}_{p^m})$ tenemos que:

$$\begin{aligned} r_0(\gamma^k a) &= r_0(a) \\ r_0(\gamma^k a)^p + pr_1(\gamma^k a)^p &= (1^p + p0)\,(r_0(a)^p + pr_1(a)^p) \\ &= r_0(a)^p + pr_1(a)^p \end{aligned}$$

cancelando términos tenemos que $r_1(\gamma^k a)^p = r_1(a)^p$, así $r_1(\gamma^k a) = r_1(a)$. Además:

$$\begin{aligned} r_0(\gamma^k a)^{p^2} + pr_1(\gamma^k a)^{p^2} + p^2 r_2(\gamma^k a)^{p^2} &= \left(1^{p^2} + p0^p + p^2(kn')^{p^2}\right)\left(r_0(a)^{p^2} + pr_1(a)^{p^2} + p^2 r_2(a)^{p^2}\right) \\ &= r_0(a)^{p^2} + pr_1(a)^{p^2} + p^2 r_2(a)^{p^2} + p^2((kn')r_0(a))^{p^2} + p^3\mathbf{T}. \end{aligned}$$

Aquí, $\mathbf{T}$ engloba a todo término resultante del producto que tiene como factor común p^3, aplicando las igualdades previas y cancelando términos:

$$r_2(\gamma^k a)^{p^2} = r_2(a)^{p^2} + ((kn')r_0(a))^{p^2} + p\mathbf{T}.$$

Analizando la expresión anterior en $\mathbb{F}_{p^m}$ llegamos a:

$$\begin{aligned} r_0(\gamma^k a) &= r_0(a) \\ r_1(\gamma^k a) &= r_1(a) \\ r_2(\gamma^k a) &= r_2(a) + (kn')_p r_0(a), \end{aligned} \tag{3.2.2}$$

dónde $(*)_p$ indica como antes, reducción módulo p.

Las palabras-código definidas sobre anillos de Galois, pueden ser relacionados con clases polinomiales, como se hace a continuación. Consideremos:

$$\mathcal{A}_n = \frac{R[x]}{(x^n - 1)}, \quad \mathcal{B}_n = \frac{R[x]}{(x^n - \lambda)}$$

y las funciones:

$$\begin{aligned} P : R^n &\to \mathcal{A}_n \\ (a_0, a_1, \ldots, a_{n-1}) &\mapsto \sum_{i=0}^{n-1} a_i x^i + (x^n - 1) \end{aligned} \qquad \begin{aligned} P' : R^n &\to \mathcal{B}_n \\ (b_0, b_1, \ldots, b_{n-1}) &\mapsto \sum_{i=0}^{n-1} b_i x^i + (x^n - \lambda) \end{aligned}$$

llamadas *representaciones polinomiales* .

Proposición 3.2.3. *Sean $\gamma = 1 + N'p^2, \lambda = 1 - p^2$ tales que $\gamma\lambda = 1$ en R. Las funciones:*

$$\begin{aligned} \mu_\gamma : \mathcal{A}_n &\to \mathcal{B}_n \\ f(x) + (x^n - 1) &\mapsto f(\gamma x) + (x^n - \lambda) \end{aligned} \quad y \quad \begin{aligned} \chi_\gamma : R^n &\to R^n \\ (a_0, a_1, \ldots, a_{n-1}) &\mapsto (a_0, \gamma a_1, \ldots, \gamma^{n-1} a_{n-1}), \end{aligned} \tag{3.2.3}$$

satisfacen:

(i) μ_γ *es un isomorfismo de anillos.*

(ii) I *es un ideal de* $\mathcal{A}_n$ *si y sólo si* $\mu_\gamma(I)$ *es un ideal de* $\mathcal{B}_n$.

(iii) $C \subset R^n$ *es un código cíclico lineal si y sólo si* $P(C)$ *es un ideal de* $\mathcal{A}_n$.

(iv) $C \subset R^n$ *es un código* λ*-cíclico lineal si y sólo si* $P(C)$ *es un ideal de* $\mathcal{B}_n$.

(v) $\mu_\gamma \circ P = P' \circ \chi_\gamma$.

Demostración. (i) Sean $f(x) + (x^n - 1), g(x) + (x^n - 1) \in \mathcal{A}_n$ dados por:

$$f(x) + (x^n - 1) = \sum_{i=0}^{n-1} a_i x^i + (x^n - 1) \quad \text{y} \quad g(x) + (x^n - 1) = \sum_{i=0}^{n-1} b_i x^i + (x^n - 1).$$

Entonces tenemos que:

$$\begin{aligned} f(x) + g(x) + (x^n - 1) &= \sum_{i=0}^{n-1} (a_i + b_i) x^i + (x^n - 1) \\ f(x)g(x) + (x^n - 1) &= h(x) + (x^n - 1), \end{aligned}$$

para algún $h(x)$ tal que $x^n - 1 \mid f(x)g(x) - h(x)$ en $R[x]$. Así:

$$\begin{aligned} \mu_\gamma(f(x) + g(x) + (x^n - 1)) &= \sum_{i=0}^{n-1} (a_i + b_i)\gamma^i x^i + (x^n - \lambda) \\ &= \sum_{i=0}^{n-1} (a_i\gamma^i + b_i\gamma^i) x^i + (x^n - \lambda) \\ &= \sum_{i=0}^{n-1} a_i\gamma^i x^i + (x^n - \lambda) + \sum_{i=0}^{n-1} b_i\gamma^i x^i + (x^n - \lambda) \\ &= \mu_\gamma(f(x) + (x^n - 1)) + \mu_\gamma(g(x) + (x^n - 1)). \end{aligned}$$

Ahora, como $f(x)g(x) - h(x) = h(x)(x^n - 1)$ tenemos que:

$$\begin{aligned} \mu_\gamma\left(f(x)g(x) + (x^n - 1) - [h(x) + (x^n - 1)]\right) &= (x^n - \lambda) \\ \mu_\gamma\left(f(x)g(x) + (x^n - 1)\right) - \mu_\gamma\left(h(x) + (x^n - 1)\right) &= (x^n - \lambda) \\ \mu_\gamma\left(f(x)g(x) + (x^n - 1)\right) &= \mu_\gamma\left(h(x) + (x^n - 1)\right), \end{aligned}$$

y por otro lado, por (3.2.3):

$$\begin{aligned} \mu_\gamma(f(x) + (x^n - 1))\mu_\gamma(+(x^n - 1)) &= [f(\gamma x) + (x^n - \lambda)]\,[g(\gamma x) + (x^n - \lambda)] \\ &= [f(\gamma x)g(\gamma x) + (x^n - \lambda)] \\ &= [h(\gamma x) + (x^n - \lambda)] \\ &= \mu_\gamma(h(x) + (x^n - 1)) \\ &= \mu_\gamma\left(f(x)g(x) + (x^n - 1)\right). \end{aligned}$$

de ahí que μ_γ es un homomorfismo. Para demostrar la inyectividad de μ_γ, supongamos que $\mu_\gamma(f(x) + (x^n - 1)) = (x^n - \lambda)$, de ser así:

$$(x^n - \lambda) \mid f(\gamma x) = \sum_{i=0}^{n-1} a_i \gamma^i x^i,$$

como $\text{grad}(f(\gamma x)) \leq (n-1)(n$ entonces $a_i\gamma^i = 0$ luego $a_i = (\lambda^i)0 = 0$ para $0 \leq i \leq n-1$, de ahí que $f(x) \mid (x^n - 1)$, así μ_γ es inyectiva. Como $|\mathcal{A}_n| = p^{smn} = |\mathcal{B}_n|$, μ_γ es sobreyectiva y por tanto biyectiva.

(ii) Como μ_γ es un isomorfismo entonces μ_γ^{-1} lo es también así que dado I un ideal de $\mathcal{A}_n$, por la sobreyectividad de μ_γ, la imagen de I bajo éste isomorfismo es un ideal de $\mathcal{B}_n$, análogamente como $\mu_\gamma^{-1}(\mu_\gamma(I)) = I$ se tiene el resultado.

(iii) ($\Rightarrow$) Supongamos que C es un código cíclico lineal y denotemos por $\hat{c}(x)$ a $c(x) + (x^n - 1)$ en $\mathcal{A}_n$, además notemos que P es claramente sobreyectiva.

Dados $\hat{c}(x), \hat{d}(x)$ en $\mathcal{A}_n$ existen $\underline{c} = (c_0, c_1, \ldots, c_{n-1})$ y $\underline{d} = (d_0, d_1, \ldots, d_{n-1})$ en C tales que $P(\underline{c}) = \hat{c}(x)$ y $P(\underline{d}) = \hat{d}(x)$. Como $\underline{c} - \underline{d} = (c_0 - d_0, c_1 - d_1, \ldots, c_{n-1} - d_{n-1}) \in C$ por su linealidad, es claro que $P(\underline{c} + \underline{d}) \in P(C)$ y además:

$$P(\underline{c} - \underline{d}) = \sum_{i=0}^{n-1} (c_i - d_i)x^i + (x^n - 1) = \hat{c}(x) - \hat{d}(x)$$

de ahí que $(P(C), +)$ es un subgrupo aditivo de $\mathcal{A}_n$.

Veamos por inducción que para todo entero $k \geq 1 : x^k\hat{c}(x) \in P(C)$. Si $k = 1$ entonces $x\hat{c}(x) = c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n + (x^n - 1)$, desde luego $x^n \equiv 1 \pmod{(x^n - 1)}$, de ahí que $x\hat{c}(x) = c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1} + (x^n - 1)$. Como C es un código cíclico dado $\underline{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ entonces $\underline{c}' = (c_{n-1}, c_0, \ldots, c_{n-2})$ también pertenece a C y resulta evidente que $P(\underline{c}') = x\hat{c}(x)$, luego $x\hat{c}(x) \in P(C)$. Supongamos que si $l(k$ entonces $x^l\hat{c}(x) \in P(C)$, luego como $x^k = xx^{k-1}$, resulta inmediato de la hipótesis inductiva que $x^k\hat{c}(x) \in P(C)$. Por otro lado, como C es un R-submódulo, (pues es lineal) tenemos que dado $r \in R$ entonces $r\underline{c} \in C$, ahora dado $\hat{r} \in \mathcal{A}_n$ y $\hat{c}(x) \in P(C)$ entonces como:

$$\begin{aligned}
\hat{r}\hat{c}(x) &= [r + (x^n - 1)] \left[\sum_{i=0}^{n-1} c_i x^i + (x^n - 1) \right] \\
&= \sum_{i=0}^{n-1} r c_i x^i + (x^n - 1) \\
&= P(r\underline{c}).
\end{aligned}$$

Consideremos $\hat{r}(x) = r_0 + r_1x + \ldots + r_{n-1}x^{n-1} + (x^n - 1) \in \mathcal{A}_n$, entonces:

$$\hat{r}(x)\hat{c}(x) = \Big(a_0\hat{c}(x) + a_1x\hat{c}(x) + \cdots + a_{n-1}x^{n-1}\hat{c}(x)\Big) + (x^n - 1),$$

por todo lo discutido con anterioridad se sigue que $a_i x^i \hat{c}(x) + (x^n - 1) \in P(C)$ para $(0 \leq i \leq n-1)$, de ahí que $\hat{r}(x)\hat{c}(x) \in P(C)$, por lo tanto éste un ideal de $\mathcal{A}_n$.

($\Leftarrow$) Supongamos que $P(C)$ es un ideal de $\mathcal{A}_n$. Sean $\underline{c}, \underline{d} \in C$, entonces

$$\begin{aligned} P(\underline{c}) - P(\underline{d}) = \hat{c}(x) - \hat{d}(x) &= \sum_{i=0}^{n-1} c_i x^i + (x^n - 1) - \sum_{i=0}^{n-1} d_i x^i + (x^n - 1) \\ &= \sum_{i=0}^{n-1} (c_i - d_i) x^i + (x^n - 1) \\ &= P(\underline{c} - \underline{d}) \end{aligned}$$

dado que $P(\underline{c}) - P(\underline{d}) \in P(C)$ pues éste es un ideal, de lo anterior se sigue que $\underline{c} - \underline{d} \in C$, de ahí que $(C, +)$ es un subrgupo de $(R^n, +)$. Sean $r \in R$, entonces $P(r) = \hat{r} = r + (x^n - 1)$ y como $P(C)$ es un ideal, entonces:

$$\begin{aligned} \hat{r}\hat{c}(x) &= r \sum_{i=0}^{n-1} c_i x^i + (x^n - 1) \\ &= \sum_{i=0}^{n-1} (rc_i) x^i + (x^n - 1) \\ &= P(r\underline{c}), \end{aligned}$$

de ahí que $r\underline{c} \in C$, es decir es un R-submódulo.

