CÓDIGOS γ-CONSTACÍCLICOS Y SUS DUALES SOBRE ANILLOS LOCALES FINITOS DE FROBENIUS NO DE CADENA Y CUYO IDEAL MAXIMAL TIENE ÍNDICE DE NILPOTENCIA 3

TESIS QUE PRESENTA

M. en C. Carlos Alberto Castillo Guillén

para obtener el grado de
Doctor en Ciencias (Matemáticas)

Asesores de tesis:
Dr. Horacio Tapia Recillas
Dr. Carlos Rentería Márquez

Sinodales
Dr. Carlos Rentería Márquez
Dr. Guillermo Benito Morales Luna
Dr. Felipe de Jesús Zaldívar Cruz
Dr. Rogelio Fernández Alonso González
Dr. José Noé Gutiérrez Herrera

Ciudad de México
30 de Octubre de 2019
Salón EP 101

Índice general

Agradecimientos

Deseo expresar mi agradecimiento a:

Mis padres, hermanos y amigos.

A los Doctores: Horacio Tapia Recillas, Carlos Rentería Márquez, Felipe Zaldívar Cruz, José Noé Gutiérrez Herrera, Guillermo Benito Morales Luna y Rogelio Fernández Alonso González por sus valiosas aportaciones en la revisión de este trabajo.

Al Departamento de Matemáticas de la Universidad Autónoma Metropolitana, Unidad Iztapalapa, por brindarme todo lo necesario durante mis estudios de Doctorado.

Al CONACYT, por la beca número 104564, otorgada para poder realizar mis estudios de Doctorado.

Resumen

En este trabajo se encuentran todos los anillos locales finitos de Frobenius no de cadena de longitud 4, como consecuencia se determinan todos los anillos locales de Frobenius, no de cadena y con p^4 elementos, p un número primo. También se determina la estructura de los códigos γ-constacíclicos y sus duales sobre anillos locales finitos de Frobenius no de cadena y cuyo ideal maximal tiene índice de nilpotencia 3, donde la longitud del código no es divisible por la característica del campo residual del anillo. La descripción de tales códigos sobre dichos anillos requiere de dos cosas: 1) la factorización del polinomio $\mathrm{T}^n - \gamma$ como producto de polinomios básicos irreducibles. 2) conocer algunas matrices en forma escalón reducida sobre ciertos campos finitos.

Introducción

Los códigos correctores de errores surgieron originalmente como respuesta a cuestiones transmisión fiable de datos codificados digitalmente. El artículo de Claude Shannon, A Mathematical Theory of Communication [26], inició la rama de la llamada teoría de códigos correctores de errores. Desde entonces la codificación algebraica ha tenido conexiones con Algebra y Combinatoria. La transmisión de información a través de teléfono celular, televisión digital, satélites no sería posible sin el desarrollo de los códigos detectores-correctores de errores.

Dado el anillo A, un código cíclico es un código invariante bajo la permutación cíclica $\sigma : \mathrm{A}^n \longrightarrow \mathrm{A}^n$ dada por $\sigma(a_0, a_1, \ldots, a_{n-1}) = (a_{n-1}, a_0, \ldots, a_{n-2})$. Muchos códigos importantes, como los códigos de Golay, los códigos de Hamming y los BCH se pueden representar como códigos cíclicos. En [12] se hace la descripción de los códigos binarios de Kerdock y de Preparata usando códigos cíclicos lineales y la función de Gray sobre el anillo de enteros módulo 4. Esto motiva el estudio de la estructura de códigos cíclicos lineales sobre anillos finitos y los códigos binarios obtenidos con funciones de Gray de tales códigos, donde una función de Gray sobre el anillo A con valores en el anillo B es una función biyectiva $\phi : \mathrm{A}^n \to \mathrm{B}^m$ que cumple $\phi(\mathrm{C}^\perp) = \phi(\mathrm{C})^\perp$, para todo código lineal C y $()^\perp$ denota el código dual con respecto al producto interno canónico en el anillo respectivo. Una generalización natural de los códigos cíclicos son los códigos γ-constacíclicos, estos son los códigos invariantes bajo la permutación γ-constacíclica $\sigma_\gamma : \mathrm{A}^n \longrightarrow \mathrm{A}^n$ dada por $\sigma_\gamma(a_0, a_1, \ldots, a_{n-1}) = (\gamma a_{n-1}, a_0, \ldots, a_{n-2})$, donde γ es una unidad del anillo A.

Se ha descrito la estructura de códigos γ-constacíclicos lineales sobre algunos anillos finitos, [2], [6], [9], [7], [14], [27], [29], y se han estudiado distintas funciones de Gray sobre diversos anillos, [11], [15], [10], [28] [30]. Lo común de estos trabajos es que los anillos considerados son anillos finitos de cadena, es decir anillos finitos ta-

les que su retícula de ideales es una cadena bajo la inclusión de conjuntos, y anillos locales finitos de Frobenius, es decir anillos locales finitos que tienen un único ideal minimal. Notar que los anillos finitos de cadena son parte de los anillos locales finitos de Frobenius.

La razón por la que los anillos finitos considerados en los trabajos de códigos lineales son anillos finitos de Frobenius, es porque en estos anillos se satisfacen las relaciones de Macwilliams y las relaciones $(\mathrm{C}^{\perp})^{\perp} = \mathrm{C}$, $|\mathrm{C}||\mathrm{C}^{\perp}| = |\mathrm{A}|^n$, donde C es un código lineal de longitud n sobre el alfabeto A. El estudio de códigos lineales sobre anillos finitos de Frobenius se reduce al estudio de códigos lineales sobre anillos locales finitos de Frobenius, pues: (1) los códigos lineales sobre una suma directa de anillos son suma directa de códigos lineales sobre los anillos de la suma directa, (2) todo anillo finito se puede descomponer en suma directa de anillos locales finitos, (ver [19]), y (3) si el anillo finito es de Frobenius entonces los anillos locales en los que se descompone también son de Frobenius.

La estructura de códigos cíclicos sobre $\mathbb{Z}_4$, de longitud impar, se hizo en [30]. Una generalización natural del estudio de códigos cíclicos sobre $\mathbb{Z}_4$ se hace en [2] y [6], donde se describe la estructura de los códigos cíclicos sobre el anillo de enteros módulo p^k, cuando la longitud del código no es divisible por p, p es un número primo y $k \geq 1$ un entero. Una generalización a lo anterior se hizo en [7], aquí se describe la estructura de códigos cíclicos y negacíclicos sobre anillos finitos de cadena, donde la longitud del código no es divisible por la característica del campo residual del anillo. El siguiente paso fue estudiar la estructura de códigos constacíclicos sobre algunos anillos locales finitos de Frobenius que no son de cadena. Por ejemplo, en [14] se describe una forma de los generadores de códigos cíclicos lineales sobre el anillo $\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$ y se define la función de Gray $\phi : \left[\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle\right]^n \to \mathbb{F}_2^{4n}$, dada por $\vec{a} + \vec{b}\mathrm{x} + \vec{c}\mathrm{y} + \vec{d}\mathrm{xy} \mapsto (\vec{a} + \vec{b} + \vec{c} + \vec{d}, \vec{c} + \vec{d}, \vec{b} + \vec{d}, \vec{d})$, donde $\vec{a}, \vec{b}, \vec{c}, \vec{d} \in \mathbb{F}_2^n$. Es importante mencionar que esta descripción no es útil, pues no se describe un método que permita conocer los códigos cíclicos, y que ningún otro trabajo ha usado esta descripción para obtener propiedades de tales códigos. En [21] las siguientes funciones de Gray fueron presentadas $\phi : \left[\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2 + \mathrm{Y}^2, \mathrm{XY}\rangle\right]^n \to \mathbb{F}_2^{4n}$ dada por $\vec{a}+\vec{b}\mathrm{x}+\vec{c}\mathrm{y}+\vec{d}\mathrm{x}^2 \mapsto (\vec{a}+\vec{d}, \vec{b}, \vec{c}, \vec{d})$, donde $\vec{a}, \vec{b}, \vec{c}, \vec{d} \in \mathbb{F}_2^n$, y $\phi : \left[\mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2+2\mathrm{X}\rangle\right]^n \to \mathbb{Z}_4^{2n}$ dada por $\vec{a}+\vec{b}\mathrm{x} \mapsto (\vec{a}+\vec{b}, \vec{b})$, donde $\vec{a}, \vec{b} \in \mathbb{Z}_4^n$. En estos tres casos las funciones de Gray son lineales, y los anillos considerados son locales de Frobenius, no son de cadena y

tienen 16 elementos.

Por otra parte, si p es un número primo, es sabido que salvo isomorfismo existe solo un anillo local con p elementos, tal anillo es el campo finito $\mathbb{F}_p$.
Los anillos locales con p^2 elementos son: 2) $\mathbb{F}_{p^2}$, 3) $\mathbb{Z}_{p^2}$ y 4) $\mathbb{F}_p[\mathrm{X}]/\langle \mathrm{X}^2\rangle$.
Si p es impar, los anillos locales de p^3 elementos son: 5) $\mathbb{F}_{p^3}$, 6) $\mathbb{Z}_{p^3}$, 7) $\mathbb{F}_p[\mathrm{X}]/\langle \mathrm{X}^3\rangle$, 8) $\mathbb{Z}_{p^2}[\mathrm{X}]/\langle \mathrm{X}^2-p, p\mathrm{X}\rangle$, 9) $\mathbb{Z}_{p^2}[\mathrm{X}]/\langle \mathrm{X}^2-\zeta p, p\mathrm{X}\rangle$, $\tilde{\zeta}$ es un elemento primitivo del campo $\mathbb{F}_p$, 10) $\mathbb{F}_p[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X},\mathrm{Y}\rangle^2$ y 11) $\mathbb{Z}_{p^2}[\mathrm{X}]/\langle \mathrm{X}^2, p\mathrm{X}\rangle$.
Si $p=2$, los únicos seis anillos locales con 2^3 elementos son: 12) $\mathbb{F}_{2^3}$, 13) $\mathbb{Z}_{2^3}$, 14) $\mathbb{F}_2[\mathrm{X}]/\langle \mathrm{X}^3\rangle$, 15) $\mathbb{Z}_{2^2}[\mathrm{X}]/\langle \mathrm{X}^2-2, 2\mathrm{X}\rangle$, 16) $\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X},\mathrm{Y}\rangle^2$ y 17) $\mathbb{Z}_{2^2}[\mathrm{X}]/\langle \mathrm{X}^2, 2\mathrm{X}\rangle$, (ver [20], Ejercicio XIX.9, página 384).
Es fácil verificar que los anillos 10), 11), 16) and 17) no son anillos locales de Frobenius, esto pues el anulador de su ideal maximal no es un ideal simple, y los otros anillos son de cadena.
Así, los anillos locales finitos de Frobenius que no son de cadena deben buscarse en los anillos locales de p^d elementos, con p un número primo y $d \geq 4$.
Recientemente los anillos locales de Frobenius que no son de cadena con 2^4 elementos fueron determinados en ([21]) y son: $\mathbb{Z}_4[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y}\rangle$, $\mathbb{Z}_4[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY}-2, 2\mathrm{X}, 2\mathrm{Y}\rangle$, $\mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2\rangle$, $\mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2-2\mathrm{X}\rangle$, $\mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2-4, 2\mathrm{X}\rangle$, $\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$, $\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$. Ahora si p es un número primo sería interesante determinar los anillos locales de Frobenius que no son de cadena con p^4 elementos y también determinar la estructura de los códigos constacíclicos sobre esos anillos.

Se denota a la familia de anillos locales finitos de Frobenius no de cadena y cuyo ideal maximal tiene índice de nilpotencia 3 por $\mathfrak{F}_3$ y a la familia de anillos locales finitos de Frobenius no de cadena de longitud 4 por $\mathfrak{L}_4$. La relación $|\mathrm{M}| = |\mathbb{F}_{p^d}|^{\ell_{\mathrm{A}}(\mathrm{M})}$, (ver Lema 1.3.4), donde M es un A-módulo sobre un anillo local finito A con campo residual $\mathbb{F}_{p^d}$ y $\ell_{\mathrm{A}}(\mathrm{M})$ es la longitud de M, y el hecho de que todo anillo de longitud uno ó dos es un anillo de cadena, (ver Lema 2.2.1), implican que si A es un anillo local finito de Frobenius no de cadena y con p^4 elementos, entonces $\mathrm{A} \in \mathfrak{L}_4$. En este trabajo se determinan todos los anillos de la familia $\mathfrak{L}_4$.
Para un anillo local A con ideal maximal $\mathfrak{m}$, el índice de nilpotencia de $\mathfrak{m}$ es el menor entero t para el cual se cumple $\mathfrak{m}^t = \langle 0\rangle$. Las relaciones (1) : $\ell_{\mathrm{A}}(\mathrm{A}) \geq t$, (ver Lema 1.3.6), (2) A es anillo de cadena si y sólo si $t = \ell_{\mathrm{A}}(\mathrm{A})$, (ver Proposición 2.1.1), (3) si A es un anillo de Frobenius y su ideal maximal tiene índice de nilpotencia uno ó

dos entonces A es anillo de cadena, (ver Lema 2.2.1), implican que si A es un anillo en la familia $\mathfrak{L}_4$ entonces el anillo pertenece a la familia $\mathfrak{F}_3$. En el Ejemplo 2.1.1 se verificará que los siguientes anillos pertenecen a la familia $\mathfrak{F}_3$

$$\mathrm{A}_{(k,q)} = \mathbb{F}_q[\mathrm{X}_1, \ldots, \mathrm{X}_k]/\langle \mathrm{X}_i\mathrm{X}_j - \mathrm{X}_1\mathrm{X}_2, \mathrm{X}_1^2, \ldots, \mathrm{X}_k^2 : (i,j), 1 \leq i < j \leq k, (i,j) \neq (1,2)\rangle,$$

donde $k \geq 3$ es un entero tal que $(k-1, q) = 1$. También se verificará que la longitud de los anillos $\mathrm{A}_{(k,q)}$ es $k+2$, así la familia $\mathfrak{F}_3$ tiene anillos de todas las longitudes.

Este trabajo tiene tres propósitos. El primero es determinar todos los anillos finitos de Frobenius que no son de cadena y de longitud 4. Este resultado generaliza el caso $p = 2$ presentado en [21] y se desarrolla en el Capítulo 2. El segundo propósito es describir los códigos γ-constacíclicos sobre anillos de la familia $\mathfrak{F}_3$, donde la longitud del código no es divisible por la característica del campo residual del anillo, lo cual se desarrolla en el Capítulo 3. El tercer propósito es la descripción de los códigos duales de los códigos γ-constacíclicos sobre anillos de la familia $\mathfrak{L}_4$, cuando la longitud del código no es divisible por la característica del campo residual del anillo. Esto se hace en el capítulo 4 y una consecuencia de este resultado es dar la caracterización de los códigos γ-constacíclicos autoduales, sobre el tipo de anillos mencionado y con la longitud mencionada.

De esta manera dado el anillo $\mathrm{A} \in \mathfrak{F}_3$, para la descripción de los códigos γ-constacíclicos sobre el anillo A, donde la longitud del código no es divisible por la característica del campo residual de A, solo se requerirán dos cosas: 1) la factorización del polinomio $\mathrm{T}^n - \gamma$ como producto de polinomios básicos irreducibles, lo cual se hace primero factorizando el polinomio $\mathrm{T}^n - \tilde{\gamma}$ sobre el campo residual del anillo A y después usando el Lema de Hensel, Lema 1.3.5, y 2) conocer algunas matrices en forma escalón reducida por filas sobre algunos campos finitos.

La distribución de esta tesis es la siguiente: En el Capítulo 1 se dan conceptos y definiciones que son fundamentales para el desarrollo de los tópicos aquí trabajados. En la Sección 1.1 se dan definiciones y resultados básicos de Algebra Conmutativa, por ejemplo acerca de ideales simples y principales, el Teorema de Correspondencia, la longitud de un módulo, la expansión de ideales en una extensión de anillos, el Teorema Chino del Residuo. En la Sección 1.2 se recuerda el cambio de anillo para un módulo y se define el coeficiente binomial Gaussiano, el cual es el número de subespacios de dimensión k de un espacio vectorial de dimensión n sobre un campo finito, con $k \leq n$.

En la Sección 1.3 se estudian propiedades generales de anillos locales finitos, por ejemplo se enuncia el Lema de Nakayama, se define conjunto mínimo de generadores de un módulo sobre un anillo local, se estudian relaciones entre el índice de nilpotencia del ideal maximal y la longitud del anillo local, relaciones entre el cardinal de módulos sobre un anillo local y su longitud. Se describen propiedades de las extensiones no ramificadas de un anillo local, estas extensiones son muy importantes pues el estudio de códigos γ-constacíclicos, sobre un anillo local, se reduce al estudio de los ideales de las extensiones no ramificadas del anillo local. Se presenta el Lema de Hensel, el cual es un método con el cual se puede obtener la factorización de ciertos polinomios en un anillo local a partir de la factorización del polinomio reducido al campo residual, este resultado es usado para reducir los códigos γ-constacíclicos, sobre un anillo local, a los ideales de ciertas extensiones no ramificadas del anillo local.

En el Capítulo 2 se describen los primeros resultados de esta tesis, correspondientes a la caracterización de que un anillo local tenga la propiedad de ser anillo de Frobenius o anillo de cadena a partir de sus extensiones no ramificadas. En la Sección 2.1 se define anillo local de Frobenius y anillo de cadena, se presentan algunas equivalencias y propiedades de este tipo de anillos y se dan resultados que caracterizan la propiedad de ser anillo de Frobenius y anillo de cadena a partir de sus extensiones no ramificadas. En la Sección 2.2 se describen todos los anillos locales de Frobenius no de cadena y de longitud 4. Una consecuencia es que los anillos locales de Frobenius no de cadena con 16 elementos son presentados, de esta manera los resultados obtenidos en [21] son generalizados.

En el Capítulo 3 se describe la estructura de códigos γ-constacíclicos sobre anillos de Frobenius no de cadena cuyo ideal maximal tiene índice de nilpotencia 3. En la Sección 3.1 inicia el análisis de los códigos γ-constacíclicos y se presenta una caracterización de anillo de cadena en términos de sus códigos γ-constacíclicos. En la Sección 3.2 se describe la retícula de ideales de un anillo en la familia $\mathfrak{F}_3$ y con ello se obtiene la caracterización de los códigos γ-constacíclicos sobre ese tipo de anillos, cuando la longitud del código no es divisible por la característica del campo residual del anillo. Algunos ejemplos son incluidos para ilustrar los resultados presentados.

El dual de un código γ-constacíclico sobre un anillo de la familia $\mathfrak{L}_4$, cuando la longitud del código no es divisible por la característica del campo residual del anillo, es determinado en el Capítulo 4. En la Sección 4.1 se determinan las extensiones

no ramificadas de un anillo en la familia $\mathfrak{L}_4$ y se describe el ideal anulador de los ideales de un anillo en la familia $\mathfrak{L}_4$. En la Sección 4.2 se describe el código dual de los códigos mencionados y en la Sección 4.3 se caracteriza a los códigos constacíclicos autoduales. Algunos ejemplos son incluidos para ilustrar los resultados presentados. Finalmente, se dan las conclusiones del trabajo y se comentan líneas de investigación que se desprenden de esta tesis.

Capítulo 1

Anillos y anillos locales

El estudio de códigos γ-constacíclicos sobre un anillo local finito, donde la longitud del código es prima relativa con la característica del campo residual del anillo, se reduce a estudiar la retícula de ideales de las extensiones no ramificadas del anillo local (ver la Proposición 3.1.1 y el Lema 3.1.1). Por ello en este capítulo presentamos resultados generales de Algebra Conmutativa que servirán para describir una parte de la retícula de ideales de las extensiones no ramificadas de un anillo local a partir de las propiedades del anillo local. Las principales referencias son [19], [20], [25] y [32]. Siempre se supondrá que los anillos considerados en este trabajo son conmutativos, finitos y con identidad, también que los módulos son finitamente generados. A^* denotará las unidades del anillo A.

1.1. Preliminares

En esta sección se presenta una caracterización para módulos simples, tal concepto será utilizado en el resto de este trabajo, por ejemplo, los módulos simples son un concepto necesario para el estudio de la longitud de los módulos, anillos que en este trabajo son estudiados están caracterizados por el hecho de tener un único ideal minimal que resulta ser simple. Se define el concepto de longitud de módulos ([20]), la cual es una generalización del concepto de dimensión para espacios vectoriales, así las propiedades de la longitud de módulos son semejantes a las propiedades de la dimensión en espacios vectoriales. Se define el concepto de expansión de ideales en una extensión de anillos, tal concepto resulta útil para estudiar la retícula de ideales

de un anillo a partir de la retícula de ideales de un subanillo. Se presenta el Teorema Chino del Residuo y un resultado que describe los ideales de un producto cartesiano de anillos, tales resultados son de importancia pues el primero se usa para descomponer un anillo en suma directa de anillos, esto cuando el anillo contiene ideales coprimos a pares, y el segundo se usa para conocer la retícula de ideales de una suma directa de anillos.

DEFINICIÓN 1.1.1 *Sea* A *un anillo y* M *un* A*-módulo.*

(*1*) *Se dice que* M *es simple si* M *no es cero y sus únicos* A*-submódulos son los triviales.*

(*2*) *Se dice que* M *es principal si existe* $m \in \mathrm{M}$ *tal que* $\mathrm{M} = \langle m \rangle = \{am : a \in \mathrm{A}\}$.

(*3*) *Se dice que* M *es libre si es isomorfo a una suma directa (finita) de copias de* A.

(*4*) $\mathrm{ann_A(M)} := \{a \in \mathrm{A} : am = 0, \forall\ m \in \mathrm{M}\ \}$, *es llamado el ideal anulador de* M.

(*5*) *La familia de* A*-submódulos de* M *es denotada por* $\mathcal{L}_\mathrm{A}(\mathrm{M})$. $\mathcal{L}_\mathrm{A}(\mathrm{A})$ *será denotado simplemente por* $\mathcal{L}(\mathrm{A})$, *el cual es la familia de ideales de* A.

Nótese que $\mathcal{L}_\mathrm{A}(\mathrm{M})$ con la inclusión de conjuntos es un conjunto parcialmente ordenado.

El siguiente resultado es el conocido Teorema de Correspondencia, su demostración se puede encontrar por ejemplo en [1].

TEOREMA 1.1.1 *Sean* M *y* N A*-módulos y* $\psi : \mathrm{N} \to \mathrm{M}$ *un epimorfismo de* A*-módulos. Sea* $\mathcal{J} = \{\mathrm{N}_1 \in \mathcal{L}_\mathrm{A}(\mathrm{N}) : \ker(\psi) \subseteq \mathrm{N}_1\}$. *Entonces existe una biyección*

$$\psi^* : \mathcal{L}_\mathrm{A}(\mathrm{M}) \longrightarrow \mathcal{J},\ \psi^*(\mathrm{M}_1) = \psi^{-1}(\mathrm{M}_1).$$

La inversa de ψ^* *está dada por* $(\psi^*)^{-1}(\mathrm{N}_1) = \psi(\mathrm{N}_1)$.

LEMA 1.1.1 *Sea* A *un anillo y* M *un* A*-módulo. Entonces:*

(*1*) M *es principal si y sólo si* $\mathrm{M} \cong \mathrm{A/J}$, *donde* J *es un ideal de* A.
Además, si $\mathrm{M} = \langle m \rangle$, *entonces* $\mathrm{J} = \mathrm{ann_A}(m)$.

(*2*) M *es simple si y sólo si* $\mathrm{M} \cong \mathrm{A/J}$*, donde* J *es un ideal maximal de* A.

En particular, si I *es un ideal de* A *que es simple, entonces* I *es un ideal principal.*

Demostración.
(1) $\Rightarrow$) Supongamos que $\mathrm{M} = \langle m \rangle$. Sea $\psi : \mathrm{A} \longrightarrow \mathrm{M}$, dada por $\psi(x) = xm$. Entonces ψ es epimorfismo de A-módulos, $\mathrm{M} \cong \mathrm{A}/\ker\psi$, por el primer teorema de isomorfismos, y $\ker\psi = \mathrm{ann_A}(m)$.
$\Leftarrow$) Supongamos ahora que $\mathrm{M} \cong \mathrm{A/J}$, con J un ideal de A. Puesto que A/J es A-módulo principal, generado por $1 + \mathrm{J}$, se sigue que M es principal.
(2) Se sigue del inciso anterior y del Teorema de correspondencia.

Definición 1.1.2 *Sea* A *un anillo y* M *un* A*-módulo.*

(*1*) *Una* ***cadena*** *de submódulos de* M *es una secuencia de submódulos de* M *de la forma:*

$$\langle 0 \rangle = \mathrm{M}_l \subset \mathrm{M}_{l-1} \subset \ldots \subset \mathrm{M}_1 \subset \mathrm{M}_0 = \mathrm{M}.$$

Decimos que la cadena tiene longitud l*.*

(*2*) *Una cadena de submódulos es llamada* ***serie de composición*** *si cada cociente* $\mathrm{M}_i/\mathrm{M}_{i+1}$ *es un módulo simple, es decir, no hay submódulos entre* M_i *y* M_{i+1} *distintos de* M_i *y* M_{i+1}*.*

El siguiente resultado permite definir la longitud de un módulo, su demostración se puede ver por ejemplo en [20].

Proposición 1.1.1 *Sea* A *un anillo y* M *un* A*-módulo. Si* M *tiene una serie de composición finita de longitud* l*, entonces cualquier cadena de submódulos de* M *tiene longitud menor o igual a* l*.*
Por lo tanto, todas las series de composición de M *tienen la misma longitud.*

Definición 1.1.3 *Sea* A *un anillo y* M *un* A*-módulo. La* ***longitud*** *del módulo* M*,* $\ell_{\mathrm{A}}(\mathrm{M})$*, es la longitud de cualquier serie de composición de* M*.*

Observación 1 *Nótese que si* A *es un campo, entonces* $\ell_{\mathrm{A}}(*) = \dim_{\mathrm{A}}(*)$

El resultado que mencionaremos a continuación no estará acompañado de una demostración, la cual se puede ver por ejemplo en [20].

LEMA 1.1.2 *Sea* A *un anillo y* M *un* A*-módulo, supóngase que* M *tiene una cadena de submódulos* $\langle 0\rangle = \mathrm{M}_l \subseteq \mathrm{M}_{l-1} \subseteq \ldots \subseteq \mathrm{M}_1 \subseteq \mathrm{M}_0 = \mathrm{M}$ *tal que* $\ell_{\mathrm{A}}(\mathrm{M}_i/\mathrm{M}_{i+1})$ *es finita, para* $0 \leq i \leq l-1$. *Entonces* $\ell_{\mathrm{A}}(\mathrm{M})$ *es finita y* $\ell_{\mathrm{A}}(\mathrm{M}) = \sum_{i=0}^{l-1} \ell_{\mathrm{A}}(\mathrm{M}_i/\mathrm{M}_{i+1})$.

DEFINICIÓN 1.1.4 *Sea* A *un anillo y* X *un subconjunto no vacio de* A. XA *denota el ideal de* A *generado por* X, *es decir,*

$$\mathrm{XA} = \{ \sum_{finita} a_i x_i : \ a_i \in \mathrm{A}, x_i \in \mathrm{X}\}.$$

DEFINICIÓN 1.1.5 *Sean* A, B *anillos,* $\psi : \mathrm{A} \to \mathrm{B}$ *un homomorfismo de anillos,* I *un ideal de* A *y* J *un ideal de* B.

(*1*) *El ideal de* A, $\psi^{-1}(\mathrm{J})$, *es llamado la restricción de* J *en* A *y es denotada por* $\mathrm{J} \cap \mathrm{A}$.

(*2*) *El ideal* $\psi(\mathrm{I})\mathrm{B}$ *es llamado la expansión de* I *en* B *y es denotado por* IB.

La notación proviene del hecho de que si A es un subanillo de B y $j : \mathrm{A} \to \mathrm{B}$ es la inclusión, entonces $j^{-1}(\mathrm{J}) = \mathrm{J} \cap \mathrm{A}$ y $j(\mathrm{I})\mathrm{B} = \mathrm{IB}$.

DEFINICIÓN 1.1.6 *Sea* A *un anillo e* I *y* J *ideales de* A.

(*1*) *El ideal* IJ, *llamado el producto del ideal* I *con* J, *está dado por*

$$\mathrm{IJ} = \{ \sum_{finita} u_i v_i : u_i \in \mathrm{I}, v_i \in \mathrm{J}\}.$$

(*2*) *Se dice que* I *y* J *son ideales coprimos si* $\mathrm{I} + \mathrm{J} = \mathrm{A}$.

El siguiente resultado es inmediato de las definiciones.

LEMA 1.1.3 *Sean* A, B *anillos,* $\psi : \mathrm{A} \to \mathrm{B}$ *un homomorfismo de anillos,* I, J *ideales de* A, *entonces:*

(*1*) *Si* $\mathrm{I} \subseteq \mathrm{J}$, *entonces* $\mathrm{IB} \subseteq \mathrm{JB}$.

(*2*) $(\mathrm{IJ})\mathrm{B} = (\mathrm{IB})(\mathrm{JB})$.

En particular, $\mathrm{I}^k\mathrm{B} = (\mathrm{IB})^k$.

Presentamos el Teorema Chino del Residuo y un resultado sobre los ideales de un producto cartesiano de anillos. El uso que se dará a estos resultados es la descomposición de ciertos anillos cociente para simplificar el estudio de ideales.

Los resultados que mencionaremos a continuación no estarán acompañados de una demostración, las cuales se pueden encontrar por ejemplo en [32].

LEMA 1.1.4 *Sean* A *un anillo e* $\mathrm{I}_1, \mathrm{I}_2, \ldots, \mathrm{I}_n$ *ideales de* A. *Entonces* $\mathrm{I}_1, \mathrm{I}_2, \ldots, \mathrm{I}_n$ *son ideales coprimos a pares si y sólo si* $\mathrm{I}_1\mathrm{I}_2 \cdots \mathrm{I}_{n-1}$ *e* I_n *son ideales coprimos.*

TEOREMA 1.1.2 (**Teorema Chino del Residuo.**)
Sean A *un anillo e* $\mathrm{I}_1, \ldots, \mathrm{I}_r$ *ideales coprimos a pares. Entonces el mapeo*

$$\begin{array}{rccl} \psi_1 & : & \mathrm{A} & \longrightarrow & \mathrm{A}/\mathrm{I}_1 \oplus \mathrm{A}/\mathrm{I}_2 \oplus \ldots \oplus \mathrm{A}/\mathrm{I}_r \\ & & a & \longmapsto & (a + \mathrm{I}_1, a + \mathrm{I}_2, \ldots, a + \mathrm{I}_r) \end{array}$$

induce el isomorfismo

$$\begin{array}{rccl} \psi & : & \mathrm{A}/\bigcap_{i=1}^{r} \mathrm{I}_i & \longrightarrow & \mathrm{A}/\mathrm{I}_1 \oplus \mathrm{A}/\mathrm{I}_2 \oplus \ldots \oplus \mathrm{A}/\mathrm{I}_r \\ & & a + \bigcap_{i=1}^{r} \mathrm{I}_i & \longmapsto & (a + \mathrm{I}_1, a + \mathrm{I}_2, \ldots, a + \mathrm{I}_r). \end{array}$$

PROPOSICIÓN 1.1.2 *Sean* $\mathrm{A}_1, \ldots, \mathrm{A}_r$ *anillos. Entonces todo ideal de* $\mathrm{A}_1 \oplus \ldots \oplus \mathrm{A}_r$ *es de la forma* $\mathrm{I}_1 \oplus \ldots \oplus \mathrm{I}_r$, *con* I_i *ideal de* A_i, $i \in \{1, \ldots, r\}$.

1.2. Cambio de anillo y subespacios de un espacio vectorial

El procedimiento del cambio de anillo simplificará el estudio de una parte de la retícula de ideales de un anillo al estudio de la retícula de subespacios de un espacio vectorial ([1]). Se presenta también la correspondencia biyectiva entre las matrices escalón reducidas por filas sobre un campo finito $\mathbb{F}_q$ y los $\mathbb{F}_q$-subespacios vectoriales que un $\mathbb{F}_q$-espacio vectorial de dimensión finita contiene. Se determina el coeficiente binomial Gaussiano, $\binom{n}{k}_q$, el cual representa el número de $\mathbb{F}_q$-subespacios vectoriales de dimensión k que un $\mathbb{F}_q$-espacio vectorial de dimensión n contiene. Se define el número de Galois, $\mathrm{G}(n, q)$, que da el número total de $\mathbb{F}_q$-subespacios vectoriales que un $\mathbb{F}_q$-espacio vectorial de dimensión n contiene.

LEMA 1.2.1 *Sea* A *un anillo,* M *un* A*-módulo y* J *un ideal de* A *tal que* $\mathrm{J} \subseteq \mathrm{ann_A(M)}$. *Entonces la función*

$$\begin{array}{rccc} * : & (\mathrm{A/J}) \times \mathrm{M} & \longrightarrow & \mathrm{M} \\ & (a+\mathrm{J}, m) & \longmapsto & am \end{array}$$

dota a M *con estructura de* (A/J)*-módulo.*

LEMA 1.2.2 *Sea* A *un anillo,* M *un* A*-módulo,* J *un ideal de* A *tal que* $\mathrm{J} \subseteq \mathrm{ann_A(M)}$ *y* N *un subgrupo aditivo de* M. *Entonces:*

(*1*) N *es* A*-submódulo de* M *si y sólo si* N *es* (A/J)*-submódulo de* M.

(*2*) $\mathcal{L}_{\mathrm{A}}(\mathrm{M}) = \mathcal{L}_{\mathrm{A/J}}(\mathrm{M})$.

Demostración.
Nótese que M es (A/J)-módulo, por el Lema 1.2.1.
(1) Supongamos que N un A-submódulo de M, es decir $\mathrm{AN} \subseteq \mathrm{N}$. Sea $a + \mathrm{J} \in (\mathrm{A/J})$ y $n \in \mathrm{N}$, entonces $(a + \mathrm{J}) * n = an \in \mathrm{N}$, lo cual implica que $(\mathrm{A/J}) * \mathrm{N} \subseteq \mathrm{N}$, de donde se sigue que N es (A/J)-submódulo de M.
Supongamos que N es un (A/J)-submódulo de M, es decir $(\mathrm{A/J}) * \mathrm{N} \subseteq \mathrm{N}$. Sea $a \in \mathrm{A}$ y $n \in \mathrm{N}$, entonces $an = (a + \mathrm{J})n \in \mathrm{N}$, lo cual implica que $\mathrm{AN} \subseteq \mathrm{N}$, de donde se sigue que N es A–submódulo de M.
(2) Se sigue del inciso anterior.

LEMA 1.2.3 *Sea* A *un anillo,* I *un ideal de* A *y* M *un* A*-módulo. Entonces* M/IM *es* (A/I)*-módulo.*

Demostración.
Se sigue del Lema 1.2.1 y el hecho de que $\mathrm{I} \subseteq \mathrm{ann_A(M/IM)}$.

Sea $\mathbb{F}_q$ el campo finito con q elementos. Se presenta la correspondencia biyectiva entre la retícula de $\mathbb{F}_q$-subespacios de un $\mathbb{F}_q$-espacio vectorial de dimensión finita con las matrices escalón reducidas por filas sobre $\mathbb{F}_q$. Esta correspondencia es válida sobre cualquier campo, pero nosotros nos concentramos en el caso en el que el campo es finito.

DEFINICIÓN 1.2.1 *Sea* $\mathbb{F}$ *un campo. Una matriz* $(k \times n)$ *sobre* $\mathbb{F}$ *se dice que está en forma escalón reducida por filas (erf) si en cada fila,* $i = 1, \ldots, k$*, la primer entrada no cero es igual a* 1*, el índice de la columna en la que el* 1 *ocurre, llamada una columna*

pivote, incrementa estrictamente con i, y las k columnas pivote son las columnas de la matriz identidad $(k \times k)$.

EJEMPLO 1.2.1 *Los siguientes son ejemplos de matrices en forma escalón reducida por filas sobre el campo finito $\mathbb{F} = \mathbb{F}_q$.*

(*1*) $(1, a_1, a_2, a_3)$, $(0, 1, b_1, b_2)$, $(0, 0, 1, c_1)$, $(0, 0, 0, 1)$, *donde* $a_1, a_2, a_3, b_1, b_2, c_1 \in \mathbb{F}$, *son todas las* (1×4) *matrices en forma escalón reducida por filas (erf) sobre* $\mathbb{F}$.

(*2*) $\begin{pmatrix} 1 & 0 & d_1 & d_2 \\ 0 & 1 & d_3 & d_4 \end{pmatrix}$, $\begin{pmatrix} 1 & e_1 & 0 & e_2 \\ 0 & 0 & 1 & e_3 \end{pmatrix}$, $\begin{pmatrix} 1 & f_1 & f_2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & 0 & g_1 \\ 0 & 0 & 1 & g_2 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & h_1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, *donde* d_i, e_i, f_i, g_i, $h_1 \in \mathbb{F}$, *son todas las* (2×4) *matrices en forma escalón reducida por filas (erf) sobre* $\mathbb{F}$.

(*3*) $\begin{pmatrix} 1 & 0 & 0 & m_1 \\ 0 & 1 & 0 & m_2 \\ 0 & 0 & 1 & m_3 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & n_1 & 0 \\ 0 & 1 & n_2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & o_1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, *donde* $m_i, n_i, o_1 \in \mathbb{F}$, *son todas las* (3×4) *matrices en forma escalón reducida por filas (erf) sobre* $\mathbb{F}$.

El siguiente resultado no estará acompañado de una demostración, la demostración se puede encontrar por ejemplo en [24].

LEMA 1.2.4 *Sea* V *un $\mathbb{F}_q$-espacio vectorial de dimensión n y $\{\alpha_1, \ldots, \alpha_n\}$ una base para* V. *Entonces*

(*1*) *Cada matriz es equivalente por filas a una única matriz escalón reducida por filas.*

(*2*) *Los subespacios de* V *de dimensión k están en correspondencia biyectiva con las matrices $(k \times n)$ sobre $\mathbb{F}_q$ en forma escalón reducida por filas.*
A la matriz $(k \times n)$, (a_{ij}), sobre el campo $\mathbb{F}_q$ en forma escalón reducida por filas le corresponde el subsepacio $\langle \sum_{i=1}^{n} a_{1i}\alpha_i, \ldots, \sum_{i=1}^{n} a_{ki}\alpha_i \rangle$.

EJEMPLO 1.2.2 *Sea* V *un espacio vectorial de dimensión 4 sobre $\mathbb{F}_q$ y suponga que $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ una base de* V. *Usando el ejemplo 1.2.1 y el inciso* (2) *del Lema 1.2.4, los subespacios de* V *son:*

Los subespacios triviales:
$\langle 0 \rangle$
$\mathrm{V} = \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$.
Los subespacios de dimensión 1*:*
$\langle \alpha_4 \rangle$,
$\langle \alpha_3 + c_1\alpha_4 \rangle$,
$\langle \alpha_2 + b_1\alpha_3 + b_2\alpha_4 \rangle$,
$\langle \alpha_1 + a_1\alpha_2 + a_2\alpha_3 + a_3\alpha_4 \rangle$,
donde $a_1, a_2, a_3, b_1, b_2, c_1 \in \mathbb{F}_q$.
Los subespacios de dimensión 2*:*
$\langle \alpha_3, \alpha_4 \rangle$,
$\langle \alpha_2 + h_1\alpha_3, \alpha_4 \rangle$,
$\langle \alpha_2 + g_1\alpha_4, \alpha_3 + g_2\alpha_4 \rangle$,
$\langle \alpha_1 + f_1\alpha_2 + f_2\alpha_3, \alpha_4 \rangle$,
$\langle \alpha_1 + e_1\alpha_2 + e_2\alpha_4, \alpha_3 + e_3\alpha_4 \rangle$,
$\langle \alpha_1 + d_1\alpha_3 + d_2\alpha_4, \alpha_2 + d_3\alpha_3 + d_4\alpha_4 \rangle$,
donde $d_i, e_i,\ f_i, g_i, h_1 \in \mathbb{F}_q$.
Los subespacios de dimensión 3*:*
$\langle \alpha_1 + m_1\alpha_4, \alpha_2 + m_2\alpha_4, \alpha_3 + m_3\alpha_4 \rangle$,
$\langle \alpha_1 + n_1\alpha_3, \alpha_2 + n_2\alpha_3, \alpha_4 \rangle$,
$\langle \alpha_1 + o_1\alpha_2, \alpha_3, \alpha_4 \rangle$, $\langle \alpha_2, \alpha_3, \alpha_4 \rangle$,
donde $m_i, n_i, o_1 \in \mathbb{F}_q$.

En los siguientes lemas se determina el coeficiente binomial Gaussiano, $\binom{n}{k}_q$, es decir, el número de $\mathbb{F}_q$-subespacios de dimensión k que un $\mathbb{F}_q$-espacio vectorial de dimensión n contiene.

DEFINICIÓN 1.2.2 *Sea* $\mathbb{F}_q$ *el campo finito con* q *elementos y* n, k *números enteros tales que* $0 \leq k \leq n$.

(*1*) *El coeficiente binomial Gaussiano,* $\binom{n}{k}_q$, *es el número de subespacios de* V *de dimensión* k.

(*2*) *El número de Galois está dado por* $\mathrm{G}(n, q) = \sum_{i=0}^{n} \binom{n}{i}_q$.

LEMA 1.2.5 *Sean* $\beta = \{I_1, I_2, \ldots, I_n\}, \beta_1 = \{J_1, J_2, \ldots, J_m\}$ *dos familias de conjuntos y* $r, s \in \mathbb{N}$. *Supóngase que cada elemento de* β *está contenido en* r *conjuntos de* β_1 *y que cada elemento de* β_1 *contiene* s *conjuntos de* β. *Entonces* $ms = nr$.

Demostración.
Para cada $k \in \{1, \ldots, m\}$, sea $X_k = \{(i,k) : I_i \subseteq J_k\}$, entonces $|X_k| = s$ y $X_{k_1} \cap X_{k_2} = \emptyset$, para $k_1 \neq k_2$. Para cada $k \in \{1, \ldots, n\}$, sea $Y_k = \{(k,i) : I_k \subseteq J_i\}$, entonces $|Y_k| = r$ y $Y_{k_1} \cap Y_{k_2} = \emptyset$, para $k_1 \neq k_2$. Finalmente obsérvese que $(\alpha, \eta) \in \bigcup_{i=1}^{m} X_i \Leftrightarrow (\alpha, \eta) \in X_\eta$, para algún $\eta \in \{1, \ldots, m\} \Leftrightarrow I_\alpha \subseteq J_\eta$, para $I_\alpha \in \beta$, $J_\eta \in \beta_1$ y algún $\eta \in \{1, \ldots, m\} \Leftrightarrow (\alpha, \eta) \in Y_\alpha \subseteq \bigcup_{i=1}^{n} Y_i$. De estas afirmaciones se sigue que $\bigcup_{i=1}^{m} X_i = \bigcup_{i=1}^{n} Y_i$ y $|\bigcup_{i=1}^{m} X_i| = |\bigcup_{i=1}^{n} Y_i| = ms = nr$.

LEMA 1.2.6 *Sea* V *un* $\mathbb{F}_q$*-espacio vectorial de dimensión* n *y* k *un número entero tal que* $0 < k < n$. *Entonces*

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)(q^n-q^2)(q^n-q^3)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)(q^k-q^2)(q^k-q^3)\cdots(q^k-q^{k-1})} =$$

$$\frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)(q^{n-3}-1)\cdots(q^{n-(k-2)}-1)(q^{n-(k-1)}-1)}{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)(q^{k-3}-1)\cdots(q^2-1)(q-1)}.$$

Demostración.
Es claro que $\binom{n}{k}_q$ solo depende de q, n y k. Sea V_1 un subespacio de dimensión 1 de V, puesto que los subespacios de V de dimensión k que contienen a V_1 están en correspondencia biyectiva con los subespacios de dimensión $k-1$ de V/V_1, por el Teorema de correspondencia, y V/V_1 es un espacio de dimensión $n-1$ que contiene $\binom{n-1}{k-1}_q$ subespacios de dimensión $k-1$, se sigue que V_1 está contenido en $\binom{n-1}{k-1}_q$ subespacios de dimensión k de V.
Por otra parte todo espacio de dimensión k contiene $\frac{q^k-1}{q-1}$ subespacios de dimensión 1. Así, por el Lema 1.2.5, se tiene que $\frac{q^k-1}{q-1}\binom{n}{k}_q = \frac{q^n-1}{q-1}\binom{n-1}{k-1}_q$ y $\binom{n}{k}_q = \frac{q^n-1}{q^k-1}\binom{n-1}{k-1}_q$, lo cual implica:

$$\binom{n}{k}_q = \frac{q^n-1}{q^k-1}\binom{n-1}{k-1}_q = \frac{(q^n-1)(q^{n-1}-1)}{(q^k-1)(q^{k-1}-1)}\binom{n-2}{k-2}_q =$$

$$\frac{(q^n-1)(q^n-q)(q^{n-2}-1)}{(q^k-1)(q^k-q)(q^{k-2}-1)}\binom{n-3}{k-3}_q =$$

$$\frac{(q^n-1)(q^n-q)(q^n-q^2)(q^{n-3}-1)}{(q^k-1)(q^k-q)(q^k-q^2)(q^{k-3}-1)}\binom{n-4}{k-4}_q =$$

$$\frac{(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{k-2})}{(q^k-1)(q^k-q)(q^k-q^2)\cdots(q^k-q^{k-2})}\binom{n-(k-1)}{1}_q =$$

$$\frac{(q^n-1)(q^n-q)(q^n-q^2)(q^n-q^3)\cdots(q^n-q^{k-2})(q^{n-(k-1)}-1)}{(q^k-1)(q^k-q)(q^k-q^2)(q^k-q^3)\cdots(q^k-q^{k-2})(q-1)} =$$

$$\frac{(q^n-1)(q^n-q)(q^n-q^2)(q^n-q^3)\cdots(q^n-q^{k-2})(q^n-q^{k-1})}{(q^k-1)(q^k-q)(q^k-q^2)(q^k-q^3)\cdots(q^k-q^{k-2})(q^k-q^{k-1})} =$$

$$\frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)(q^{n-3}-1)\cdots(q^{n-(k-2)}-1)(q^{n-(k-1)}-1)}{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)(q^{k-3}-1)\cdots(q^2-1)(q-1)}.$$

Observación 2 *Observar que si* $n>1$, $s>1$, $\mathrm{r}(\mathrm{X}) = \sum_{i=0}^{s-1} \mathrm{X}^i \in \mathbb{Z}[\mathrm{X}]$ *y* k *un entero con* $0<k\leq n$, *entonces* $\mathrm{r}(q^{n-i}) > \mathrm{r}(q^{k-i})$, *para* $i\in\{0,\ldots,k-1\}$ *y*

$$\binom{n}{k}_{q^s} = \frac{(q^{ns}-1)(q^{(n-1)s}-1)(q^{(n-2)s}-1)\cdots(q^{(n-k+1)s}-1)}{(q^{ks}-1)(q^{(k-1)s}-1)(q^{(k-2)s}-1)\cdots(q^s-1)} =$$

$$\frac{(q^n-1)\mathrm{r}(q^n)(q^{n-1}-1)\mathrm{r}(q^{n-1})(q^{n-2}-1)\mathrm{r}(q^{n-2})\cdots(q^{n-k+1}-1)\mathrm{r}(q^{n-k+1})}{(q^k-1)\mathrm{r}(q^k)(q^{k-1}-1)\mathrm{r}(q^{k-1})(q^{k-2}-1)\mathrm{r}(q^{k-2})\cdots(q-1)\mathrm{r}(q)} =$$

$$\frac{(q^n-1)(q^{n-1}-1)(q^{n-2}-1)\cdots(q^{n-k+1}-1)\mathrm{r}(q^n)\mathrm{r}(q^{n-1})\mathrm{r}(q^{n-2})\cdots\mathrm{r}(q^{n-k+1})}{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)\cdots(q-1)\mathrm{r}(q^k)\mathrm{r}(q^{k-1})\mathrm{r}(q^{k-2})\cdots\mathrm{r}(q)} =$$

$$\binom{n}{k}_q \frac{\mathrm{r}(q^n)\mathrm{r}(q^{n-1})\mathrm{r}(q^{n-2})\cdots\mathrm{r}(q^{n-k+1})}{\mathrm{r}(q^k)\mathrm{r}(q^{k-1})\mathrm{r}(q^{k-2})\cdots\mathrm{r}(q)}.$$

En consecuencia $\binom{n}{k}_q < \binom{n}{k}_{q^s}$ *y* $\mathrm{G}(n,q) < \mathrm{G}(n,q^s)$ *si y sólo si* $1<n$ *y* $1<s$.

1.3. Anillos locales finitos

En [19] se demuestra que todo anillo finito es isomorfo a una suma directa de anillos locales finitos, (ver observación 3), de esta descomposición se sigue que los códigos lineales sobre el anillo finito se expresan como suma directa de códigos lineales sobre los anillos locales finitos en los cuales se descompone el anillo finito. Así se reduce el estudio de códigos lineales sobre anillos finitos al estudio de códigos lineales sobre

anillos locales finitos.
En la presente sección se incluyen resultados generales sobre anillos locales finitos, el Lema de Hensel y algunas propiedades de las extensiones no ramificadas de anillos locales finitos.

1.3.1. Resultados básicos

En esta sección se recuerdan resultados acerca de conjunto mínimo de generadores para un módulo sobre un anillo local y se define el índice de nilpotencia del ideal maximal de un anillo local finito. Para mayores detalles ver [19] y [20].

DEFINICIÓN 1.3.1 *Un anillo* A *con un único ideal maximal* $\mathfrak{m}$ *es llamado local y* $\mathrm{A}/\mathfrak{m}$ *es llamado su campo residual. La terna* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *significa que* A *es un anillo local finito,* $\mathfrak{m}$ *es su único ideal maximal y* $\mathrm{k} = \mathrm{A}/\mathfrak{m}$ *es su campo residual.*

Observese que si $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ es un anillo local finito entonces $\mathrm{k} = \mathbb{F}_q$ es el campo finito con $q = p^d$ elementos.

Para obtener anillos locales finitos se puede usar el siguiente resultado.

LEMA 1.3.1 *Sea* A *un anillo finito,* $\mathfrak{q}$ *un ideal maximal de* A *y* $k \geq 1$ *un entero. Entonces* $\mathrm{A}/\mathfrak{q}^k$ *es un anillo local con ideal maximal* $\mathfrak{q}/\mathfrak{q}^k$ *y campo residual* $\mathrm{A}/\mathfrak{q}$.

Demostración.
Sea $\mathfrak{q}_1$ un ideal maximal de A tal que $\mathfrak{q}^k \subseteq \mathfrak{q}_1$ y sea $\alpha \in \mathfrak{q}$ entonces $\alpha^k \in \mathfrak{q}^k \subseteq \mathfrak{q}_1$, en consecuencia $\alpha \in \mathfrak{q}_1$, pues $\mathfrak{q}_1$ es ideal primo, así $\mathfrak{q} = \mathfrak{q}_1$. Del Teorema de correspondencia se sigue que $\mathrm{A}/\mathfrak{q}^k$ es un anillo local con ideal maximal $\mathfrak{q}/\mathfrak{q}^k$. La afirmación acerca del campo residual se sigue de la ralación: $\mathrm{A}/\mathfrak{q}^k/\mathfrak{q}/\mathfrak{q}^k \cong \mathrm{A}/\mathfrak{q}$.

Presentamos el siguiente resultado sin una demostración, su demostración se puede encontrar por ejemplo en [19] o [20].

TEOREMA 1.3.1 (**Lema de Nakayama**).
Sea $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local (no necesariamente finito),* M *un* A*-módulo y* N *un* A*-submódulo de* M.

(*1*) *Si* $\mathfrak{m}\mathrm{M} = \mathrm{M}$, *entonces* $\mathrm{M} = \langle 0 \rangle$;

(*2*) *Si* $\mathrm{M} = \mathrm{N} + \mathfrak{m}\mathrm{M}$, *entonces* $\mathrm{N} = \mathrm{M}$.

LEMA 1.3.2 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local (no necesariamente finito),* M *un* A*-módulo y* $m_1, \ldots, m_s$ *elementos de* M*. Entonces,*

(*1*) $\mathrm{M}/\mathfrak{m}\mathrm{M}$ *es* k*-espacio vectorial.*

(*2*) *El número de elementos de cualquier conjunto de generadores de* M *es mayor o igual a* $\dim_{\mathrm{k}}(\mathrm{M}/\mathfrak{m}\mathrm{M})$*.*

(*3*) *Si* $\{m_1+\mathfrak{m}\mathrm{M}, \ldots, m_s+\mathfrak{m}\mathrm{M}\}$ *es una base de* $\mathrm{M}/\mathfrak{m}\mathrm{M}$ *sobre* k*, entonces* $m_1, \ldots, m_s$ *generan* M*.*

Demostración.
(1) La afirmación se sigue del Lema 1.2.3.
(2) Si $m_1, \ldots, m_s$ generan M, entonces $m_1 + \mathfrak{m}\mathrm{M}, \ldots, m_s + \mathfrak{m}\mathrm{M}$ generan $\mathrm{M}/\mathfrak{m}\mathrm{M}$ sobre A y sobre k, en consecuencia $s \leq \dim_{\mathrm{k}}(\mathrm{M}/\mathfrak{m}\mathrm{M})$.
(3) Sea $m \in \mathrm{M}$, puesto que $\{m_1 + \mathfrak{m}\mathrm{M}, \ldots, m_s + \mathfrak{m}\mathrm{M}\}$ es base de $\mathrm{M}/\mathfrak{m}\mathrm{M}$ sobre k, existen $a_1, \ldots, a_s \in \mathrm{A}$ tales que $m + \mathfrak{m}\mathrm{M} = a_1m_1 + \ldots + a_sm_s + \mathfrak{m}\mathrm{M}$, lo cual implica que $m \in \langle m_1, \ldots, m_s\rangle + \mathfrak{m}\mathrm{M}$, de donde se sigue que $\mathrm{M} = \langle m_1, \ldots, m_s\rangle + \mathfrak{m}\mathrm{M}$. En consecuencia $\mathrm{M} = \langle m_1, \ldots, m_s\rangle$, por el Lema de Nakayama.

Sea $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ un anillo local (no necesariamente finito) y M un A-módulo. Del Lema 1.3.2 se sigue que para obtener un conjunto de generadores de M basta con hallar una base para el k-espacio vectorial $\mathrm{M}/\mathfrak{m}\mathrm{M}$ y despúes obtener las preimagenes de los elementos de esa base. A un conjunto obtenido de esta forma se le llamará conjunto mínimo de generadores de M. El número de elementos que hay en un conjunto mínimo de generadores de M es denotado por $\mathrm{v}_{\mathrm{A}}(\mathrm{M})$ y se tiene $\dim_{\mathrm{k}}(\mathrm{M}/\mathfrak{m}\mathrm{M}) = \mathrm{v}_{\mathrm{A}}(\mathrm{M})$.

DEFINICIÓN 1.3.2 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local.*

(*1*) *Si* $a \in \mathrm{A}$*, el elemento* $a + \mathfrak{m} \in \mathrm{k}$ *se denota simplemente por* $\tilde{a}$*.*

(*2*) *Un subconjunto* $\mathbb{T}$ *de* A *se dice que es un conjunto de representantes de* k *si para cualquier* $a \in \mathrm{k}$ *existe un único* $b \in \mathbb{T}$ *tal que* $\tilde{b} = a$*.*

Para el siguiente resultado recordemos que la longitud del A-módulo M, $\ell_{\mathrm{A}}(\mathrm{M})$, es la longitud de alguna serie de composición de M, ver Definición 1.1.3.

LEMA 1.3.3 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* $\mathbb{T} \subset \mathrm{A}$ *un conjunto de representantes de* $\mathbb{F}_q$*,* M *un* A*-módulo y* $\{\alpha_1, \ldots, \alpha_l\}$ *un conjunto mínimo de generadores de* M*. Entonces los* A*-submódulos de* M *entre* M *y* $\mathfrak{m}$M *de longitud* $k + \ell_{\mathrm{A}}(\mathfrak{m}\mathrm{M})$*, donde* $0 < k < l = \dim_{\mathbb{F}_q}(\mathrm{M}/\mathfrak{m}\mathrm{M})$*, están en correspondencia biyectiva con las* $(k \times l)$ *matrices sobre* $\mathbb{F}_q$ *en forma escalón reducida por filas (erf). A la matriz* $\mathrm{H} = (\tilde{a}_{ij})$ *le corresponde el submódulo* $\langle \sum_{i=1}^{n} a_{1i}\alpha_i, \ldots, \sum_{i=1}^{n} a_{ki}\alpha_i \rangle + \mathfrak{m}\mathrm{M}$*.*
En particular, el número de A*-submódulos de* M *entre* M *y* $\mathfrak{m}$M *es el número de Galois* $\mathrm{G}(l, q)$*.*

Demostración.
Obsérvese que M/$\mathfrak{m}$M es A-módulo, con la estructura del módulo cociente, M/$\mathfrak{m}$M es k-espacio vectorial, por el inciso (1) del Lema 1.3.2 y que cada matriz con coeficientes en $\mathbb{F}_q$ es de la forma $(\tilde{a}_{ij})$, donde $a_{ij} \in \mathbb{T}$.
A la matriz $(\tilde{a}_{ij})$ con coeficientes en $\mathbb{F}_q$ le corresponde el $\mathbb{F}_q$-subspacio de M/$\mathfrak{m}$M, $\langle \sum_{i=1}^{n} \tilde{a}_{1i}\tilde{\alpha}_i, \ldots, \sum_{i=1}^{n} \tilde{a}_{ki}\tilde{\alpha}_i \rangle$. Este $\mathbb{F}_q$-subespacio de M/$\mathfrak{m}$M, el cual por cambio de anillo es el A-submódulo de M/$\mathfrak{m}$M, $\langle \sum_{i=1}^{n} a_{1i}\tilde{\alpha}_i, \ldots, \sum_{i=1}^{n} a_{ki}\tilde{\alpha}_i \rangle$, y a este A-submódulo de M/$\mathfrak{m}$M le corresponde el A-submódulo de M, $\langle \sum_{i=1}^{n} a_{1i}\alpha_i, \ldots, \sum_{i=1}^{n} a_{ki}\alpha_i \rangle + \mathfrak{m}\mathrm{M}$, por el Teorema de Correspondencia.

Una consecuencia del Lema 1.3.3 es el caso en el que se toma $\mathrm{M} = \mathfrak{m}$.

COROLARIO 1.3.1 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* $l = \dim_{\mathbb{F}_q}(\mathfrak{m}/\mathfrak{m}^2)$*,* $\mathbb{T} \subset \mathrm{A}$ *un conjunto de representantes de* $\mathbb{F}_q$ *y* $\{\alpha_1, \ldots, \alpha_l\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$*. Entonces los ideales de* A *entre* $\mathfrak{m}$ *y* $\mathfrak{m}^2$ *de longitud* $k + \ell_{\mathrm{A}}(\mathfrak{m}^2)$*, donde* $0 < k < l$*, están en correspondencia biyectiva con las* $(k \times l)$ *matrices sobre* $\mathbb{F}_q$ *en forma escalón reducida por filas (erf). A la matriz* $\mathrm{H} = (\tilde{a}_{ij})$ *le corresponde el ideal* $\langle \sum_{i=1}^{n} a_{1i}\alpha_i, \ldots, \sum_{i=1}^{n} a_{ki}\alpha_i \rangle + \mathfrak{m}^2$*. En particular, el número de ideales de* A *entre* $\mathfrak{m}$ *y* $\mathfrak{m}^2$ *es el número de Galois* $\mathrm{G}(l, q)$*.*

Recordemos que si A es un anillo local finito, su campo residual es un campo finito $\mathbb{F}_q$, donde $q = p^d$ con p un número primo y $d \geq 1$ un entero.

LEMA 1.3.4 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito y* M *un* A*-módulo de longitud* $\ell_{\mathrm{A}}(\mathrm{A})$*. Entonces:*

$$|\mathrm{M}| = |\mathrm{k}|^{\ell_{\mathrm{A}}(\mathrm{M})}.$$

Demostración.
La prueba se hace por inducción sobre $\ell_{\mathrm{A}}(\mathrm{M})$. Si $\ell_{\mathrm{A}}(\mathrm{M}) = 1$, entonces M es un

A-módulo simple, así $\mathrm{M} \cong \mathrm{k}$, por el inciso (2) del Lema 1.1.1, de donde se sigue la afirmación. Si $l := \ell_{\mathrm{A}}(\mathrm{M}) > 1$, entonces existe una serie de composición de submódulos de M, $\langle 0 \rangle = \mathrm{M}_l \subset \mathrm{M}_{l-1} \subset \ldots \subset \mathrm{M}_1 \subset \mathrm{M}_0 = \mathrm{M}$. Puesto que $\ell_{\mathrm{A}}(\mathrm{M}_1) = l - 1$, por hipótesis de inducción, $|\mathrm{M}_1| = |\mathrm{k}|^{l-1}$. En consecuencia $|\mathrm{M}| = |\mathrm{M}/\mathrm{M}_1||\mathrm{M}_1| = |\mathrm{k}||\mathrm{k}|^{l-1} = |\mathrm{k}|^l$, como se esperaba.

LEMA 1.3.5 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito. Entonces existe* $t \in \mathbb{N}$ *tal que* $\mathfrak{m}^t = \langle 0 \rangle$.

Demostración.
Si A es un campo la afirmación es trivial. Supóngase que A no es un campo. Considerar la cadena de ideales $\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \ldots \supseteq \mathfrak{m}^k \supseteq \ldots$, puesto que A es finito, existe $t \in \mathbb{N}$ tal que $\mathfrak{m}^t = \mathfrak{m}^{t+r}$, para cualquier $r \in \mathbb{N}$. En consecuencia $\mathfrak{m}^t = \mathfrak{m}^{t+1} = \mathfrak{m}\mathfrak{m}^t$, de donde se sigue que $\mathfrak{m}^t = \langle 0 \rangle$, por el Lema de Nakayama.

DEFINICIÓN 1.3.3 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito. El menor entero,* t*, para el cual se cumple* $\mathfrak{m}^t = 0$*, es llamado el índice de nilpotencia de* $\mathfrak{m}$.

LEMA 1.3.6 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito y* t *el índice de nilpotencia de* $\mathfrak{m}$. *Entonces* $t \leq \ell_{\mathrm{A}}(\mathrm{A})$.

Demostración.
Nótese que si $i \in \{1, \ldots, t-1\}$, la igualdad $\mathfrak{m}^i = \mathfrak{m}^{i+1}$, implica que $\mathfrak{m}^i = \langle 0 \rangle$, por el Lema de Nakayama, lo cual es una contradicción. De esta manera, la afirmación se sigue del hecho de que A tiene la cadena de ideales $\mathrm{A} \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \ldots \supset \mathfrak{m}^t = \langle 0 \rangle$.

1.3.2. Extensiones no ramificadas de un anillo local

Sea $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ un anillo local finito. En lo que resta de este trabajo, A[T] denotará el anillo de polinomios con coeficientes en A. En ocaciones el polinomio $\mathrm{f(T)} \in \mathrm{A[T]}$ será denotado simplemente por f. Sea $\mathrm{f(T)} \in \mathrm{A[T]}$ un polinomio básico irreducible, en esta subsección se estudian algunas propiedades del anillo $\mathrm{B} = \mathrm{A[T]}/\langle \mathrm{f(T)} \rangle$. Se concluye que el anillo B es un anillo local con ideal maximal $\mathfrak{m}\mathrm{B}$, se obtienen propiedades de la retícula de ideales del anillo B a partir de la retícula de ideales del anillo A, por ejemplo la conservación de la longitud de un ideal de A al ser expandido al anillo B, el anulador de la expansión de un ideal de A en el anillo B se puede describir

a partir del anulador del ideal en el anillo A, y finalmente un conjunto mínimo de generadores del ideal maximal del anillo A es un conjunto mínimo de generadores del ideal maximal del anillo B.

DEFINICIÓN 1.3.4 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito,* $\mathrm{A}[\mathrm{T}]$ *el anillo de polinomios con coeficientes en* A, $\mathrm{f}(\mathrm{T}), \mathrm{g}(\mathrm{T}) \in \mathrm{A}[\mathrm{T}]$ *polinomios e* I *un ideal de* A.

(*1*) $\mathrm{I}[\mathrm{T}]$ *denota el conjunto de polinomios en* $\mathrm{A}[\mathrm{T}]$ *cuyos coeficientes son elementos de* I. *Es decir,*

$$\mathrm{I}[\mathrm{T}] = \{a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2 + \ldots + a_n\mathrm{T}^n \in \mathrm{A}[\mathrm{T}] : a_i \in \mathrm{I}\}.$$

(*2*) *La proyección canónica,* $\pi : \mathrm{A} \longrightarrow \mathrm{k}$ *es el epimorfismo que a cada elemento de* A *le asigna su clase módulo* $\mathfrak{m}$.

(*3*) *La proyección natural* $\tilde{} : \mathrm{A}[\mathrm{T}] \longrightarrow \mathrm{k}[\mathrm{T}]$ *es el epimorfismo que aplica* π *a los coeficientes de los polinomios. Es decir, si* $\mathrm{f} = a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2 + \ldots + a_n\mathrm{T}^n$ *entonces* $\tilde{\mathrm{f}} = \pi(a_0) + \pi(a_1)\mathrm{T} + \pi(a_2)\mathrm{T}^2 + \ldots + \pi(a_n)\mathrm{T}^n$.