(iv) ($\Rightarrow$) Dado que P' es sobreyectiva, ver que $(P'(C), +)$ es un subrgupo de $(\mathcal{B}_n, +)$ es análogo a la prueba anterior. Denotemos por $\tilde{f}(x)$ a $f(x) + (x^n - \lambda)$. Veamos por inducción que para todo $k \geq 1$, $\tilde{x}^k \tilde{c}(x) \in P'(C)$, para esto notemos que, para $k = 1$:

$$\begin{aligned} \tilde{x}\tilde{c}(x) &= x \sum_{i=0}^{n-1} (c_i x^i) + (x^n - \lambda) \\ &= c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} + c_{n-1} x^n + (x^n - \lambda). \end{aligned}$$

Dado que $x^n \equiv \lambda \pmod{(x^n - \lambda)}$ entonces:

$$\tilde{x}\tilde{c}(x) = \lambda c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1} + (x^n - \lambda).$$

Puesto que C es un código λ-cíclico, tenemos que $\underline{c}' = (\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in C$ y así:

$$P'(\underline{c}') = \lambda c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1} + (x^n - \lambda) = \tilde{x}\tilde{c}(x),$$

de ahí que $\tilde{x}\tilde{c}(x) \in P'(C)$, de manera análoga a la primera implicación de (iii) tenemos que $P'(C)$ es un ideal. ($\Leftarrow$) Supongamos que $P'(C)$ es un ideal de $\mathcal{B}_n$. Dados $\underline{c}, \underline{d} \in C$ tenemos que:

$$\begin{aligned} P'(\underline{c}) - P'(\underline{d}) = \tilde{c}(x) + \tilde{d}(x) &= \sum_{i=0}^{n-1} c_i x^i + (x^n - \lambda) - \sum_{i=0}^{n-1} d_i x^i + (x^n - \lambda) \\ &= \sum_{i=0}^{n-1} (c_i - d_i) x^i + (x^n - \lambda) \\ &= P'(\underline{c} - \underline{d}) \end{aligned}$$

dado que $P'(\underline{c}) - P'(\underline{d}) \in P'(C)$ pues éste es un ideal, de lo anterior se sigue que $\underline{c} - \underline{d} \in C$, de ahí que $(C, +)$ es un subgrupo de $(R^n, +)$. Sea $r \in R$ y consideremos $\tilde{r} = r + (x^n - \lambda)$ ahora, como $P'(C)$ es un ideal, entonces:

$$\begin{aligned} \tilde{r}\tilde{c}(x) &= r \sum_{i=0}^{n-1} c_i x^i + (x^n - 1) \\ &= \sum_{i=0}^{n-1} (rc_i) x^i + (x^n - 1) \\ &= P'(r\underline{c}), \end{aligned}$$

de ahí que $r\underline{c} \in C$, es decir, es un código lineal. Ahora veamos que $\nu_\lambda(\underline{c}) = (\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \in C$, para esto consideremos $\tilde{x} = x + (x^n - \lambda)$. Como $P'(C)$ es un ideal, entonces dado $\tilde{c}(x)$ tenemos que $\tilde{x}\tilde{c}(c) \in P'(C)$, pero:

$$\begin{aligned} \tilde{x}\tilde{c}(x) &= \lambda c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1} + (x^n - \lambda) \\ &= P'(\nu_\lambda(\underline{c})). \end{aligned}$$

es decir, $P'(\nu_\lambda(\underline{c})) \in P'(C)$, por consiguiente, $\nu_\lambda(\underline{c}) \in C$ como deseabamos.

(v) Sea $\underline{c} \in R^n$, entonces:

$$\begin{aligned} \mu_\gamma(P(\underline{c})) &= \mu_\gamma\left(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} + (x^n - 1)\right) \\ &= c_0 + c_1 \gamma x + \cdots + c_{n-1} \gamma^{n-1} x^{n-1} + (x^n - \lambda) \\ &= P'\left(\left(c_0, \gamma c_1, \ldots, \gamma^{n-1} c_{n-1}\right)\right) \\ &= P'(\chi_\gamma(c_0, c_1, \ldots, c_{n-1})) = P'(\chi_\gamma(\underline{c})). \qquad (\underline{c} \in R^n) \end{aligned}$$

En consecuencia: $\mu_\gamma \circ P = P' \circ \chi_\gamma$. □

3.2.2 Códigos γ-cíclicos y la permutación de Nechaev

Definición 3.2.4. Sea χ_γ definida como en (3.2.3). Un código C sobre R se dice γ-cíclico si y sólo si $\chi_\gamma(C) = C$.

Proposición 3.2.5. *Sean $C \subseteq R^n$ un código, $\gamma, \lambda \in R$ tales que $\gamma = 1 + N'p^2$, $\lambda = 1 - p^2$ y $\gamma\lambda = 1$. C es un código cíclico lineal si y sólo si $\chi_\gamma(C)$ es un código λ-cíclico lineal.*

Demostración. Aplicaremos la Proposición 3.2.3. Supongamos que C es un código cíclico lineal $\Leftrightarrow$ $P(C)$ es un ideal de $\mathcal{A}_n$ $\Leftrightarrow$ $\mu_\gamma(P(C))$ es un ideal de $\mathcal{B}_n$, como $\mu_\gamma \circ P = P' \circ \chi_\gamma$, lo anterior ocurre si y sólo si $P'(\chi_\gamma(C))$ es un ideal de $\mathcal{B}_n$ $\Leftrightarrow$ $\chi_\gamma(C)$ es un código λ-cíclico lineal. □

Definición 3.2.6. (i) Sea π la permutación en $\{0, 1, \ldots, np-1\}$ dada por:

$$\pi(x) = \left(n\left(n'x - u\right)_p + x\right)_{np} \tag{3.2.4}$$

donde $nn' \equiv 1 \pmod{p}$, $0 \leq u \leq p-1$ y $nu \leq x \leq n(u+1) - 1$.

(ii) La *permutación de Nechaev* en $\mathbb{F}_q^{np}$ se define como:

$$\Pi((c_0, \ldots, c_x, \ldots, c_{np-1})) = \left(c_{\pi(0)}, \ldots, c_{\pi(x)}, \ldots, c_{\pi(np-1)}\right) \tag{3.2.5}$$

La permutación π se define en [1] con la notación de ciclos y transposiciones, sin embargo, la expresión (3.2.4) tomada de [13] es bastante clara y fácil de aplicar.

Ejemplo 3.2.7. (i) Sean $p = 2$, $n = 3$ entonces $n' = 1$, $0 \leq u \leq 1$ y $3u \leq x \leq 3u + 2$.

x	u	$3(x-u)_2 + x$	$\pi(x)$
0	0	$3(0-0)_2 + 0 = 0$	0
1	0	$3(1-0)_2 + 1 = 4$	4
2	0	$3(2-0)_2 + 2 = 2$	2
3	1	$3(3-1)_2 + 3 = 3$	3
4	1	$3(4-1)_2 + 4 = 7$	1
5	1	$3(5-1)_2 + 5 = 5$	5

Cuadro 1.: Permutación π en $\{0, 1, 2, 3, 4, 5\}$.

(ii) Sean $p = 5$, $n = 3$ entonces $n' = 2$, $0 \leq u \leq 4$, $3u \leq x \leq 3u + 2$.

x	u	$3(x-u)_5 + x$	$\pi(x)$
0	0	$3(2(0)-0)_5 + 0 = 0$	0
1	0	$3(2(1)-0)_5 + 1 = 7$	7
2	0	$3(2(2)-0)_5 + 2 = 14$	14
3	1	$3(2(3)-1)_5 + 3 = 3$	3
4	1	$3(2(4)-1)_5 + 4 = 10$	10
5	1	$3(2(5)-1)_5 + 5 = 17$	2

6	2	$3(2(6)-2)_5+6=6$	6
7	2	$3(2(7)-2)_5+7=13$	13
8	2	$3(2(8)-2)_5+8=20$	5
9	3	$3(2(9)-3)_5+9=9$	9
10	3	$3(2(10)-3)_5+10=16$	1
11	3	$3(2(11)-3)_5+11=23$	8
12	4	$3(2(12)-4)_5+12=12$	12
13	4	$3(2(13)-4)_5+13=19$	4
14	4	$3(2(14)-4)_5+14=26$	11

Cuadro 2.: Permutación π en $\{0,1,\ldots,13,14\}$.

(iii) En [13] se nos presenta un proceso simple y elegante para obtener la permutación π, valiéndose de la aplicación sucesiva del corrimiento cíclico $\overline{\sigma}$. Consideremos el conjunto de enteros $\{0,1,\ldots,np-1\}$ y coloquemos sus elementos en un arreglo de tamaño $p\times n$ como sigue:

$$\begin{array}{cccccc}
\overline{\sigma}^{(0n')_p} & \overline{\sigma}^{(1n')_p} & \cdots & \overline{\sigma}^{(ln')_p} & \cdots & \overline{\sigma}^{((n-1)n')_p} \\
0 & 1 & \cdots & l & \cdots & n-1 \\
n & n+1 & \cdots & n+l & \cdots & 2n-1 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
n(p-1) & n(p-1)+1 & \cdots & n(p-1)+i & \cdots & np-1
\end{array}$$

Cada $\overline{\sigma}^{(ln')_p}$ es el corrimiento cíclico "hacia arriba", $(ln')_p$ lugares con $0\leq l\leq n-1$, posteriormente concatenamos las filas del arreglo y el resultado es la permutación π. Aplicando este proceso a (ii) de este ejemplo:

$$\begin{array}{ccc}
\overline{\sigma}^{(0)_5} & \overline{\sigma}^{(2)_5} & \overline{\sigma}^{(4)_5} \\
0 & 1 & 2 \\
3 & 4 & 5 \\
6 & 7 & 8 \\
9 & 10 & 11 \\
12 & 13 & 14
\end{array}
\rightarrow
\begin{array}{ccc}
0 & 7 & 14 \\
3 & 10 & 2 \\
6 & 13 & 5 \\
9 & 1 & 8 \\
12 & 4 & 11
\end{array}$$

$$\pi=\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 0 & 7 & 14 & 3 & 10 & 2 & 6 & 13 & 5 & 9 & 1 & 8 & 12 & 4 & 11 \end{pmatrix},$$

como afirmamos.

Definición 3.2.8. Sea t un entero positivo, dado que $\left(\mathbb{F}_q^{np}\right)^t$ es isomorfo a $\mathbb{F}_q^{npt}$, sea:

$$\Pi^{\otimes t}:\mathbb{F}_q^{npt}\rightarrow\mathbb{F}_q^{npt}$$

la permutación definida como:

$$\Pi^{\otimes t}\left(\underline{c}^{[1]} \mid \cdots \mid \underline{c}^{[k]} \mid \cdots \mid \underline{c}^{[t]}\right) = \left(\Pi\left(\underline{c}^{[1]}\right) \mid \cdots \mid \Pi\left(\underline{c}^{[k]}\right) \mid \cdots \mid \Pi\left(\underline{c}^{[t]}\right)\right) \tag{3.2.6}$$

donde $\underline{c}^{[1]}, \ldots, \underline{c}^{[t]} \in \mathbb{F}_q^{np}$ y Π es como en (3.2.5).

Proposición 3.2.9. *Sea Φ la función de Gray, entonces:*

$$\Phi \circ \chi_\gamma = \Pi^{\otimes p^{2m-1}} \circ \Phi \tag{3.2.7}$$

Demostración. Sea $A = (a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \in R^n$ y $D = \chi_\gamma(A)$, entonces:

$$d_i = \gamma^i a_i \qquad (0 \leq i \leq n-1).$$

Entonces aplicando la función de Gray:

$$\Phi(\chi_\gamma(A)) = \phi(D) = r_0(D) \otimes c_0 + r_1(D) \otimes c_1 + r_2(D) \otimes c_2,$$

procediendo como en la Proposición 3.1.3, el k-ésimo bloque de longitud nq de $\Phi(D)$ esta dado por:

$$\begin{aligned}\Phi(D)^{[k]} &= r_0(D) \otimes u + r_1(D) \otimes \langle \omega_k \rangle_{p^m} + r_2(D) \otimes v \\ &= r_0(D) \otimes (\Omega_0, \ldots, \Omega_i, \ldots, \Omega_{p^m-1}) + r_1(D) \otimes (\langle \omega_k \rangle_p, \ldots, \langle \omega_k \rangle_p, \ldots, \langle \omega_k \rangle_p) + \\ &\quad r_2(D) \otimes (\langle 1 \rangle_p, \ldots, \langle 1 \rangle_p, \ldots, \langle 1 \rangle_p),\end{aligned}$$

y en consecuencia el i-ésimo bloque de longitud np, el cual denotaremos por $\mathcal{D}_i$ es:

$$\mathcal{D}_i = r_0(D) \otimes \Omega_i + r_1(D) \otimes \langle \omega_k \rangle_p + r_2(D) \otimes \langle 1 \rangle_p, \tag{3.2.8}$$

y así, el j-ésimo bloque de longitud n de $\mathcal{D}_i$ es:

$$\begin{aligned}\mathcal{D}_{ij} &= \omega_{ip+j} r_0(D) + \omega_k r_1(D) + r_2(D) \\ &= \omega_{ip+j}(r_0(a_0), \ldots, r_0(\gamma^l a_l), \ldots, r_0(\gamma^{n-1} a_{n-1})) \\ &\quad + \omega_k (r_1(a_0), \ldots, r_1(\gamma^l a_l), \ldots, r_1(\gamma^{n-1} a_{n-1})) \\ &\quad + (r_2(a_0), \ldots, r_2(\gamma^l a_l), \ldots, r_2(\gamma^{n-1} a_{n-1}))\end{aligned} \tag{3.2.9}$$

aplicando a esto las relaciones (3.2.2) se consigue:

$$\begin{aligned}\mathcal{D}_{ij} &= (\omega_{ip+j} r_0(a_0) + \omega_k r_1(a_0) + r_2(a_0), \ldots, \omega_{ip+j} r_0(a_l) + \omega_k r_1(a_l) + r_2(a_0) + \\ &\quad (ln')_p r_0(a_l), \ldots, \omega_{ip+j} r_0(a_{n-1}) + \omega_k r_1(a_{n-1}) + r_2(a_{n-1}) + ((n-1)n')_p r_0(a_{n-1})) \\ &= (\omega_{ip+j} r_0(a_0) + \omega_k r_1(a_0) + r_2(a_0), \ldots, (\omega_{ip+j} + (ln')_p) r_0(a_l) + \omega_k r_1(a_l) + \\ &\quad r_2(a_l), \ldots, (\omega_{ip+j} + ((n-1)n')_p) r_0(a_{n-1}) + \omega_k r_1(a_{n-1}) + r_2(a_{n-1}))\end{aligned} \tag{3.2.10}$$

entonces, aplicando (2.3.7) a la ultima igualdad de (3.2.10) tenemos que el j-ésimo bloque de longitud n es:

$$\Big(\omega_{ip+j}r_0(a_0)+\omega_k r_1(a_0)+r_2(a_0),\ldots,\omega_{ip+(j+ln')_p}r_0(a_l)+\omega_k r_1(a_l)+r_2(a_l),\ldots,\\ \omega_{ip+(j+(n-1)n')_p}r_0(a_{n-1})+\omega_k r_1(a_{n-1})+r_2(a_{n-1})\Big). \tag{3.2.11}$$

Por otro lado, el i-ésimo bloque de longitud np de $\Phi(A)$ está dado por:

$$\mathcal{A}_i = r_0(A)\otimes\Omega_i + r_1(A)\otimes\langle\omega_k\rangle_p + r_2(A)\otimes\langle 1\rangle_p.$$

Ahora, como en el Ejemplo 3.2.7 coloquemos este bloque en un arreglo de tamaño $p\times n$:

$$\begin{pmatrix} \omega_{ip}r_0(a_0)+\omega_k r_1(a_0)+r_2(a_0) & \cdots & \omega_{ip}r_0(a_l)+\omega_k r_1(a_l)+r_2(a_l) & \cdots & \omega_{ip}r_0(a_{n-1})+\omega_k r_1(a_{n-1})+r_2(a_{n-1}) \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \omega_{ipj+j}r_0(a_0)+\omega_k r_1(a_0)+r_2(a_0) & \cdots & \omega_{ip+j}r_0(a_l)+\omega_k r_1(a_l)+r_2(a_l) & \cdots & \omega_{ip+j}r_0(a_{n-1})+\omega_k r_1(a_{n-1})+r_2(a_{n-1}) \\ \vdots & \cdots & \vdots & \cdots & \vdots \\ \omega_{ip+(p-1)}r_0(a_0)+\omega_k r_1(a_0)+r_2(a_0) & \cdots & \omega_{ip+(p-1)}r_0(a_l)+\omega_k r_1(a_l)+r_2(a_l) & \cdots & \omega_{ip+(p-1)}r_0(a_{n-1})+\omega_k r_1(a_{n-1})+r_2(a_{n-1}) \end{pmatrix}.$$

Para analizar $\Pi(\mathcal{A}_i)$ basta con recordar que como se hizo en el Ejemplo 3.2.7, aplicaremos $\overline{\sigma}^{(ln')_p}$ en la l-ésima columa del arreglo, es decir, sus elementos se recorren $(ln')_p$ lugares hacia arriba dejando:

$$\begin{pmatrix} \omega_{ip+(ln')_p}r_0(a_l)+\omega_k r_1(a_l)+r_2(a_l) \\ \cdots \\ \omega_{ip+(j+ln')_p}r_0(a_l)+\omega_k r_1(a_l)+r_2(a_l) \\ \cdots \\ \omega_{ip+((p-1)+ln')_p}r_0(a_{n-1})+\omega_k r_1(a_{n-1})+r_2(a_{n-1}) \end{pmatrix}$$

por consiguiente la j-ésima fila del arreglo, es decir, el j-ésimo bloque de longitud n de $\mathcal{A}_i$ está dado por:

$$\Big(\omega_{ip+j}r_0(a_0)+\omega_k r_1(a_0)+r_2(a_0),\ldots,\omega_{ip+(j+ln')_p}r_0(a_l)+\omega_k r_1(a_l)+r_2(a_l),\ldots,\\ \omega_{ip+(j+(n-1)n')_p}r_0(a_{n-1})+\omega_k r_1(a_{n-1})+r_2(a_{n-1})\Big). \tag{3.2.12}$$

un rápida inspección arroja a la luz que las expresiones (3.2.11) y (3.2.12) son iguales, esto es:

$$\Phi(\chi_\gamma(A))^{[k]} = \Pi(\Phi(A)^{[k]})$$

de esto y (3.2.6) se tiene que para cada $A\in R^n$:

$$\Phi(\chi_\gamma(A)) = \Pi^{\otimes p^{2m-1}}(\Phi(A)).$$

como afirmamos. $\square$

Como cierre para este capítulo y por ende a este trabajo de tesis, enunciamos un teorema que es consecuencia inmediata de lo estudiado en este capítulo.

Teorema 3.2.10. *Sea $C \subseteq R^n$ un código. Entonces C es un código cíclico lineal si y sólo si $\Pi^{\otimes p^{2m-1}}(\Phi(C))$ es un código cuasi-cíclico de índice p^{2m-1} y longitud nq^2 sobre $\mathbb{F}_q^{nq^2}$.*

Demostración. C es un código cíclico lineal sobre R si y sólo si $\chi_\gamma(C)$ es un código λ-cíclico lineal (por (iv) y (v) de la Proposición 3.2.3). Pero por el Teorema 3.1.4 esto pasa si y sólo si $\Phi(\chi_\gamma(C))$ es un código cuasi-cíclico de índice p^{2m-1} y longitud nq^2 y finalmente, por la Proposición 3.2.9 se tiene los anterior si y sólo $\Pi^{\otimes p^{2m-1}}(\Phi(C))$ es un código cuasi-cíclico de índice p^{2m-1} y longitud nq^2, como queríamos demostrar. □

Ejemplo 3.2.11. Consideremos el anillo de Galois $R = GR(2^3, 2)$, $n = 3$ y el código definido en R^3:

$$\begin{aligned} C = \{&(0,0,0),(2,2,2),(4,4,4),(6,6,6),(2x,2x,2x),(2x+2,2x+2,2x+2),\\ &(2x+4,2x+4,2x+4),(2x+6,2x+6,2x+6),(4x,4x,4x),\\ &(4x+2,4x+2,4x+2),(4x+4,4x+4,4x+4),(4x+6,4x+6,4x+6),\\ &(6x,6x,6x),(6x+2,6x+2,6x+2),(6x+4,6x+4,6x+4),\\ &(6x+6,6x+6,6x+6)\}. \end{aligned}$$

Éste es un código cíclico lineal que también puede describirse como $C = \langle(1,1,1)\rangle$, como en el ejemplo 1.3.6.

Apliquemos a C el Teorema 3.2.10 para esto notemos que $\lambda = 5$, y además ya que $5(2) \equiv 2 \pmod 8$, $5(4) \equiv 4 \pmod 8$ y $5(6) \equiv 6 \pmod 8$ resulta fácil ver que $\nu_\lambda(C) = C$, es decir, éste también es un código λ-cíclico, ahora, como se hizo en el Ejemplo 3.1.5 tomaremos algunos elementos de C:

$$\begin{aligned} &\Phi((6x+2,6x+2,6x+2))\\ &(111111 \mid 111111 \mid \omega\omega\omega\omega\omega\omega \mid \omega\omega\omega\omega\omega\omega \mid 000000 \mid 000000 \mid\\ &\quad \omega^2\omega^2\omega^2\omega^2\omega^2\omega^2 \mid \omega^2\omega^2\omega^2\omega^2\omega^2\omega^2)\\ &\Phi((4x+6,4x+6,4x+6))\\ &(\omega^2\omega^2\omega^2\omega^2\omega^2\omega^2 \mid \omega^2\omega^2\omega^2\omega^2\omega^2\omega^2 \mid \omega\omega\omega\omega\omega\omega \mid \omega\omega\omega\omega\omega\omega \mid\\ &\quad 111111 \mid 111111 \mid 000000 \mid 000000) \end{aligned}$$

Notemos que cada uno de los 8 bloques de longitud 6 son invariantes bajo la permutación de Nechaev, lo mismo ocurre con todos los elementos de C, con lo cual tenemos que:

$$\Pi^{\otimes 8}(\Phi(C)) = C$$

y también es claro que éste es un código cuasi-cíclico de índice $p^{2m-1} = 8$ y longitud $nq^2 = 48$, con lo cual se confirma el teorema.