(*4*) *Se dice que* $\mathrm{f}(\mathrm{T}) \in \mathrm{A}[\mathrm{T}]$ *es polinomio básico irreducible si* $\tilde{\mathrm{f}}(\mathrm{T}) \in \mathrm{k}[\mathrm{T}]$ *es polinomio irreducible.*

(*5*) *Se dice que* $\mathrm{f}(\mathrm{T})$ *y* $\mathrm{g}(\mathrm{T})$ *son coprimos si* $\langle \mathrm{f}(\mathrm{T}) \rangle + \langle \mathrm{g}(\mathrm{T}) \rangle = \mathrm{A}[\mathrm{T}]$.

Nótese que el kernel de la proyección natural es $\mathfrak{m}[\mathrm{T}]$.

El ideal I del anillo A se llama *primario* si para todo a, b tales que $\mathrm{ab} \in \mathrm{I}$, si $\mathrm{a} \notin \mathrm{I}$ entonces $\mathrm{b}^n \in \mathrm{I}$, para algún número natural n. El elemento α de un anillo A es llamado *regular* si no es divisor de cero y es llamado primario si $\langle \alpha \rangle$ es ideal primario.

El siguiente resultado garantiza que todo polinomio regular con coeficientes en un anillo local se puede factorizar de manera única como producto de polinomios regulares primarios, su demostración se puede consultar por ejemplo en [20].

TEOREMA 1.3.2 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito y* $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio regular, entonces existen* $\mathrm{g}_1, \ldots, \mathrm{g}_r$ *polinomios regulares primarios coprimos a pares y* u *una unidad tales que* $\mathrm{f} = \mathrm{ug}_1 \cdots \mathrm{g}_r$. *Y si existen* $\mathrm{h}_1, \ldots, \mathrm{h}_s$ *polinomios regulares primarios coprimos a pares y* v *una unidad tales que* $\mathrm{f} = \mathrm{vh}_1 \cdots \mathrm{h}_s$, *entonces* $r = s$, *y después de renumerar,* $\langle \mathrm{g}_i \rangle = \langle \mathrm{h}_i \rangle$, $1 \leq i \leq r$.

El siguiente resultado es una caracterización para polinomios regulares con coeficientes en un anillo local, su demostración se puede consultar por ejemplo en [20]. Una consecuencia de este resultado es que los polinomios básicos irreducibles son regulares.

LEMA 1.3.7 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito y* $\mathrm{f(T)} = a_0 + a_1\mathrm{T} + \ldots + a_n\mathrm{T}^n \in \mathrm{A[T]}$ *un polinomio. Las siguientes afirmaciones son equivalentes:*

(*1*) $\mathrm{f(T)}$ *es regular;*

(*2*) $\tilde{\mathrm{f}} \neq 0$*;*

(*3*) a_i *es unidad, para algún* $0 \leq i \leq n$*.*

El siguiente resultado es el conocido Algoritmo de la División para polinomios sobre anillos conmutativos, su demostración se puede consultar por ejemplo en [17].

TEOREMA 1.3.3 *Sea* A *un anillo conmutativo y* $\mathrm{f}, \mathrm{g} \in \mathrm{A[X]}$*. Supongase que* f *es mónico, entonces existen únicos polinomios* $\mathrm{q}, \mathrm{r} \in \mathrm{A[X]}$ *tales que*

$$\mathrm{g} = \mathrm{fq} + \mathrm{r}, \text{ donde } \mathrm{r} = 0 \text{ ó } \deg(\mathrm{r}) < \deg(\mathrm{f}).$$

De los siguientes tres resultados se obtendrá que en el estudio del anillo $\mathrm{B} = \mathrm{A[T]}/\langle \mathrm{f} \rangle$, donde $\mathrm{f} \in \mathrm{A[T]}$ es un polinomio regular, se puede suponer que f es mónico.

LEMA 1.3.8 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito,* $i \geq 1$ *un entero,* $\mathrm{f} \in \mathrm{A[T]}$ *un polinomio mónico y* $\mathrm{g} \in \mathfrak{m}^i[\mathrm{T}]$*. Si* q *y* r *son el cociente y el residuo de la división de* g *por* f*, entonces* q *y* r *tienen todos sus coeficientes en* $\mathfrak{m}^i$*.*

Demostración.
Sea $\mathrm{f} = a_0 + a_1\mathrm{T} + \ldots + \mathrm{T}^s$ y $\mathrm{g} = b_0 + b_1\mathrm{T} + \ldots + b_u\mathrm{T}^u$. Si $\deg(\mathrm{g}) < \deg(\mathrm{f})$, entonces $\mathrm{q} = 0$ y $\mathrm{r} = \mathrm{g}$, de donde se sigue la afirmación. Si $\deg(\mathrm{g}) = \deg(\mathrm{f})$, entonces $\mathrm{q} = b_u$ y $\mathrm{r} = \mathrm{g} - \mathrm{f}b_u$, de donde se sigue la afirmación. Suponer que $\deg(\mathrm{f}) < \deg(\mathrm{g})$ y la prueba será por inducción sobre $\deg(\mathrm{g})$. Puesto que $\mathrm{g} - b_u\mathrm{T}^{u-s}\mathrm{f}$ es un polinomio de grado menor a $\deg(\mathrm{g})$ con coeficientes en $\mathfrak{m}^i$, entonces $\mathrm{g} - b_u\mathrm{T}^{u-s}\mathrm{f} = \mathrm{fq}_1 + \mathrm{r}_1$, donde $\mathrm{r}_1 = 0$ ó $\deg(\mathrm{r}_1) < \deg(\mathrm{f})$, q_1 y r_1 tienen coeficientes en $\mathfrak{m}^i$, por hipótesis de inducción. Lo cual implica que $\mathrm{g} = (b_u\mathrm{T}^{u-s} + \mathrm{q}_1)\mathrm{f} + \mathrm{r}_1$, de donde se sigue la afirmación.

PROPOSICIÓN 1.3.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito,* $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio regular y* $\deg(\tilde{\mathrm{f}}) = s$. *Entonces existen* $\{\mathrm{f}_1, \mathrm{f}_2, \ldots\} \subset \mathrm{A}[\mathrm{T}]$, $\{\mathrm{h}_1, \mathrm{h}_2, \ldots\} \subset \mathrm{A}[\mathrm{T}]$, $\{\mathrm{g}_1, \mathrm{g}_2, \ldots\} \subset \mathfrak{m}[\mathrm{T}]$ *y* $\{b_1, b_2, \ldots\} \subset \mathrm{A}^*$ *tal que:*

(*1*) *Cada* f_k *es mónico de grado* s,

(*2*) $\mathrm{f}_k \equiv \mathrm{f}_{k+1} \bmod \mathfrak{m}^k[\mathrm{T}]$,

(*3*) $b_k\mathrm{f} - [\mathrm{f}_k + \mathrm{g}_k\mathrm{f}_k] = \mathrm{h}_k \in \mathfrak{m}^k[\mathrm{T}]$.

Demostración.
La prueba será por inducción sobre k.
Caso $k = 1$.
Sea $m = \deg(\mathrm{f})$ entonces $\mathrm{f} = a_0 + \ldots + a_s\mathrm{T}^s + \sum_{i=s+1}^{m} a_i\mathrm{T}^i$, a_s es unidad de A y $a_{s+1}, \ldots, a_m$ son nilpotentes. De la igualdad:

$$a_s^{-1}\mathrm{f} - [a_0a_s^{-1} + a_1a_s^{-1}\mathrm{T} + \ldots + \mathrm{T}^s] = a_s^{-1}\sum_{i=s+1}^{m} a_i\mathrm{T}^i \in \mathfrak{m}[\mathrm{T}],$$

resta tomar $\mathrm{f}_1 = a_0a_s^{-1} + a_1a_s^{-1}\mathrm{T} + \ldots + \mathrm{T}^s$, $b_1 = a_s^{-1}$, $\mathrm{g}_1 = 0$ y $\mathrm{h}_1 = a_s^{-1}\sum_{i=s+1}^{m} a_i\mathrm{T}^i$. Supóngase cierto el resultado para algún k. Es decir, se tienen $\mathrm{f}_k \in \mathrm{A}[\mathrm{T}]$, b_k una unidad de A, $\mathrm{g}_k \in \mathfrak{m}[\mathrm{T}]$ y $\mathrm{h}_k \in \mathfrak{m}^k[\mathrm{T}]$ que satisfacen

(1) Cada f_k es mónico de grado s,

(2) $\mathrm{f}_{k-1} \equiv \mathrm{f}_k \bmod \mathfrak{m}^{k-1}[\mathrm{T}]$,

(3) $b_k\mathrm{f} - [\mathrm{f}_k + \mathrm{g}_k\mathrm{f}_k] = \mathrm{h}_k \in \mathfrak{m}^k[\mathrm{T}]$.

Puesto que f_k es mónico, entonces $h_k = \mathrm{f}_kq_k + r_k$, donde $r_k = 0$ ó $\deg(r_k) < s$, y q_k y r_k tienen coeficientes en $\mathfrak{m}^k$, por el Lema 1.3.8. De la igualdad:

$$b_k\mathrm{f} = \mathrm{f}_k + \mathrm{g}_k\mathrm{f}_k + \mathrm{f}_kq_k + r_k = (\mathrm{f}_k + r_k) + (\mathrm{g}_k + q_k)(\mathrm{f}_k + r_k) - r_k(\mathrm{g}_k + q_k),$$

resta tomar $\mathrm{f}_{k+1} = \mathrm{f}_k + r_k$, $\mathrm{g}_{k+1} = \mathrm{g}_k + q_k$, $b_{k+1} = b_k$ y $\mathrm{h}_{k+1} = -r_k(\mathrm{g}_k + q_k)$ para obtener la afirmación.

PROPOSICIÓN 1.3.2 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito y* $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio regular. Entonces existe un polinomio mónico* $\mathrm{f}_1 \in \mathrm{A}[\mathrm{T}]$ *y una unidad* $v \in \mathrm{A}[\mathrm{T}]$ *tales que* $v\mathrm{f} = \mathrm{f}_1$.

Demostración.
Sea t el índice de nilpotencia de $\mathfrak{m}$, por el Lema 1.3.1, existen $\{\mathrm{f}_1, \mathrm{f}_2, \ldots\} \subset \mathrm{A}[\mathrm{T}]$, $\{\mathrm{g}_1, \mathrm{g}_2, \ldots\} \subset \mathfrak{m}[\mathrm{T}]$ y $\{b_1, b_2, \ldots\} \subset \mathrm{A}^*$ tales que para cada $k \geq 1$:

(1) Cada f_k es mónico de grado $\deg(\tilde{\mathrm{f}})$,

(2) $\mathrm{f}_k \equiv \mathrm{f}_{k+1} \bmod \mathfrak{m}^k[\mathrm{T}]$,

(3) $b_k\mathrm{f} \equiv \mathrm{f}_k + \mathrm{g}_k\mathrm{f}_k \bmod \mathfrak{m}^k[\mathrm{T}]$.

Así, f_t es mónico de grado $\deg(\tilde{\mathrm{f}})$ y $b_t\mathrm{f} = \mathrm{f}_t + \mathrm{g}_t\mathrm{f}_t = (1 + \mathrm{g}_t)\mathrm{f}_t$. La afirmación se sigue del hecho de que $\mathrm{g}(\mathrm{T})$ es nilpotente, pues sus coeficientes son nilpotentes, y $1 + \mathrm{g}_t$ es unidad.

En los siguientes dos ejemplos se aplica el método de la prueba del Proposición 1.3.1 y la Proposición 1.3.2.

Ejemplo 1.3.1 *Sea* $\mathrm{A} = \mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X}\rangle$. *Es fácil verificar que* A *es local, sus elementos se pueden expresar de manera única en la forma* $a + b\mathrm{x}$, *donde* $a \in \mathbb{Z}_8$ *y* $b \in \{0, 1\} \subset \mathbb{Z}_8$, *sus unidades son* $\mathrm{A}^* = \{1 + 2a + 4b + c\mathrm{x} : a, b, c \in \{0, 1\}\}$, *el ideal maximal de* A *es* $\mathfrak{m} = \{2a + 4b + c\mathrm{x} : \ a, b, c \in \{0, 1\}\}$, *y tiene índice de nilpotencia* 3. *Sea* $\mathrm{m} = 2a + 4b + c\mathrm{x}$, *donde* $a, b, c \in \{0, 1\}$, *y* $\mathrm{f} = \mathrm{m}^2\mathrm{T}^4 + \mathrm{T}^3 + (3 + 4a + 3\mathrm{m})\mathrm{T}^2 + (2 + \mathrm{m}^2)\mathrm{T} + 7 + \mathrm{m}^2 + 3\mathrm{m}$. *Entonces:*

$$\mathrm{f} = [1 + \mathrm{m}^2(\mathrm{T} + 1)][\mathrm{T}^3 + (3 + 4c + 3\mathrm{m})\mathrm{T}^2 + 2\mathrm{T} + 7 + 3\mathrm{m}].$$

Paso $k = 1$*:*
Se tiene $\deg(\tilde{\mathrm{f}}) = 3$ *y* $a_3 = 1$, *entonces*
$\mathrm{f}_1 = \mathrm{T}^3 + (3 + 4a + 3\mathrm{m})\mathrm{T}^2 + (2 + \mathrm{m}^2)\mathrm{T} + 7 + \mathrm{m}^2 + 3\mathrm{m}$, $b_1 = a_3^{-1} = 1$, $\mathrm{g}_1 = 0$ *y* $\mathrm{h}_1 = \mathrm{m}^2\mathrm{T}^4$ *y se tiene*

(*1*) f_1 *es mónico de grado* 3,

(*2*) $b_1\mathrm{f} - [\mathrm{f}_1 + \mathrm{g}_1\mathrm{f}_1] = \mathrm{h}_1 = \mathrm{m}^2\mathrm{T}^4 \in \mathfrak{m}[\mathrm{T}]$.

Paso $k = 2$*:*
Puesto que $\mathrm{h}_1 = \mathrm{m}^2\mathrm{T}^4 = \mathrm{f}_1\mathrm{q}_1 + \mathrm{r}_1$, *donde* $\mathrm{f}_1 = \mathrm{T}^3 + (3 + 4a + 3\mathrm{m})\mathrm{T}^2 + (2 + \mathrm{m}^2)\mathrm{T} + 7 + \mathrm{m}^2 + 3\mathrm{m}$, $q_1 = \mathrm{m}^2(\mathrm{T} + 1)$ *y* $r_1 = \mathrm{m}^2(\mathrm{T}^2 + \mathrm{T} + 1)$, *entonces:*
$\mathrm{f}_2 = \mathrm{f}_1 + \mathrm{r}_1 = \mathrm{T}^3 + (3 + 4a + 3\mathrm{m})\mathrm{T}^2 + (2 + \mathrm{m}^2)\mathrm{T} + 7 + \mathrm{m}^2 + 3\mathrm{m} + \mathrm{m}^2(\mathrm{T}^2 + \mathrm{T} + 1) = \mathrm{T}^3 + (3 + 4c + 3\mathrm{m})\mathrm{T}^2 + 2\mathrm{T} + 7 + 3\mathrm{m}$, $\mathrm{g}_2 = \mathrm{g}_1 + q_1 = \mathrm{m}^2(\mathrm{T} + 1)$, $b_2 = b_1 = 1$ *y* $\mathrm{h}_2 = -\mathrm{r}_1(\mathrm{g}_1 + \mathrm{q}_1) = \mathrm{m}^2(\mathrm{T}^2 + \mathrm{T} + 1)\mathrm{m}^2(\mathrm{T} + 1) = 0$ *satisfacen:*

(*1*) f_2 *es mónico de grado* 3,

(*2*) $\mathrm{f}_1 \equiv \mathrm{f}_2 \bmod \mathfrak{m}[\mathrm{T}]$,

(*3*) $b_2\mathrm{f} - [\mathrm{f}_2 + \mathrm{g}_2\mathrm{f}_2] = \mathrm{h}_2 = 0$.

De donde se obtiene $\mathrm{f} = (1+\mathrm{g}_2)\mathrm{f}_2 = [1+\mathrm{m}^2(\mathrm{T}+1)][\mathrm{T}^3+(3+4c+3\mathrm{m})\mathrm{T}^2+2\mathrm{T}+7+3\mathrm{m}]$.

EJEMPLO 1.3.2 *Sea* $\mathrm{A} = \mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X}\rangle$, *el anillo local del ejemplo 1.3.1,* $\mathrm{m} = 2a + 4b + c\mathrm{x}$, *donde* $a, b, c \in \{0, 1\}$, *y* $\mathrm{f} = \mathrm{m}^2\mathrm{T}^2 + \mathrm{T} + 7 + \mathrm{m}$. *Entonces:*

$$\mathrm{f} = [1 + \mathrm{m}^2(\mathrm{T} + 1)][\mathrm{T} + 7 + \mathrm{m} + \mathrm{m}^2].$$

Paso $k = 1$*:*
Se tiene $\deg(\tilde{\mathrm{f}}) = 1$ *y* $a_1 = 1$, *entonces*
$\mathrm{f}_1 = \mathrm{T} + 7 + \mathrm{m}$, $b_1 = a_1^{-1} = 1$, $\mathrm{g}_1 = 0$ *y* $\mathrm{h}_1 = \mathrm{m}^2\mathrm{T}^2$ *y se tiene*

(*1*) f_1 *es mónico de grado* 1,

(*2*) $b_1\mathrm{f} - [\mathrm{f}_1 + \mathrm{g}_1\mathrm{f}_1] = \mathrm{h}_1 = \mathrm{m}^2\mathrm{T}^2 \in \mathfrak{m}[\mathrm{T}]$.

Paso $k = 2$*:*
Puesto que $\mathrm{h}_1 = \mathrm{m}^2\mathrm{T}^2 = \mathrm{f}_1\mathrm{q}_1 + \mathrm{r}_1$, *donde* $\mathrm{f}_1 = \mathrm{T} + 7 + \mathrm{m}$, $q_1 = \mathrm{m}^2(\mathrm{T} + 1)$ *y* $r_1 = \mathrm{m}^2$, *entonces:*
$\mathrm{f}_2 = \mathrm{f}_1 + \mathrm{r}_1 = \mathrm{T} + 7 + \mathrm{m} + \mathrm{m}^2$, $\mathrm{g}_2 = \mathrm{g}_1 + q_1 = \mathrm{m}^2(\mathrm{T} + 1)$, $b_2 = b_1 = 1$ *y* $\mathrm{h}_2 = -\mathrm{r}_1(\mathrm{g}_1 + \mathrm{q}_1) = -\mathrm{m}^2\mathrm{m}^2(\mathrm{T} + 1) = 0$ *satisfacen:*

(*1*) f_2 *es mónico de grado* 1,

(*2*) $\mathrm{f}_1 \equiv \mathrm{f}_2 \bmod \mathfrak{m}[\mathrm{T}]$,

(*3*) $b_2\mathrm{f} - [\mathrm{f}_2 + \mathrm{g}_2\mathrm{f}_2] = \mathrm{h}_2 = 0$.

De donde se obtiene $\mathrm{f} = (1 + \mathrm{g}_2)\mathrm{f}_2 = [1 + \mathrm{m}^2(\mathrm{T} + 1)][\mathrm{T} + 7 + \mathrm{m} + \mathrm{m}^2]$.

Sean $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ y $(\mathrm{B}, \mathfrak{n}, \mathrm{k}_1)$ anillos locales. El hecho de que $\mathrm{A} \subset \mathrm{B}$ no implica que $\mathfrak{m} \subseteq \mathfrak{n}$, como ejemplo elegir A como cualquier anillo local que sea dominio entero y B al campo se cocientes de A.

DEFINICIÓN 1.3.5 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *y* $(\mathrm{B}, \mathfrak{n}, \mathrm{k}_1)$ *anillos locales tales que* $\mathrm{A} \subseteq \mathrm{B}$.

(*1*) *Se dice que la extensión* $\mathrm{A} \subseteq \mathrm{B}$ *es una extensión de anillos locales si* $\mathfrak{m} \subseteq \mathfrak{n}$.

(*2*) *Se dice que* B *es una extensión no ramificada de* A *si* $\mathfrak{m}\mathrm{B} = \mathfrak{n}$. *Es decir, si* $\mathfrak{m}$ *genera el ideal maximal de* B.

El resultado que mencionaremos a continuación no estará acompañado de una demostración, la cual se puede encontrar por ejemplo en [20].

PROPOSICIÓN 1.3.3 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *y* $(\mathrm{B}, \mathfrak{n}, \mathrm{k}_1)$ *anillos locales tales que* $\mathrm{A} \subseteq \mathrm{B}$. *Las siguientes condiciones son equivalentes:*

(*1*) B *es una extensión no ramificada de* A*;*

(*2*) $\mathrm{B} \cong \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}(\mathrm{T})\rangle$, *donde* $\mathrm{f}(\mathrm{T}) \in \mathrm{A}[\mathrm{T}]$ *es un polinomio mónico básico irreducible.*

LEMA 1.3.9 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* $\mathbb{T} \subset \mathrm{A}$ *un conjunto de representantes de* $\mathbb{F}_q$, $\mathrm{f}(\mathrm{T}) \in \mathrm{A}[\mathrm{T}]$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}(\mathrm{T})\rangle$ *la extensión no ramificada de* A *determinada por* f. *Entonces*

(*1*) *Cualquier elemento de* B *se puede expresar de manera única en la forma:*

$$a_0 + a_1\mathrm{T} + \cdots + a_{s-1}\mathrm{T}^{s-1} + \langle \mathrm{f}(\mathrm{T})\rangle,$$

donde $a_i \in \mathbb{T}$.

(*2*) *El ideal maximal de* B *es* $\mathfrak{m}\mathrm{B}$.

(*3*) *El campo residual de* B *es isomorfo a* $\mathbb{F}_{q^s} = \mathbb{F}_q[\mathrm{T}]/\langle \tilde{\mathrm{f}}\rangle$.

(*4*) $\mathbb{T}_s := \{a_0 + a_1\mathrm{T} + \cdots + a_{s-1}\mathrm{T}^{s-1} + \langle \mathrm{f}(\mathrm{T})\rangle : a_i \in \mathbb{T}\} \subset \mathrm{B}$ *es un conjunto de representantes de* $\mathbb{F}_{q^s}$.

Demostración.
(1) Por la Proposición 1.3.2, sea $\mathrm{f}_1, v \in \mathrm{A}[\mathrm{T}]$, con v unidad de $\mathrm{A}[\mathrm{T}]$ y f_1 polinomio mónico tales que $\mathrm{f} = v\mathrm{f}_1$, entonces $\langle \mathrm{f}\rangle = \langle \mathrm{f}_1\rangle$ y la afirmación se sigue del algoritmo de la división.
(2) La afirmación se sigue de la Proposición 1.3.3.
(3) Por el tercer Teorema de isomorfismos, se tiene

$$\mathrm{B}/\mathfrak{m}\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}(\mathrm{T})\rangle/\mathfrak{m}\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}(\mathrm{T})\rangle \cong \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}(\mathrm{T})\rangle/\langle \mathfrak{m}, \mathrm{f}(\mathrm{T})\rangle/\langle \mathrm{f}(\mathrm{T})\rangle \cong$$

$$\mathrm{A[T]}/\langle \mathfrak{m}, \mathrm{f(T)}\rangle \cong \mathbb{F}_q[\mathrm{T}]/\langle \tilde{\mathrm{f}}\rangle.$$

(4) Es inmediato.

Sean $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ un anillo local finito, $\mathrm{f(T)} \in \mathrm{A[T]}$ un polinomio básico irreducible y $\mathrm{B} = \mathrm{A[T]}/\langle \mathrm{f(T)}\rangle$ la extensión no ramificada de A determinada por f(T). En lo que resta de este trabajo, el elemento $\mathrm{g(T)} + \langle \mathrm{f(T)}\rangle \in \mathrm{B}$ será denotado simplemente por g(T).

LEMA 1.3.10 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* I *y* J *ideales de* A, $\mathrm{f(T)} \in \mathrm{A[T]}$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A[T]}/\langle \mathrm{f(T)}\rangle$ *la extensión no ramificada de* A *determinada por* f(T)*. Entonces*

(*1*) $\mathrm{IB} \subseteq \mathrm{JB}$ *si y sólo si* $\mathrm{I} \subseteq \mathrm{J}$*. En particular* $\mathrm{IB} = \mathrm{JB}$ *si y sólo si* $\mathrm{I} = \mathrm{J}$*.*

(*2*) *Mediante la expansión de ideales, la retícula de ideales de* A *se incluye en la retícula de ideales de* B*.*

(*3*) *El índice de nilpotencia de los ideales maximales de* A *y* B *es la misma.*

Demostración.
(1) $\Rightarrow$ Por el inciso (1) del Lema 1.3.9, B es A-módulo libre con base $\{1, \mathrm{T}, \ldots, \mathrm{T}^{s-1}\}$ e $\mathrm{IB} = \{\sum_i c_i(a_0^i + a_1^i\mathrm{T} + \ldots + a_{s-1}^i\mathrm{T}^{s-1}) : i \in \mathbb{N}, c_i \in \mathrm{I}, a_j^i \in \mathrm{A}\} = \{b_0 + b_1\mathrm{T} + \ldots + b_{s-1}\mathrm{T}^{s-1} : b_i \in \mathrm{I}\}$. En consecuencia $\{b_0 + b_1\mathrm{T} + \cdots + b_{s-1}\mathrm{T}^{s-1} : b_i \in \mathrm{I}\} \subseteq \{b_0 + b_1\mathrm{T} + \cdots + b_{s-1}\mathrm{T}^{s-1} : b_i \in \mathrm{J}\}$ y puesto que $\{1, \mathrm{T}, \ldots, \mathrm{T}^{s-1}\}$ es un conjunto linealmente independente sobre A, entonces $\mathrm{I} \subseteq \mathrm{J}$. $\Leftarrow$) es trivial.
(2) Se sigue del inciso anterior.
(3) Sea t la nilpotencia de $\mathfrak{m}$ y t_1 la nilpotencia de $\mathfrak{m}\mathrm{B}$. Por el Lema 1.1.3, se tiene $(\mathfrak{m}\mathrm{B})^t = (\mathfrak{m}^t)\mathrm{B} = 0$, así, $t_1 \leq t$. Por otra parte, por el Lema 1.1.3, $(\mathfrak{m}\mathrm{B})^{t_1} = \mathfrak{m}^{t_1}\mathrm{B} = 0$. Así, por el inciso (1), $\mathfrak{m}^{t_1} = 0$, de donde se sigue que $t \leq t_1$, que es lo que se esperaba.

LEMA 1.3.11 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* $\{\alpha_1, \ldots, \alpha_l\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$*,* I *un ideal de* A*,* $\mathrm{f} \in \mathrm{A[T]}$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A}/\langle \mathrm{f}\rangle$ *la extensión no ramificada de* A *determinada por* f*. Entonces*

(*1*) $\ell_{\mathrm{A}}(\mathrm{I}) = \ell_{\mathrm{B}}(\mathrm{IB})$.
En particular $\ell_{\mathrm{B}}(\mathrm{B}) = \ell_{\mathrm{A}}(\mathrm{A})$*.*

(*2*) $\{\alpha_1, \ldots, \alpha_l\}$ *es un conjunto mínimo de generadores de* $\mathfrak{m}\mathrm{B}$*.*

($\mathcal{3}$) $[\mathrm{ann_A(I)}]\mathrm{B} = \mathrm{ann_B(IB)}$.
En particular $\mathrm{ann_B}(\mathfrak{m}\mathrm{B}) = [\mathrm{ann_A}(\mathfrak{m})]\mathrm{B}$

Demostración.
(1) Por la prueba del inciso (1) del Lema 1.3.10, se tiene

$$\mathrm{IB} = \{b_0 + b_1\mathrm{T} + \ldots + b_{s-1}\mathrm{T}^{s-1} : b_i \in \mathrm{I}\},$$

con $\{1, \mathrm{T}, \ldots, \mathrm{T}^{s-1}\}$ linealmente independientes sobre A. Por el inciso (3) del Lema 1.3.9, el campo residual de B es $\mathbb{F}_{q^s}$. Así, por el Lema 1.3.4, $|\mathrm{I}| = |\mathbb{F}_q|^{\ell_\mathrm{A}(\mathrm{I})}$ y $|\mathrm{IB}| = |\mathbb{F}_{q^s}|^{\ell_\mathrm{B}(\mathrm{IB})}$. Entonces $|\mathrm{IB}| = |\mathrm{I}|^s$. Combinando estas relaciones se obtiene $|\mathrm{IB}| = |\mathrm{I}|^s = (|\mathbb{F}_q|^{\ell_\mathrm{A}(\mathrm{I})})^s = |\mathbb{F}_{q^s}|^{\ell_\mathrm{B}(\mathrm{IB})} = q^{s\ell_\mathrm{A}(\mathrm{I})} = q^{s\ell_\mathrm{B}(\mathrm{IB})}$. Por lo tanto $\ell_\mathrm{B}(\mathrm{IB}) = \ell_\mathrm{A}(\mathrm{I})$. Para obtener la observación basta tomar $\mathrm{I} = \mathrm{A}$.
(2) El ideal maximal de A genera al ideal maximal de B, entonces $\{\alpha_1, \ldots, \alpha_l\}$ genera el ideal maximal de B. Resta verificar que el número mínimo de generadores de $\mathfrak{m}$ es el número mínimo de generadores de $\mathfrak{m}\mathrm{B}$, es decir $\mathrm{v_A}(\mathfrak{m}) = \mathrm{v_B}(\mathfrak{m}\mathrm{B})$. Por el Lema 1.1.3, se tiene $\mathfrak{m}^i\mathrm{B} = [\mathfrak{m}\mathrm{B}]^i$ y, por el inciso (1), se tiene $\ell_\mathrm{A}(\mathfrak{m}^i) = \ell_\mathrm{B}(\mathfrak{m}^i\mathrm{B}) = \ell_\mathrm{B}([\mathfrak{m}\mathrm{B}]^i)$, para cualquier i. Entonces $\mathrm{v_A}(\mathfrak{m}) = \ell_\mathrm{A}(\mathfrak{m}/\mathfrak{m}^2) = \ell_\mathrm{A}(\mathfrak{m}) - \ell_\mathrm{A}(\mathfrak{m}^2) = \ell_\mathrm{B}(\mathfrak{m}\mathrm{B}) - \ell_\mathrm{B}(\mathfrak{m}^2\mathrm{B}) = \ell_\mathrm{B}(\mathfrak{m}\mathrm{B}/\mathfrak{m}^2\mathrm{B}) = \mathrm{v_B}(\mathfrak{m}\mathrm{B})$.
(3) Por el inciso (2) del Lema 1.1.3, $[\mathrm{ann_A(I)I}]\mathrm{B} = [\mathrm{ann_A(I)B}][\mathrm{IB}] = \langle 0\rangle$, entonces $\mathrm{ann_A(I)B} \subseteq \mathrm{ann_B(IB)}$.
Por otra parte, sea $a_0 + a_1\mathrm{T} + \cdots + a_{s-1}\mathrm{T}^{s-1} \in \mathrm{ann_B(IB)}$ y $b \in \mathrm{I} \subset \mathrm{IB}$, entonces $(a_0 + a_1\mathrm{T} + \cdots + a_{s-1}\mathrm{T}^{s-1})b = a_0b + a_1b\mathrm{T} + \cdots + a_{s-1}b\mathrm{T}^{s-1} = 0$, así $a_i \in \mathrm{ann_A(I)}$, pues $\{1, \mathrm{T}, \ldots, \mathrm{T}^{s-1}\}$ es un conjunto linealmente independente sobre A, lo cual implica que $a_0 + a_1\mathrm{T} + \cdots + a_{s-1}\mathrm{T}^{s-1} \in (\mathrm{ann_A(I)})\mathrm{B}$. De donde se sigue que $\mathrm{ann_B(IB)} \subseteq \mathrm{ann_A(I)B}$. Para obtener la observación basta tomar $\mathrm{I} = \mathfrak{m}$.

Definición 1.3.6 *Sea p un número primo y $\mathrm{f} \in \mathbb{Z}_{p^k}[\mathrm{T}]$ es mónico básico irreducible de grado r. El anillo $\mathbb{Z}_{p^k}[\mathrm{T}]/\langle \mathrm{f}\rangle$ es llamado anillo de Galois y es denotado por* $\mathrm{GR}(p^k, r)$.

El siguiente es un resultado conocido de anillos locales finitos, su demostración se puede encontrar por ejemplo en [20].

Teorema 1.3.4 *Sea $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ un anillo local finito de característica p^k, $\{\alpha_1, \ldots, \alpha_r\}$ un conjunto mínimo de generadores del ideal maximal de* A *y $d = [\mathrm{k} : \mathbb{F}_p]$. Entonces existe un subanillo* S *de* A *tal que*

(*1*) $\mathrm{S} \cong \mathrm{GR}(p^k, d)$, S *es único y es el mayor anillo de Galois en* A.

(*2*) A *es una imagen de* $\mathrm{S}[\mathrm{X}_1, \ldots, \mathrm{X}_r]$, *es decir,* $\mathrm{A} = \mathrm{S}[\alpha_1, \ldots, \alpha_r]$.

LEMA 1.3.12 *Sea* I *un ideal del anillo* $\mathrm{GR}(p^k, d)[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ *tal que para cada* $i \in \{1, \ldots, n\}$, $\mathrm{X}_i^{k_i} \in \mathrm{I}$, *para algún* $k_i \in \mathbb{N}$. *Entonces el anillo* $\mathrm{GR}(p^k, d)[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathrm{I}$ *es local con ideal maximal* $\langle p, \mathrm{X}_1, \ldots, \mathrm{X}_n \rangle / \mathrm{I}$ *y campo residual* $\mathbb{F}_{p^d}$.

Demostración.
Sea J un ideal maximal de $\mathrm{GR}(p^k, d)[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ tal que $\mathrm{I} \subseteq \mathrm{J}$. Puesto que $\mathrm{X}_i^{k_i} \in \mathrm{J}$, $p^k = 0$ y J es ideal primo, entonces $\langle p, \mathrm{X}_1, \ldots, \mathrm{X}_n \rangle \subseteq \mathrm{J}$ y puesto que $\langle p, \mathrm{X}_1, \ldots, \mathrm{X}_n \rangle$ es maximal, $\langle p, \mathrm{X}_1, \ldots, \mathrm{X}_n \rangle = \mathrm{J}$. La primera afirmación se sigue del Teorema de correspondencia. Para la segunda parte, notar los siguiente

$$\big(\mathrm{GR}(p^k, d)[\mathrm{X}_1, \ldots, \mathrm{X}_n]/\mathrm{I}\big)/\big(\langle p, \mathrm{X}_1, \ldots, \mathrm{X}_n \rangle/\mathrm{I}\big) \cong \mathbb{F}_{p^d}.$$

1.3.3. Lema de Hensel

El anillo de polinomios con coeficientes en un anillo local finito no es de factorización única, por ejemplo, el elemento 0 se puede expresar como cualquier elemento nilpotente elevado al índice de nilpotencia del ideal maximal del anillo, por ello la importancia del Lema de Hensel el cual proporciona el método para obtener la factorización de un polinomio a partir de la factorización del polinomio obtenido al reducir sus coeficientes módulo el ideal maximal del anillo. En esta sección se demuestra el Lema de Hensel y se describen ejemplos de su uso.

LEMA 1.3.13 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito y* $\mathrm{f}(\mathrm{T}) = a_0 + \ldots + a_n \mathrm{T}^n \in \mathrm{A}[\mathrm{T}]$ *un polinomio. Las siguientes afirmaciones son equivalentes:*

(*1*) f(T) *es unidad;*

(*2*) $\tilde{\mathrm{f}}$ *es unidad;*

(*3*) a_0 *es unidad y* $a_1, \ldots, a_n$ *son nilpotentes.*

Demostración.
(1) $\Rightarrow$ (2) Si $\mathrm{fg} = 1$, entonces $\tilde{\mathrm{f}}\tilde{\mathrm{g}} = \tilde{1}$.
(2) $\Rightarrow$ (3) Puesto que $\tilde{\mathrm{f}}$ es unidad, entonces $\pi(a_0) \neq 0$ y $\pi(a_i) = 0$, de donde se sigue la afirmación.

(3) $\Rightarrow$ (1) La afirmación se sigue del hecho de que si u es unidad y m es nilpotente con nilpotencia t, entonces $u + \mathrm{m}$ es unidad y su inverso está dado por $(u+\mathrm{m})^{-1} = \frac{1}{u} - \frac{\mathrm{m}}{u^2} + \frac{\mathrm{m}^2}{u^3} - \frac{\mathrm{m}^3}{u^4} + \ldots + (-1)^{t-1}\frac{\mathrm{m}^{t-1}}{u^t}$.

EJEMPLO 1.3.3 *En* $\mathbb{Z}_8[\mathrm{T}]$ *se tiene*

$$[1 + 2(3\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3)]^{-1} = 1 - 2(3\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3) + 4(3\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3)^2 =$$

$$1 + 6(3\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3) + 4(9\mathrm{T}^2 + 6\mathrm{T}^3 + 13\mathrm{T}^4 + 4\mathrm{T}^5 + 4\mathrm{T}^6) = 1 + 2(\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3 + 2\mathrm{T}^4).$$

El siguiente resultado no estará acompañado de una demostración, la cual se puede encontrar por ejemplo en [20].

LEMA 1.3.14 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito,* $\mathrm{f}, \mathrm{g} \in \mathrm{A}[\mathrm{T}]$ *polinomios. Entonces* f *y* g *son coprimos sí y sólo si* $\tilde{\mathrm{f}}$ *y* $\tilde{\mathrm{g}}$ *son coprimos en* $\mathrm{k}[\mathrm{T}]$.

LEMA 1.3.15 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito,* $\mathrm{f}, \mathrm{g}, \mathrm{h} \in \mathrm{A}[\mathrm{T}]$, $v \in \mathfrak{m}[\mathrm{T}]$. *Supóngase que* $\mathrm{f} = \mathrm{gh} - v$ *y que* g *y* h *son coprimos. Si* $\mathrm{s}_1, \mathrm{s}_2 \in \mathrm{A}[\mathrm{T}]$ *son tales que* $\mathrm{gs}_1 + \mathrm{hs}_2 = 1$, *entonces los polinomios* $\mathrm{g}_1 = \mathrm{g} - \mathrm{s}_2 v$ *y* $\mathrm{h}_1 = \mathrm{h} - \mathrm{s}_1 v$ *satisfacen:*

(*1*) $\tilde{\mathrm{g}}_1 = \tilde{\mathrm{g}}$ *y* $\tilde{\mathrm{h}}_1 = \tilde{\mathrm{h}}$;

(*2*) g_1 *y* h_1 *son coprimos;*

(*3*) $\mathrm{f} = \mathrm{g}_1\mathrm{h}_1 - \mathrm{s}_1\mathrm{s}_2 v^2$.

Demostración.
(1) $\tilde{\mathrm{g}}_1 = \tilde{\mathrm{g}} - \tilde{\mathrm{s}}_2\tilde{v} = \tilde{\mathrm{g}}$, pues $v \in \mathfrak{m}[\mathrm{T}]$. De forma similar se obtiene $\tilde{\mathrm{h}}_1 = \tilde{\mathrm{h}}$.
(2) Se sigue del Lema 1.3.14 y del inciso (1).
(3) Se sigue de la relación:

$$\mathrm{f} = \mathrm{gh} - v = \big[(\ \mathrm{g} - \mathrm{s}_2 v\ ) + \mathrm{s}_2 v\big]\big[(\ \mathrm{h} - \mathrm{s}_1 v\ ) + \mathrm{s}_1 v\big] - v =$$

$$[\mathrm{g} - \mathrm{s}_2 v][\mathrm{h} - \mathrm{s}_1 v] + [\mathrm{g} - \mathrm{s}_2 v]\mathrm{s}_1 v + [\mathrm{h} - \mathrm{s}_1 v]\mathrm{s}_2 v + \mathrm{s}_1\mathrm{s}_2 v^2 - v =$$

$$\mathrm{g}_1\mathrm{h}_1 + \mathrm{gs}_1 v - \mathrm{s}_1\mathrm{s}_2 v^2 + \mathrm{hs}_2 v - \mathrm{s}_1\mathrm{s}_2 v^2 + \mathrm{s}_1\mathrm{s}_2 v^2 - v =$$

$$\mathrm{g}_1\mathrm{h}_1 + [\mathrm{gs}_1 + \mathrm{hs}_2]v - \mathrm{s}_1\mathrm{s}_2 v^2 - v = \mathrm{g}_1\mathrm{h}_1 - \mathrm{s}_1\mathrm{s}_2 v^2 + v - v = \mathrm{g}_1\mathrm{h}_1 - \mathrm{s}_1\mathrm{s}_2 v^2.$$

COROLARIO 1.3.2 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito y* $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$. *Supóngase que* $\tilde{\mathrm{f}} = \tilde{\mathrm{g}}\tilde{\mathrm{h}}$, *donde* $\tilde{\mathrm{g}}, \tilde{\mathrm{h}} \in \mathrm{k}[\mathrm{T}]$ *son polinomios coprimos. Entonces existen* $\mathrm{G}, \mathrm{H} \in \mathrm{A}[\mathrm{T}]$ *tales que*

(*1*) $\tilde{\mathrm{G}} = \tilde{\mathrm{g}}$ *y* $\tilde{\mathrm{H}} = \tilde{\mathrm{h}}$;

(*2*) G *y* H *son coprimos;*

(*3*) $\mathrm{f} = \mathrm{GH}$.

Demostración.
Puesto que $\tilde{\mathrm{f}} = \tilde{\mathrm{g}}\tilde{\mathrm{h}}$ y $\ker(\tilde{\ }) = \mathfrak{m}[\mathrm{T}]$, sea $v \in \mathfrak{m}[\mathrm{T}]$ tal que $\mathrm{f} = \mathrm{gh} + v$. Por el Lema 1.3.14, g y h son coprimos. Así, por el Lema 1.3.15, existen $\mathrm{g}_1, \mathrm{h}_1, \mathrm{s}_1 \in \mathrm{A}[\mathrm{T}]$ tales que

(1) $\tilde{\mathrm{g}}_1 = \tilde{\mathrm{g}}$ y $\tilde{\mathrm{h}}_1 = \tilde{\mathrm{h}}$;

(2) g_1 y h_1 son coprimos;

(3) $\mathrm{f} = \mathrm{g}_1\mathrm{h}_1 + \mathrm{s}_1 v^2$.

Continuando el proceso, por el Lema 1.3.15, existen $\mathrm{g}_k, \mathrm{h}_k, \mathrm{s}_k \in \mathrm{A}[\mathrm{T}]$ tales que

(1) $\tilde{\mathrm{g}_k} = \tilde{\mathrm{g}}_{k-1} = \tilde{\mathrm{g}}$ y $\tilde{\mathrm{h}_k} = \tilde{\mathrm{h}}_{k-1} = \tilde{\mathrm{h}}$;

(2) g_k y h_k son coprimos;

(3) $\mathrm{f} = \mathrm{g}_k\mathrm{h}_k + \mathrm{s}_k v^{2^k}$.

Sea t la nilpotencia de $\mathfrak{m}$ y $r \in \mathbb{N}$ tal que $t < 2^r$. Puesto que $v^{2^r} \in \mathfrak{m}^{2^r} = \langle 0 \rangle$, se sigue que

(1) $\tilde{\mathrm{g}}_r = \tilde{\mathrm{g}}$ y $\tilde{\mathrm{h}}_r = \tilde{\mathrm{h}}$;

(2) g_r y h_r son coprimos;

(3) $\mathrm{f} = \mathrm{g}_r\mathrm{h}_r$.

Por lo tanto, tomando $\mathrm{G} = \mathrm{g}_r$ y $\mathrm{H} = \mathrm{h}_r$ se tiene la afirmación.

El siguiente resultado es el caso particular de nilpotencia 3 del Corolario 1.3.2.

LEMA 1.3.16 *Sean* $(A, \mathfrak{m}, k)$ *un anillo local finito cuyo ideal maximal tiene índice de nilpotencia* 3, $f, g, h \in A[T]$ *y* $v \in \mathfrak{m}[T]$. *Supóngase que* g *y* h *son coprimos,* $f = gh - v$ *y sean* $s_1, s_2 \in A[T]$ *tales que* $gs_1 + hs_2 = 1$. *Entonces los polinomios*

$$G = g - s_2v - s_1s_2^2v^2 \qquad y \qquad H = h - s_1v - s_1^2s_2v^2$$

satisfacen:

(*1*) $\tilde{G} = \tilde{g}$ *y* $\tilde{H} = \tilde{h}$;

(*2*) G *y* H *son coprimos;*

(*3*) $f = GH$.

Demostración.
Por el Lema 1.3.15, los polinomios $g_1 = g - s_2v$ y $h_1 = h - s_1v$ satisfacen:

(1) $\tilde{g}_1 = \tilde{g}$ y $\tilde{h}_1 = \tilde{h}$;

(2) g_1 y h_1 son coprimos; de hecho

$$g_1(s_1 + 2s_1^2s_2v + 4s_1^3s_2^2v^2) + h_1(s_2 + 2s_1s_2^2v + 4s_1^2s_2^3v^2) = 1,$$

esto se obtiene de las relaciones:

$$g_1s_1 + h_1s_2 = (g - s_2v)s_1 + (h - s_1v)s_2 = 1 - 2s_1s_2v$$

y

$$(1 - 2s_1s_2v)^{-1} = 1 + 2s_1s_2v + 4s_1^2s_2^2v^2$$

(3) $f = g_1h_1 - s_1s_2v^2$.

Nuevamente, usando el Lema 1.3.15 y el hecho que $\mathfrak{m}$ tiene índice de nilpotencia 3, los polinomios $G = g_1 - (s_2 + 2s_1s_2^2v + 4s_1^2s_2^3v^2)(s_1s_2v^2) = g - s_2v - s_1s_2^2v^2$ y $H = h_1 - (s_1s_2v^2)(s_1 + 2s_1^2s_2v + 4s_1^3s_2^2v^2) = h - s_1v - s_1^2s_2v^2$ satisfacen:

(1) $\tilde{G} = \tilde{g}_1 = \tilde{g}$ y $\tilde{H} = \tilde{h}_1 = \tilde{h}$;

(2) G y H son coprimos;

(3) $f = GH - (s_1 + 2s_1^2s_2v + 4s_1^3s_2^2v^2)(s_2 + 2s_1s_2^2v + 4s_1^2s_2^3v^2)(s_1s_2v^2)^2 = GH$.

TEOREMA 1.3.5 (**Lema de Hensel. [20]**)
Sea $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito y* $\mathrm{f}(\mathrm{T})$ *un polinomio con coeficientes en* A. *Supóngase que* $\tilde{\mathrm{f}} = \tilde{\mathrm{g}}_1 \cdots \tilde{\mathrm{g}}_n$, *donde* $\tilde{\mathrm{g}}_1, \ldots, \tilde{\mathrm{g}}_n \in \mathrm{k}[\mathrm{T}]$ *son coprimos a pares. Entonces existen* $\mathrm{f}_1, \ldots, \mathrm{f}_n \in \mathrm{A}[\mathrm{T}]$ *tales que:*

(*1*) $\mathrm{f}_1, \ldots, \mathrm{f}_n$ *son coprimos a pares;*

(*2*) $\tilde{\mathrm{f}}_i = \tilde{\mathrm{g}}_i$, $1 \leq i \leq n$;

(*3*) $\mathrm{f} = \mathrm{f}_1 \cdots \mathrm{f}_n$

Demostración.
La prueba será por inducción sobre n. El caso $n = 2$ es la conclusión del Corolario 1.3.2. Supongamos cierto el resultado para $n - 1 \geq 2$. Por el Lema 1.1.4, $\tilde{\mathrm{g}}_1\tilde{\mathrm{g}}_2 \cdots \tilde{\mathrm{g}}_{n-1}, \tilde{\mathrm{g}}_n$ son coprimos. Así, por el caso $n = 2$, existen $\mathrm{F}, \mathrm{f}_n \in \mathrm{A}[\mathrm{T}]$ tales que $\tilde{\mathrm{F}} = \tilde{\mathrm{g}}_1\tilde{\mathrm{g}}_2 \cdots \tilde{\mathrm{g}}_{n-1}$ y $\tilde{\mathrm{f}}_n = \tilde{\mathrm{g}}_n$, F y f_n son coprimos y $\mathrm{f} = \mathrm{F}\mathrm{f}_n$. Por otra parte, por hipótesis de induccción, aplicada a F, existen $\mathrm{f}_1, \ldots, \mathrm{f}_{n-1} \in \mathrm{A}[\mathrm{T}]$ tales que $\tilde{\mathrm{f}}_i = \tilde{\mathrm{g}}_i$, $1 \leq i \leq n-1$, $\mathrm{f}_1, \ldots, \mathrm{f}_{n-1}$ son coprimos a pares y $\mathrm{F} = \mathrm{f}_1 \cdots \mathrm{f}_{n-1}$.
Finalmente, $\mathrm{f} = \mathrm{F}\mathrm{f}_n = \mathrm{f}_1 \cdots \mathrm{f}_{n-1}\mathrm{f}_n$. Puesto que $\mathrm{f}_1 \cdots \mathrm{f}_{n-1}$ y f_n son coprimos, se sigue, por el Lema 1.1.4, que $\mathrm{f}_1, \ldots, \mathrm{f}_{n-1}, \mathrm{f}_n$ son coprimos a pares.

LEMA 1.3.17 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito y* $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio mónico con ceros distintos en alguna cerradura algebraica de* $\mathbb{F}_q$, *entonces existen únicos polinomios básicos irreducibles,* $\mathrm{f}_1, \ldots, \mathrm{f}_r \in \mathrm{A}[\mathrm{T}]$, *con las siguientes propiedades:*

(*1*) $\mathrm{f}_1, \ldots, \mathrm{f}_n$ *son coprimos a pares;*

(*2*) $\mathrm{f} = \mathrm{f}_1 \cdots \mathrm{f}_n$

En particular, si γ *es una unidad de* A *y* n *un entero positivo primo relativo con* q, *entonces existen únicos polinomios básicos irreducibles coprimos a pares tales que*

$$\mathrm{T}^n - \gamma = \mathrm{f}_1 \ldots \mathrm{f}_r$$

Demostración.
Sea $\tilde{\mathrm{f}} = \tilde{\mathrm{G}}_1 \cdots \tilde{\mathrm{G}}_n$ la factorización de $\tilde{\mathrm{f}}$ como producto de polinomios irreducibles en $\mathbb{F}_q[\mathrm{T}]$. Por el Lema de Hensel, existen polinomios $\mathrm{F}_1, \ldots, \mathrm{F}_n \in \mathrm{A}[\mathrm{T}]$ tales que:

(1) $\mathrm{F}_1, \ldots, \mathrm{F}_n$ son coprimos a pares;

(2) $\tilde{\mathrm{F}}_i = \tilde{\mathrm{G}}_i$, $1 \leq i \leq n$;

(3) $\mathrm{f} = \mathrm{F}_1 \cdots \mathrm{F}_n$.

Entonces los polinomios $\mathrm{F}_1, \ldots, \mathrm{F}_n$ son básicos irreducibles y por lo tanto polinomios regulares. Por la Proposición 1.3.2, $\mathrm{F}_i = u_i \mathrm{f}_i$, para $1 \leq i \leq n$ y donde u_i es una unidad de A[T] y f_i es polinomio mónico, entonces:

(1) $\mathrm{f}_1, \ldots, \mathrm{f}_n$ son coprimos a pares;

(2) $\tilde{\mathrm{f}}_i = \tilde{u}_i^{-1} \tilde{\mathrm{F}}_i = \tilde{u}_i^{-1} \tilde{\mathrm{G}}_i$ es asociado a $\tilde{\mathrm{G}}_i$, $1 \leq i \leq n$;

(3) $\mathrm{f} = u_1 \cdots u_n \mathrm{f}_1 \cdots \mathrm{f}_n$

Así, los polinomios $\mathrm{f}_1, \ldots, \mathrm{f}_n$ son básicos irreducibles y puesto que f y $\mathrm{f}_1, \ldots, \mathrm{f}_n$ son mónicos entonces $u_1 \cdots u_n = 1$ y se tiene la afirmación. La última afirmación se sigue del hecho de que si n es primo relativo con q, entonces las raices de $\mathrm{T}^n - \tilde{\gamma}$ son simples.

En los siguientes dos ejemplos se aplica el método de la prueba de los Lemas 1.3.15, 1.3.16 y el Teorema 1.3.5, y sus conclusiones se usarán más adelante.

Ejemplo 1.3.4 *Sea* A *un anillo local finito en el que todo elemento nilpotente tiene índice de nilpotencia* 2 *y* γ *una unidad de* A. *Supóngase que la característica de* A *es* 2 *y que su campo residual es* $\mathbb{F}_2$. *Entonces*

$$\mathrm{T}^7 - \lambda = (\mathrm{T} + \lambda)(\mathrm{T}^3 + \lambda \mathrm{T}^2 + \lambda)(\mathrm{T}^3 + \mathrm{T} + \lambda).$$

Nótese que $\mathbb{F}_2 \subseteq$ A *y que las unidades de* A *son de la forma* $1 + \mathrm{m}$, *donde* m *es nilpotente.*
Puesto que $\mathrm{T}^7 - 1 = (\mathrm{T} - 1)(\mathrm{T}^3 + \mathrm{T}^2 + 1)(\mathrm{T}^3 + \mathrm{T} + 1) = \mathrm{gh}$ *en* $\mathbb{F}_2[\mathrm{T}]$, *donde* $\mathrm{g} = \mathrm{T}^4 + \mathrm{T}^2 + \mathrm{T} + 1$ *y* $\mathrm{h} = \mathrm{T}^3 + \mathrm{T} + 1$, *entonces* $\mathrm{T}^7 - \lambda = \mathrm{T}^7 - 1 - \mathrm{m} = \mathrm{gh} - \mathrm{m}$.
Por el Lema 1.3.15 y el hecho de que $\mathrm{g} + \mathrm{hT} = 1$, *se sigue que los polinomios* $\mathrm{g}_1 = \mathrm{g} + \mathrm{Tm} = \mathrm{T}^4 + \mathrm{T}^2 + (1 + \mathrm{m})\mathrm{T} + 1$ *y* $\mathrm{h}_1 = \mathrm{h} + \mathrm{m} = \mathrm{T}^3 + \mathrm{T} + 1 + \mathrm{m}$ *satisfacen:*

(*1*) $\tilde{\mathrm{g}}_1 = \tilde{\mathrm{g}} = \mathrm{T}^4 + \mathrm{T}^2 + \mathrm{T} + 1$ *y* $\tilde{\mathrm{h}}_1 = \tilde{\mathrm{h}} = \mathrm{T}^3 + \mathrm{T} + 1$;

(*2*) g_1 *y* h_1 *son coprimos;*

(*3*) $\mathrm{T}^7 - \lambda = \mathrm{g}_1 \mathrm{h}_1 + \mathrm{s}_1 \mathrm{s}_2 \mathrm{m}^2 = \mathrm{g}_1 \mathrm{h}_1$.

Obsérvese que en esta factorización de $\mathrm{T}^7 - \lambda$ *solo el factor* $\mathrm{T}^3 + \mathrm{T} + 1 + \mathrm{m}$ *es básico irreducible. Pasamos ahora a la factorización de* $\mathrm{T}^4 + \mathrm{T}^2 + (1 + \mathrm{m})\mathrm{T} + 1$.
Con la notación del Lema 1.3.15. Sea $\mathrm{g} = \mathrm{T} - 1$ *y* $\mathrm{h} = \mathrm{T}^3 + \mathrm{T}^2 + 1 + \mathrm{m}$, *al dividir* $\mathrm{T}^4 + \mathrm{T}^2 + (1 + \mathrm{m})\mathrm{T} + 1$ *por* $\mathrm{g} = \mathrm{T} - 1$ *se obtiene* $\mathrm{T}^4 + \mathrm{T}^2 + (1 + \mathrm{m})\mathrm{T} + 1 = \mathrm{gh} + \mathrm{m}$. *Además, al dividir* h *por* g *se obtiene* $\mathrm{h} = \mathrm{gT}^2 + 1 + \mathrm{m}$. *De donde se sigue que* $\mathrm{h}(1 + \mathrm{m}) + \mathrm{g}(1 + \mathrm{m})\mathrm{T}^2 = 1$. *En consecuencia, por el Lema 1.3.15, los polinomios* $\mathrm{g}_1 = \mathrm{g} + \mathrm{m}(1 + \mathrm{m}) = \mathrm{T} - 1 + \mathrm{m}$ *y* $\mathrm{h}_1 = \mathrm{h} + \mathrm{m}[(1 + \mathrm{m})\mathrm{T}^2] = \mathrm{T}^3 + \mathrm{T}^2 + 1 + \mathrm{m} + \mathrm{mT}^2 = \mathrm{T}^3 + (1 + \mathrm{m})\mathrm{T}^2 + 1 + \mathrm{m}$ *satisfacen:*

(*1*) $\tilde{\mathrm{g}}_1 = \tilde{\mathrm{g}} = \mathrm{T} - 1$ *y* $\tilde{\mathrm{h}}_1 = \tilde{\mathrm{h}} = \mathrm{T}^3 + \mathrm{T}^2 + 1$;

(*2*) g_1 *y* h_1 *son coprimos;*

(*3*) $\mathrm{T}^4 + \mathrm{T}^2 + (1 + \mathrm{m})\mathrm{T} + 1 = \mathrm{g}_1\mathrm{h}_1 + \mathrm{s}_1\mathrm{s}_2\mathrm{m}^2 = \mathrm{g}_1\mathrm{h}_1$.

De donde se obtiene la afirmación.

Ejemplos de anillos con las propiedades mencionadas en el Ejemplo 1.3.4 incluyen a los anillos $\mathbb{F}_2[\mathrm{X}_1, \ldots, \mathrm{X}_k]/\langle \mathrm{X}_1^2, \ldots, \mathrm{X}_k^2, \mathrm{X}_i\mathrm{X}_j - \mathrm{X}_1\mathrm{X}_2 : \ i < j, \ (i, j) \neq (1, 2)\rangle$ y $\mathbb{F}_2[\mathrm{X}_1, \ldots, \mathrm{X}_k]/\langle \mathrm{X}_1^2, \ldots, \mathrm{X}_k^2\rangle$.

Ejemplo 1.3.5 *Sea* $\mathrm{A} = \mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X}\rangle$, *el anillo local del ejemplo 1.3.1.*
Sea $\mathrm{m} = 2a + 4b + c\mathrm{x}$, *con* $a, b, c \in \{0, 1\}$. *Entonces*

$$\mathrm{T}^7 - (1 + \mathrm{m}) = \mathrm{f}_1\mathrm{f}_2\mathrm{f}_3$$

donde
$\mathrm{f}_1 = \mathrm{T}^3 + (6 + 4a)\mathrm{T}^2 + (5 + 4c)\mathrm{T} + 7 + 7\mathrm{m}$,
$\mathrm{f}_2 = \mathrm{m}^2\mathrm{T}^2 + \mathrm{T} + 7 + \mathrm{m}$,
$\mathrm{f}_3 = \mathrm{m}^2\mathrm{T}^4 + \mathrm{T}^3 + (3 + 4a + 3\mathrm{m})\mathrm{T}^2 + (2 + \mathrm{m}^2)\mathrm{T} + 7 + \mathrm{m}^2 + 3\mathrm{m}$.
Se tiene $\mathrm{T}^7 - 1 = \mathrm{gh}$ *en* $\mathbb{Z}_8[\mathrm{T}]$ *y* $\mathrm{T}^7 - 1 - \mathrm{m} = \mathrm{gh} - \mathrm{m}$ *en* $\mathrm{A}[\mathrm{T}]$, *donde:*
$\mathrm{g} = \mathrm{T}^4 + 2\mathrm{T}^3 + 7\mathrm{T}^2 + 5\mathrm{T} + 1$ *y*
$\mathrm{h} = \mathrm{T}^3 + 6\mathrm{T}^2 + 5\mathrm{T} + 7$.
De las relaciones

$$\mathrm{g} = \mathrm{Th} + 1 + 2(3\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3)$$

y

$$[1 + 2(3\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3)]^{-1} = 1 + 2(\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3 + 2\mathrm{T}^4)$$

se sigue que $\mathrm{gs}_1 + \mathrm{hs}_2 = 1$, *donde* $\mathrm{s}_1 = 1 + 2(\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3 + 2\mathrm{T}^4)$ *y* $\mathrm{s}_2 = 7\mathrm{Ts}_1$.
Usando el Lema 1.3.16 y las relaciones:

$$\mathrm{m}^2 = 4(a + c),$$

$$\mathrm{s}_1\mathrm{m} = [1 + 2(\mathrm{T} + \mathrm{T}^2 + 2\mathrm{T}^3 + 2\mathrm{T}^4)][2a + 4b + c\mathrm{x}] = \mathrm{m} + 4a(\mathrm{T} + \mathrm{T}^2),$$

$$\mathrm{s}_1^3\mathrm{m}^2 = \mathrm{s}_1(\mathrm{s}_1\mathrm{m})^2 = \mathrm{s}_1[\mathrm{m} + 4a(\mathrm{T} + \mathrm{T}^2)]^2 = \mathrm{s}_1\mathrm{m}^2 = \mathrm{m}^2 = 4(a + c),$$

los siguientes polinomios:

$$\mathrm{G} = \mathrm{g} - \mathrm{s}_2\mathrm{m} - \mathrm{s}_1\mathrm{s}_2^2\mathrm{m}^2 = \mathrm{g} - 7\mathrm{mTs}_1 - \mathrm{s}_1(7\mathrm{Ts}_1)^2\mathrm{m}^2 = \mathrm{g} + \mathrm{mTs}_1 + 7\mathrm{T}^2\mathrm{s}_1^3\mathrm{m}^2 =$$

$$\mathrm{T}^4 + 2\mathrm{T}^3 + 7\mathrm{T}^2 + 5\mathrm{T} + 1 + \mathrm{T}[\mathrm{m} + 4a(\mathrm{T} + \mathrm{T}^2)] + 7\mathrm{T}^2[4(a + c)] =$$

$$\mathrm{T}^4 + (2 + 4a)\mathrm{T}^3 + (7 + 4c)\mathrm{T}^2 + (5 + \mathrm{m})\mathrm{T} + 1$$

y

$$\mathrm{H} = \mathrm{h} - \mathrm{s}_1\mathrm{m} - \mathrm{s}_1^2\mathrm{s}_2\mathrm{m}^2 = \mathrm{h} - \mathrm{ms}_1 - \mathrm{s}_1^2(7\mathrm{Ts}_1)\mathrm{m}^2 = \mathrm{h} + 7\mathrm{ms}_1 + \mathrm{s}_1^3\mathrm{Tm}^2 =$$

$$\mathrm{T}^3 + 6\mathrm{T}^2 + 5\mathrm{T} + 7 + 7[\mathrm{m} + 4a(\mathrm{T} + \mathrm{T}^2)] + \mathrm{T}[4(a + c)] =$$

$$\mathrm{T}^3 + (6 + 4a)\mathrm{T}^2 + (5 + 4c)\mathrm{T} + 7 + 7\mathrm{m}$$

satisfacen:

(*1*) $\tilde{\mathrm{G}} = \tilde{\mathrm{g}} = \mathrm{T}^4 + \mathrm{T}^2 + \mathrm{T} + 1$ *y* $\tilde{\mathrm{H}} = \tilde{\mathrm{h}} = \mathrm{T}^3 + \mathrm{T} + 1$*;*

(*2*) G *y* H *son coprimos;*

(*3*) $\mathrm{T}^7 - (1 + \mathrm{m}) = \mathrm{GH}$.