A continuación consideremos un código cíclico lineal definido sobre el anillo de Galois $R = GR(3^3, 2)$ con $n = 2$ y que es el submódulo generado por las filas de la matriz:

$$G = \begin{pmatrix} 9 & 0 \\ 0 & 9 \end{pmatrix}$$

Consideremos que los elementos del código C son de tres tipos a saber: (c, c), (c, d) y (d, c) ya que éste es un código cíclico y las entradas de sus palabras código pueden repetirse, así que, dados los parámetros $p = 3$, $s = 3$, $m = 2$ y $n = 2$ calculemos la imágen bajo la función de Gray de estos tipos de palabras código:

Retomando la ecuación (2.3.8) tenemos los vectores:

$$\begin{aligned} u &= (0, 1, 2, \omega, \omega^2, \omega^7, \omega^5, \omega^3, \omega^6) \\ v &= (1, 1, 1, 1, 1, 1, 1, 1) \end{aligned}$$

Ahora, como en las ecuaciones (2.3.11) calcularemos los coeficientes $\mathbf{c}_0, \mathbf{c}_1$ y $\mathbf{c}_2$, sin embargo debido a la longitud de las palabras código utilizaremos la siguiente notación, si una entrada o secuencia de entradas se repite una cantidad k de veces encerraremos a ésta(s) entrada(s) con el símbolo $\langle \cdot \rangle_k$, es decir:

$$\begin{aligned} \mathbf{c}_0 &= (0, 1, 2, \omega, \omega^2, \omega^7, \omega^5, \omega^3, \omega^6) \times (\langle 1 \rangle_9) \\ \mathbf{c}_1 &= (\langle 1 \rangle_9) \times (0, 1, 2, \omega, \omega^2, \omega^7, \omega^5, \omega^3, \omega^6) \\ \mathbf{c}_2 &= (\langle 1 \rangle_9) \times (\langle 1 \rangle_9) \end{aligned}$$

Aplicando el producto de Kronecker y con la notación que hemos mencionado tenemos que:

$$\begin{aligned} \mathbf{c}_0 &= (\langle 0, 1, 2, \omega, \omega^2, \omega^7, \omega^5, \omega^3, \omega^6 \rangle_9) \\ \mathbf{c}_1 &= (\langle 0 \rangle_9, \langle 1 \rangle_9, \langle 2 \rangle_9, \langle \omega \rangle_9, \langle \omega^2 \rangle_9, \langle \omega^7 \rangle_9, \langle \omega^5 \rangle_9, \langle \omega^3 \rangle_9, \langle \omega^6 \rangle_9,) \\ \mathbf{c}_2 &= (\langle 1 \rangle_{81}) \end{aligned}$$

así usando la función de Gray tal como en la Definición 2.3.7 en cada uno de los tipos de palabras código de C se tiene que[2]:

$$\begin{aligned} \Phi((c, c)) &= (\langle c', c', c', c', c', c' \rangle_{27}) \\ \Phi((c, d)) &= (\langle c', d', c', d', c', d' \rangle_{27}) \\ \Phi((d, c)) &= (\langle d', c', d', c', d', c' \rangle_{27}) \end{aligned} \tag{3.2.13}$$

Dado que nuestra intención es corroborar el Teorema 3.2.10 hemos colocado a las imágenes de Gray de los tres tipos de palabras código de C notando que se repiten 27 veces los bloques de longitud $np = 6$, ahora veamos como

2 Aquí los símbolos c', d' son los elementos asociados a c y d en el campo finito $\mathbb{F}_q$ respectivamente.

actuará la permutación de Nechaev, analizando la permutación π como en iii) del Ejemplo 3.2.7:

$$\begin{array}{cc} \overline{\sigma}^{(0)_3} & \overline{\sigma}^{(2)_3} \\ 0 & 1 \\ 2 & 3 \\ 4 & 5 \end{array} \rightarrow \begin{array}{cc} 0 & 5 \\ 2 & 1 \\ 4 & 3 \end{array}$$

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

Ahora, si tomamos la permutación de Nechaev para una palabra código $(d_0, d_1, d_2, d_3, d_4, d_5)$ tenemos que:

$$\Pi((d_0, d_1, d_2, d_3, d_4, d_5)) = (d_{\pi(0)}, d_{\pi(1)}, d_{\pi(2)}, d_{\pi(3)}, d_{\pi(4)}, d_{\pi(5)}) = (d_0, d_5, d_2, d_1, d_4, d_3),$$

entonces notemos que al aplicar la permutación de Nechaev a los bloques de longitud $np = 6$ de las imágenes bajo la función de Gray en la Ecuación (3.2.13) obtenemos lo siguiente:

$$\begin{aligned} \Pi(\Phi(c,c)) &= (c', c', c', c', c', c') \\ \Pi(\Phi(c,d)) &= (c', d', c', d', c', d') \\ \Pi(\Phi(d,c)) &= (d', c', d', c', d', c'), \end{aligned}$$

y finalmente, aplicando el corrimiento cíclico a cada uno de estos bloques tenemos que:

$$\begin{aligned} \overline{\sigma}\left(\Pi(\Phi(c,c))\right) &= (c', c', c', c', c', c') \\ \overline{\sigma}\left(\Pi(\Phi(c,d))\right) &= (d', c', d', c', d', c') \\ \overline{\sigma}\left(\Pi(\Phi(d,c))\right) &= (c', d', c', d', c', d'), \end{aligned}$$

entonces es claro que esto se repetirá en cada uno de los 27 bloques de las imágenes bajo la función de Gray tras ser permutadas por la función $\Pi^{\otimes 27}$, lo cual implica que:

$$\sigma^{\otimes 27}\left(\Pi^{\otimes 27}\left(\Phi(C)\right)\right) = \Pi^{\otimes 27}\left(\Phi(C)\right). \tag{3.2.14}$$

Lo cual coincide con el Teorema 3.2.10 tal como queríamos.

A continuación, se exhibe el código de C, las imágenes bajo la función de Gray dado que el resultado de aplicar la permutación $\Pi^{\otimes 27}$ a las imágenes no alteran a las palabras código basta con exhibir estas listas y de esta manera, el lector podrá confirmar de manera concreta nuestras afirmaciones.

$$C = \left\{ \begin{array}{cccccc}
(0,0) & (9,0) & (18,0) & (9w,0) & (9w+9,0) & (9w+18,0) \\
(0,9) & (9,9) & (18,9) & (9w,9) & (9w+9,9) & (9w+18,9) \\
(0,18) & (9,18) & (18,18) & (9w,18) & (9w+9,18) & (9w+18,18) \\
(0,9w) & (9,9w) & (18,9w) & (9w,9w) & (9w+9,9w) & (9w+18,9w) \\
(0,18w) & (9,18w) & (18,18w) & (9w,18w) & (9w+9,18w) & (9w+18,18w) \\
(0,9w+9) & (9,9w+9) & (18,9w+9) & (9w,9w+9) & (9w+9,9w+9) & (9w+18,9w+9) \\
(0,9w+18) & (9,9w+18) & (18,9w+18) & (9w,9w+18) & (9w+9,9w+18) & (9w+18,9w+18) \\
(0,18w+9) & (9,18w+9) & (18,18w+9) & (9w,18w+9) & (9w+9,18w+9) & (9w+18,18w+9) \\
(0,18w+18) & (9,18w+18) & (18,18w+18) & (9w,18w+18) & (9w+9,18w+18) & (9w+18,18w+18) \\
 & & & & & \\
(18w,0) & & (18w+9,0) & & (18w+18,0) & \\
(18w,9) & & (18w+9,9) & & (18w+18,9) & \\
(18w,18) & & (18w+9,18) & & (18w+18,18) & \\
(18w,9w) & & (18w+9,9w) & & (18w+18,9w) & \\
(18w,18w) & & (18w+9,18w) & & (18w+18,18w) & \\
(18w,9w+9) & & (18w+9,9w+9) & & (18w+18,9w+9) & \\
(18w,9w+18) & & (18w+9,9w+18) & & (18w+18,9w+18) & \\
(18w,18w+9) & & (18w+9,18w+9) & & (18w+18,18w+9) & \\
(18w,18w+18) & & (18w+9,18w+18) & & (18w+18,18w+18) &
\end{array} \right\}$$

$$
\Phi(C)=\left\{\begin{array}{cccccc}
\langle(000000)\rangle_{27} & \langle(101010)\rangle_{27} & \langle(202020)\rangle_{27} & \langle(\omega 0\omega 0\omega 0)\rangle_{27} & \langle(\omega^2 0\omega^2 0\omega^2 0)\rangle_{27} & \langle(\omega^7 0\omega^7 0\omega^7 0)\rangle_{27} \\
\langle(010101)\rangle_{27} & \langle(111111)\rangle_{27} & \langle(212121)\rangle_{27} & \langle(\omega 1\omega 1\omega 1)\rangle_{27} & \langle(\omega^2 1\omega^2 1\omega^2 1)\rangle_{27} & \langle(\omega^7 1\omega^7 1\omega^7 1)\rangle_{27} \\
\langle(020202)\rangle_{27} & \langle(121212)\rangle_{27} & \langle(222222)\rangle_{27} & \langle(\omega 2\omega 2\omega 2)\rangle_{27} & \langle(\omega^2 2\omega^2 2\omega^2 2)\rangle_{27} & \langle(\omega^7 2\omega^7 2\omega^7 2)\rangle_{27} \\
\langle(0\omega 0\omega 0\omega)\rangle_{27} & \langle(1\omega 1\omega 1\omega)\rangle_{27} & \langle(2\omega 2\omega 2\omega)\rangle_{27} & \langle(\omega\omega\omega\omega\omega\omega)\rangle_{27} & \langle(\omega^2\omega\omega^2\omega\omega^2\omega)\rangle_{27} & \langle(\omega^7\omega\omega^7\omega\omega^7\omega)\rangle_{27} \\
\langle(0\omega^5 0\omega^5 0\omega^5)\rangle_{27} & \langle(1\omega^5 1\omega^5 1\omega^5)\rangle_{27} & \langle(2\omega^5 2\omega^5 2\omega^5)\rangle_{27} & \langle(\omega\omega^5\omega\omega^5\omega\omega^5)\rangle_{27} & \langle(\omega^2\omega^5\omega^2\omega^5\omega^2\omega^5)\rangle_{27} & \langle(\omega^7\omega^5\omega^7\omega^5\omega^7\omega^5)\rangle_{27} \\
\langle(0\omega^2 0\omega^2 0\omega^2)\rangle_{27} & \langle(1\omega^2 1\omega^2 1\omega^2)\rangle_{27} & \langle(2\omega^2 2\omega^2 2\omega^2)\rangle_{27} & \langle(\omega\omega^2\omega\omega^2\omega\omega^2)\rangle_{27} & \langle(\omega^2\omega^2\omega^2\omega^2\omega^2\omega^2)\rangle_{27} & \langle(\omega^7\omega^2\omega^7\omega^2\omega^7\omega^2)\rangle_{27} \\
\langle(0\omega^7 0\omega^7 0\omega^7)\rangle_{27} & \langle(1\omega^7 1\omega^7 1\omega^7)\rangle_{27} & \langle(2\omega^7 2\omega^7 2\omega^7)\rangle_{27} & \langle(\omega\omega^7\omega\omega^7\omega\omega^7)\rangle_{27} & \langle(\omega^2\omega^7\omega^2\omega^7\omega^2\omega^7)\rangle_{27} & \langle(\omega^7\omega^7\omega^7\omega^7\omega^7\omega^7)\rangle_{27} \\
\langle(0\omega^3 0\omega^3 0\omega^3)\rangle_{27} & \langle(1\omega^3 1\omega^3 1\omega^3)\rangle_{27} & \langle(2\omega^3 2\omega^3 2\omega^3)\rangle_{27} & \langle(\omega\omega^3\omega\omega^3\omega\omega^3)\rangle_{27} & \langle(\omega^2\omega^3\omega^2\omega^3\omega^2\omega^3)\rangle_{27} & \langle(\omega^7\omega^3\omega^7\omega^3\omega^7\omega^3)\rangle_{27} \\
\langle(0\omega^6 0\omega^6 0\omega^6)\rangle_{27} & \langle(1\omega^6 1\omega^6 1\omega^6)\rangle_{27} & \langle(2\omega^6 2\omega^6 2\omega^6)\rangle_{27} & \langle(\omega\omega^6\omega\omega^6\omega\omega^6)\rangle_{27} & \langle(\omega^2\omega^6\omega^2\omega^6\omega^2\omega^6)\rangle_{27} & \langle(\omega^7\omega^6\omega^7\omega^6\omega^7\omega^6)\rangle_{27} \\
 & & & & & \\
\langle(\omega^5 0\omega^5 0\omega^5 0)\rangle_{27} & & \langle(\omega^3 0\omega^3 0\omega^3 0)\rangle_{27} & & \langle(\omega^6 0\omega^6 0\omega^6 0)\rangle_{27} & \\
\langle(\omega^5 1\omega^5 1\omega^5 1)\rangle_{27} & & \langle(\omega^3 1\omega^3 1\omega^3 1)\rangle_{27} & & \langle(\omega^6 1\omega^6 1\omega^6 1)\rangle_{27} & \\
\langle(\omega^5 2\omega^5 2\omega^5 2)\rangle_{27} & & \langle(\omega^3 2\omega^3 2\omega^3 2)\rangle_{27} & & \langle(\omega^6 2\omega^6 2\omega^6 2)\rangle_{27} & \\
\langle(\omega^5\omega\omega^5\omega\omega^5\omega)\rangle_{27} & & \langle(\omega^3\omega\omega^3\omega\omega^3\omega)\rangle_{27} & & \langle(\omega^6\omega\omega^6\omega\omega^6\omega)\rangle_{27} & \\
\langle(\omega^5\omega^5\omega^5\omega^5\omega^5\omega^5)\rangle_{27} & & \langle(\omega^3\omega^5\omega^3\omega^5\omega^3\omega^5)\rangle_{27} & & \langle(\omega^6\omega^5\omega^6\omega^5\omega^6\omega^5)\rangle_{27} & \\
\langle(\omega^5\omega^2\omega^5\omega^2\omega^5\omega^2)\rangle_{27} & & \langle(\omega^3\omega^2\omega^3\omega^2\omega^3\omega^2)\rangle_{27} & & \langle(\omega^6\omega^2\omega^6\omega^2\omega^6\omega^2)\rangle_{27} & \\
\langle(\omega^5\omega^7\omega^5\omega^7\omega^5\omega^7)\rangle_{27} & & \langle(\omega^3\omega^7\omega^3\omega^7\omega^3\omega^7)\rangle_{27} & & \langle(\omega^6\omega^7\omega^6\omega^7\omega^6\omega^7)\rangle_{27} & \\
\langle(\omega^5\omega^3\omega^5\omega^3\omega^5\omega^3)\rangle_{27} & & \langle(\omega^3\omega^3\omega^3\omega^3\omega^3\omega^3)\rangle_{27} & & \langle(\omega^6\omega^3\omega^6\omega^3\omega^6\omega^3)\rangle_{27} & \\
\langle(\omega^5\omega^6\omega^5\omega^6\omega^5\omega^6)\rangle_{27} & & \langle(\omega^3\omega^6\omega^3\omega^6\omega^3\omega^6)\rangle_{27} & & \langle(\omega^6\omega^6\omega^6\omega^6\omega^6\omega^6)\rangle_{27} &
\end{array}\right\}
$$