Notar que el polinomio $\mathrm{T}^3 + (6 + 4a)\mathrm{T}^2 + (5 + 4c)\mathrm{T} + 7 + 7\mathrm{m}$ *es básico irreducible.*
Pasamos ahora a la factorización de $\mathrm{T}^4 + (2 + 4a)\mathrm{T}^3 + (7 + 4c)\mathrm{T}^2 + (5 + \mathrm{m})\mathrm{T} + 1$.
Se usa la notación del Lema 1.3.15, sean:
$\mathrm{f} = \mathrm{T}^4 + (2 + 4a)\mathrm{T}^3 + (7 + 4c)\mathrm{T}^2 + (5 + \mathrm{m})\mathrm{T} + 1$,
$\mathrm{g} = \mathrm{T} - 1$ *y*
$\mathrm{h} = \mathrm{T}^3 + (3 + 4a)\mathrm{T}^2 + (2 + \mathrm{m}^2)\mathrm{T} + 7 + \mathrm{m}^2 + \mathrm{m}$.
Al dividir f *por* g *se obtiene* $\mathrm{f} = \mathrm{gh} + \mathrm{m}^2 + \mathrm{m} = \mathrm{gh} - (\mathrm{m}^2 + 7\mathrm{m})$.
Al dividir h *por* g *se obtiene* $\mathrm{h} = \mathrm{g}[\mathrm{T}^2 + (4 + 4a)\mathrm{T} + 6 + 4c] + 5 + 4a + \mathrm{m}$ *y dado que* $(5 + 4a + \mathrm{m})^{-1} = 5 + 4c - \mathrm{m}$*, se sigue que*

$$\mathrm{g}7[5 + 4c - \mathrm{m}][\mathrm{T}^2 + (4 + 4a)\mathrm{T} + 6 + 4c] + \mathrm{h}[5 + 4c - \mathrm{m}] =$$

$$\mathrm{g}[(3+4c+\mathrm{m})\mathrm{T}^2+(4+4a)\mathrm{T}+2+4c+2\mathrm{m}]+\mathrm{h}[5+4c-\mathrm{m}]=1.$$

Ahora sean:
$\mathrm{s}_1=(3+4c+\mathrm{m})\mathrm{T}^2+(4+4a)\mathrm{T}+2+4c+2\mathrm{m}$,
$\mathrm{s}_2=5+4c-\mathrm{m}$ *y*
$\mathrm{v}=\mathrm{m}^2+7\mathrm{m}$.
Usando el Lema 1.3.15 y las relaciones:

$$\mathrm{s}_1\mathrm{v}=[(3+4c+\mathrm{m})\mathrm{T}^2+(4+4a)\mathrm{T}+2+4c+2\mathrm{m}][\mathrm{m}^2+7\mathrm{m}]=\mathrm{mT}^2+2\mathrm{m},$$

$$\mathrm{s}_2\mathrm{v}=[5+4c-\mathrm{m}][\mathrm{m}^2+7\mathrm{m}]=3\mathrm{m},\quad \mathrm{s}_1\mathrm{s}_2\mathrm{v}^2=(\mathrm{s}_1\mathrm{v})(\mathrm{s}_2\mathrm{v})=[\mathrm{mT}^2+2\mathrm{m}][3\mathrm{m}]=\mathrm{m}^2\mathrm{T}^2,$$

$$\mathrm{s}_1^2\mathrm{s}_2\mathrm{v}^2=\mathrm{s}_1[\mathrm{s}_1\mathrm{s}_2\mathrm{v}^2]=[(3+4c+\mathrm{m})\mathrm{T}^2+(4+4a)\mathrm{T}+2+4c+2\mathrm{m}][\mathrm{m}^2\mathrm{T}^2]=\mathrm{m}^2\mathrm{T}^4,$$

$$\mathrm{s}_1\mathrm{s}_2^2\mathrm{v}^2=\mathrm{s}_2[\mathrm{s}_1\mathrm{s}_2\mathrm{v}^2]=[5+4c-\mathrm{m}][\mathrm{m}^2\mathrm{T}^2]=\mathrm{m}^2\mathrm{T}^2.$$

Los siguientes polinomios

$$\mathrm{G}=\mathrm{g}-\mathrm{s}_2\mathrm{v}-\mathrm{s}_1\mathrm{s}_2^2\mathrm{v}^2=\mathrm{T}-1-[3\mathrm{m}]-[\mathrm{m}^2\mathrm{T}^2]=\mathrm{m}^2\mathrm{T}^2+\mathrm{T}-1+\mathrm{m},$$

$$\mathrm{H}=\mathrm{h}-\mathrm{s}_1\mathrm{v}-\mathrm{s}_1^2\mathrm{s}_2\mathrm{v}^2=\mathrm{T}^3+(3+4a)\mathrm{T}^2+(2+\mathrm{m}^2)\mathrm{T}+7+\mathrm{m}^2+\mathrm{m}-[\mathrm{mT}^2+2\mathrm{m}]-[\mathrm{m}^2\mathrm{T}^4]=$$
$$\mathrm{m}^2\mathrm{T}^4+\mathrm{T}^3+(3+4a+3\mathrm{m})\mathrm{T}^2+(2+\mathrm{m}^2)\mathrm{T}+7+\mathrm{m}^2+3\mathrm{m},$$

satisfacen:

(*1*) $\tilde{\mathrm{G}}=\tilde{\mathrm{g}}=\mathrm{T}-1$ *y* $\tilde{\mathrm{H}}=\tilde{\mathrm{h}}=\mathrm{T}^3+\mathrm{T}^2+1$*;*

(*2*) G *y* H *son coprimos;*

(*3*) $\mathrm{T}^4+(2+4a)\mathrm{T}^3+(7+4c)\mathrm{T}^2+(5+\mathrm{m})\mathrm{T}+1=\mathrm{GH}$.

De donde se obtiene la afirmación.

Capítulo 2

Anillos locales finitos de Frobenius no de cadena y de longitud 4

En la mayoría de los trabajos en teoría de códigos, los alfabetos para los códigos son anillos finitos de Frobenius, pues tomando un anillo A de esta naturaleza como alfabeto de un código las identidades de Macwilliams se satisfacen, también las relaciones $(\mathrm{C}^{\perp})^{\perp} = \mathrm{C}$ y $|\mathrm{C}^{\perp}||\mathrm{C}| = |\mathrm{A}^{n}|$, (ver [31]), donde C es un código de longitud n y $()^{\perp}$ denota el dual con respecto al producto interno canónico sobre A.
Hay varias definiciones equivalentes para anillo de Frobenius, las cuales incluyen el caso no conmutativo y cuando el anillo no es finito, (ver [13], [16],[22], [23]). En este trabajo usamos la caracterización de anillo finito de Frobenius dada en [13], consideramos solo el caso conmutativo y concluimos que los anillos locales conmutativos de Frobenius son aquellos que tienen un único ideal minimal.
Puesto que un anillo conmutativo finito de Frobenius se descompone en anillos conmutativos locales de Frobenius, entonces todo se reduce al estudio de anillos locales finitos de Frobenius. Un anillo local finito es de Frobenius si el anulador de su ideal maximal es un ideal simple (ver Definición 2.1.2) y un anillo de cadena es un anillo cuya retícula de ideales es una cadena con la inclusión de conjuntos.

Por otra parte, ver [20], si p es un número primo, es sabido que salvo isomorfismo existe únicamente un anillo local con p elementos, el cual es el campo finito: 1) $\mathbb{F}_p$.
Los anillos locales con p^2 elementos son:
2) $\mathbb{F}_{p^2}$,
3) $\mathbb{Z}_{p^2}$ y

4) $\mathbb{F}_p[\mathrm{X}]/\langle \mathrm{X}^2\rangle$.
Si p es un número primo impar, los anillos locales con p^3 elementos son:
5) $\mathbb{F}_{p^3}$,
6) $\mathbb{Z}_{p^3}$,
7) $\mathbb{F}_p[\mathrm{X}]/\langle \mathrm{X}^3\rangle$,
8) $\mathbb{Z}_{p^2}[\mathrm{X}]/\langle \mathrm{X}^2 - p, p\mathrm{X}\rangle$,
9) $\mathbb{Z}_{p^2}[\mathrm{X}]/\langle \mathrm{X}^2 - \zeta p, p\mathrm{X}\rangle$, donde $\tilde{\zeta}$ es un elemento primitivo de $\mathbb{F}_p$,
10) $\mathbb{F}_p[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X},\mathrm{Y}\rangle^2$,
11) $\mathbb{Z}_{p^2}[\mathrm{X}]/\langle \mathrm{X}^2, p\mathrm{X}\rangle$.
Si $p = 2$, los anillos locales con 2^3 elementos son:
12) $\mathbb{F}_{2^3}$,
13) $\mathbb{Z}_{2^3}$,
14) $\mathbb{F}_2[\mathrm{X}]/\langle \mathrm{X}^3\rangle$,
15) $\mathbb{Z}_{2^2}[\mathrm{X}]/\langle \mathrm{X}^2 - 2, 2\mathrm{X}\rangle$,
16) $[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X},\mathrm{Y}\rangle^2$ y
17) $\mathbb{Z}_{2^2}[\mathrm{X}]/\langle \mathrm{X}^2, 2\mathrm{X}\rangle$.
Es fácil verificar que los anillos 10), 11), 16) y 17) no son anillos de Frobenius y el resto de los anillos mencionados son de cadena.
Los anillos locales de Frobenius no de cadena con 2^4 elementos recientemente descritos en [21], son:
18) $\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$,
19) $\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$,
20) $\mathbb{Z}_4[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - 2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y}\rangle$,
21) $\mathbb{Z}_4[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY} - 2, 2\mathrm{X}, 2\mathrm{Y}\rangle$,
22) $\mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2\rangle$,
23) $\mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2 - 2\mathrm{X}\rangle$,
24) $\mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X}\rangle$.
Ahora si $p > 2$ es un número primo sería interesante describir la familia de anillos locales de Frobenius no de cadena con p^4 elementos, estos anillos tienen longitud 4, por eso en este Capítulo nuestro objetivo será determinar todos los anillos locales finitos de Frobenius no de cadena y con longitud 4.

2.1. Anillos de cadena y anillos locales de Frobenius

En esta sección se define anillo de Frobenius, únicamente se da la definición para cuando el anillo es finito, y anillo de cadena. Se da una caracterización de estos anillos en términos de sus extensiones no ramificadas, las cuales se usarán más adelante. Recordemos que los anillos considerados en este trabajo son finitos, conmutativos y con elemento identidad.

DEFINICIÓN 2.1.1 *Sea* A *un anillo y* M *un* A*-módulo.*

(*1*) *Se dice que* M *es Artiniano si cualquier cadena descendente de* A*-submódulos de* M *se estaciona, es decir si* $\mathrm{M}_1 \supset \mathrm{M}_2 \supset \ldots \supset \mathrm{M}_l \supset \ldots$*, es una cadana descendente de* A*-submódulos de* M *entonces existe* l_0 *tal que* $\mathrm{M}_l = \mathrm{M}_{l_0}$*, para todo* $l \geq l_0$*.*

(*2*) *El zoclo de* M*, denotado por* $\mathrm{Soc_A(M)}$*, es el* A*-submódulo de* M *generado por los* A*-submódulos simples de* M*.*

(*3*) *El radical de Jacobson de* A*, denotado por* $\mathrm{Rad(A)}$*, es la intersección de todos los ideales maximales de* A*.*

LEMA 2.1.1 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local, entonces*

(*1*) $\mathrm{Rad(A)} = \mathfrak{m}$*,*

(*2*) $\mathrm{Soc_A(A)} = \mathrm{ann_A}(\mathfrak{m})$*.*

Demostración.
(1) Es trivial.
(2) Sea I un ideal simple de A, entonces $\mathfrak{m}\mathrm{I} \neq \mathrm{I}$ y $\mathfrak{m}\mathrm{I} = \langle 0 \rangle$, por el Lema de Nakayama, de donde se sigue que $\mathrm{I} \subseteq \mathrm{ann_A}(\mathfrak{m})$ y $\mathrm{Soc(A)} \subseteq \mathrm{ann_A}(\mathfrak{m})$. Sea $\alpha \in \mathrm{ann_A}(\mathfrak{m})$, puesto que $\alpha\mathfrak{m} = \langle 0 \rangle$, entonces $\mathrm{ann_A}(\alpha) = \mathfrak{m}$, así $\langle \alpha \rangle$ es ideal simple, por el Lema 1.1.1, de donde se sigue que $\alpha \in \mathrm{Soc(A)}$.

El siguiente resultado no estará acompañado de una demostración, su demostración se puede encontrar por ejemplo en [19].

Lema 2.1.2 ([19], Teorema 3.2) *Sea* A *un anillo Artiniano, entonces:*

(*1*) A *tiene una cantidad finita de ideales maximales.*

(*2*) *Existe un entero positivo* k *tal que* $\mathrm{Rad(A)}^k = \langle 0 \rangle$.

Observación 3 *Una consecuencia del Lema 2.1.2 es que si* A *es un anillo Artiniano,* $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ *son todos sus ideales maximales, y* k *es un entero tal que* $\mathrm{Rad(A)}^k = \langle 0 \rangle$*, entonces* $\mathrm{A} \cong \mathrm{A}/\langle 0 \rangle = \mathrm{A}/\mathfrak{q}_1^k \cdots \mathfrak{q}_r^k \cong \mathrm{A}/\mathfrak{q}_1^k \oplus \cdots \oplus \mathrm{A}/\mathfrak{q}_r^k$*, donde cada anillo* $\mathrm{A}/\mathfrak{q}_i^k$ *es local con ideal maximal* $\mathfrak{q}_i/\mathfrak{q}_i^k$*, por el Lema 1.3.1.*

Definición 2.1.2 *[13] Un anillo finito* A *es llamado de Frobenius si* $\mathrm{A/Rad(A)} \cong \mathrm{Soc(A)}$.

Ejemplos de anillos locales de Frobenius incluyen al anillo del Ejemplo 2.1.1 y al anillo $\mathbb{F}_2[\mathrm{X}_1, \ldots, \mathrm{X}_k]/\langle \mathrm{X}_1^2, \ldots, \mathrm{X}_k^2 \rangle$ (ver [9]).

El siguiente resultado nos ayudará a reducir el estudio de anillos de Frobenius al estudio de anillos locales de Frobenius, su demostración se puede encontrar por ejemplo en [31].

Lema 2.1.3 ([31], Observación 1.3) *Sea* A *un anillo conmutativo Artiniano y* $\mathrm{A}_1, \ldots, \mathrm{A}_k$ *anillos locales tales que* $\mathrm{A} \cong \mathrm{A}_1 \oplus \cdots \oplus \mathrm{A}_k$*, (ver Observación 3). Entonces* A *es de Frobenius si y sólo si cada* A_i *es de Frobenius.*

Lema 2.1.4 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito. Las siguientes afirmaciones son equivalentes:*

(*1*) A *es de Frobenius;*

(*2*) $\mathrm{ann_A}(\mathfrak{m})$ *es un ideal simple;*

(*3*) A *tiene un único ideal minimal, tal ideal es* $\mathrm{ann_A}(\mathfrak{m})$.

Demostración.
Notese que en un anillo local se tiene $\mathrm{A/Rad(A)} = \mathrm{A}/\mathfrak{m} \cong \mathrm{k}$.
(1) $\Rightarrow$ (2) Por el Lema 2.1.1, $\mathrm{Soc(A)} = \mathrm{ann_A}(\mathfrak{m})$. Así, el isomorfismo $\mathrm{A/Rad(A)} \cong \mathrm{Soc(A)}$ implica $\mathrm{ann_A}(\mathfrak{m}) \cong \mathrm{k}$, de donde se sigue que $\mathrm{ann_A}(\mathfrak{m})$ es ideal simple, por el inciso (2) del Lema 1.1.1.

(2) $\Rightarrow$ (3) Sea I un ideal minimal de A, entonces $\mathfrak{m}\mathrm{I} \subset \mathrm{I}$, y por el Lema de Nakayama, $\mathfrak{m}\mathrm{I} = 0$ e $\mathrm{I} \subseteq \mathrm{ann_A}(\mathfrak{m})$. La afirmación se sigue del hecho que $\mathrm{ann_A}(\mathfrak{m})$ es ideal simple de A.
(3) $\Rightarrow$ (1) Puesto que los ideales simples son los ideales minimales, $\mathrm{Soc(A)} = \mathrm{ann_A}(\mathfrak{m})$ es el único ideal minimal de A. Por el inciso (2) del Lema 1.1.1 $\mathrm{ann_A}(\mathfrak{m}) \cong \mathrm{k}$, de donde se sigue que $\mathrm{A/Rad(A)} \cong \mathrm{Soc(A)}$.

DEFINICIÓN 2.1.3 *Un anillo* A *es llamado de cadena si su retícula de ideales es una cadena con la inclusión de conjuntos.*

Ejemplos de anillos de cadena es el anillo $\mathbb{F}_q[\mathrm{X}]/\langle \mathrm{X}^k \rangle$ y los anillos $\mathbb{Z}_{p^k}$, donde p es un número primo y k un entero no negativo.

El siguiente resultado no estará acompañado de una demostración, la demostración se puede encontrar por ejemplo en [6].

PROPOSICIÓN 2.1.1 *Sea* A *un anillo finito. Las siguientes afirmaciones son equivalentes:*

(*1*) *El anillo* A *es de cadena;*

(*2*) *El anillo* A *es local y su ideal maximal es principal;*

(*3*) *El anillo* A *es local y sus ideales son principales;*

(*4*) *El anillo* A *es local y* $\dim_{\mathrm{k}}(\mathfrak{m}/\mathfrak{m}^2) \leq 1$, *donde* $\mathfrak{m}$ *es el único ideal maximal de* A *y* $\mathrm{k} = \mathrm{A}/\mathfrak{m}$ *es el campo residual de* A*;*

(*5*) *El anillo* A *es local y* $\ell_{\mathrm{A}}(\mathrm{A}) = t$, *donde* t *es el índice de nilpotencia de su ideal maximal.*

Sea $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ un anillo finito de cadena, π un generador del ideal maximal $\mathfrak{m}$ de A y t el índice de nilpotencia del ideal maximal de A. Los ideales de A forman la cadena:

$$\mathrm{A} = \langle \pi^0 \rangle \supset \langle \pi \rangle \supset \ldots \supset \langle \pi^{t-1} \rangle \supset \langle \pi^t \rangle = \langle 0 \rangle.$$

TEOREMA 2.1.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A}/\langle \mathrm{f} \rangle$ *la extensión no ramificada de* A *determinada por* f. *Las siguientes afirmaciones son equivalentes:*

(*1*) A *es un anillo de cadena;*

(*2*) B *es un anillo de cadena;*

(*3*) $|\mathcal{L}(\mathrm{A})| = |\mathcal{L}(\mathrm{B})|$, *donde* $\mathcal{L}(*)$ *denota la retícula de ideales del anillo.*

Demostración.
(1) $\Rightarrow$ (2): Por la Proposición 1.3.3, $\mathfrak{m}$B es el único ideal maximal de B, el cual es principal pues $\mathfrak{m}$ es principal. En consecuencia, B es un anillo de cadena, por la Proposición 2.1.1.
(2) $\Rightarrow$ (1): Sean I y J ideales de A. Puesto que B es un anillo de cadena, IB $\subseteq$ JB o JB $\subseteq$ IB. Entonces I $\subseteq$ J o J $\subseteq$ I, por el inciso (1) del Lema 1.3.10. En consecuencia, A es un anillo de cadena.
(1) $\Rightarrow$ (3): Sea t el índice de nipotencia de π. Por (1) $\Rightarrow$ (2) y el inciso (3) del Lema 1.3.10, se tiene que B es un anillo de cadena con ideal maximal $\langle\pi\rangle$B y $\mathfrak{m}$B tienen índice de nilpotencia t. Entonces A y B tienen $t+1$ ideales.
(3) $\Rightarrow$ (1): Por el inciso (3) del Lema 1.3.9, el campo residual de B es $\mathbb{F}_{q^s}$. Por el inciso (2) del Lema 1.3.11, cualquier conjunto mínimo de generadores de $\mathfrak{m}$ es un conjunto mínimo de generadores de $\mathfrak{m}$B. Sea $r = \mathrm{v_A}(\mathfrak{m}) = \mathrm{v_B}(\mathfrak{m}\mathrm{B})$, entonces el número de ideales de B entre $\mathfrak{m}$B y $\mathfrak{m}^2$B es $\mathrm{G}(r, q^s)$ y el número de ideales de A entre $\mathfrak{m}$ y $\mathfrak{m}^2$ es $\mathrm{G}(r, q)$, por el Corolario 1.3.1. Por hipótesis y el inciso (2) del Lema 1.3.10 se sigue que $\mathcal{L}(\mathrm{B}) = \{\mathrm{IB} \ : \ \mathrm{I} \in \mathcal{L}(\mathrm{A})\}$, de donde se sigue que los ideales de B entre $\mathfrak{m}$B y $\mathfrak{m}^2$B se obtienen al expandir los ideales de A entre $\mathfrak{m}$ y $\mathfrak{m}^2$, lo cual implica que $\mathrm{G}(r, q^s) \leq \mathrm{G}(r, q)$. En consecuencia $r \leq 1$ y A es un anillo de cadena, por la Proposición 2.1.1.

Nótese que si A es un anillo finito de cadena, π el generador de su ideal maximal y t es el índice de nilpotencia de π, entonces $\mathrm{ann_A}(\pi) = \langle\pi^{t-1}\rangle$ es un ideal simple, en consecuencia A es anillo local de Frobenius.

Ejemplo 2.1.1 *Sean* $k \geq 3$ *un entero,* $\mathbb{F}_q$ *el campo finito con* q *elementos,* $q = p^d$, $\mathrm{I}_{(k,q)} = \langle \mathrm{X}_1^2, \ldots, \mathrm{X}_k^2, \mathrm{X}_i\mathrm{X}_j - \mathrm{X}_1\mathrm{X}_2 \ : \ 1 \leq i < j \leq k, (i,j) \neq (1,2)\rangle$ *un ideal de* $\mathbb{F}_q[\mathrm{X}_1, \ldots, \mathrm{X}_k]$, $\mathrm{A}_{(k,q)} = \mathbb{F}_q[\mathrm{X}_1, \ldots, \mathrm{X}_k]/\mathrm{I}_{(k,q)}$ *y* $\mathrm{x}_i = \mathrm{X}_i + \mathrm{I}_{(k,q)}$. *Entonces:*

(*1*) *Cualquier elemento de* $\mathrm{A}_{(k,q)}$ *puede ser escrito de manera única en la forma:*

$$a_0 + a_1\mathrm{x}_1 + a_2\mathrm{x}_2 + \cdots + a_k\mathrm{x}_k + a_{k+1}\mathrm{x}_1\mathrm{x}_2, \quad a_i \in \mathbb{F}_q.$$

(*2*) $\mathrm{A}_{(k,q)}$ *es un anillo local con ideal maximal* $\mathfrak{m} = \langle \mathrm{x}_1, \ldots, \mathrm{x}_k \rangle$ *y su campo residual es isomorfo a* $\mathbb{F}_q$.

(*3*) $\mathfrak{m}^2 = \langle \mathrm{x}_1\mathrm{x}_2 \rangle$, $\mathfrak{m}^3 = \langle 0 \rangle$ *y* $\ell_{\mathrm{A}_{(k,q)}}(\mathrm{A}_{(k,q)}) = k + 2$.

(*4*) $\mathrm{A}_{(k,q)}$ *no es anillo de cadena.*

(*5*) $a_0 + a_1\mathrm{x}_1 + a_2\mathrm{x}_2 + \cdots + a_k\mathrm{x}_k + a_{k+1}\mathrm{x}_1\mathrm{x}_2 \in \mathrm{ann}_{\mathrm{A}_{(k,q)}}(\mathfrak{m}) \Leftrightarrow a_0 = 0$ *y* $(a_1, \ldots, a_k)$ *es solución de* $\mathrm{D}\vec{\mathrm{x}} = \vec{0}$, *donde* D *es la matriz con ceros en la diagonal y unos en el resto de sus entradas.*

(*6*) $\mathrm{A}_{(k,q)}$ *es anillo de Frobenius si y sólo si* $(k-1, q) = 1$.

Demostración.
(1) Con el orden lexicográfico tal que $\mathrm{X}_k > \ldots > \mathrm{X}_2 > \mathrm{X}_1$, el conjunto $\mathrm{G} = \{\mathrm{X}_1^2, \ldots, \mathrm{X}_k^2, \mathrm{X}_i\mathrm{X}_j - \mathrm{X}_1\mathrm{X}_2 : 1 \leq i < j \leq k, (i,j) \neq (1,2)\}$ es una base de Groebner. La afirmación se sigue del hecho de que los únicos monomios no divisibles por $\mathrm{LM(G)} = \{\mathrm{X}_1^2, \ldots \mathrm{X}_k^2, \mathrm{X}_i\mathrm{X}_j : 1 \leq i < j \leq k, (i,j) \neq (1,2)\}$ son $\mathrm{X}_1, \mathrm{X}_2, \ldots, \mathrm{X}_k$ y $\mathrm{X}_1\mathrm{X}_2$.
(2) La afirmación se sigue del Lema 1.3.12.
(3) Puesto que $\mathfrak{m} = \langle \mathrm{x}_1, \ldots, \mathrm{x}_k \rangle$, entonces $\mathfrak{m}^2 = \langle \mathrm{x}_1^2, \ldots, \mathrm{x}_k^2, \mathrm{x}_i\mathrm{x}_j : 1 \leq i, j \leq k \rangle = \langle \mathrm{x}_1\mathrm{x}_2 \rangle$. Puesto que en $\mathrm{A}_{(k,q)}$ se satisface $\mathrm{x}_i\mathrm{x}_1\mathrm{x}_2 = 0$, para cualquier $i \in \{1, \ldots, k\}$, entonces $\mathfrak{m}^3 = \langle \mathrm{x}_1, \mathrm{x}_2 \ldots, \mathrm{x}_k \rangle \langle \mathrm{x}_1\mathrm{x}_2 \rangle = \langle \mathrm{x}_1\mathrm{x}_1\mathrm{x}_2, \mathrm{x}_2\mathrm{x}_1\mathrm{x}_2, \ldots, \mathrm{x}_k\mathrm{x}_1\mathrm{x}_2 \rangle = \langle 0 \rangle$.
Finalmente, por el inciso (2), el campo residual de $\mathrm{A}_{(k,q)}$ es $\mathbb{F}_q$, y por el inciso (1), $|\mathrm{A}_{(k,q)}| = |\mathbb{F}_q|^{k+2}$. La afirmación se sigue del Lema 1.3.4.
(4) Puesto que $\ell_{\mathrm{A}_{(k,q)}}(\mathrm{A}_{(k,q)}) = k + 2 \geq 5$, pues $k \geq 3$, y el índice de nilpotencia de $\mathfrak{m}$ es 3, por el inciso (3). Entonces $\mathrm{A}_{(k,q)}$ no es anillo de cadena, por la Proposición 2.1.1.
(5) Sea $\alpha = a_0 + a_1\mathrm{x}_1 + a_2\mathrm{x}_2 + \ldots + a_k\mathrm{x}_k + a_{k+1}\mathrm{x}_1\mathrm{x}_2 \in \mathrm{A}_{(k,q)}$ y D es la matriz $k \times k$ con ceros en la diagonal y unos en el resto de sus entradas. Puesto que en $\mathrm{A}_{(k,q)}$ se satisface $\mathrm{x}_i\mathrm{x}_1\mathrm{x}_2 = 0$ y $\mathrm{x}_i\mathrm{x}_j = \mathrm{x}_1\mathrm{x}_2$, para cualquier $i, j \in \{1, \ldots, k\}$, $i \neq j$, entonces:

$$\alpha \in \mathrm{ann}_{\mathrm{A}}(\mathfrak{m}) \Leftrightarrow$$

$$\alpha\mathrm{x}_1 = a_0\mathrm{x}_1 + (a_2 + a_3 + \ldots + a_k)\mathrm{x}_1\mathrm{x}_2 = 0,$$

$$\alpha\mathrm{x}_2 = a_0\mathrm{x}_2 + (a_1 + a_3 + \ldots + a_k)\mathrm{x}_1\mathrm{x}_2 = 0,$$

$$\vdots$$

$$\alpha\mathrm{x}_{k-1} = a_0\mathrm{x}_{k-1} + (a_1 + a_2 + \ldots + a_{k-2} + a_k)\mathrm{x}_1\mathrm{x}_2 = 0,$$

$$\alpha \mathrm{x}_k = a_0\mathrm{x}_k + (a_1 + a_2 + \ldots + a_{k-1})\mathrm{x}_1\mathrm{x}_2 = 0 \Leftrightarrow$$
$$a_0 = 0 \text{ } y \text{ } (a_1, a_2, \ldots, a_k) \text{ } es \text{ } solución \text{ } de \text{ } \mathrm{D}\vec{\mathrm{x}} = \vec{0},$$

(6) Primero se calculará el determinante de la matriz a la que se hace referencia en el inciso (5), se aplicarán operaciones elementales para llevarla a una matriz triangular superior.

$$\det \begin{pmatrix} 0 & 1 & 1 & 1 & \ldots & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & \ldots & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & \ldots & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & \ldots & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 1 & 1 & 1 & 1 & \ldots & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 & 1 & 0 \end{pmatrix} = \det \begin{pmatrix} -1 & 0 & 0 & 0 & \ldots & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & \ldots & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \ldots & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & -1 & 1 \\ 1 & 1 & 1 & 1 & \ldots & 1 & 1 & 0 \end{pmatrix} =$$

$$\det \begin{pmatrix} -1 & 0 & 0 & 0 & \ldots & 0 & 0 & 1 \\ 0 & -1 & 0 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & \ldots & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & \ldots & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & 0 & 0 & \ldots & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & 0 & k-1 \end{pmatrix} = (-1)^{k-1}(k-1)$$

$\Rightarrow$) Por el inciso (5), $\langle \mathrm{x}_1\mathrm{x}_2 \rangle \subseteq \mathrm{ann}_{\mathrm{A}_{(k,q)}}(\mathfrak{m})$. Puesto que $\mathrm{ann}_{\mathrm{A}_{(k,q)}}(\mathfrak{m})$ es ideal simple de $\mathrm{A}_{(k,q)}$, por hipótesis, se sigue que $\langle \mathrm{x}_1\mathrm{x}_2 \rangle = \mathrm{ann}_{\mathrm{A}_{(k,q)}}(\mathfrak{m})$.
Sea $(a_1, a_2, \ldots, a_k)$ una solución de $\mathrm{D}\vec{\mathrm{x}} = \vec{0}$, entonces $a_1\mathrm{x}_1 + a_2\mathrm{x}_2 + \ldots + a_k\mathrm{x}_k \in \mathrm{ann}_{\mathrm{A}_{(k,q)}}(\mathfrak{m}) = \langle \mathrm{x}_1\mathrm{x}_2 \rangle$, por el inciso (5). En consecuencia $(a_1, a_2, \ldots, a_k) = \vec{0}$, por el inciso (1). Así, D es no singular, lo cual implica que $\det(\mathrm{D}) = (-1)^{k-1}(k-1) \in (\mathrm{A}_{(k,q)})^*$ y $(k-1, q) = 1$.
$\Leftarrow$) Puesto que $\det(\mathrm{D}) = (-1)^{k-1}(k-1)$ y $(q, k-1) = 1$ entonces D es invertible y las soluciones del sistema $\mathrm{D}\vec{\mathrm{x}} = \vec{0}$ son solo las triviales. Por el inciso (5), $\{a\mathrm{x}_1\mathrm{x}_2 : a \in \mathbb{F}_q\} = \mathrm{ann}_{\mathrm{A}_{(k,q)}}(\mathfrak{m})$ y $|\mathrm{ann}_{\mathrm{A}_{(k,q)}}(\mathfrak{m})| = |\mathbb{F}_q|$. Puesto que $\mathbb{F}_q$ es el campo residual de $\mathrm{A}_{(k,q)}$, entonces por el Lema 1.3.4, se tiene, $\ell_{\mathrm{A}_{(k,q)}}(\mathrm{ann}_{\mathrm{A}_{(k,q)}}(\mathfrak{m})) = 1$, de donde se sigue la afirmación.

LEMA 2.1.5 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito de Frobenius y* t *el índice de nilpotencia de* $\mathfrak{m}$. *Entonces* $\mathrm{ann_A}(\mathfrak{m}) = \mathfrak{m}^{t-1}$.

Demostración.
El hecho de que $\mathfrak{m}^t = \mathfrak{m}^{t-1}\mathfrak{m} = \langle 0 \rangle$, implica que $\mathfrak{m}^{t-1} \subseteq \mathrm{ann_A}(\mathfrak{m})$, y la afirmación se sigue del hecho de que $\mathrm{ann_A}(\mathfrak{m})$ es ideal simple de A.

Sea A un anillo conmutativo con identidad. El conjunto A^n es considerado como A-módulo de la manera usual. Un subconjunto C de A^n es llamado código lineal de longitud n sobre A si C es un A-submódulo de A^n. El producto interno canónico sobre A^n está dado por $(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = a_1b_1 + \ldots + a_nb_n$. Para un código lineal C, sobre A, el código ortogonal de C es definido por $\mathrm{C}^\perp = \{\vec{a} \in \mathrm{A}^n : \vec{a} \cdot \vec{b} = 0 \ \forall \ \vec{b} \in \mathrm{C}\}$. Obsérvese que si C es un código lineal sobre A de longitud 1, entonces C es un ideal de A y $\mathrm{C}^\perp = \mathrm{ann_A}(\mathrm{C})$.

El siguiente resultado es una caracterización de anillos locales de Frobenius en términos de sus códigos lineales, su demostración se puede encontrar por ejemplo en [31].

LEMA 2.1.6 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito de Frobenius y* C *un código lineal de longitud* n *sobre* A, *entonces*

$$(\mathrm{C}^\perp)^\perp = \mathrm{C} \quad y \quad |\mathrm{C}||\mathrm{C}^\perp| = |\mathrm{A}|^n.$$

En particular, si I *es un ideal de* A, *entonces*

$$\mathrm{ann_A}(\mathrm{ann_A}(\mathrm{I})) = \mathrm{I} \quad y \quad |\mathrm{I}||\mathrm{ann_A}(\mathrm{I})| = |\mathrm{A}|.$$

LEMA 2.1.7 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito de Frobenius e* I *un ideal de* A, *entonces*

$$\ell_\mathrm{A}(\mathrm{I}) + \ell_\mathrm{A}(\mathrm{ann_A}(\mathrm{I})) = \ell_\mathrm{A}(\mathrm{A}).$$

Demostración.
Por el Lema 1.3.4, se tienen las siguientes relaciones:

(1) $|\mathrm{I}| = q^{\ell_\mathrm{A}(\mathrm{I})}$,

(2) $|\mathrm{ann_A}(\mathrm{I})| = q^{\ell_\mathrm{A}(\mathrm{ann_A}(\mathrm{I}))}$,

(3) $|\mathrm{A}| = q^{\ell_\mathrm{A}(\mathrm{A})}$.

La afirmación se sigue de la relación $|\mathrm{I}||\mathrm{ann_A(I)}| = |\mathrm{A}|$, del Lema 2.1.6.

El siguiente resultado es una caracterización de anillos locales de Frobenius en términos de sus extensiones no ramificadas.

TEOREMA 2.1.2 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* $\mathrm{f} \in \mathrm{A[T]}$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A}/\langle \mathrm{f} \rangle$ *la extensión no ramificada de* A *determinada por* f. *Las siguientes afirmaciones son equivalentes:*

(*1*) A *es un anillo de Frobenius;*

(*2*) $\mathrm{ann_A}(\mathfrak{m})$ *es el único ideal minimal de* A*;*

(*3*) $\mathrm{ann_B}(\mathfrak{m}\mathrm{B})$ *es el único ideal minimal de* B*;*

(*4*) B *es un anillo de Frobenius.*

Demostración.
(1) $\Rightarrow$ (2): Sea I un ideal minimal de A, por el Lema de Nakayama, $\mathfrak{m}\mathrm{I} \subsetneq \mathrm{I}$. Entonces $\mathfrak{m}\mathrm{I} = 0$ lo cual implica que $\mathrm{I} \subseteq \mathrm{ann_A}(\mathfrak{m})$ y $\mathrm{I} = \mathrm{ann_A}(\mathfrak{m})$, pues $\mathrm{ann_A}(\mathfrak{m})$ es ideal simple.
(2) $\Rightarrow$ (1): Si $\mathrm{ann_A}(\mathfrak{m})$ es un ideal minimal, entonces $\mathrm{ann_A}(\mathfrak{m})$ es un ideal simple.
(1) $\Leftrightarrow$ (4): $\mathfrak{m}\mathrm{B}$ es el ideal maximal de B y, por el inciso (1) del Lema 1.3.11, se tiene $\ell_{\mathrm{A}}(\mathrm{ann_A}(\mathfrak{m})) = \ell_{\mathrm{B}}(\mathrm{ann_A}(\mathfrak{m})\mathrm{B})$, además, por el inciso (3) del Lema 1.3.11, se tiene $\mathrm{ann_A}(\mathfrak{m})\mathrm{B} = \mathrm{ann_B}(\mathfrak{m}\mathrm{B})$. En consecuencia, $\mathrm{ann_A}(\mathfrak{m})$ es un ideal simple de A $\Leftrightarrow$ $\ell_{\mathrm{A}}(\mathrm{ann_A}(\mathfrak{m})) = \ell_{\mathrm{B}}(\mathrm{ann_B}(\mathfrak{m}\mathrm{B})) = 1 \Leftrightarrow \mathrm{ann_B}(\mathfrak{m}\mathrm{B})$ es un ideal simple de B.
(4) $\Leftrightarrow$ (3) Es análogo a la implicación (1) $\Leftrightarrow$ (2).

2.2. Anillos locales finitos de Frobenius no de cadena y de longitud 4

El objetivo de esta sección es describir la familia de anillos locales finitos de Frobenius no de cadena y de longitud 4. Una consecuencia es que los anillos locales finitos de Frobenius no de cadena y con p^4 elementos, p un número primo, son descritos. Este resultado generaliza el caso $p = 2$ presentado en [21].

LEMA 2.2.1 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito. Si* A *posee alguna de las siguientes propiedades, entonces es anillo de cadena.*

(*1*) A *tiene longitud* 1*;*

(*2*) $\mathfrak{m}$ *tiene índice de nilpotencia* 1*;*

(*3*) A *tiene longitud* 2*;*

(*4*) A *es anillo de Frobenius y* $\mathfrak{m}$ *tiene índice de nilpotencia* 2*.*

Demostración.
Observar que un campo es anillo de cadena.
(1) Si A tiene longitud 1, entonces $\mathrm{A} \supset \langle 0 \rangle$ es una serie de composición, $\mathfrak{m} = \langle 0 \rangle$ y A es un campo finito.
(2) Si se cumple que $\mathfrak{m}^1 = \mathfrak{m} = \langle 0 \rangle$, entonces A es un campo finito.
(3) A no es un campo y $\mathfrak{m}$ tiene índice de nilpotencia mayor a 1, por el inciso anterior. Por el Lema 1.3.6, el hecho de que A tiene longitud 2 y la observación anterior, el índice de nilpotencia de $\mathfrak{m}$ es 2. La afirmación se sigue de la Proposición 2.1.1.
(4) Si $\mathfrak{m}$ tiene índice de nilpotencia 2 entonces, por el Lema 2.1.5 y porque A es anillo de Frobenius, $\mathrm{ann}_{\mathrm{A}}(\mathfrak{m}) = \mathfrak{m}$ es un ideal simple, en consecuencia $\mathfrak{m}$ es ideal principal, por el Lema 1.1.1. Por lo tanto A es anillo de cadena, por la Proposición 2.1.1.

Lema 2.2.2 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito, no de cadena y con* p^4*elementos, entonces* A *tiene longitud* 4*.*

Demostración.
Sea $q = p^d$, con d entero positivo. Por el Lema 1.3.4, $|\mathrm{A}| = p^4 = q^{\ell_{\mathrm{A}}(\mathrm{A})} = p^{d\ell_{\mathrm{A}}(\mathrm{A})}$, por el Lema 1.3.4, lo cual implica $\ell_{\mathrm{A}}(\mathrm{A}) \in \{1, 2, 4\}$. La afirmación se sigue del Lema 2.2.1.

Lema 2.2.3 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito de Frobenius no de cadena y con longitud* 4*, entonces* $\mathfrak{m}$ *tiene índice de nilpotencia* 3*.*

Demostración.
Por el Lema 1.3.6, la Proposición 2.1.1 y el hecho de que A no es anillo de cadena, se tiene que el índice de nilpotencia del ideal maximal de A es menor a 4. La afirmación se sigue del Lema 2.2.1.

Definición 2.2.1 .

(*1*) *Sea* $\mathfrak{L}_4$ *la familia de anillos locales finitos de Frobenius no de cadena y de longitud* 4*.*

(*2*) *Sea* $\mathfrak{F}_3$ *la familia de anillos locales finitos de Frobenius no de cadena y cuyo ideal maximal tiene índice de nilpotencia* 3*.*

La familia $\mathfrak{F}_3$ es grande pues incluye a los anillos $\mathrm{A}_{(k,p^d)}$, donde $(k-1,p)=1$, del ejemplo 2.1.1. Puesto que la longitud del anillo $\mathrm{A}_{(k,p^d)}$ es $k+2$, esta familia contiene anillos de todas las longitudes. Además, $\mathfrak{L}_4 \subset \mathfrak{F}_3$, por el Lema 2.2.3.

LEMA 2.2.4 *Sea* $(\mathrm{A},\mathfrak{m},\mathbb{F}_{p^d}) \in \mathfrak{L}_4$, $\mathbb{T} \subset \mathrm{A}$ *un conjunto de representantes de* $\mathbb{F}_{p^d}$ *y* $\mathrm{x} \in \mathfrak{m} \setminus \mathfrak{m}^2$*. Entonces existe* $\mathrm{y} \in \mathfrak{m} \setminus \mathfrak{m}^2$ *tal que* $\{\mathrm{x},\mathrm{y}\}$ *es un conjunto mínimo de generadores de* $\mathfrak{m}$*,* $\mathrm{x}^3=\mathrm{y}^3=\mathrm{x}^2\mathrm{y}=\mathrm{x}\mathrm{y}^2=0$ *y alguna de las siguientes relaciones se debe satisfacer:*

(*1*) $\mathrm{x}\mathrm{y}=0$ *y* $\mathrm{x}^2=f\mathrm{y}^2\neq 0$ *para algún* $f \in \mathbb{T}\setminus\{0\}$*.*

(*2*) $\mathrm{x}\mathrm{y}\neq 0$*,* $\mathrm{x}^2+u\mathrm{x}\mathrm{y}=0$ *y* $\mathrm{y}^2+v\mathrm{x}\mathrm{y}=0$ *para algunos* $u,v \in \mathbb{T}$ *tales que* $\tilde{u}\tilde{v}\neq\tilde{1}$ *en* $\mathbb{F}_{p^d}$*.*

Demostración.
Por el Lema 2.2.3, $\mathfrak{m}$ tiene índice de nilpotencia 3, por los Lemas 2.1.4 y 2.1.5, $\mathrm{ann}_{\mathrm{A}}(\mathfrak{m})=\mathfrak{m}^2$ es el único ideal minimal de A, así

$$\mathrm{v}(\mathfrak{m})=\ell_{\mathrm{A}}(\mathfrak{m}/\mathfrak{m}^2)=\ell_{\mathrm{A}}(\mathfrak{m})-\ell_{\mathrm{A}}(\mathfrak{m}^2)=2.$$

En consecuencia, puesto que $\mathrm{x}\in\mathfrak{m}\setminus\mathfrak{m}^2$, existe $\mathrm{y}\in\mathfrak{m}\setminus\mathfrak{m}^2$ tal que $\{\mathrm{x},\mathrm{y}\}$ es un conjunto mínimo de generadores de $\mathfrak{m}$ y se tendrá $\mathrm{x}^3=\mathrm{y}^3=\mathrm{x}^2\mathrm{y}=\mathrm{x}\mathrm{y}^2=0$. Si $\mathrm{ann}_{\mathrm{A}}(\mathrm{x})=\mathfrak{m}^2$, por el Lema 2.1.6, $\langle\mathrm{x}\rangle=\mathrm{ann}_{\mathrm{A}}(\mathrm{ann}_{\mathrm{A}}(\mathrm{x}))=\mathrm{ann}_{\mathrm{A}}(\mathfrak{m}^2)=\mathfrak{m}$, que es una contradicción. Si $\mathrm{ann}_{\mathrm{A}}(\mathrm{x})=\mathfrak{m}$, entonces $\langle\mathrm{x}\rangle=\mathrm{ann}_{\mathrm{A}}(\mathrm{ann}_{\mathrm{A}}(\mathrm{x}))=\mathrm{ann}_{\mathrm{A}}(\mathfrak{m})=\mathfrak{m}^2$, lo cual no es posible. Entonces $\mathfrak{m}^2\subset\mathrm{ann}_{\mathrm{A}}(\mathrm{x})$. Y de manera análoga se concluye que $\mathrm{ann}_{\mathrm{A}}(\mathrm{y})\subset\mathfrak{m}$ y $\mathrm{ann}_{\mathrm{A}}(\mathrm{x})\neq\mathrm{ann}_{\mathrm{A}}(\mathrm{y})$.
Por el Corolario 1.3.1 y puesto que $(0,1)$ y $(1,\lambda)$, donde $\lambda\in\mathbb{F}_{p^d}$, son todas las 1×2 matrices en forma escalón reducida por filas (erf) sobre $\mathbb{F}_{p^d}$, se tiene que $\mathrm{ann}_{\mathrm{A}}(\mathrm{x})\in\{\langle\mathrm{y}\rangle,\langle\mathrm{x}+u\mathrm{y}\rangle\}$ y $\mathrm{ann}_{\mathrm{A}}(\mathrm{y})\in\{\langle\mathrm{y}\rangle,\langle\mathrm{x}+v\mathrm{y}\rangle\}$, donde $u,v\in\mathbb{T}$. En las siguientes líneas las afirmaciones 1) y 2) se probarán.
1) Usando el Lema 2.1.6 y el hecho de que A es anillo de Frobenius, se tiene:

$$\mathrm{ann}_{\mathrm{A}}(\mathrm{x})=\langle\mathrm{y}\rangle \Leftrightarrow \mathrm{ann}_{\mathrm{A}}(\mathrm{y})=\mathrm{ann}_{\mathrm{A}}(\mathrm{ann}_{\mathrm{A}}(\mathrm{x}))=\langle\mathrm{x}\rangle.$$

En este caso, $xy = 0$ y puesto que $x \notin \langle y \rangle = \mathrm{ann_A}(x)$, $y \notin \langle x \rangle = \mathrm{ann_A}(y)$, entonces $x^2 \neq 0$ y $y^2 \neq 0$. Puesto que $\mathfrak{m}^2$ es generado por cualquiera de sus elementos no cero, pues es un ideal simple de A, $\mathfrak{m}^2 = \langle x^2, xy, y^2 \rangle = \langle x^2 \rangle = \langle y^2 \rangle$ lo cual implica que $x^2 = fy^2$, para algún $f \in \mathbb{T} \setminus \{0\}$.
2) Obsérvese que

$$\mathrm{ann_A}(x) = \langle x + uy \rangle, \text{ donde } u \in \mathbb{T} \Leftrightarrow$$

$$\mathrm{ann_A}(y) \in \{\langle y \rangle, \langle x + v_1 y \rangle\}, \text{ donde } v_1 \in \mathbb{T} \setminus \{0\} \Leftrightarrow$$

$$\mathrm{ann_A}(y) = \langle y + vx \rangle, \text{ donde } v \in \mathbb{T}.$$

En este caso $x^2 + uxy = 0$ y $y^2 + vxy = 0$, donde $u, v \in \mathbb{T}$.
Resta verificar $xy \neq 0$ y $\tilde{u}\tilde{v} \neq \tilde{1}$ en $\mathbb{F}_{p^d}$, si $xy = 0$ entonces $x^2 = y^2 = 0$ y $\mathfrak{m}^2 = \langle x^2, xy, y^2 \rangle = \langle 0 \rangle$, lo cual es una contradicción. Si $u = 0$ o $v = 0$ se tiene la afirmación. Si $uv = 1 + m$, donde $m \in \mathfrak{m}$, entonces $uvx^2 = x^2$ y $x^2 + uxy = uvx^2 + uxy = ux(y + vx) = 0$, lo cual implica que $\mathrm{ann_A}(y) = \langle y + vx \rangle \subseteq \mathrm{ann_A}(x)$, en consecuencia $\langle y \rangle \subseteq \langle x \rangle$, que no es posible.

Los siguientes resultados sobre campos finitos posiblemente se encuentran en la literatura, se incluyen en este trabajo para facilitar la lectura.

PROPOSICIÓN 2.2.1 *Sea $\mathbb{F} = \mathbb{F}_{p^d}$ el campo finito con p^d elementos y ζ un elemento primitivo de este campo. Entonces:*

(*1*) *Existen $\gamma_1, \gamma_2 \in \mathbb{F}$ tales que $\zeta = \gamma_1^2 + \gamma_2^2$.*

(*2*) *$\sqrt{-1} \in \mathbb{F}$ si y sólo si $p = 2$ ó $p^d \equiv 1 \bmod 4$.*

(*3*) *La ecuación $X^2\zeta + Y^2 = 0$ tiene soluciones no triviales en $\mathbb{F}$ si y sólo si $p = 2$ ó $p^d \equiv 3 \bmod 4$, si y sólo si $p = 2$ ó $\sqrt{-1} \notin \mathbb{F}$.*

(*4*) *Si $u, v \in \mathbb{F}$ son tales que $\sqrt{u} \notin \mathbb{F}$ y $\sqrt{v} \notin \mathbb{F}$, entonces $\sqrt{\frac{u}{v}} \in \mathbb{F}$.*

(*5*) *Sean $u, v, w \in \mathbb{F}$ con $uw \neq 0$. Entonces el sistema de ecuaciones*
(*a*) $X^2 + Y^2 = uw$,
(*b*) $Z^2 + W^2 = vw$,
(*c*) $XZ + YW = w$,
tiene solución en $\mathbb{F}$ si y sólo si $\sqrt{uv - 1} \in \mathbb{F}$.
Cuando $\sqrt{uv - 1} \in \mathbb{F}$, una solución al sistema de ecuaciones es:

(*i*) $\zeta^k(u, 0, 1, \sqrt{uv-1})$, *cuando* p *es impar y* $\frac{w}{u} = \zeta^{2k}$.

(*ii*) $\zeta^k(u\gamma_1, u\gamma_2, \gamma_1 + \gamma_2\sqrt{uv-1}, \gamma_2 - \gamma_1\sqrt{uv-1})$, *donde* γ_1, γ_2 *son como en el inciso* (1) *de este lema, cuando* p *es impar y* $\frac{w}{u} = \zeta^{2k+1}$.

(*iii*) $(\sqrt{uw}, 0, \sqrt{\frac{w}{u}}, \sqrt{\frac{w}{u}}\sqrt{uv-1})$, *cuando* $p = 2$.

(*6*) *Las siguientes condiciones*
(a) $\mathrm{X}^2 + \mathrm{Y}^2 = \zeta(\mathrm{Z}^2 + \mathrm{W}^2)$,
(b) $\mathrm{Z}^2 + \mathrm{W}^2 \neq 0$,
(c) $\mathrm{XZ} + \mathrm{YW} = 0$,
se satisfacen en $\mathbb{F}$ *si y sólo si* $p = 2$.
Cuando $p = 2$ *el conjunto de* $\mathbb{F}^4$ *que satisface las condiciones es* $(\sqrt{\zeta}, 0, 0, 1)$.

Demostración.
(1): El caso $p = 2$ es trivial pues $(\mathbb{F}^*)^2 = \mathbb{F}^*$.
Sea p un número primo impar y sean

$$\Gamma_1 = \{\zeta^{2i} : 1 \leq i \leq \frac{p^d - 1}{2} - 1\},$$

$$\Gamma_2 = \{\zeta^{2i+1} : 0 \leq i \leq \frac{p^d - 1}{2} - 1\},$$

$$\Gamma_3 = 1 - \Gamma_2 = \{1 - \zeta^{2i+1} : 0 \leq i \leq \frac{p^d - 1}{2} - 1\}.$$

Se tienen las siguientes relaciones

$$\Gamma_1 \cup \Gamma_2 = \mathbb{F} \setminus \{0, 1\}, \qquad |\Gamma_1| = \frac{p^d - 1}{2} - 1,$$

$$|\Gamma_2| = |\Gamma_3| = \frac{p^d - 1}{2}, \qquad 0, 1 \notin \Gamma_3,$$

así, $\Gamma_3 \subset \Gamma_1 \cup \Gamma_2$ y $\Gamma_3 \cap \Gamma_2 \neq \emptyset$. De la última relación se sigue la afirmación.

(2): $\Rightarrow$) Si $p = 2$, entonces $(\mathbb{F}^*)^2 = \mathbb{F}^*$ de donde se sigue la afirmación. Sea p un número primo impar, entonces $\sqrt{-1} \in \mathbb{F}^*$ tiene orden multiplicativo 4 y la afirmación se sigue del Teorema de Lagrange.
$\Leftarrow$) Si $p^d = 4h + 1$, entonces $\sqrt{-1} = \zeta^h \in \mathbb{F}$.

(3): $\Rightarrow$) Si $p = 2$ la afirmación se sigue del hecho que $(\mathbb{F}^*)^2 = \mathbb{F}^*$. Si p es un número primo impar y (a, b) es una solución no trivial de la ecuación, entonces $a \neq 0$ y $\zeta^k = \frac{b}{a}$, para algún $k \in \{0, 1, \ldots, p^d - 1\}$. Así,

$$\zeta + (\frac{b}{a})^2 = \zeta + \zeta^{2k} = \zeta(1 + \zeta^{2k-1}) = 0,$$

lo cual implica que

$$\zeta^{2k-1} = -1 = \zeta^{\frac{p^d-1}{2}}$$

que es equivalente a

$$\zeta^{\frac{p^d-1}{2}-(2k-1)} = 1$$

en consecuencia $p^d - 1 \mid \frac{p^d-1}{2} - (2k-1)$, $p^d - 1 \mid \frac{p^d-4k+1}{2}$ y $p^d \equiv 3 \bmod 4$.
$\Leftarrow$) Si $p^d = 4h + 3$, entonces $(1, \zeta^{h+1})$ es una solución de $\mathrm{X}^2\zeta + \mathrm{Y}^2 = 0$.

(4): Puesto que $\mathbb{F}_{p^{2d}} \cong \mathbb{F}_{p^d}(\sqrt{u}) = \mathbb{F}_{p^d}(\sqrt{v})$, entonces $\sqrt{u} = a + b\sqrt{v}$, donde $a, b \in \mathbb{F}_{p^d}$ y $b \neq 0$, $2ab\sqrt{v} = u - a^2 - b^2v$, en consecuencia $a = 0$ y $b^2 = \frac{u}{v} \in \mathbb{F}_{p^d}$.

(5): $\Rightarrow$) Supóngase que p es impar, Z y W se encontrarán en términos de los valores de $\mathrm{X}, \mathrm{Y}, u$ y v.
Si $\mathrm{Y} = 0$, entonces el sistema de ecuaciones se transforma en:
(a) $\mathrm{X}^2 = uw$,
(b) $\mathrm{Z}^2 + \mathrm{W}^2 = vw$,
(c) $\mathrm{XZ} = w$;
de donde se obtiene:

$$\mathrm{X} \neq 0, \qquad \mathrm{Z} = \frac{w}{\mathrm{X}} = \frac{uw}{u\mathrm{X}} = \frac{\mathrm{X}^2}{u\mathrm{X}} = \frac{\mathrm{X}}{u},$$

$$\frac{\mathrm{W}^2u^2}{\mathrm{X}^2} = \frac{(vw - \mathrm{Z}^2)u^2}{uw} = uv - \frac{u\mathrm{Z}^2}{w} = uv - \frac{uw\mathrm{Z}^2}{w^2} = uv - 1,$$

$$\mathrm{W} = \pm\frac{\mathrm{X}\sqrt{uv-1}}{u}.$$

Si $\mathrm{Y} \neq 0$. De (c) se obtiene

$$\mathrm{W} = \frac{-\mathrm{XZ} + w}{\mathrm{Y}} \ldots (d)$$

Combinando (d) con (a) y (b) se obtiene:

$$\mathrm{Z}^2 + \mathrm{W}^2 = vw = \mathrm{Z}^2 + (\frac{-\mathrm{XZ} + w}{\mathrm{Y}})^2 =$$

$$\frac{\mathrm{Y}^2\mathrm{Z}^2+\mathrm{X}^2\mathrm{Z}^2-2w\mathrm{XZ}+w^2}{\mathrm{Y}^2}=\frac{uw\mathrm{Z}^2-2w\mathrm{XZ}+w^2}{\mathrm{Y}^2}$$

de donde se sigue que

$$u\mathrm{Z}^2-2\mathrm{XZ}+w-v\mathrm{Y}^2=0$$

$$\mathrm{Z}=\frac{2\mathrm{X}\pm\sqrt{4\mathrm{X}^2-4u(w-v\mathrm{Y}^2)}}{2u}=\frac{\mathrm{X}\pm\mathrm{Y}\sqrt{uv-1}}{u}$$

y

$$\mathrm{W}=\frac{-\mathrm{XZ}+w}{\mathrm{Y}}=\frac{\mathrm{Y}\mp\mathrm{X}\sqrt{uv-1}}{u}.$$

En cualquiera de los casos se tiene $\sqrt{uv-1}\in\mathbb{F}$.
$\Leftarrow$) Supóngase que $\sqrt{uv-1}\in\mathbb{F}$.
Si $u^{-1}w=\zeta^{2k+1}$, sean γ_1,γ_2 como en el inciso (1). Entonces $uw=u^2u^{-1}w=u^2\zeta^{2k}\zeta=(u\zeta^k)^2(\gamma_1^2+\gamma_2^2)=(u\zeta^k\gamma_1)^2+(u\zeta^k\gamma_2)^2$, Elegir $\mathrm{X}=u\zeta^k\gamma_1$ y $\mathrm{Y}=u\zeta^k\gamma_2$, y de acuerdo a la implicación anterior, caso $\mathrm{Y}\neq 0$, se obtiene, $\mathrm{Z}=\zeta^k\gamma_1\pm\zeta^k\gamma_2\sqrt{uv-1}$ y $\mathrm{W}=\zeta^k\gamma_2\mp\zeta^k\gamma_1\sqrt{uv-1}$.
Si $u^{-1}w=\zeta^{2k}$, entonces $uw=u^2u^{-1}w=(u\zeta^k)^2$. Elegir $\mathrm{X}=u\zeta^k$ y $\mathrm{Y}=0$, y de acuerdo a la implicación anterior, caso $\mathrm{Y}=0$, se obtiene $\mathrm{Z}=\zeta^k$ y $\mathrm{W}=\pm\zeta^k\sqrt{uv-1}$.
El caso $p=2$ es trivial dado que todo elemento posee raiz cuadrada en el campo, así siempre se cumple que $\sqrt{uv-1}\in\mathbb{F}$, y una solución del sistema de ecuaciones es $\mathrm{X}=\sqrt{uw}$, $\mathrm{Y}=0$, $\mathrm{Z}=\sqrt{wu^{-1}}$, $\mathrm{W}=\sqrt{wu^{-1}}\sqrt{uv-1}$.

(6): $\Rightarrow$) Si $\mathrm{Y}=0$, entonces $\mathrm{X}^2=\zeta(\mathrm{Z}^2+\mathrm{W}^2)\neq 0$ y $\mathrm{XZ}=0$ de donde se sigue que $\mathrm{Z}=0$, $\mathrm{W}\neq 0$, $\mathrm{X}^2=\zeta\mathrm{W}^2$, $\zeta\in(\mathbb{F}^*)^2$, $\mathbb{F}^*=(\mathbb{F}^*)^2$ y $p=2$.
Si $\mathrm{Y}\neq 0$, entonces $\mathrm{W}=-\frac{\mathrm{XZ}}{\mathrm{Y}}$ y $\mathrm{Z}^2+\mathrm{W}^2=\frac{\mathrm{Z}^2\mathrm{Y}^2+\mathrm{X}^2\mathrm{Z}^2}{\mathrm{Y}^2}=\frac{\mathrm{Z}^2\zeta(\mathrm{Z}^2+\mathrm{W}^2)}{\mathrm{Y}^2}$ lo cual implica que $\zeta\in(\mathbb{F}^*)^2$, $\mathbb{F}^*=(\mathbb{F}^*)^2$ y $p=2$;
$\Leftarrow$) Elegir $\mathrm{X}=\sqrt{\zeta},\mathrm{Y}=0,\mathrm{Z}=0,\mathrm{W}=1$.

Las siguientes Proposiciones son las partes más importante de esta sección. Se encontrarán todos los anillos locales finitos de Frobenius no de cadena y de longitud 4.

Recordar que si $(\mathrm{A},\mathfrak{m},\mathbb{F}_{p^d})$ es un anillo local finito y M es un A-módulo de longitud finita, $\ell_{\mathrm{A}}(\mathrm{M})$, entonces $|\mathrm{M}|=p^{d\ell_{\mathrm{A}}(\mathrm{M})}$, por el Lema 1.3.4. La característica de A, denotada por $\mathrm{car}(\mathrm{A})$, es el menor entero positivo, n, que satisface $n\mathrm{A}=\{0\}$. Se cumple que $\mathrm{car}(\mathrm{A})=p^k$, para algún $k\in\mathbb{N}$. Si $(\mathrm{A},\mathfrak{m},\mathbb{F}_{p^d})$ es anillo local finito de Frobenius y t es el índice de nilpotencia de $\mathfrak{m}$, entonces $\mathrm{ann}_{\mathrm{A}}(\mathfrak{m})=\mathfrak{m}^{t-1}$ es el único ideal minimal de A, por el Lema 2.1.5.

Sea $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_{p^d}) \in \mathfrak{L}_4$, entonces $|\mathrm{A}| = p^{4d}$, el índice de nilpotencia de $\mathfrak{m}$ es 3, por el Lema 2.2.3, así $\mathrm{ann}_{\mathrm{A}}(\mathfrak{m}) = \mathfrak{m}^2$ es el único ideal minimal de A y $p^3 \in \mathfrak{m}^3 = (0)$, de esto se obtiene que $\mathrm{car}(\mathrm{A}) \in \{p, p^2, p^3\}$.
En lo que concierne a la característica del anillo A, las únicas posibilidades son las siguientes:
(1): $\mathrm{car}(\mathrm{A}) = p^2$ y $p \in \mathfrak{m}^2$.
(2): $\mathrm{car}(\mathrm{A}) = p^2$ y $p \notin \mathfrak{m}^2$.
(3): $\mathrm{car}(\mathrm{A}) = p^3$ y $p \in \mathfrak{m}^2$.
(4): $\mathrm{car}(\mathrm{A}) = p^3$ y $p \notin \mathfrak{m}^2$.
(5): $\mathrm{car}(\mathrm{A}) = p$.

Cada uno de estos casos es tratado en las siguientes Proposiciones. Obsérvese que el caso (3): $\mathrm{car}(\mathrm{A}) = p^3$ y $p \in \mathfrak{m}^2$ no es posible, pues si $p \in \mathfrak{m}^2$, entonces $p^2 \in \mathfrak{m}^4 = \langle 0 \rangle$.

PROPOSICIÓN 2.2.2 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_{p^d}) \in \mathfrak{L}_4$ *tal que* $\mathrm{car}(\mathrm{A}) = p^2$ *y* $p \in \mathfrak{m}^2$. *Entonces*

(*1*) *Si* p *es impar, el anillo* A *es isomorfo a alguno de los siguientes anillos*
$\mathrm{GR}(p^2, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$,
ó
$\mathrm{GR}(p^2, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta\mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$, $\{0, 1, \ldots, \zeta^{p^d-2}\}$ *es el conjunto de Teichmüller del anillo de Galois* $\mathrm{GR}(p^2, d)$.

(*2*) *Si* $p = 2$, *el anillo* A *es isomorfo a alguno de los siguientes anillos*
$\mathrm{GR}(4, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - 2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y} \rangle$,
ó
$\mathrm{GR}(4, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY} - 2, 2\mathrm{X}, 2\mathrm{Y} \rangle$.

Demostración.
Por el Teorema 1.3.4 se puede suponer que el anillo de Galois $\mathrm{GR}(p^2, d)$ está contenido en A y sea $\mathbb{T} = \{0, 1, \zeta, \ldots, \zeta^{p^d-2}\}$ el conjunto de Teichmüller de este anillo de Galois. Sea $\{\mathrm{x}, \mathrm{y}\}$ un conjunto mínimo de generadores del idea maximal $\mathfrak{m}$ que satisface las afirmaciones (1) o (2) del Lema 2.2.4 para algunos valores $f_1, u_1, v_1 \in \mathbb{T}$, con $f_1 \neq 0$ y $\tilde{u}_1\tilde{v}_1 \neq 1$ en $\mathbb{F}_{p^d}$. Puesto que $p \in \mathfrak{m}^2$, entonces $p\mathrm{x}, p\mathrm{y} \in \mathfrak{m}^3 = (0)$. Dado que $\mathfrak{m}^2$ es un ideal simple de A entonces es generado por cualquiera de sus elementos no cero. En el caso (1) del Lema 2.2.4, $\mathfrak{m}^2 = \langle \mathrm{y}^2 \rangle = \langle p \rangle$ esto implica $\mathrm{y}^2 = g_1 p$ para algún $g_1 \in \mathbb{T} \setminus \{0\}$.

En el caso (2), $\mathfrak{m}^2 = \langle \mathrm{xy} \rangle = \langle p \rangle$ implica $\mathrm{xy} = w_1 p$, para algún $w_1 \in \mathbb{T} \setminus \{0\}$. Nuevamente, por el Teorema 1.3.4, en el caso (1) hay un epimorfismo

$$\mathrm{A}_{(f_1,g_1)} := \mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2 - f_1\mathrm{Y}^2, \mathrm{Y}^2 - g_1 p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle \to \mathrm{A},$$

y en el caso (2), hay un epimorfismo

$$\mathrm{B}_{(u_1,v_1,w_1)} := \mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2 - u_1\mathrm{XY}, \mathrm{Y}^2 - v_1\mathrm{XY}, \mathrm{XY} - w_1 p, p\mathrm{X}, p\mathrm{Y} \rangle \to \mathrm{A},$$

donde $u_1, v_1, w_1, f_1, g_1 \in \mathbb{T}$ son tales que w_1, f_1 y g_1 son no cero y $\tilde{u}_1\tilde{v}_1 \neq \tilde{1}$ en $\mathbb{F}_{p^d}$. Por el Lema 1.3.12 se sigue que $\mathrm{A}_{(f_1,g_1)}$ y $\mathrm{B}_{(u_1,v_1,w_1)}$ son anillos locales con ideal maximal $\langle \mathrm{x}, \mathrm{y} \rangle$ y campo residual $\mathbb{F}_{p^d}$. Obsérvese que cualquier elemento de los anillos $\mathrm{A}_{(f_1,g_1)}$ o $\mathrm{B}_{(u_1,v_1,w_1)}$ se pueden escribir de manera única como $a + b\mathrm{x} + c\mathrm{y}$, donde $a \in \mathrm{GR}(p^2,d)$ y $b, c \in \mathbb{T}$, y los elementos de sus ideales maximales están dados por $ap + b\mathrm{x} + c\mathrm{y}$, donde $a, b, c \in \mathbb{T}$. En consecuencia $|\mathrm{A}_{(f_1,g_1)}| = |\mathrm{B}_{(u_1,v_1,w_1)}| = p^{4d}$ y en cada caso el epimorfismo mencionado es un isomorfismo.