A RESULTADOS COMPLEMENTARIOS

A.1 INMERSIÓN DE LA ESTRUCTURA DE ANILLO

Sean R un anillo conmutativo con identidad, S un conjunto no vacío y $\phi : R \to S$ una función biyectiva, luego podemos inducir la estructura de anillo en $S = \phi(R)$ definiendo dos operaciones $\oplus$ y $\odot$ en S de la siguiente manera:

Dados $s_1, s_2 \in S$ existen $r_1, r_2 \in R$ tales que $\phi(r_1) = s_1$ y $\phi(r_2) = s_2$ entonces:

$$\begin{aligned} s_1 \oplus s_2 &= \phi(r_1 + r_2) \\ s_1 \odot s_2 &= \phi(r_1 r_2) \end{aligned} \tag{A.1.1}$$

Teorema A.1.1. $(S, \oplus, \odot)$ *es un anillo conmutativo con identidad.*

Demostración. La cerradura de ambas operaciones es inmediata de su definición. Ahora, dados $s_1, s_2, s_3 \in S$, denotemos mediante $s = s_1 \oplus s_2$, $s' = s_2 \oplus s_3$, $t = s_1 \odot s_2$, $t' = s_2 \odot s_3$ y por otro lado si $\phi(r_i) = s_i$ para algunos $i \in \{1, 2, 3\}$ denotemos $r = r_1 + r_2$, $r' = r_2 + r_3$, $q = r_1 r_2$ y $q' = r_2 r_3$. Luego, de (A.1.1) tenemos que $\phi(r) = s$, $\phi(q) = t$, $\phi(r') = s'$ y $\phi(q') = t'$. Así:

$$\begin{aligned} (s_1 \oplus s_2) \oplus s_3 &= s \oplus s_3 \\ &= \phi(r + r_3) \\ &= \phi((r_1 + r_2) + r_3) \\ &= \phi(r_1 + r') \\ &= s_1 \oplus s' \\ \therefore (s_1 \oplus s_2) \oplus s_3 &= s_1 \oplus (s_2 \oplus s_3) \end{aligned} \qquad \begin{aligned} (s_1 \odot s_2) \odot s_3 &= t \odot s_3 \\ &= \phi(q r_3) \\ &= \phi((r_1 r_2) r_3) \\ &= \phi(r_1 q') \\ &= s_1 \odot t' \\ \therefore (s_1 \odot s_2) \odot s_3 &= s_1 \odot (s_2 \odot s_3) \end{aligned}$$

A continuación, si denotamos $\hat{0} = \phi(0)$ y $\hat{1} = \phi(1)$, luego dado $s \in S$ tal que $\phi(r) = s$ con $r \in R$ entonces:

$$\begin{aligned} \hat{0} \oplus s &= \phi(0 + r) \\ &= \phi(r) \\ \therefore \hat{0} \oplus s &= s \end{aligned} \qquad \begin{aligned} s \oplus \hat{0} &= \phi(r + 0) \\ &= \phi(r) \\ \therefore s \oplus \hat{0} &= s \end{aligned} \qquad \begin{aligned} \hat{1} \odot s &= \phi(1r) \\ &= \phi(r) \\ \therefore \hat{1} \odot s &= s \end{aligned} \qquad \begin{aligned} s \odot \hat{1} &= \phi(r1) \\ &= \phi(r) \\ \therefore s \odot \hat{1} &= s \end{aligned}$$

por consiguiente $(S, \oplus)$ y $(S, \odot)$ son monoides. Por otro lado, considere que dado un elemento $r \in R$ entonces existe $-r \in R$ tal que $r + (-r) = 0$ luego

si denotamos por $\hat{s} = \phi(-r)$ tenemos que si $r, r_1, r_2 \in R$ y $\phi(r) = s, \phi(r_i) = s_i$ con $i \in \{1, 2\}$, luego:

$$\begin{aligned} s_1 \oplus s_2 &= \phi(r_1 + r_2) \\ &= \phi(r_2 + r_1) \\ \therefore s_1 \oplus s_2 &= s_2 \oplus s_1 \end{aligned} \qquad \begin{aligned} s_1 \odot s_2 &= \phi(r_1 r_2) \\ &= \phi(r_2 r_1) \\ \therefore s_1 \odot s_2 &= s_2 \odot s_1 \end{aligned} \qquad \begin{aligned} s \oplus \hat{s} &= \phi(r + (-r)) \\ &= \phi(0) \\ \therefore s \oplus \hat{s} &= \hat{0} \end{aligned}$$

De lo anterior se sigue que $(S, \oplus)$ es un grupo abeliano y $(S, \odot)$ es un monoide conmutativo, así que finalmente si denotamos $s = s_2 \oplus s_3$, $s' = s_1 \odot s_2$, $s'' = s_1 \odot s_3$ y si $\phi(r) = s$, $r = r_2 + r_3$, $r' = r_1 r_2$ y $r'' = r_1 r_3$ entonces

$$\begin{aligned} s_1 \odot (s_2 \oplus s_3) &= s_1 \odot s \\ &= \phi(r_1 r) \\ &= \phi(r_1(r_2 + r_3)) \\ &= \phi(r' + r'') \\ &= s' \oplus s'' \\ \therefore s_1 \odot (s_2 \oplus s_3) &= (s_1 \odot s_2) \oplus (s_1 \odot s_3) \end{aligned}$$

□

A.2 POLINOMIOS EN VARIAS VARIABLES

En este apartado, exhibiremos propiedades relativas a anillos de polinomios en varias variables sobre anillos conmutativos con identidad. Dichas propiedades serán demostradas para los casos de una o dos variables entendiendo que pueden generalizarse por inducción.

Definición A.2.1. Sean R un anillo conmutativo con identidad 1_R, 0_R el elemento neutro de la suma del grupo $(R, +)$ y $R[x]$ el anillo de polinomios en la indeterminada x con coeficientes en R, entonces:

(i) El anillo de polinomios en las indeterminadas x_1 y x_2 con coeficientes en R denotado por $R[x_1, x_2]$ es el anillo polinomial $S[x_2]$ donde $S = R[x_1]$, en general, si k es un entero positivo entonces el anillo de polinomios en las k indeterminadas $x_1, x_2, \ldots, x_k$ es el anillo polinomial $S[x_k]$ donde $S = R[x_1, x_2, \ldots, x_{k-1}]$.

(ii) Dado un polinomio en k indeterminadas $f(x_1, x_2, \ldots, x_k)$, el *grado relativo* de f respecto a la variable x_j se denota por $\delta_j(f)$ para $(0 \leq j \leq k)$ y es el grado del polinomio en el anillo polinomial $S[x_j]$ donde $S = R[x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_k]$.

Observación A.2.2. En lo sucesivo denotaremos a un polinomio en k indeterminadas $f(x_1, x_2, \ldots, x_k)$ y al anillo $R[x_1, x_2, \ldots, x_k]$ mediante $f(\underline{x})$ y $R[\underline{x}]$ respectivamente. Cada vez que la variable x_j no aparezca en un polinomio, éste se denotará como $f(\hat{x}_j)$, con está notación tenemos que dado $f(\underline{x})$ tal que $\delta_j(f) = n_j$ existen polinomios $g_i(\hat{x}_j)$ con $0 \leq i \leq k$ tales que:

$$f(\underline{x}) = \sum_{i=0}^{n_j} g_i(\hat{x}_j) x_j^i. \tag{A.2.1}$$

Además, en lo sucesivo trataremos de manera indistinta a los polinomios en k variables como sumas formales así como funciones polinomiales y diremos que el *término constante* de $f(\underline{x})$ es el elemento $f(0_R, 0_R, \ldots, 0_R) \in R$.

Ejemplo A.2.3. (i) Sea $f(\underline{x}) \in \mathbb{Z}[x_1, x_2, x_3]$ dado por $f(\underline{x}) = x_1^2 x_2 + 2x_1 x_3^2 - x_1 x_2 x_3 + x_1 + 1$ entonces notemos que $f(\underline{x})$ puede escribirse de 3 formas:

$$\begin{aligned}
&1 + (2x_3^2 - x_2 x_3 + 1)x_1 + (x_2)x_1^2 \\
&(1 + x_1 + 2x_1 x_3^2) + (x_1^2 - x_1 x_3)x_2 \\
&(1 + x_1 + x_1^2 x_2) + (x_1 x_2)x_3 + (2x_1)x_3^2
\end{aligned}$$

y de ahí que $\delta_1(f) = 2$, $\delta_2(f) = 1$, $\delta_3(f) = 2$ y el término constante es $f(0, 0, 0) = 1$.

Lema A.2.4. *Sean $\phi(x) = c_0 + c_1 x + \ldots + c_r x^r \in \mathbb{Z}[x]$, $r \in \mathbb{N}$ y p un número primo. Entonces $(\phi(x))^p \equiv \hat{\phi}(x^p) \pmod{p}$ donde $\hat{\phi}(t) \in \mathbb{Z}[t]$.*

Demostración. Hagamos inducción en r. Para $r = 1$ tenemos que $\phi(x) = c_0 + c_1 x$ luego es claro que:

$$(\phi(x))^p = (c_0 + c_1 x)^p = c_0^p + \sum_{j=1}^{p-1} \binom{p}{j} (c_0)^{p-j} (c_1 x)^j + c_1^p x^p$$

entonces se sigue que $(\phi(x))^p - \left[c_0^p + c_1^p x^p\right] = \sum_{j=1}^{p-1} \binom{p}{j} (c_0)^{p-j} (c_1 x)^j$ y dado que $p \mid \binom{p}{j}$ cada vez que $1 \leq j \leq p-1$ es claro que si elegimos $\hat{\phi}(t) = c_0^p + c_1^p t$ entonces $(\phi(x))^p \equiv \hat{\phi}(x^p) \pmod{p}$.