Obsérvese que los anillos $\mathrm{A}_{(f_1,g_1)}$ y $\mathrm{B}_{(u_1,v_1,w_1)}$ son determinados por elementos particulares $u_1, v_1, w_1, f_1, g_1 \in \mathbb{T}$ tales que w_1, f_1 y g_1 no son cero y $\tilde{u}_1\tilde{v}_1 \neq \tilde{1}$ en $\mathbb{F}_{p^d}$. Nuestro objetivo será probar que para cualesquiera elementos $u, v, w, f, g \in \mathbb{T}$ tales que w, f y g no son cero y $\tilde{u}\tilde{v} \neq \tilde{1}$ en $\mathbb{F}_{p^d}$, los anillos $\mathrm{A}_{(f,g)}$ y $\mathrm{B}_{(u,v,w)}$ definidos de la misma forma, es decir remplazando u, v, w, f, g por u_1, v_1, w_1, f_1, g_1 respectivamente, son los que se afirman en la Proposición. Sean x y y los elementos en estos anillos que conrresponden a la clase de X y Y, respectivamente, módulo sus ideales respectivos. Por el Lema 1.3.12 se tiene que estos anillos son locales con ideal maximal $\mathfrak{m} = \langle \mathrm{x}, \mathrm{y} \rangle$ y se satisfacen las relaciones $\mathrm{x}^2 = f\mathrm{y}^2, \mathrm{y}^2 = gp, \mathrm{xy} = p\mathrm{x} = p\mathrm{y} = 0$ en el caso del anillo $\mathrm{A}_{(f,g)}$; y $\mathrm{x}^2 = u\mathrm{xy}, \mathrm{y}^2 = v\mathrm{xy}, \mathrm{xy} = wp, p\mathrm{x} = p\mathrm{y} = 0$ en el caso del anillo $\mathrm{B}_{(u,v,w)}$. Sus elementos se pueden escribir de manera única como $a + bx + cy$, donde $a \in \mathrm{GR}(p^2,d)$ y $b, c \in \mathbb{T}$; y los elementos del ideal maximal se pueden escribir de manera única como $ap + b\mathrm{x} + c\mathrm{y}$, donde $a, b, c \in \mathbb{T}$.

Obsérvese que si $u, v, w \in \mathbb{T}$ son tales que u y w son no cero, entonces $\mathrm{B}_{(u,v,w)} \cong \mathrm{A}_{(1,1)}$ si y sólo si existen $a, a_1, b, b_1, c, c_1 \in \mathbb{T}$ tales que $\{\alpha = ap + b\mathrm{x} + c\mathrm{y}, \beta = a_1 p + b_1\mathrm{x} + c_1\mathrm{y}\}$ es un conjunto mínimo de generadores del ideal maximal de $\mathrm{A}_{(1,1)}$ y estos elementos satisfacen las relaciones que satisfacen x y y en $\mathrm{B}_{(u,v,w)}$, es decir, $\alpha^2 = u\alpha\beta, \beta^2 = v\alpha\beta, \alpha\beta = wp, p\alpha = p\beta = 0$. De estas relaciones, la aritmética en $\mathrm{A}_{(1,1)}$ y las expresiones para α y β se tiene:
$(b^2 + c^2)p = uwp$,

$(b_1^2 + c_1^2)p = vwp$ y
$(bb_1 + cc_1)p = wp$, en $\mathrm{GR}(p^2, d)$.
Estas relaciones son ciertas si y sólo si existen $b, b_1, c, c_1 \in \mathbb{T}$ tales que
$\tilde{b}^2 + \tilde{c}^2 = \tilde{u}\tilde{w}$,
$\tilde{b}_1^2 + \tilde{c}_1^2 = \tilde{v}\tilde{w}$ y
$\tilde{b}\tilde{b}_1 + \tilde{c}\tilde{c}_1 = \tilde{w}$ en $\mathbb{F}_{p^d}$
estas ecuaciones tienen solución si y sólo si $\sqrt{\tilde{u}\tilde{v} - \tilde{1}} \in \mathbb{F}_{p^d}$, por el inciso (5) de la Proposición 2.2.1.
Por el argumento anterior, cuando $u, v, w \in \mathbb{T}$ son tales que u y w no son cero y $\sqrt{\tilde{u}\tilde{v} - \tilde{1}} \in \mathbb{F}_{p^d}$, es fácil ver que un isomorfismo de $\mathrm{B}_{(u,v,w)}$ en $\mathrm{A}_{(1,1)}$ está dado por: $\mathrm{x} \mapsto b\mathrm{x} + c\mathrm{y}$ y $\mathrm{y} \mapsto b_1\mathrm{x} + c_1\mathrm{y}$, donde $b, b_1, c, c_1 \in \mathbb{T}$ son tales que su imagen en $\mathbb{F}_{p^d}$ es una solución del sistema de ecuaciones del inciso (5) de la Proposición 2.2.1. Esto es:

(1) Si p es impar, u y w no son cero, $\sqrt{\tilde{u}\tilde{v} - \tilde{1}} \in \mathbb{F}_{p^d}$ y $\frac{\tilde{w}}{\tilde{u}} = \tilde{\zeta}^{2k}$.
Un isomorfismo de $\mathrm{B}_{(u,v,w)}$ en $\mathrm{A}_{(1,1)}$ está dado por:

$$\mathrm{x} \mapsto u\zeta^k\mathrm{x} \qquad \mathrm{y} \mapsto \zeta^k\mathrm{x} + \zeta^k\xi\mathrm{y},$$

donde $\xi \in \mathbb{T}$ es tal que $\tilde{\xi} = \sqrt{\tilde{u}\tilde{v} - \tilde{1}}$.

(2) Si p es impar, u y w no son cero, $\sqrt{\tilde{u}\tilde{v} - \tilde{1}} \in \mathbb{F}_{p^d}$ y $\frac{\tilde{w}}{\tilde{u}} = \tilde{\zeta}^{2k+1}$.
Un isomorfismo de $\mathrm{B}_{(u,v,w)}$ en $\mathrm{A}_{(1,1)}$ está dado por:

$$\mathrm{x} \mapsto u\zeta^k[\gamma_1\mathrm{x} + \gamma_2\mathrm{y}] \qquad \mathrm{y} \mapsto \zeta^k[(\gamma_1 + \gamma_2\xi)\mathrm{x} + (\gamma_2 - \gamma_1\xi)\mathrm{y}],$$

donde $\xi, \gamma_1, \gamma_2 \in \mathbb{T}$ son tales que $\tilde{\xi} = \sqrt{\tilde{u}\tilde{v} - \tilde{1}}$ y $\tilde{\gamma}_1^2 + \tilde{\gamma}_2^2 = \tilde{\zeta}$.

(3) Si $p = 2$ y u y w no son cero.
Un isomorfismo de $\mathrm{B}_{(u,v,w)}$ en $\mathrm{A}_{(1,1)}$ está dado por:

$$\mathrm{x} \mapsto a\mathrm{x} \qquad \mathrm{y} \mapsto a_1\mathrm{x} + b_1\mathrm{y},$$

donde $a, a_1, b_1 \in \mathbb{T}$ son tales que $\tilde{a} = \sqrt{\tilde{u}\tilde{w}}$, $\tilde{a}_1 = \sqrt{\frac{\tilde{w}}{\tilde{u}}}$ y $\tilde{b}_1 = \sqrt{\frac{\tilde{w}}{\tilde{u}}}\sqrt{\tilde{u}\tilde{v} - \tilde{1}}$.

De manera similar se obtienen los siguientes mapeos, que es fácil verificar son isomorfismos entre los respectivos anillos.

(4) Si p es impar, u y w son no cero, $\sqrt{\tilde{u}\tilde{v}-\tilde{1}} \notin \mathbb{F}_{p^d}$ y $\frac{\tilde{w}}{\tilde{u}} = \tilde{\zeta}^{2k}$.
Un isomorfismo de $\mathrm{B}_{(u,v,w)}$ en $\mathrm{A}_{(\zeta,1)}$ está dado por:

$$\mathrm{x} \mapsto u\zeta^k \mathrm{y} \qquad \mathrm{y} \mapsto \zeta^k[\mathrm{y} + \xi \mathrm{x}],$$

donde $\xi \in \mathbb{T}$ es tal que $\tilde{\xi} = \sqrt{\frac{\tilde{u}\tilde{v}-\tilde{1}}{\tilde{\zeta}}}$.

(5) Si p es impar, u y w son no cero, $\sqrt{\tilde{u}\tilde{v}-\tilde{1}} \notin \mathbb{F}_{p^d}$ y $\frac{\tilde{w}}{\tilde{u}} = \tilde{\zeta}^{2k+1}$.
Un isomorfismo de $\mathrm{B}_{(u,v,w)}$ en $\mathrm{A}_{(\zeta,1)}$ está dado por:

$$\mathrm{x} \mapsto u\zeta^k \mathrm{x} \qquad \mathrm{y} \mapsto \zeta^k[\mathrm{x} + \xi\zeta \mathrm{y}],$$

donde $\xi \in \mathbb{T}$ es tal que $\tilde{\xi} = \sqrt{\frac{\tilde{u}\tilde{v}-\tilde{1}}{\tilde{\zeta}}}$.

(6) Si p es impar y $\sqrt{-\tilde{1}} \in \mathbb{F}_{p^d}$.
Un isomorfismo de $\mathrm{B}_{(0,0,w)}$ en $\mathrm{A}_{(1,1)}$ está dado por:

$$\mathrm{x} \mapsto w(\mathrm{x} + \xi \mathrm{y}) \qquad \mathrm{y} \mapsto \frac{1}{2}\mathrm{x} - \frac{\xi}{2}\mathrm{y},$$

donde $\xi \in \mathbb{T}$ es tal que $\tilde{\xi} = \sqrt{-\tilde{1}}$.

(7) Si p es impar y $\sqrt{-\tilde{1}} \notin \mathbb{F}_{p^d}$.
Un isomorfismo de $\mathrm{B}_{(0,0,w)}$ en $\mathrm{A}_{(\zeta,1)}$ está dado por:

$$\mathrm{x} \mapsto w(\mathrm{x} + \zeta^{h+1}\mathrm{y}) \qquad \mathrm{y} \mapsto \frac{1}{2\zeta}[\mathrm{x} + \frac{\mathrm{y}}{\zeta^h}],$$

donde $p^d = 4h + 3$ y $(\tilde{1}, \pm\tilde{\zeta}^{h+1})$ es una solución de $\mathrm{X}^2\tilde{\zeta} + \mathrm{Y}^2 = 0$ en $\mathbb{F}_{p^d}$.

(8) Un isomorfismo de $\mathrm{B}_{(u,0,w)}$ en $\mathrm{B}_{(0,u,w)}$ está dado por:

$$\mathrm{x} \mapsto \mathrm{y} \qquad \mathrm{y} \mapsto \mathrm{x}.$$

(9) Un isomorfismo de $\mathrm{B}_{(0,0,w)}$ en $\mathrm{B}_{(0,0,1)}$ está dado por:

$$\mathrm{x} \mapsto \mathrm{x} \qquad \mathrm{y} \mapsto w\mathrm{y}.$$

(10) Un isomorfismo de $A_{(\zeta^{2i+1},\zeta^{2j})}$ en $A_{(\zeta,1)}$ está dado por:

$$x \mapsto \zeta^{i+j}x \qquad y \mapsto \zeta^{j}y.$$

(11) Un isomorfismo de $A_{(\zeta^{2i},\zeta^{2j})}$ en $A_{(1,1)}$ está dado por:

$$x \mapsto \zeta^{i+j}x \qquad y \mapsto \zeta^{j}y.$$

(12) Un isomorfismo de $A_{(\zeta^{2i+1},\zeta^{2j+1})}$ en $A_{(\zeta,1)}$ está dado por:

$$x \mapsto \zeta^{i+j+1}y \qquad y \mapsto \zeta^{j}x.$$

(13) Un isomorfismo de $A_{(\zeta^{2i},\zeta^{2j+1})}$ en $A_{(1,1)}$ está dado por:

$$x \mapsto \zeta^{i+j}(\gamma_1 x + \gamma_2 y) \qquad y \mapsto \zeta^{j}(-\gamma_2 x + \gamma_1 y),$$

donde $\gamma_1, \gamma_2 \in \mathbb{T}$ son tales que $\tilde{\gamma}_1^2 + \tilde{\gamma}_2^2 = \tilde{\zeta}$.

Por otra parte, $A_{(1,1)} \cong A_{(\zeta,1)}$ si y sólo si existen $a, a_1, b, b_1, c, c_1 \in \mathbb{T}$ tales que $\{\alpha = ap + bx + cy, \beta = a_1 p + b_1 x + c_1 y\}$ es un conjunto mínimo de generadores del ideal maximal de $A_{(1,1)}$, y esos elementos deben satisfacer las relaciones que satisfacen x y y en $A_{(\zeta,1)}$, es decir, $\alpha^2 = \zeta\beta^2$, $\beta^2 = p$, $\alpha\beta = 0$ y $p\alpha = p\beta = 0$. Estas relaciones, la aritmética en $A_{(1,1)}$ y las expresiones para α y β son equivalentes a:

(1) $(b^2 + c^2)p = \zeta(b_1^2 + c_1^2)p$,

(2) $(b_1^2 + c_1^2)p = p$,

(3) $(bb_1 + cc_1)p = 0$, en $\mathrm{GR}(p^2, d)$.

Estas relaciones son ciertas si y sólo si existen $b, b_1, c, c_1 \in \mathbb{T}$ tales que

(1) $\tilde{b}^2 + \tilde{c}^2 = \tilde{\zeta}$,

(2) $\tilde{b}_1^2 + \tilde{c}_1^2 = \tilde{1}$,

(3) $\tilde{b}\tilde{b}_1 + \tilde{c}\tilde{c}_1 = 0$.

si y sólo si $p = 2$, por (6) de la Proposición 2.2.1.
Finalmente, para $p = 2$, puesto que todos los elementos del ideal maximal de $\mathrm{B}_{(0,0,1)}$ tienen cuadrado cero y el elemento $\mathrm{x} \in \mathrm{A}_{(1,1)}$ es tal que $\mathrm{x}^2 = \mathrm{y}^2 \neq 0$, entonces $\mathrm{B}_{(0,0,1)} \ncong \mathrm{A}_{(1,1)}$.

PROPOSICIÓN 2.2.3 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_{p^d}) \in \mathfrak{L}_4$ *tal que* $\mathrm{car}(\mathrm{A}) = p^2$ *y* $p \notin \mathfrak{m}^2$. *Entonces*

(*1*) *Si* p *es impar, el anillo* A *es isomorfo al siguiente anillo*
$\mathrm{GR}(p^2, d)[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$.

(*2*) *Si* $p = 2$, *el anillo* A *es isomorfo a alguno de los siguientes anillos*
$\mathrm{GR}(4, d)[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$,
ó
$\mathrm{GR}(4, d)[\mathrm{X}]/\langle \mathrm{X}^2 - 2\mathrm{X} \rangle$.

Demostración.
Por el Teorema 1.3.4 se puede suponer que el anillo de Galois $\mathrm{GR}(p^2, d)$ está contenido en A y sea $\mathbb{T} = \{0, 1, \zeta, \ldots, \zeta^{p^d-2}\}$ el conjunto de Teichmüller de este anillo de Galois. Sea $\mathrm{x} \in \mathfrak{m} \setminus \mathfrak{m}^2$ tal que $\{p, \mathrm{x}\}$ es un conjunto mínimo de generadores del ideal maximal $\mathfrak{m}$ que satisface las afirmaciones (1) o (2) del Lema 2.2.4 para algunos valores $f_1, u_1, v_1 \in \mathbb{T}$, con $f_1 \neq 0$ y $\tilde{u}_1\tilde{v}_1 \neq 1$ en $\mathbb{F}_{p^d}$.
Notar que en el caso (1) del Lema 2.2.4 se debe tener, $p\mathrm{x} = 0$, $\mathrm{x}^2 = f_1 p^2 \neq 0$, que es una contradición.
De esta manera resta analizar el caso (2) del Lema 2.2.4. Las relaciones son $p\mathrm{x} \neq 0$, $\mathrm{x}^2 + u_1 p\mathrm{x} = 0$ y $v_1 p\mathrm{x} = 0$, lo cual implica que $v_1 \neq 0$. Nuevamente, por el Teorema 1.3.4, en el caso (2) hay un epimorfismo

$$\mathrm{A}_{u_1} = \mathrm{GR}(p^2, d)[\mathrm{X}]/\langle \mathrm{X}^2 + u_1 p\mathrm{X} \rangle \to \mathrm{A}.$$

Puesto que $\mathrm{X}^4 = \mathrm{X}^4 - u_1^2 p^2 \mathrm{X}^2 = (\mathrm{X}^2 - u_1 p\mathrm{X})(\mathrm{X}^2 + u_1 p\mathrm{X}) \in \langle \mathrm{X}^2 + u_1 p\mathrm{X} \rangle$, entonces A_{u_1} es anillo local con ideal maximal $\langle p, \mathrm{x} \rangle$ y campo residual $\mathbb{F}_{p^d}$, por el Lema 1.3.12. Obsérvese que cualquier elemento de este anillo se pueden escribir de manera única como $a + b\mathrm{x}$, donde $a, b \in \mathrm{GR}(p^2, d)$, y los elementos de su ideal maximal se pueden escribir de manera única como $ap + b\mathrm{x}$, donde $a \in \mathbb{T}$ y $b \in \mathrm{GR}(p^2, d)$. En consecuencia $|\mathrm{A}_{u_1}| = p^{4d}$ y el epimorfismo mencionado es un isomorfismo. Puesto que el anillo A_{u_1} es determinado por un elemento particular $u_1 \in \mathbb{T}$. Nuestro objetivo será probar que para cualquier elemento $u \in \mathbb{T}$ los anillos A_u definidos de la misma forma, es decir

remplazando u por u_1, son los que se afirman en la Proposición. Esto se logra usando los mismos argumentos en la demostración de la Proposición 2.2.2 y así se obtienen los siguientes isomorfismos:

(1) Si p es impar.
Un isomorfismo de A_0 en A_u está dado por,

$$\mathrm{x} \mapsto 2\mathrm{x} - up.$$

(2) Si $p = 2$ y $u \neq 0$.
Un isomorfismo de A_u en A_1 está dado por,

$$\mathrm{x} \mapsto u\mathrm{x}.$$

Finalmente, para $p = 2$, puesto que todos los elementos del ideal maximal de A_0 tienen cuadrado cero y el elemento $\mathrm{x} \in \mathrm{A}_1$ es tal que $\mathrm{x}^2 = 2\mathrm{x} \neq 0$, entonces $\mathrm{A}_1 \ncong \mathrm{A}_0$.

PROPOSICIÓN 2.2.4 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_{p^d}) \in \mathfrak{L}_4$ *tal que* $\mathrm{car}(\mathrm{A}) = p^3$ *y* $p \notin \mathfrak{m}^2$. *Entonces*

(*1*) *Si* p *es impar, el anillo* A *es isomorfo a alguno de los siguientes anillos*
$\mathrm{GR}(p^3, d)[\mathrm{X}]/\langle \mathrm{X}^2 - p^2, p\mathrm{X}\rangle$,
ó
$\mathrm{GR}(p^3, d)[\mathrm{X}]/\langle \mathrm{X}^2 - \zeta p^2, p\mathrm{X}\rangle$, $\{0, 1, \ldots, \zeta^{p^d-2}\}$ *es el conjunto de Teichmüller del anillo de Galois* $\mathrm{GR}(p^3, d)$.

(*2*) *Si* $p = 2$, *el anillo* A *es isomorfo al siguiente anillo*
$\mathrm{GR}(8, d)[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X}\rangle$.

Demostración.
Al usar los mismos argumentos que en las Proposiciones 2.2.2 y 2.2.3, ahora con los anillos

$$\mathrm{A}_{(u,v)} = \mathrm{GR}(p^3, d)[\mathrm{X}]/\langle \mathrm{X}^2 - up\mathrm{X}, p^2 - vp\mathrm{X}, \mathrm{X}^3\rangle$$

y

$$\mathrm{B}_w = \mathrm{GR}(p^3, d)[\mathrm{X}]/\langle \mathrm{X}^2 - wp^2, p\mathrm{X}\rangle,$$

donde u, v, w son elementos del conjunto de Teichmüller del anillo de Galois $\mathrm{GR}(p^3, d)$, $vw \neq 0$, tales que $\tilde{u}\tilde{v} \neq \tilde{1}$ en $\mathbb{F}_{p^d}$; se obtienen los siguientes isomorfismos:

(1) Si $\sqrt{\tilde{u}\tilde{v}-\tilde{1}} \in \mathbb{F}_{p^d}$.
Un isomorfismo de B_1 en $\mathrm{A}_{(u,v)}$ está dado por:

$$\mathrm{x} \mapsto -\xi p + v\xi \mathrm{x},$$

donde $\xi \in \mathbb{T}$ es tal que $\tilde{\xi} = \frac{\tilde{1}}{\sqrt{\tilde{u}\tilde{v}-\tilde{1}}}$.

(2) Si $\sqrt{\tilde{u}\tilde{v}-\tilde{1}} \notin \mathbb{F}_{p^d}$.
Un isomorfismo de B_ζ en $\mathrm{A}_{(u,v)}$ está dado por:

$$\mathrm{x} \mapsto -\xi p + v\xi \mathrm{x},$$

donde $\xi \in \mathbb{T}$ es tal que $\tilde{\xi} = \sqrt{\frac{\tilde{\zeta}}{\tilde{u}\tilde{v}-\tilde{1}}}$.

(3) Un isomorfismo de $\mathrm{B}_{\zeta^{2k}}$ en B_1 está dado por:

$$\mathrm{x} \mapsto \zeta^k \mathrm{x}.$$

(4) Un isomorfismo de $\mathrm{B}_{\zeta^{2k+1}}$ en B_ζ está dado por:

$$\mathrm{x} \mapsto \zeta^k \mathrm{x}.$$

Finalmente, $\mathrm{B}_1 \cong \mathrm{B}_\zeta$ si y sólo si existen $a, b, c \in \mathbb{T}$ tales que $\{\alpha = ap + bp^2 + c\mathrm{x}, p\}$ es un conjunto mínimo de generadores del ideal maximal de B_1, y estos elementos deben satisfacer las relaciones que satisfacen p y x en B_ζ, es decir, $\alpha^2 = \zeta p^2$ y $p\alpha = 0$. Estas relaciones, la aritmética en B_1 y la expresión para α son equivalentes a: $(a^2 + c^2)p^2 = \zeta p^2$, $ap^2 = 0$. Estas relaciones se satisfacen si y sólo si $\tilde{c}^2 = \tilde{\zeta}$ si y sólo si $p = 2$.

PROPOSICIÓN 2.2.5 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_{p^d}) \in \mathfrak{L}_4$ *tal que* $\mathrm{car}(\mathrm{A}) = p$. *Entonces*

(*1*) *Si* p *es impar, el anillo* A *es isomorfo a alguno de los siguientes anillos*
$\mathbb{F}_{p^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$,
ó
$\mathbb{F}_{p^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$, *donde* ζ *es un elemento primitivo de* $\mathbb{F}_{p^d}$.

(*2*) *Si* $p = 2$, *el anillo* A *es isomorfo a alguno de los siguientes anillos*
$\mathbb{F}_{2^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2 \rangle$,
ó
$\mathbb{F}_{2^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$.

Demostración.
Los mismos argumentos que en las Proposiciones 2.2.2 y 2.2.3 pueden ser usados ahora con los anillos

$$\mathrm{A}_{(u,v)} = \mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2 - u\mathrm{XY}, \mathrm{Y}^2 - v\mathrm{XY}, \mathrm{Y}^3, \mathrm{X}^2\mathrm{Y}\rangle$$

y

$$\mathrm{B}_w = \mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2 - w\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle,$$

donde $u, v, w \in \mathbb{F}_{p^d}$ son tales que $uv \neq 1$ y $w \neq 0$, y se obtienen los isomorfismos:

(1) Si $\sqrt{uv-1} \in \mathbb{F}_{p^d}$ y $u \neq 0$.
Un isomorfismo de $\mathrm{A}_{(u,v)}$ en B_1 está dado por:

$$\mathrm{x} \mapsto u\mathrm{x} \qquad \mathrm{y} \mapsto \mathrm{x} - \sqrt{uv-1}\mathrm{y}.$$

(2) Si $\sqrt{uv-1} \notin \mathbb{F}_{p^d}$ y $u \neq 0$, entonces $\sqrt{\zeta(uv-1)} \in \mathbb{F}_{p^d}$, por el inciso (4) de la Proposición 2.2.1.
Un isomorfismo de $\mathrm{A}_{(u,v)}$ en B_ζ está dado por:

$$\mathrm{x} \mapsto u\mathrm{x} \qquad \mathrm{y} \mapsto \mathrm{x} + \sqrt{\zeta(uv-1)}\mathrm{y}.$$

(3) Si p es impar y $\sqrt{-1} \in \mathbb{F}_{p^d}$.
Un isomorfismo de $\mathrm{A}_{(0,0)}$ en B_1 está dado por:

$$\mathrm{x} \mapsto \mathrm{x} + \sqrt{-1}\mathrm{y} \qquad \mathrm{y} \mapsto \mathrm{x} - \sqrt{-1}\mathrm{y}.$$

(4) Si $\sqrt{-1} \notin \mathbb{F}_{p^d}$ entonces $p^d = 4h+3$ y $(1, \pm\zeta^{h+1})$ es una solución de $\mathrm{X}^2\zeta + \mathrm{Y}^2 = 0$, por el inciso (3) de la Proposición 2.2.1.
Un isomorfismo de $\mathrm{A}_{(0,0)}$ en B_ζ está dado por:

$$\mathrm{x} \mapsto \zeta^{h+1}\mathrm{x} \qquad \mathrm{y} \mapsto \mathrm{x} - \zeta^{h+1}\mathrm{y}.$$

(5) Un isomorfismo de $\mathrm{B}_{\zeta^{2k}}$ en B_1 está dado por:

$$\mathrm{x} \mapsto \zeta^k\mathrm{x} \qquad \mathrm{y} \mapsto \mathrm{y}.$$

(6) Un isomorfismo de $\mathrm{B}_{\zeta^{2k+1}}$ en B_ζ está dado por:

$$\mathrm{x} \mapsto \zeta^k \mathrm{x} \qquad \mathrm{y} \mapsto \mathrm{y}.$$

(7) Un isomorfismo de $\mathrm{A}_{(u,v)}$ en $\mathrm{A}_{(v,u)}$ está dado por:

$$\mathrm{x} \mapsto \mathrm{y} \qquad \mathrm{y} \mapsto \mathrm{x}.$$

Finalmente, $\mathrm{B}_1 \cong \mathrm{B}_\zeta$ si y sólo si existen $a, a_1, b, b_1 \in \mathbb{T}$ tales que $\{\alpha = a\mathrm{x} + b\mathrm{y}, \beta = a_1\mathrm{x} + b_1\mathrm{y}\}$ es un conjunto mínimo de generadores del ideal maximal de B_1, y esos elementos deben satisfacer las relaciones que satisfacen x y y en B_ζ, es decir, $\alpha^2 = \zeta\beta^2$, $\beta^2 \neq 0$ y $\alpha\beta = 0$. De estas relaciones y expresiones para α y β se tiene: $a^2 + b^2 = \zeta(a_1^2 + b_1^2)$, $a_1^2 + b_1^2 \neq 0$ y $aa_1 + bb_1 = 0$ si y sólo si $p = 2$, por el inciso (6) de la Proposición 2.2.1.
Para $p = 2$, puesto que los elementos del ideal maximal de $\mathrm{A}_{(0,0)}$ tienen cuadrado cero y el elemento $\mathrm{x} \in \mathrm{B}_1$ es tal que $\mathrm{x}^2 = \mathrm{y}^2 \neq 0$, entonces $\mathrm{A}_{(0,0)} \ncong \mathrm{B}_1$.

El siguiente Teorema es un resumen de los resultados de las Proposiciones anteriores.

TEOREMA 2.2.1 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_{p^d})$ *un anillo local finito de Frobenius no de cadena y de longitud* 4. *Entonces* A *es isomorfo a alguno de los siguientes anillos:*

(*a*) *Si* p *es impar*

(*1*) $\mathrm{GR}(p^2, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$.
Este anillo tiene característica p^2 *y* $p \in \mathfrak{m}^2$.

(*2*) $\mathrm{GR}(p^2, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta\mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$,
donde $\{0, 1, \ldots, \zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^2, d)$.
Este anillo tiene característica p^2 *y* $p \in \mathfrak{m}^2$.

(*3*) $\mathrm{GR}(p^2, d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$.
Este anillo tiene característica p^2 *y* $p \notin \mathfrak{m}^2$.

(*4*) $\mathrm{GR}(p^3, d)[\mathrm{X}]/\langle \mathrm{X}^2 - p^2, p\mathrm{X}\rangle$.
Este anillo tiene característica p^3 *y* $p \notin \mathfrak{m}^2$.

(*5*) $\mathrm{GR}(p^3, d)[\mathrm{X}]/\langle \mathrm{X}^2 - \zeta p^2, p\mathrm{X}\rangle$,
donde $\{0, 1, \ldots, \zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^3, d)$.
Este anillo tiene característica p^3 *y* $p \notin \mathfrak{m}^2$.

(*6*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$.
Este anillo tiene característica p.

(*7*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$,
donde ζ *es un elemento primitivo de* $\mathbb{F}_{p^d}$.
Este anillo tiene característica p.

(*b*) *Si* $p=2$*:*

(*8*) $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y}\rangle$.
Este anillo tiene característica 4 *y* $2\in\mathfrak{m}^2$.

(*9*) $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY}-2, 2\mathrm{X}, 2\mathrm{Y}\rangle$.
Este anillo tiene característica 4 *y* $2\in\mathfrak{m}^2$.

(*10*) $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$.
Este anillo tiene característica 4 *y* $2\notin\mathfrak{m}^2$.

(*11*) $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2-2\mathrm{X}\rangle$.
Este anillo tiene característica 4 *y* $2\notin\mathfrak{m}^2$.

(*12*) $\mathrm{GR}(8,d)[\mathrm{X}]/\langle \mathrm{X}^2-4, 2\mathrm{X}\rangle$.
Este anillo tiene característica 8 *y* $2\notin\mathfrak{m}^2$.

(*13*) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$.
Este anillo tiene característica 2.

(*14*) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$.
Este anillo tiene característica 2.

Observación 4 *Observar que los conjuntos mínimos de generadores de los ideales maximales de los anillos* $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$ *y* $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$, *donde* $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^2,d)$, *no satisfacen las mismas relaciones.*
La misma observación para los pares de anillos siguientes:

(*1*) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-p^2, p\mathrm{X}\rangle$ *y* $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-\zeta p^2, p\mathrm{X}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^3,d)$.

(*2*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$ *y* $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$,
donde ζ *es un elemento primitivo de* $\mathbb{F}_{p^d}$.

(*3*) $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y}\rangle$ *y* $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY}-2, 2\mathrm{X}, 2\mathrm{Y}\rangle$.

(*4*) $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$ *y* $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2-2\mathrm{X}\rangle$.

(*5*) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$ *y* $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$.

Observación 5 *Para el anillo* $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$, *donde* $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller del anillo de Galois* $\mathrm{GR}(p^2,d)$, ζ *se puede cambiar por cualquier elemento* η *del conjunto de Teichmüller tal que* $\tilde{\eta}$ *sea un elemento primitivo de* $\mathbb{F}_{p^d}$. *Pues si* $\zeta=\eta+m$, *donde* m *es un elemento en el ideal maximal del anillo, entonces* $m\mathrm{y}^2=0$ *y* $\mathrm{x}^2-\zeta\mathrm{y}^2=\mathrm{x}^2-\eta\mathrm{y}^2$, *pues el índice de nilpotencia del ideal maximal es* 3.
La misma afirmación se tiene para los siguientes anillos

(*1*) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-\zeta p^2, p\mathrm{X}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^3,d)$.

(*2*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$,
donde ζ *es un elemento primitivo de* $\mathbb{F}_{p^d}$.

Sea $(\mathrm{A},\mathfrak{m},\mathbb{F}_{p^d})\in\mathfrak{F}_3$ tal que A tiene p^4 elementos. Por el Lema 1.3.6, $3\leq\ell_{\mathrm{A}}(\mathrm{A})$, por el inciso (4) del Lema 2.1.1 y dado que A no es anillo de cadena $4\leq\ell_{\mathrm{A}}(\mathrm{A})$. Puesto que $|\mathrm{A}|=p^4=(p^d)^{\ell_{\mathrm{A}}(\mathrm{A})}$, entonces $d=1$, $\ell_{\mathrm{A}}(\mathrm{A})=4$ y se tiene el siguiente resultado:

Corolario 2.2.1 *Sea* $(\mathrm{A},\mathfrak{m},\mathbb{F}_p)$ *un anillo local finito de Frobenius no de cadena y con* p^4 *elementos. Entonces* A *es isomorfo a uno de los siguientes anillos:*

(*1*) $\mathrm{car}(\mathrm{A})=p^2$ *y* $p\in\mathfrak{m}^2$.
Si p *es impar y* $\zeta\in\mathbb{Z}_{p^2}$ *es tal que* $\tilde{\zeta}$ *es un elemento primitivo de* $\mathbb{F}_p$:
$\mathbb{Z}_{p^2}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$
ó
$\mathbb{Z}_{p^2}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$.
Si $p=2$:
$\mathbb{Z}_4[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y}\rangle$
ó
$\mathbb{Z}_4[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY}-2, 2\mathrm{X}, 2\mathrm{Y}\rangle$.