Suponagmos que si $grad(\phi) \leq r - 1$ entonces el resultado es válido y sea $\phi(x) = c_0 + c_1 x + \ldots + c_r x^r$. Entonces $f(x) = \phi(x) - c_r x^r \in \mathbb{Z}[x]$ y es tal que $grad f = r - 1$ entonces por hipótesis inductiva se sigue que:

$$(f(x))^p \equiv \hat{f}(x^p) \pmod{p}$$

donde $\hat{f}(t) \in \mathbb{Z}[t]$. Más aún, ya que $(\phi(x) - c_r x^r)^p = (f(x))^p$ entonces:

$$(\phi(x) - c_r x^r)^p \equiv \hat{f}(x^p) \pmod{p} \tag{A.2.2}$$

Por otro lado, es fácil ver que procediendo como antes $(\phi(x) - c_r x^r)^p \equiv (\phi(x))^p - c_r^p x^{pr} \pmod{p}$ así que combinando esto con (A.2.2) se concluye que:

$$(\phi(x))^p - c_r^p x^{pr} \equiv \hat{f}(x^p) \pmod{p}$$

definamos $\hat{\phi}(t) = \hat{f}(t) + c_r^p t^r$ y de lo anterior se sigue el resultado. □

Este resultado puede extenderse de manera natural por inducción a polinomios en múltiples variables $x_1, x_2, \ldots, x_k$ para k un entero positivo como sigue:

Corolario A.2.5. *Sean $f(\underline{x}) \in \mathbb{Z}[\underline{x}]$ y p un número primo. Entonces $(f(\underline{x}))^p \equiv \hat{f}(\underline{x}^p) \pmod{p}$ para algún $\hat{f}(\underline{t}) \in \mathbb{Z}[\underline{t}]$.*

A.3 RAÍCES p-ÉSIMAS EN CAMPOS FINITOS

Sea $\mathbb{F}_q$ un campo finito con $q = p^m$ elementos y $\mathbb{F}_p (\simeq \mathbb{Z}_p)$ su campo primo. Como se mencionó en la Sección 1.1 existe un polinomio primitivo $f(x)$ de grado m tal que $\mathbb{F}_q \simeq \frac{\mathbb{Z}_p[x]}{\langle f(x) \rangle}$ y donde $\hat{\beta} = \{1, \omega, \omega^2, \ldots, \omega^{m-1}\}$ es una base del espacio vectorial ${}_{\mathbb{F}_p}\mathbb{F}_q$ al cual denotaremos mediante $\mathbb{F}_p[\omega]$, es decir el conjunto de todas la expresiones polinomiales de grado a lo más $m-1$ con coeficientes en $\mathbb{F}_p$.

Por otro lado consideremos el automorfismo de Frobenius:

$$\begin{aligned} \sigma : \mathbb{F}_p[\omega] &\to \mathbb{F}_p[\omega] \\ v &\mapsto v^p \end{aligned}$$

el cual es un isomorfismo que deja fijos a los elementos de $\mathbb{F}_p$, con esto veamos el siguiente:

Lema A.3.1. *El automorfismo de Frobenius es un operador lineal invertible.*

Demostración. Como σ es biyectivo, solo resta ver que es un operador lineal. En efecto, dados dos elementos $u, v \in \mathbb{F}_p[\omega]$, como σ es homomorfismo entonces $\sigma(u+v) = \sigma(u) + \sigma(v)$ y dado $\lambda \in \mathbb{F}_p$ entonces:

$$\begin{aligned} \sigma(\lambda v) &= \sigma(\lambda)\sigma(v) && (\sigma \text{ es homomorfismo}) \\ &= \lambda\sigma(v) && (\sigma \text{ deja fijo a } \mathbb{F}_p) \end{aligned}$$

por consiguiente es un operador lineal invertible. □

Por el lema anterior, tenemos que si $P := [\sigma]_{\hat{\beta}}$ es la representación matricial del automorfismo de Frobenius en la base $\hat{\beta}$, ésta es invertible y su inversa P^{-1} es tal que para todo $a \in \mathbb{F}_q$:

$$P\left(P^{-1}[a]_{\hat{\beta}}\right) = [a]_{\hat{\beta}} \tag{A.3.1}$$

abusando de la notación si $b \in \mathbb{F}_q$ es tal que $[b]_{\hat{\beta}} = P^{-1}[a]_{\hat{\beta}}$ entonces $b^p = P[b]_{\hat{\beta}} = a$, por lo cual presentamos la siguiente:

Definición A.3.2. Sea $\mathbb{F}_q$ un campo finito y $a \in \mathbb{F}_q$. Un elemento $b \in \mathbb{F}_q$ es la *raíz q-ésima* de a si y sólo si $b^q = a$, lo cual denotaremos mediante $b = \sqrt[q]{a}$ o bien $b = a^{1/q}$.

Nótese que todo lo discutido antes de la Definición A.3.2 (cf. [11]) nos otorga un procedimiento para obtener las raíces p-ésimas de elementos en un campo finito y más aún, la forma de expresar dichas raíces en términos de la base $\hat{\beta}$. A continuación, mostramos algunos ejemplos de campos finitos y las respectivas tablas de las raíces p-ésimas de sus elementos.

Ejemplo A.3.3. Por simplicidad denotaremos $[a]_{\hat{\beta}}$ solamente como $[a]$.

- Como σ deja fijo a $\mathbb{F}_p$, entonces para todo $a \in \mathbb{F}_p$ se tiene que $\sigma(a) = a$, es decir, es su propia raíz p-ésima.
- Supongamos que $p = 2$ y $m = 2$. Entonces $f(x) = x^2 + x + 1$ y $\hat{\beta} := \{1, \omega\}$, de ahí que, $\sigma(1) = 1$ y $\sigma(\omega) = \omega^2 = 1 + \omega$, luego $[1] = (1,0)$ y $[\omega] = (1,1)$ entonces:

$$P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad P^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

a	$\sqrt[2]{a}$
0	0
1	1
ω	$1+\omega$
$1+\omega$	ω

Cuadro 3.: Raíces cuadradadas en $\mathbb{F}_2^2$

- Consideremos $p = 2$ y $m = 3$. Entonces $f(x) = x^3 + x + 1$ y $\hat{\beta} := \{1, \omega, \omega^2\}$ entonces $\sigma(1) = 1$, $\sigma(\omega) = \omega^2$ y $\sigma(\omega^2) = \omega^4 = \omega^2 + \omega$, luego $[1] = (1,0,0)$, $[\omega] = (0,1,0)$ y $[\omega^2] = (0,1,1)$ entonces:

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

- Para los parámetros $p = 3$, $m = 2$, entonces $f(x) = x^2 + 2x + 2$.

a	$\sqrt[2]{a}$	a	$\sqrt[2]{a}$
0	0	ω^2	ω
1	1	ω^2+1	$\omega+1$
ω	$\omega+\omega^2$	$\omega^2+\omega$	ω^2
$1+\omega$	$1+\omega+\omega^2$	$\omega^2+\omega+1$	ω^2+1

Cuadro 4.: Raíces cuadradadas en $\mathbb{F}_2^3$

$$P = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \qquad P^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$$

a	$\sqrt[3]{a}$	a	$\sqrt[3]{a}$	a	$\sqrt[3]{a}$
0	0	ω	$1+2\omega$	2ω	$2+\omega$
1	1	$1+\omega$	$2\omega+2$	$2\omega+1$	ω
2	2	$2+\omega$	2ω	$2\omega+2$	$1+\omega$

Cuadro 5.: Raíces cúbicas en $\mathbb{F}_3^2$

Recordemos también que el automorfismo de Frobenius forma un grupo cíclico de orden m con la composición de funciones, de donde se sigue que $\sigma^m = id_{\mathbb{F}_q}$, de ahí que $\sigma^{m-1} = \sigma^{-1}$ y luego tenemos que $P^{-1} = P^{m-1}$. Usemos esto para ver un ejemplo más elaborado, si $p = 5$ y $m = 4$ entonces el campo finito $\mathbb{F}_q$ tiene $q = 5^4 = 625$ elementos, además hemos tomado como polinomio primitivo asociado al campo finito a $f(x) = x^4 + 4x^2 + 4x + 2$ y $\hat{\beta} = \{1, \omega, \omega^2, \omega^3\}$ y dado que: $[\sigma(1)] = (1,0,0,0)$ $[\sigma(\omega)] = (0,3,1,1)$, $[\sigma(\omega^2)] = (4,4,2,4)$ y $[\sigma(\omega^3)] = (1,2,1,4)$.

$$P = \begin{pmatrix} 1 & 0 & 4 & 1 \\ 0 & 3 & 4 & 2 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 4 & 4 \end{pmatrix} \qquad P^3 = \begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 0 \\ 0 & 3 & 0 & 1 \\ 0 & 3 & 3 & 3 \end{pmatrix} = P^{-1}$$

B MAGMA

SageMath es un software matemático de código abierto el cual permite la compilación de lenguajes de programación basados en Phyton. MAGMA es un software especializado en el álgebra abstracta, teoría de números, geometría algebraica y combinatoria, posee un riguroso entorno que permite la manipulación de estructuras como grupos, anillos, campos, módulos, étc.

En este trabajo de tesis, nos hemos apoyado en el uso del entorno gráfico *notebook* en línea de Sage y los comandos del software MAGMA para la implementación de ejemplos sobre anillos de Galois y los códigos mencionados. En este apéndice presentamos algunos de los *programas* u *hojas de trabajo* usadas en la elaboración de este escrito.

A lo largo de este apéndice, los comandos aparecen precedidos por el símbolo $>$. Hemos colocado comentarios de ayuda, éstos están precedidos de // y el resultado de la compilación del programa se mostrará en una caja sin estar precedido de ningún símbolo.

El lector podrá consultar el manual de usuario de MAGMA para observar las funciones e instrucciones nativos en el manual, disponible en:

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

o su versión en pdf:

`https://www.math.uzh.ch/sepp/magma-2.19.8-cr/Handbook.pdf`.

B.1 REPRESENTACIONES p-ÁDICAS

MAGMA provee al usuario de los comandos básicos para la construcción del anillo de Galois $GR(p^s, m)$ mediante la instrucción `GaloisRing(p,s,h)` donde p, s son enteros positivos y h es un polinomio mónico básico primitivo de grado m.

```
>Z:=IntegerRing();
>P<x>:=PolynomialRing(Z);
>s:=3;//Introduzca un entero positivo.
>m:=3;// Introduzca un entero positivo.
>p:=2;//Introduzca un numero primo.
>h:=x^3 + 3*x^2 + 2*x + 7;// Introduzca un polinomio basico
    irreducible de grado "m".
>R<w>:=GaloisRing(p,s,h);
>R;
```

```
GaloisRing(2,3,x^3 + 3*x^2 + 2*x + 7)
```

Observación B.1.1. `R<w>` indica al programa que R es el identificador del anillo y la indeterminada del anillo de Galois visto como clases polinomiales es w.

Una vez construido el anillo de Galois, MAGMA nos permite obtener el campo residual mediante la instrucción `ResidueField` y podemos construir el conjunto de Teichmüller usando las potencias de w.

```
>RF<t>:=ResidueField(R);//Campo residual de R.
>T:=[0]cat[w^i: i in [0..(p^m-1)]];// Conjunto de Teichmuller.
>"Campo Residual";
>RF;
"Conjunto de Teichmuller";
>T;
```

```
Campo Residual
[0,1,t,t^2,t^3,t^4,t^5,t^6]
Conjunto de Teichmuller
[ 0, w, w^2, 5*w^2 + 6*w + 1, 7*w^2 + 7*w + 5, 2*w^2 + 7*w + 7, w
   ^2 +
3*w + 2, 1 ]
```

Otro elemento importante en el manejo de los anillos de Galois es la μ-reducción y las componentes p-ádicas. MAGMA cuenta con la instrucción nativa `function` la cual usamos para calcular las componentes p-ádicas, al dar un elemento c en el anillo de Galois nos es devuelto un vector $< \rho_0(c), \rho_1(c), \ldots, \rho_{s-1}(c) >$.

```
Padic:=function(c)
    W:=[Random(T): i in [1..s]];
    while (c eq &+[W[i]*p^(i-1): i in [1..s]]) eq false do
        W:=[Random(T): i in [1..s]];
```

```
    end while;
    V:=<W[i]:i in [1..#W]>;
    return V;
end function;// Funcion que calcula las componentes p-adicas.
```

Observación B.1.2. En la siguiente instrucción, tenemos que los símbolos `R` y `RF` son los identificadores del anillo de Galois y su campo residual respectivamente. Mediante la función nativa `Coercion`, renombrada por `Mu` es la μ-reducción y con ésta misma, podemos construir una función que calcule la μ-reducción de las componentes p-ádicas de los elementos en el anillo de Galois, es decir, dado un elemento en R nos devuelve un vector $< r_0(c), r_1(c), \ldots, r_{s-1}(c) >$.

```
>Mu:=Coercion(R,RF);// Mu-reduccion.
MRPadic:=function(r)
    S:=<>;
    for i in [1..s] do
        e:=Mu(Padic(r)[i]);
        Append(~S,e);
    end for;
    return S;
end function;// Mu-reduccion de las componentes p-adicas de un
   elemento de R.
```

Ejemplo B.1.3. En el presente apéndice estamos desarrollando al anillo de Galois $R{=}GR(2^3,3)$. Considere los elementos $2w+2$, w^2+1 y calculemos sus componentes p-ádicas:

$$2w+2 = 0 + 2(2w^2+7w+7) + 2^2(7w^2+7w+5)$$
$$w^2+1 = (5w^2+6w+1) + 2(w) + 2^2(w^2)$$

podemos verificar con el programa:

```
>Padic(2*w+2);
 <0, 2*w^2 + 7*w + 7, 7*w^2 + 7*w + 5>
>Padic(w^2+1);
<5*w^2 + 6*w + 1, w, w^2>
```

y las μ-reducciones de éstas:

```
>MRPadic(2*w+2);
<0, t^5, t^4>
>MRPadic(w^2+1);
<t^3, t, t^2>
```

B.1.1 Polinomios Mónicos Básicos Primitivos

Cuando se genera un anillo de Galois, es necesario introducir un polinomio mónico básico primitivo, la siguiente serie de instrucciones permite generar de manera aleatoria un polinomio mónico básico primitivo de grado m con los parámetros dados p, s.

```
>p:=2;//Introduza un numero primo.
>s:=3;//Introduzca un entero.
>m:=3;//Introduca un entero.
//Generador de h(x) polinomio monico basico primitivo.
>ZZ<x>:=PolynomialRing(IntegerRing());
>Z:=IntegerRing(p^s);
>P<x>:=PolynomialRing(Z);
>K:=GF(p);
>L<t>:=PolynomialRing(GF(p))>Mum:=Coercion(P,L);
>J:=[Random(Z): i in [1..m]] cat [1];
>h:=elt<P|J>;
while ((x^(p^m-1) mod h) eq 1) eq false do
    J:=[Random(Z): i in [1..m]] cat [1];
    h:=elt<P|J>;
    while (IsPrimitive(Mum(h)) eq false) do
        J:=[Random(Z): i in [1..m]] cat [1];
        h:=elt<P|J>;
    end while;
end while;
>"h(x)=",h;//Polinomio monico basico primitivo.
```

```
h(x)= x^3 + 3*x^2 + 2*x + 7
```

B.2 LA FUNCIÓN DE GRAY

MAGMA cuenta con la función nativa `KroneckerProduct`, la cual realiza el producto de Kronecker, expandido de derecha a izquierda, sin embargo para nuestros fines, se generó el producto de Kronecker de izquiera a derecha mediante las siguientes instrucciones.

```
//Producto de Kronecker (expandido de izquierda a derecha).
>KP:=function(u,v)
    S:=< >;
    i:=1;
    j:=1;
        while i lt (#v+1) do
```

```
            for j in [1..#u] do
            e:=v[i]*u[j];
            Append(~S,e);
        end for;
        i+:=1;
    end while;
    return S;
end function;
```

Ejemplo B.2.1. Para los parámetros que estamos trabajando en el presente apéndice $p = 2, s = 3$ y $m = 3$ obtuvimos que su campo residual está dado por:

$$\mathbb{F}_{2^3} := \{0, 1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7\}$$

Como se analizó en la sección 2.3 existe un orden específico de los elementos del campo residual que nos permite definir a los vectores $\mathbf{c}_0, \mathbf{c}_1$ y $\mathbf{c}_2$ en la construcción de la función de Gray. En función de esto, se forman las siguientes instrucciones:

```
>Zp:=[i:i in [0..(p-1)]];//Anillo de enteros modulo p^s.
>Ugen:=function(c)
    W:=[Random(Zp): i in [1..m]];
    while (c eq &+[W[i]*p^(i-1): i in [1..m]]) eq false do
        W:=[Random(Zp): i in [1..m]];
    end while;
        Y:=[W[i]:i in [1..#W]];
return Y;
end function;
>U:=<elt<F|Ugen(i)>: i in [0..(p^m)-1]>;//Vector u;
>V:=<1: i in [1..p^m]>;//Vector v;
>"u =",U;
>"v =",V;
```

```
u = <0, 1, t, t^5, t^2, t^3, t^6, t^4>
v = <1, 1, 1, 1, 1, 1, 1, 1>
```

Dichas instrucciones nos permiten generar los vectores u y v los que son puntos clave para los vectores introducidos en la ecuación (2.3.11):

$$\begin{aligned} \mathbf{c}_0 &= u \otimes v \\ \mathbf{c}_1 &= v \otimes u \\ \mathbf{c}_2 &= v \otimes v \end{aligned} \tag{B.2.1}$$

```
>c0:=KP(U,V);
>c1:=KP(V,U);
>c2:=KP(V,V);
c0 = <0, 1, t, t^5, t^2, t^3, t^6, t^4, 0, 1, t, t^5, t^2, t^3, t
   ^6,
t^4, 0, 1, t, t^5, t^2, t^3, t^6, t^4, 0, 1, t, t^5, t^2, t^3, t
   ^6, t^4,
0, 1, t, t^5, t^2, t^3, t^6, t^4, 0, 1, t, t^5, t^2, t^3, t^6, t
   ^4, 0,
1, t, t^5, t^2, t^3, t^6, t^4, 0, 1, t, t^5, t^2, t^3, t^6, t^4>
c1 = <0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, t, t, t, t,
    t,
t, t, t, t^5, t^5, t^5, t^5, t^5, t^5, t^5, t^5, t^2, t^2, t^2, t
   ^2,
t^2, t^2, t^2, t^2, t^3, t^3, t^3, t^3, t^3, t^3, t^3, t^3, t^6,
   t^6,
t^6, t^6, t^6, t^6, t^6, t^6, t^4, t^4, t^4, t^4, t^4, t^4, t^4,
   t^4>
c2 = <1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
    1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
    1, 1,
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1>
```

Como podemos ver, la función producto de Kronecker que hemos diseñado nos permite realizar el cálculo preciso y salvar tiempo.

B.2.1 MAGMA en anillos de índice de nilpotencia 3

MAGMA provee una función de Gray para poder operar elementos de espacios vectoriales, a partir de este momento, nos concentraremos únicamente en los anillos de Galois de índice de nilpotencia 3, y por lo tanto las hojas de trabajo presentadas estarán adaptadas para este fin.

Además, introducimos un encabezado para cada programa que nos permite definir el anillo de Galois, las representaciones p-ádicas y los vectores $\mathbf{c}_0, \mathbf{c}_1$ y $\mathbf{c}_2$.

```
>Z:=IntegerRing();
>P<x>:=PolynomialRing(Z);
>s:=3;//Introduzca un entero positivo.
>m:=3;// Introduzca un entero positivo.
>p:=2;//Introduzca un numero primo.
```

```
>h:=x^3 + 3*x^2 + 2*x + 7;// Introduzca un polinomio basico
    irreducible de grado "m".
>R<w>:=GaloisRing(p,s,h);
>R;
>RF<t>:=ResidueField(R);//Campo residual de R.
>T:=[0]cat[w^i: i in [0..(p^m-1)]];// Conjunto de Teichmuller.
>"Campo Residual";
>RF;
"Conjunto de Teichmuller";
>T;
Padic:=function(c)
    W:=[Random(T): i in [1..s]];
    while (c eq &+[W[i]*p^(i-1): i in [1..s]]) eq false do
        W:=[Random(T): i in [1..s]];
    end while;
    V:=<W[i]:i in [1..#W]>;
    return V;
end function;// Funcion que calcula las componentes p-adicas.
>Mu:=Coercion(R,RF);// Mu-reduccion.
MRPadic:=function(r)
    S:=<>;
    for i in [1..s] do
        e:=Mu(Padic(r)[i]);
        Append(~S,e);
    end for;
    return S;
end function;// Mu-reduccion de las componentes p-adicas de un
    elemento de R.
//Producto de Kronecker (expandido de izquierda a derecha).
>KP:=function(u,v)
    S:=< >;
    i:=1;
    j:=1;
        while i lt (#v+1) do
            for j in [1..#u] do
            e:=v[i]*u[j];
            Append(~S,e);
        end for;
        i+:=1;
    end while;
    return S;
end function;
>Zp:=[i:i in [0..(p-1)]];//Anillo de enteros modulo p^s.
>Ugen:=function(c)
```

```
    W:=[Random(Zp): i in [1..m]];
    while (c eq &+[W[i]*p^(i-1): i in [1..m]]) eq false do
        W:=[Random(Zp): i in [1..m]];
    end while;
        Y:=[W[i]:i in [1..#W]];
return Y;
end function;
>U:=<elt<F|Ugen(i)>: i in [0..(p^m)-1]>;//Vector u;
>V:=<1: i in [1..p^m]>;//Vector v;
>"u =",U;
>"v =",V;
>c0:=KP(U,V);
>c1:=KP(V,U);
>c2:=KP(V,V);
```

B.2.2 La función de Gray

Dados todos estos elementos podemos generar un programa que representa a la función de Gray para los códigos definidos sobre anillos de Galois de índice de nilpotencia 3.

$$\Phi : GR(p^s, m)^n \mapsto \mathbb{F}_q^{nq^2} \tag{B.2.2}$$

además presentamos la instrucción `MR` la cual permite obtener un vector con las μ-reducciones de las componentes p-ádicas de las palabras código.

```
//Mu-Reduccion de componentes para palabras codigo.
>MR:=function(c)
    r0:=<MRPadic(c[i])[1]:i in [1..#c]>;
    r1:=<MRPadic(c[i])[2]:i in [1..#c]>;
    r2:=<MRPadic(c[i])[3]:i in [1..#c]>;
    return <r0,r1,r2>;
end function;
//Funcion de Gray.
>Phi:=function(c)
    GM0:=KP(MR(c)[1],c0);
    GM1:=KP(MR(c)[2],c1);
    GM2:=KP(MR(c)[3],c2);
    A:=[GM0[i]:i in [1..#GM0]];
    B:=[GM1[i]:i in [1..#GM1]];
    C:=[GM2[i]:i in [1..#GM2]];
    return [A[i]+B[i]+C[i]:i in [1..#A]];
end function;
```

B.3 CÓDIGOS EN MAGMA

El manual dedica el capítulo 21 a la teoría de códigos definidos sobre campos finitos, al darles un tratamiento como vectores, sin embargo para códigos definidos sobre anillos de Galois, deben ser operados como elementos de un módulo, y para ello se diseñaron programas para crear y manipular dichos códigos los cuales se exhiben a continuación.

B.3.1 Códigos constacíclicos

Como ya se mencionó en la sección 3.1 dado un entero positivo n primo relativo con p para un anillo de Galois $R = GR(p^s, m)$, la imágen bajo la función de Gray de un código constacíclico es cuasi-cíclica de índice p^{2m-1} y longitud nq^2 con $q = p^m$.

El siguiente programa nos permite que, dados un anillo de Galois $GR(p^s, m)$, un entero positivo n tal que $(n, p) = 1$ y un conjunto de n-adas $\{\underline{c}_1, \underline{c}_2, \ldots, \underline{c}_k\} \subseteq R^n$, generar un código constacíclico, como sigue:

```
>l:=(1-p^2) mod (p^s);//Unidad l=1-p^2.
>Nul:=function(x)
    C:=[x];
    n:=#C[1];
    while ([l*x[n]] cat [x[i]: i in [1..n-1]]) ne C[1] do
        x:=[l*x[n]] cat [x[i]: i in [1..n-1]];
        Include(~C,x);
    end while;
    return C;
end function;//Funcion corrimiento constaciclico.
>ConsC:=function(G)
    CC:=[];
    for i:=1 to #G do
        y:=Nul(G[i]);
        Include(~CC,y);
    end for;
    return &cat CC;
end function;Generador de codigos constaciclicos.
//Ingrese una cantidad finita de n-adas de elementos de R^n.
>Cod:=ConsC([[1,w,7*w,0,1],[w^2,1,w,2*w+2,3]]);
    C:=[];
for c in Cod do
    d:=<c[i]: i in [1..#c]>;
    Include(~C,d);
end for;
```

```
"Codigo constaciclico";
>"C =",C;
```

```
Codigo constaciclico
C = [ <1, w, 7*w>, <3*w, 1, w>, <5*w, 3*w, 1>, <5, 5*w, 3*w>, <7*
    w, 5, 5*w>, <w, 7*w, 5> ]
```

Una vez que se ha construido el código constacíclico C de longitud n, podemos utilizar la instrucción `for` que genera un ciclo simple para calcular la imágen bajo la función de Gray de todas las palabras código de C:

```
>PHI:=function(C);//Ciclo de c\'alculo de la imagen bajo la
    funcion de Gray
    D:=[];
    for c in C do
        d:=Phi(c);
        Include(~D,d);
    end for;
    return D;
end function;
>PHI(C);//Imagen de Gray del codigo C.
```

Ahora, para la verificación del Teorema 3.1.4 definimos en MAGMA las funciones σ y $\sigma^{\otimes p^{2m-1}}$

```
//Corrimiento Ciclico.
>Sigma:=function(x)
    return [x[#x]]cat [x[i]: i in [1..(#x-1)]];
end function;
//Corrimiento cuasi-ciclico
>SigmaT:=function(c)
    SC:=[];
    n:=#c div (p^(2*m));
    k:=n*p;
    j:=0;
    while j lt (p^(2*m-1)) do
        if j eq 0 then
            b:=Sigma([c[i+1]: i in [0..(k-1)]]);
            Append(~SC,b);
        else
            b:=Sigma([c[i]: i in [((j*k)+1)..(j+1)*(k)]]);
            Append(~SC,b);
        end if;
    j+:=1;
    end while;
    return &cat SC;
```

```
end function;
```

Finalmente un ciclo simple nos permite la verificación del teorema definiendo la instrucción condicional `IsCuasiCyclic` la cual nos devolverá `true` si el código en cuestión es cuasi-cíclico y `false` de lo contrario.

```
>IsCuasiCyclic:=function(x)
    for c in x do
        t:=SigmaT(c) in x;
        if t eq false then
            a:="false";
            break;
        else
            a:="true";
        end if;
    end for;
    return a;
end function;
```

B.3.2 Códigos cíclicos lineales

Para la sección 3.2, se introdujo una permutación particular para los elementos del conjunto de enteros $\{0, 1, \ldots, np-1\}$ donde $(n, p) = 1$ y la cual es denotada por π, es necesario hallar el inverso módulo p, n' de n, todo esto se hace a continuación:

```
//Introduzca un entero n coprimo con p
>n:=3;
//Calculo del inverso 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;
>"n'=",q;
"Permutacion Pi en el conjunto {0,1,...,",n*p-1,"}";
Pi:=function(x)
    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;
```

```
for x in [0..n*p-1] do
    x,"--->",Pi(x);
end for;
"Parametros de la permutacion"
>"p =",p;
>"n =",n;
>"n' =",q;
for x in [0..n*p-1] do
x,"--->",Pi(x);
end for;
```

```
Parametros de la permutacion
p = 2
n = 3
n'= 1
Permutacion Pi en el conjunto {0,1,..., 5}
0 ---> 0
1 ---> 4
2 ---> 2
3 ---> 3
4 ---> 1
5 ---> 5
```

Observación B.3.1. Para determinar el valor de p, es necesario iniciar cada programa con el encabezado proporcionado en la subsección B.2.1 por lo cual el anillo de Galois sobre el que definimos el código se encuentra determinado.

Además la generación de los elementos λ y γ está proporcionada por las siguientes instrucciones:

```
>t:=p^(2*m-1);//indice del codigo
>l:=1-p^2 mod p;
>"Unidades en el anillo de Galois"
>"lambda =",l;//parametro lambda

for k in T do
y:= k mod p;
    if y eq q then
    N:=y;
end if;
end for;//Factor del conjunto de Teichmuller para Gamma.
>g:=1+N*p^2;
>"gamma =",g;//parametro gamma
```

```
Unidades en el anillo de Galois
lambda= 1
gamma= 5
```

Con estos elementos, podemos definir la generalización de la permutación de Nechaev $\Pi^{\otimes p^{2m-1}}$ utilizando el lenguaje de MAGMA mediante:

```
//Pi Tensor p^(2m-1).
PI:=function(x)
    z:=(#x) div (n*p);
    PIC:=[];
    for k:=0 to (z-1) do
        if k eq 0 then
            y:=[x[Pi(i)+1]: i in [k*(n*p)..(k+1)*(n*p)-1]];
            Append(~PIC,y);
        else
            y:=[x[(k*(n*p)+1)+Pi(i mod (n*p))]: i in [k*(n*p)..(k
                +1)*(n*p)-1]];
            Append(~PIC,y);
        end if;
    end for;
    //Y:=[PIC[i]: i in [1..#PIC]];
    //Z:=[Tuplist(Y[i]): i in [1..z]];
    return &cat PIC;
end function;
```

MAGMA contiene la instrucción `LinearCode` la cual permite la construcción de un código lineal generado por las filas de una matriz, si estas filas poseen un comportamiento cíclico se genera un código cíclico lineal como en los siguientes ejemplos:

Ejemplo B.3.2. (i) El código de repetición de longitud 3 sobre $GR(2,3,2)$.

```
>L:=LinearCode(Matrix(R,1,3[1,1,1]));
>L;
>LL:=[*Eltseq(c): c in L*];
>C:=[<LL[i][j]: j in [1..#LL[i]]>: i in [1..#LL]];
```

```
(3, 64, 3) Cyclic Linear Code over GaloisRing(2, 3, x^2 + x
    + 1)
Generator matrix:
[1 1 1]
```

(ii) El código cíclico lineal de longitud 3 generado por los vectores $\{(2,0,0),(0,2,0),(0,0,2)\}$.

```
>L:=LinearCode(Matrix(R,3,3[[2,0,0],[0,2,0],[0,0,2]]));
>L;
>LL:=[*Eltseq(c): c in L*];
>C:=[<LL[i][j]: j in [1..#LL[i]]>: i in [1..#LL]];
```

```
(3, 4096, 1) Cyclic Linear Code over GaloisRing(2, 3, x^2 +
    x + 1)
Generator matrix:
[2 0 0]
[0 2 0]
[0 0 2]
```

Podemos verificar el Teorema 3.2.10 usando las instrucciones de la subsección anterior para calcular la imagen de Gray y verificar la cuasiciclicidad.

BIBLIOGRAFÍA

[1] Blackford J. T. and Ling S., "$\mathbb{Z}_{p^{k+1}}$-linear codes". IEEE Trans. Inform. Theory. **48**. 2592–2605 pp. (2002).

[2] Calderbank A. R., Hammons Jr. A. R., Kumar P. V., Sloane J. A. and Solé P. "The $\mathbb{Z}$_4-linearity of kerdock, preparata, goethals, and related codes". IEEE Trans. Inform. Theory. **40**. 301–319 pp. (1994).

[3] García Ramírez, A. R. "Anillos de Galois". Tesis de Licenciatura, Benemérita Universidad Autónoma de Puebla, (2017).

[4] Greferath M. and Schmidt, S. E. "Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code". IEEE Trans. Inform. Theory. **45**. 2522–2524 pp.(1999).

[5] Helleseth T., Kummar P. V. and Shanbhag A. G., "An Upper Bound for the Extended Kloosterman Sums over Galois Rings". Finite Fields and Their Applications. 218-238 pp. (1989).

[6] Honold T. and Nechaev A. A., "Weighted Modules and Representations of Codes". Problems of Information Transmission **35**. 205–223pp. (1999).

[7] Jacobson N., "Basic Algebra, Vol. 2".W. H. Freeman and Company. ISBN: 978-0486471877. (1910).

[8] Jitman S. and Udomkavanich P., "The Gray Image of Codes Over Finite Chain Rings", Int. J. Contemp. Math. Sciences. **5**. 449-458 pp. (2010).

[9] Kanwar P. and López-Permouth S. R. , "Cyclic codes over the integers modulo p^m", Finite Fields and Their Applications. **3**. 334–352 pp. (1997).

[10] Karpilovsky G., "Topics in Field Theory". Elsevier Science Publishers. ISBN: 9780444872975 .(1989).

[11] Lidl R. and Niederreiter H., "Introduction to finite fields and their applications". Cambridge University Press. ISBN: 978-0521460941. (1994).

[12] López-Andrade C. A., "Códigos de Hamming". En F. Macías Romero (Ed.), *Matemáticas y sus aplicaciones 4* (1a ed., Cap. 1, pp. 5-33, ISBN: 978-607-487-791-5). Textos Científicos, Fomento Editorial de la Benemérita Universidad Autónoma de Puebla, México. (2014).

[13] López-Andrade C.A., "Imágenes de Gray sobre anillos de Galois" Tesis de Doctorado. Universidad Autónoma Metropolitana. (2013).

[14] López Andrade C.A. and Tapia Recillas H., " On the linearity and quasi-cyclicity of the gray image of codes over a galois ring". Groups, Algebras and Applications, vol. CONM/537, AMS. 255–268 pp. (2011).

[15] Mac Williams F. J. and Sloane N. J., " The theory of error-correcting codes". North-Holland.ISBN: 9780444851932. (1977).

[16] Nechaev A.A., "Kerdock codes in a cyclic form". Discr. Math. Appl. **1**. 365-384 pp. (1991).

[17] Roman S., "Coding and information theory".Springer-Verlag. ISBN: 9780387978123. (1992).

[18] Wan Z. X., " Quaternary Codes". World Scientific Pub. Co. Inc. ISBN: 9789810232740. (2003).

[19] Wan Z. X., "Lectures on finite fields and Galois rings". World Scientific Pub. Co. Inc. ISBN: 9789812385703.(2003).

[20] Wolfmann J., " Binary images of cyclic codes over $\mathbb{Z}_4$". IEEE, Trans. Inform. Theory. **47**. 1773-1779 pp. (2001).

ÍNDICE ALFABÉTICO

$[n, k, d]$-código lineal, 7
$[n, k]$-código lineal, 6

alfabeto, 6
anillo de Galois, 4
anillo de vectores de Witt, 18
anillo finito de cadena, 4
anillo local, 4
anillo truncado de vectores de Witt, 23
automorfismo de Frobenius, 3
automorfismo generalizado de Frobenuis, 6

código, 6
código γ-cíclico, 63
código cíclico, 6
código constacíclico, 53
código cuasi-cíclico, 7
código cuaternario, 9
código cuaternario lineal, 9
código de repetición binario, 8
código lineal, 6
campo, 1
campo finito, 1
campo primo, 1
campo residual, 4
componentes p-ádicas, 5
conjunto de Teichmüller, 5
corrimiento cíclico, 6
corrimiento causi-cíclico, 7
corrimiento constacíclico, 53

distancia de Hamming, 7
distancia de Lee, 9
distancia homogénea, 12
distancia mínima de Hamming, 7

elemento primitivo, 2
extensión de un campo, 1

función de Gray, 37

grado de una extensión, 2
grupo de Galois, 3

homomorfismo canónico, 3

imagen binaria, 40
intersección de palabras código, 7

matriz de chequeo de paridad, 8
mu-reducción, 3

palabra código, 6
permutación de Nechaev, 64
peso de Hamming, 7
peso de Lee, 9
peso homogéneo, 12
polinomio mínimo, 2
polinomio mónico básico irreducible, 3
polinomio mónico básico primitivo, 3
polinomio primitivo, 2
producto de Kronecker, 42
  de derecha a izquierda, 42
  de izquierda a derecha, 42

raíz p-ésima, 77
representación aditiva, 5
representaciones polinomiales, 59

símbolos, 6
subcampo, 1
subcampo primo, 1

ÍNDICE DE FIGURAS

Figura 1 Peso de Lee en $\mathbb{Z}_4$. 10
Figura 2 Tabla de Cayley $(\mathbb{Z}_4, +)$ 26
Figura 3 Tabla de Cayley $(\mathbb{Z}_4, \cdot)$ 26
Figura 4 Tabla de Cayley para $(W_2(\mathbb{F}_2), +)$ 27
Figura 5 Tabla de Cayley para $(W_2(\mathbb{F}_2), \cdot)$ 27
Figura 6 Comparación de w_L y $w_H \circ \psi$ 37
Figura 7 Comparación entre d_L y $d_H \circ \psi$ 38
Figura 8 Imágenes de α, β, γ sobre $\mathbb{Z}_4$ 39

ÍNDICE DE CUADROS

Cuadro 1 Permutación π en $\{0, 1, 2, 3, 4, 5\}$. 64
Cuadro 2 Permutación π en $\{0, 1, \ldots, 13, 14\}$. 65
Cuadro 3 Raíces cuadradadas en $\mathbb{F}_2^2$ 77
Cuadro 4 Raíces cuadradadas en $\mathbb{F}_2^3$ 78
Cuadro 5 Raíces cúbicas en $\mathbb{F}_3^2$ 78