(*2*) $\mathrm{car}(\mathrm{A}) = p^2$ *y* $p \notin \mathfrak{m}^2$.
Si p *es impar:*
$\mathbb{Z}_{p^2}[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$.
Si $p = 2$*:*
$\mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$
ó
$\mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2 - 2\mathrm{X} \rangle$.

(*3*) $\mathrm{car}(\mathrm{A}) = p^3$, $p \notin \mathfrak{m}^2$.
Si p *es impar y* $\zeta \in \mathbb{Z}_{p^3}$ *es tal que* $\tilde{\zeta}$ *es un elemento primitivo de* $\mathbb{F}_p$*:*
$\mathbb{Z}_{p^3}[\mathrm{X}]/\langle \mathrm{X}^2 - p^2, p\mathrm{X} \rangle$
ó
$\mathbb{Z}_{p^3}[\mathrm{X}]/\langle \mathrm{X}^2 - \zeta p^2, p\mathrm{X} \rangle$.
Si $p = 2$*:*
$\mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X} \rangle$.

(*4*) $\mathrm{car}(\mathrm{A}) = p$.
Si p *es impar y* ζ *es un elemento primitivo de* $\mathbb{F}_p$*:*
$\mathbb{F}_p[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$
ó
$\mathbb{F}_p[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$.
Si $p = 2$*:*
$\mathbb{F}_2[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2 \rangle$
ó
$\mathbb{F}_2[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$.

Es importante mencionar que el caso $p = 2$ de este Corolario se puede encontrar en [21].

Capítulo 3

Códigos constacíclicos

Recordemos que $\mathfrak{F}_3$ denota la familia de anillos finitos de Frobenius que no son de cadena y cuyo ideal maximal tiene índice de nilpotencia 3. En este capítulo se definen los códigos γ-constacíclicos sobre anillos, se determina la estructura y el número de códigos constacíclicos sobre los anillos de la familia $\mathfrak{F}_3$, de longitud prima relativa con la característica del campo residual del anillo.

3.1. Códigos constacíclicos lineales sobre anillos

Definición 3.1.1 *Sea* A *un anillo finito conmutativo con identidad. El conjunto* A^n *es considerado como* A*-módulo de la manera usual. Un subconjunto* C *de* A^n *es llamado código lineal de longitud* n *sobre* A *si* C *es un* A*-submódulo de* A^n.

Definición 3.1.2 *Sea* A *un anillo conmutativo con identidad y* γ *una unidad de* A.

(*1*) *La permutación* γ*-constacíclico de* A^n, σ_γ, *es la permutación de* A^n *dada por* $\sigma_\gamma(a_0, a_1, \ldots, a_i, \ldots, a_{n-1}) = (\gamma a_{n-1}, a_0, a_1, \ldots, a_i, \ldots, a_{n-2})$.

(*2*) *Un código lineal de longitud* n *sobre* A *es* γ*-constacíclico si* $\sigma_\gamma(\mathrm{C}) = \mathrm{C}$.

(*3*) *La función* $\rho_\gamma : \mathrm{A}^n \to \mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$, *dada por*

$$\rho_\gamma(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2 + \ldots + a_{n-1}\mathrm{T}^{n-1} + \langle \mathrm{T}^n - \gamma \rangle,$$

es un isomorfismo de A*-módulos, llamada la representación polinomial de* A^n.

(*4*) *Si* $\gamma = 1$, *entonces los códigos* γ*-constacíclicos son llamados simplemente códigos cíclicos.*

(*5*) *Si* $\gamma = -1$, *entonces los códigos* γ*-constacíclicos son llamados simplemente códigos negacíclicos.*

Presentamos el siguiente resultado sin una demostración, su demostración se puede encontrar por ejemplo en ([6]).

PROPOSICIÓN 3.1.1 *Sean* A *un anillo conmutativo con identidad,* γ *una unidad de* A *y* C *un código lineal de longitud* n *sobre* A. *Entonces* C *es* γ*-constacíclico si y sólo si* $\rho_\gamma(\mathrm{C})$ *es un ideal de* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$.

Para el siguiente Lema recordar que si A es un anillo, $\mathcal{L}(\mathrm{A})$ es la retícula de ideales de A.

LEMA 3.1.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* $l = \ell_{\mathrm{A}}(\mathrm{A})$, γ *una unidad de* A *y* n *un entero primo relativo con* q. *Sean* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$, *la representación de* $\mathrm{T}^n - \gamma$ *como producto de polinomios básicos irreducibles coprimos a pares de* $\mathrm{A}[\mathrm{T}]$, $s_i = \deg(\tilde{\mathrm{f}}_i)$ *y* $\mathrm{B}_i = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_i \rangle$. *Entonces*

(*1*) $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle \cong \oplus_{i=1}^{r} \mathrm{B}_i$.

(*2*) *Cada ideal* I *de* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$ *es una suma directa de ideales de los anillos* B_i *y hay una partición de* $[1, \ldots, r]$, *digamos* $\mathrm{U}_0, \mathrm{U}_1, \ldots, \mathrm{U}_l$, *donde* $\mathrm{U}_i = \{u \in [1, r] : \ell_{\mathrm{B}_u}(\mathrm{I}_u) = i\}$, *tal que:*

$$\mathrm{I} = \bigoplus_{u \in \mathrm{U}_0} \mathrm{I}_u \oplus \bigoplus_{u \in \mathrm{U}_1} \mathrm{I}_u \oplus \ldots \oplus \bigoplus_{u \in \mathrm{U}_{l-1}} \mathrm{I}_u \oplus \bigoplus_{u \in \mathrm{U}_l} \mathrm{I}_u.$$

(*3*) *Sea* I *y* $\mathrm{U}_0, \mathrm{U}_1, \ldots, \mathrm{U}_l$ *como en el inciso* (*2*), *entonces:*

$$|\mathrm{I}| = q^{\sum_{u \in \mathrm{U}_1} s_u + 2 \sum_{u \in \mathrm{U}_2} s_u + \ldots + (l-1) \sum_{u \in \mathrm{U}_{l-1}} s_u + l \sum_{u \in \mathrm{U}_l} s_u}.$$

(*4*) *El número de códigos* γ*-constacíclicos de longitud* n *sobre* A *es:*

$$|\mathcal{L}(\mathrm{B}_1)| \cdots |\mathcal{L}(\mathrm{B}_r)|.$$

Demostración.
(1) El hecho de que el polinomio $\mathrm{T}^n - \gamma$ se pueda expresar como producto de polinomios básicos irreducibles coprimos a pares lo garantiza el Lema 1.3.17. El resultado se sigue del Teorema Chino del Residuo.
(2) La primera afirmación se sigue de la Proposición 1.1.2. Sea $\mathrm{I} \cong \mathrm{I}_1 \oplus \mathrm{I}_2 \oplus \ldots \oplus \mathrm{I}_r$, donde cada I_i es un ideal de B_i. Por el inciso (1) del Lema 1.3.11, A y B_i tienen la misma longitud. En consecuencia para cada $i \in \{1, \ldots, r\}$, se tiene $\ell_{\mathrm{B}_i}(\mathrm{I}_i) \in \{0, 1, \ldots, \ell_{\mathrm{A}}(\mathrm{A})\}$. Sea $\mathrm{U}_i = \{u \in [1, r] : \ell_{\mathrm{B}_u}(\mathrm{I}_u) = i\}$, es decir U_i es el conjunto de índices $1 \leq u \leq r$ con la propiedad que la componente I_u del ideal I tiene longitud i. Después de renumerar si es necesario, es claro que los conjuntos $\mathrm{U}_0, \mathrm{U}_1, \ldots, \mathrm{U}_r$ satisfacen la afirmación.
(3) Sea $u \in \mathrm{U}_i$, por el inciso (3) del Lema 1.3.9, el campo residual de B_u es $\mathbb{F}_{q^{s_u}}$. Por otra parte, por la fórmula del Lema 1.3.4, $|\mathrm{M}| = |\mathbb{F}_q|^{\ell_{\mathrm{A}}(\mathrm{M})}$, donde $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ es un anillo local y M un A-módulo, se tiene que $|\mathrm{I}_u| = |\mathbb{F}_{q^{s_u}}|^i = q^{is_u}$. De donde se sigue la afirmación.
(4) Se sigue del hecho de que la retícula de ideales de un producto cartesiano finito de anillos es el producto cartesiano de las retículas de ideales de los factores del producto, por la Proposición 1.1.2.

COROLARIO 3.1.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* γ *una unidad de* A *y* n *un entero primo relativo con* q. *Sea* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$, *la representación de* $\mathrm{T}^n - \gamma$ *como producto de polinomios básicos irreducibles coprimos a pares de* $\mathrm{A}[\mathrm{T}]$. *Entonces el número de códigos* γ*-constacíclicos lineales de longitud* n *sobre* A *es mayor o igual a* $|\mathcal{L}(\mathrm{A})|^r$.

Demostración.
Sea $\mathrm{B}_i = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_i \rangle$, para $1 \leq i \leq r$. Por el inciso (2) del Lema 1.3.10, $|\mathcal{L}(\mathrm{A})| \leq |\mathcal{L}(\mathrm{B}_i)|$. Por el inciso (4) del Lema 3.1.1, el número de códigos cíclicos lineales de longitud n sobre A es $|\mathcal{L}(\mathrm{B}_1)||\mathcal{L}(\mathrm{B}_2)| \cdots |\mathcal{L}(\mathrm{B}_r)|$. De las dos relaciones se sigue la afirmación.

El siguiente resultado es una caracterización de anillos finitos de cadena en términos del número de sus códigos constacíclicos, de longitud prima relativa con la característica del campo residual del anillo.

TEOREMA 3.1.1 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathrm{k})$ *un anillo local finito,* γ *una unidad de* A *y* n *un entero primo relativo con* q. *Sea* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$, *la representación de* $\mathrm{T}^n - \gamma$ *como producto*

de polinomios básicos irreducibles coprimos a pares de $\mathrm{A}[\mathrm{T}]$*. Entonces el número de códigos* γ*-constacíclicos de longitud* n *es* $|\mathcal{L}(\mathrm{A})|^r$ *si y sólo si* A *es un anillo de cadena.*

Demostración.
$\Rightarrow$) Sea $\mathrm{B}_i = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_i \rangle$, para $1 \leq i \leq r$. Por el inciso (2) del Lema 1.3.10, $|\mathcal{L}(\mathrm{A})| \leq |\mathcal{L}(\mathrm{B}_i)|$. Supóngase que A no es anillo de cadena, entonces $|\mathcal{L}(\mathrm{A})| < |\mathcal{L}(\mathrm{B}_i)|$, para cualquier $1 \leq i \leq r$, por el Teorema 2.1.1 y la observación anterior. Sea $s_i = \deg(\tilde{\mathrm{f}}_i)$ para $1 \leq i \leq r$. Entonces, $|\mathcal{L}(\mathrm{A})|^r < |\mathcal{L}(\mathrm{B}_1)| \cdots |\mathcal{L}(\mathrm{B}_r)|$, lo cual es una contradicción, por el inciso (4) del Lema 3.1.1 y por nuestra hipótesis. Por lo tanto, A es anillo de cadena.
$\Leftarrow$) Supóngase ahora que A es anillo de cadena, la afirmación se sigue del inciso (4) Lema 3.1.1 y el Teorema 2.1.1

Para hacer más fácil la notación, si $\mathrm{f}(\mathrm{T})$ es un factor de $\mathrm{T}^n - \gamma$, sea $\widehat{\mathrm{f}}(\mathrm{T}) = \frac{\mathrm{T}^n - \gamma}{\mathrm{f}(\mathrm{T})}$ y también sólo escribimos $a_0 + a_1\mathrm{T} + \ldots + a_{n-1}\mathrm{T}^{n-1}$ para la clase que corresponde a $a_0 + a_1\mathrm{T} + \ldots + a_{n-1}\mathrm{T}^{n-1} + \langle \mathrm{T}^n - \gamma \rangle$ en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$.

El siguiente Corolario es el resultado que da la estructura de los códigos γ-constacíclicos sobre anillos de cadena, este resultado es obtenido en [6] y nosotros lo obtenemos a partir de nuestros resultados.

Corolario 3.1.2 *Sea* $(\mathrm{A}, \langle \pi \rangle, \mathbb{F}_q)$ *un anillo de cadena finito,* t *el índice de nilpotencia de* π*,* n *un entero primo relativo con* q *e* I *un ideal de* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$*. Sea* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$*, la representación de* $\mathrm{T}^n - \gamma$ *como producto de polinomios básicos irreducibles coprimos a pares de* $\mathrm{A}[\mathrm{T}]$*. Entonces existen* $\mathrm{F}_0, \mathrm{F}_1, \ldots, \mathrm{F}_t$ *tales que*

(*1*) $\mathrm{T}^n - \gamma = \mathrm{F}_0\mathrm{F}_1 \cdots \mathrm{F}_t$*;*

(*2*) $\mathrm{I} = \langle \pi^{t-1}\widehat{\mathrm{F}}_1, \pi^{t-2}\widehat{\mathrm{F}}_2, \ldots, \pi\widehat{\mathrm{F}}_{t-1}, \widehat{\mathrm{F}}_t \rangle$*;*

(*3*) $|\mathrm{I}| = q^{\deg(\mathrm{F}_1) + 2\deg(\mathrm{F}_2) + \ldots + (t-1)\deg(\mathrm{F}_{t-1}) + t\deg(\mathrm{F}_t)}$.

Demostración.
Sea $\mathrm{B}_i = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_i \rangle$, para $1 \leq i \leq r$. Por el Teorema 2.1.1, B_i es anillo de cadena y su cadena de ideales es

$$\mathrm{B}_i \supset \pi\mathrm{B}_i \supset \pi^2\mathrm{B}_i \supset \ldots \supset \pi^{t-1}\mathrm{B}_i \supset \langle 0 \rangle.$$

Así $\ell_{\mathrm{B}_i}(\mathrm{B}_i) = t$ y $\ell_{\mathrm{B}_i}(\pi^i \mathrm{B}_i) = t-i$. Por el Lema 3.1.1, existe una partición de $[1, \ldots, r]$, $\mathrm{U}_0, \mathrm{U}_1, \ldots, \mathrm{U}_t$, donde $\mathrm{U}_i = \{u \in [1,r] : \ell_{\mathrm{B}_u}(\mathrm{I}_u) = i\}$, tal que:

$$\mathrm{I} = \bigoplus_{u \in \mathrm{U}_0} \mathrm{I}_u \oplus \bigoplus_{u \in \mathrm{U}_1} \mathrm{I}_u \oplus \ldots \oplus \bigoplus_{u \in \mathrm{U}_{t-1}} \mathrm{I}_u \oplus \bigoplus_{u \in \mathrm{U}_t} \mathrm{I}_u$$

y $|\mathrm{I}| = q^{\sum_{u \in \mathrm{U}_1} s_u + 2\sum_{u \in \mathrm{U}_2} s_u + \ldots + (t-1)\sum_{u \in \mathrm{U}_{t-1}} s_u + t\sum_{u \in \mathrm{U}_t} s_u}$. De donde se sigue que

$$\mathrm{I} = \pi^{t-1} \bigoplus_{u \in \mathrm{U}_1} \mathrm{B}_u \oplus \pi^{t-2} \bigoplus_{u \in \mathrm{U}_2} \mathrm{B}_u \oplus \ldots \oplus \pi \bigoplus_{u \in \mathrm{U}_{t-1}} \mathrm{B}_u \oplus \bigoplus_{u \in \mathrm{U}_t} \mathrm{B}_u$$

Del Teorema Chino del Residuo se obtiene que el ideal $\bigoplus_{u \in \mathrm{U}_i} \mathrm{B}_u$ se identifica en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$ con $\langle \widehat{\mathrm{F}}_i \rangle$, donde $\mathrm{F}_i = \prod_{u \in \mathrm{U}_i} \mathrm{f}_u$. De donde se siguen las afirmaciones

3.2. Códigos constacíclicos sobre anillos locales finitos de Frobenius no de cadena y cuyo ideal maximal tiene índice de nilpotencia 3

Recordar que $\mathfrak{F}_3$ es la familia de anillos locales finitos de Frobenius no de cadena y cuyo ideal maximal tiene índice de nilpotencia 3, $\ell_{\mathrm{A}}(\mathrm{M})$ y $\mathrm{v}_{\mathrm{A}}(\mathrm{M})$ denotan la longitud y el número mínimo de generadores del A-módulo M, respectivamente. En esta sección se describe la estructura de códigos γ-constacíclicos sobre la familia $\mathfrak{F}_3$.

LEMA 3.2.1 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{F}_3$ *y* $l = \ell_{\mathrm{A}}(\mathrm{A})$. *Entonces* $l \geq 4$ *y* $\mathrm{v}(\mathfrak{m}) = l - 2$.

Demostración.
Por hipótesis y el Lema 2.1.5, se tiene que $\mathrm{ann}_{\mathrm{A}}(\mathfrak{m}) = \mathfrak{m}^2$ es ideal simple. En consecuencia, por el Lema 1.1.2, $\ell_{\mathrm{A}}(\mathrm{A}) = \ell_{\mathrm{A}}(\mathrm{A}/\mathfrak{m}) + \ell_{\mathrm{A}}(\mathfrak{m}/\mathfrak{m}^2) + \ell_{\mathrm{A}}(\mathfrak{m}^2) = 2 + \ell_{\mathrm{A}}(\mathfrak{m}/\mathfrak{m}^2)$. Puesto que A no es anillo de cadena, entonces $\mathrm{v}(\mathfrak{m}) = \dim_{\mathbb{F}_q}(\mathfrak{m}/\mathfrak{m}^2) = \ell_{\mathrm{A}}(\mathfrak{m}/\mathfrak{m}^2) \geq 2$, de donde se siguen la afirmaciones.

En lo que resta de este trabajo se usará la siguiente notación. Dado un anillo local finito $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ un polinomio básico irreducible, $s = \deg(\tilde{\mathrm{f}})$, $\mathrm{B} = \mathrm{A}/\langle \mathrm{f} \rangle$ la extensión no ramificada de A determinada por f, $\mathbb{T} \subset \mathrm{A}$ un conjunto de representantes de $\mathbb{F}_q$, M un B-módulo, $\overline{\alpha} = \{\alpha_1, \ldots, \alpha_l\}$ una secuencia de elementos de M y $\mathrm{H} = (a_{ij})$ una $(k \times l)$ matriz sobre $\mathbb{F}_{q^s}$.

(1) $\mathbb{T}_s \subset \mathrm{B}$ denotará el conjunto de representantes de $\mathrm{B}/\mathfrak{m}\mathrm{B} = \mathbb{F}_{q^s}$ dado por:

$$\{a_0 + a_1\mathrm{T} + \cdots + a_{s-1}\mathrm{T}^{s-1} : a_i \in \mathbb{T}\}$$

ver inciso (3) del Lema 1.3.9.

(2) Si $a \in \mathbb{F}_{q^s}$, el único representante de a en $\mathbb{T}_s$ será denotado por $a(\mathbb{T}_s)$.

(3) El B-submódulo de M,

$$\langle \sum_{i=1}^{l} a_{1i}(\mathbb{T}_s)\alpha_i, \ldots, \sum_{i=1}^{l} a_{ki}(\mathbb{T}_s)\alpha_i \rangle,$$

será denotado por $\mathrm{H}_{\mathbb{T}_s}(\overline{\alpha})$.

Ejemplo 3.2.1 *Sea* $\mathrm{A} = \mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$, *el anillo local del inciso (2) del Corolario 2.2.1,* $\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^3 + \mathrm{T} + 1 \rangle$, M *un* B*-módulo,* $\overline{\alpha} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ *una secuencia de elementos de* M *y* $\mathrm{H} = \begin{pmatrix} \mathrm{T}^2+\mathrm{T} & 0 & \mathrm{T}+1 & 1 \\ \mathrm{T}^2 & \mathrm{T} & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$ *sobre* $\mathbb{F}_{2^3} \cong \mathbb{F}_2[\mathrm{T}]/\langle \mathrm{T}^3 + \mathrm{T} + 1 \rangle$. *Puesto que* $\mathbb{T} = \{0, 1\} \subset \mathbb{Z}_4 \subset \mathrm{A}$ *es un conjunto de representantes para el campo residual de* A, $\mathbb{T}_3 = \{a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2 : a_i \in \{0, 1\}\} \subset \mathrm{B}$ *es un conjunto de representantes para el campo residual de* B. *Entonces*

$$\mathrm{H}_{\mathbb{T}_3}(\overline{\alpha}) = \langle (\mathrm{T}^2 + \mathrm{T})\alpha_1 + (\mathrm{T} + 1)\alpha_3 + \alpha_4, \mathrm{T}^2\alpha_1 + \mathrm{T}\alpha_2 + \alpha_3, \alpha_1 + \alpha_4 \rangle.$$

Obsérvese que el 1 *en la matriz* H *tiene orden aditivo* 2 *y el* 1 *en* $\mathrm{H}_{\mathbb{T}_3}(\overline{\alpha})$ *tiene orden aditivo* 4.

Para nuestros propósitos requerimos conocer la retícula de ideales de un anillo en la familia $\mathfrak{F}_3$, esto se hará en el siguiente resultado.

Recordar que si $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ es un anillo local finito, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ es un polinomio básico irreducible, $s = \deg(\tilde{\mathrm{f}})$ y $\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f} \rangle$ es la extensión no ramificada de A determinada por f, entonces se tienen las siguientes propiedades, ver Lemas 1.3.9 y 1.3.11.

(1) A y B tienen la misma longitud,

(2) el ideal maximal de B es la expansión del ideal $\mathfrak{m}$ en B,

(3) un conjunto mínimo de generadores de $\mathfrak{m}$ es un conjunto mínimo de generadores de $\mathfrak{m}$B,

(4) el campo residual de B es $\mathbb{F}_{q^s}$.

PROPOSICIÓN 3.2.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{F}_3$, $l = \ell_{\mathrm{A}}(\mathrm{A})$, $\overline{\alpha} = \{\alpha_1, \ldots, \alpha_{l-2}\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$, $\mathbb{T} \subset \mathrm{A}$ *un conjunto de representantes de* $\mathbb{F}_q$, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f} \rangle$ *la extensión no ramificada de* A *determinada por* f. *Entonces los ideales de longitud* $k \in \{2, \ldots, l-2\}$ *de* B *están en correspondencia uno a uno con las* $(k-1) \times (l-2)$ *matrices sobre* $\mathbb{F}_{q^s}$ *en forma escalón reducida por filas. A una matriz* H *le corresponde el ideal* $\mathrm{H}_{\mathbb{T}_s}(\overline{\alpha})$.
En particular, el número de ideales de B *es* $\mathrm{G}(l-2, q^s)+2$, *el número de Galois, (ver Definición 1.2.2).*

Demostración.
Por el inciso (3) del Lema 1.3.10, el índice de nilpotencia del ideal maximal de B es 3. Por el Teorema 2.1.2 y el Lema 2.1.5, B es anillo local de Frobenius y su único ideal minimal es $\mathfrak{m}^2$B. Puesto que A y B tienen la misma longitud, entonces los ideales de longitud $k \in \{2, \ldots, l-2\}$ de B son los que están entre $\mathfrak{m}$B y $\mathfrak{m}^2$B. La afirmación se sigue del Corolario 1.3.1 y del hecho de que $\overline{\alpha} = \{\alpha_1, \ldots, \alpha_{l-2}\}$ es también un conjunto mínimo de generadores de $\mathfrak{m}$B.

El siguiente ejemplo ilustra los resultados de la Proposición anterior.

EJEMPLO 3.2.2 *Sean*

$$\mathrm{I} = \langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{Z}^2, \mathrm{W}^2, \mathrm{XZ} - \mathrm{XY}, \mathrm{XW} - \mathrm{XY}, \mathrm{YZ} - \mathrm{XY}, \mathrm{YW} - \mathrm{XY}, \mathrm{ZW} - \mathrm{XY} \rangle,$$

ideal de $\mathbb{F}_2[\mathrm{X}, \mathrm{Y}, \mathrm{Z}, \mathrm{W}]$, $\mathrm{A}_{(4,2)} = \mathbb{F}_2[\mathrm{X}, \mathrm{Y}, \mathrm{Z}, \mathrm{W}]/\mathrm{I}$, *el anillo del ejemplo 2.1.1,* $\mathrm{x} = \mathrm{X}+\mathrm{I}$, $\mathrm{y} = \mathrm{Y} + \mathrm{I}$, $\mathrm{z} = \mathrm{Z} + \mathrm{I}$, $\mathrm{w} = \mathrm{W} + \mathrm{I}$, $\mathrm{f} \in \mathrm{A}_{(4,2)}[\mathrm{T}]$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A}_{(4,2)}[\mathrm{T}]/\langle \mathrm{f} \rangle$ *la extensión no ramificada de* $\mathrm{A}_{(4,2)}$ *determinada por* f. *Elegir* $\mathbb{T} = \mathbb{F}_2 \subset \mathrm{A}_{(4,2)}$ *como conjunto de representantes para el campo residual de* $\mathrm{A}_{(4,2)}$, *así* $\mathbb{T}_s = \{a_0 + a_1\mathrm{T} + \ldots + a_{s-1}\mathrm{T}^{s-1} : a_i \in \mathbb{F}_2\}$ *es el conjunto de representantes para el campo residual de* B.

(*1*) $\{\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{w}\}$ *es un conjunto mínimo de generadores del ideal maximal de* $\mathrm{A}_{(4,2)}$, $(1, a_1, a_2, a_3)$, $(0, 1, b_1, b_2)$, $(0, 0, 1, c_1)$, $(0, 0, 0, 1)$ *donde* $a_1, a_2, a_3, b_1, b_2, c_1 \in \mathbb{F}_{p^s}$, *son todas las* 1×4 *matrices en forma escalón reducida por filas sobre* $\mathbb{F}_{p^s}$.

$\begin{pmatrix} 1 & 0 & d_1 & d_2 \\ 0 & 1 & d_3 & d_4 \end{pmatrix}, \begin{pmatrix} 1 & e_1 & 0 & e_2 \\ 0 & 0 & 1 & e_3 \end{pmatrix}, \begin{pmatrix} 1 & f_1 & f_2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & g_1 \\ 0 & 0 & 1 & g_2 \end{pmatrix},$
$\begin{pmatrix} 0 & 1 & h_1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, *donde* d_i, e_i ,$f_i, g_i, h_1 \in \mathbb{F}_{p^s}$, *son todas las* 2×4 *matrices en forma escalón reducida por filas sobre* $\mathbb{F}_{p^s}$.

$$\begin{pmatrix} 1 & 0 & 0 & m_1 \\ 0 & 1 & 0 & m_2 \\ 0 & 0 & 1 & m_3 \end{pmatrix}, \begin{pmatrix} 1 & 0 & n_1 & 0 \\ 0 & 1 & n_2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & o_1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

donde $m_i, n_i, o_1 \in \mathbb{F}_{p^s}$, *son todas las* 3×4 *matrices en forma escalón reducida por filas sobre* $\mathbb{F}_{p^s}$. *Entonces los ideales de* $\mathrm{A}_{(4,2)}$ *son:*
Los ideales triviales:

$$\langle 0 \rangle, \ \langle 1 \rangle.$$

El ideal minimal y el ideal maximal:

$$\langle \mathrm{xy} \rangle, \ \langle \mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{w} \rangle.$$

Los ideales de longitud 2*:*

$$\langle \mathrm{x}+a_1\mathrm{y}+a_2\mathrm{z}+a_3\mathrm{w} \rangle, \langle \mathrm{y}+b_1\mathrm{z}+b_2\mathrm{w} \rangle, \langle \mathrm{z}+c_1\mathrm{w} \rangle, \langle \mathrm{w} \rangle, \text{ donde } a_1, a_2, a_3, b_1, b_2, c_1 \in \mathbb{F}_2.$$

Los ideales de longitud 3*:*

$$\langle \mathrm{x} + d_1\mathrm{z} + d_2\mathrm{w}, \mathrm{y} + d_3\mathrm{z} + d_4\mathrm{w} \rangle, \langle \mathrm{x} + e_1\mathrm{y} + e_2\mathrm{w}, \mathrm{z} + e_3\mathrm{w} \rangle, \langle \mathrm{x} + f_1\mathrm{y} + f_2\mathrm{z}, \mathrm{w} \rangle,$$

$$\langle \mathrm{y} + g_1\mathrm{w}, \mathrm{z} + g_2\mathrm{w} \rangle, \langle \mathrm{y} + h_1\mathrm{z}, \mathrm{w} \rangle, \langle \mathrm{z}, \mathrm{w} \rangle, \text{ donde } d_i, e_i, f_i, g_i, h_1 \in \mathbb{F}_2.$$

Los ideales de longitud 4*:*

$$\langle \mathrm{x} + m_1\mathrm{w}, \mathrm{y} + m_2\mathrm{w}, \mathrm{z} + m_3\mathrm{w} \rangle, \langle \mathrm{x} + n_1\mathrm{z}, \mathrm{y} + n_2\mathrm{z}, \mathrm{w} \rangle, \langle \mathrm{x} + o_1\mathrm{y}, \mathrm{z}, \mathrm{w} \rangle,$$

$$\langle \mathrm{y}, \mathrm{z}, \mathrm{w} \rangle, \text{ donde } m_i, n_i, o_1 \in \mathbb{F}_2.$$

(*2*) *Los ideales de* B *tienen la misma expresión que los ideales de* $\mathrm{A}_{(4,2)}$ *pero con los coeficientes* $a_1, a_2, a_3, b_1, b_2, c_1, d_i, e_i, f_i, g_i, h_1, m_i, n_i, o_1$ *en* $\mathbb{T}_s$.

EJEMPLO 3.2.3 *Sean* $\mathrm{A} = \mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X}\rangle$*, el anillo local del inciso (3) del Corolario 2.2.1,* $\mathbb{T} = \{0, 1\} \subset \mathbb{Z}_8 \subset \mathrm{A}$ *es un conjunto de representantes para el campo residual de* A, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$ *la extensión no ramificada de* A *determinada por* f *y* $\mathbb{T}_s = \{a_0 + a_1\mathrm{T} + \ldots + a_{s-1}\mathrm{T}^{s-1} : a_i \in \{0, 1\}\} \subset \mathrm{B}$ *el conjunto de representantes del campo residual de* B.

(*1*) *Puesto que* $\{\mathrm{x}, 2\}$ *es un conjunto mínimo de generadores del ideal maximal de* A, $(1, a)$ *y* $(0, 1)$ *donde* $a \in \mathbb{F}_{2^s}$*, son todas las* 1×2 *matrices en forma escalón reducida por filas sobre* $\mathbb{F}_{2^s}$*. Entonces los ideales de* A *son:*
Los ideales triviales

$$\langle 0\rangle, \langle 1\rangle.$$

El ideal minimal y el ideal maximal

$$\langle 4\rangle, \langle \mathrm{x}, 2\rangle.$$

Los ideales de longitud 2

$$\langle \mathrm{x}\rangle, \langle \mathrm{x} + 2\rangle, \langle 2\rangle.$$

(*2*) *Los ideales de* B *tienen la misma expresión que los ideales de* A *pero con los coeficientes a en* $\mathbb{T}_s$*.*

COROLARIO 3.2.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{F}_3$*,* $l = \ell_{\mathrm{A}}(\mathrm{A})$*,* γ *una unidad de* A *y* n *un entero primo relativo con* q*. Sea* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$*, donde los* $\mathrm{f}_i's$ *son polinomios básicos irreducibles coprimos a pares en* $\mathrm{A}[\mathrm{T}]$*, y* $s_i = \deg(\tilde{\mathrm{f}}_i)$*, para* $i = 1, \ldots, r$*. Entonces el número de códigos* γ*-constacíclicos de longitud* n *sobre* A *es:*

$$[\mathrm{G}(l - 2, q^{s_1}) + 2][\mathrm{G}(l - 2, q^{s_2}) + 2] \cdots [\mathrm{G}(l - 2, q^{s_r}) + 2].$$

Demostración.
La afirmación se sigue del inciso (4) del Lema 3.1.1 y la Proposición 3.2.1.

El resultado principal de esta sección, sobre la estructura de códigos γ-constacíclicos sobre anillos de la familia $\mathfrak{F}_3$, ahora se puede establecer.

Recordemos que si f(T) es un factor de $\mathrm{T}^n - \gamma$, entonces $\widehat{\mathrm{f}}(\mathrm{T}) = \frac{\mathrm{T}^n - \gamma}{\mathrm{f}(\mathrm{T})}$.

TEOREMA 3.2.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{F}_3$*,* $\overline{\alpha} = \{\alpha_1, \ldots, \alpha_{l-2}\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$*,* γ *una unidad de* A*,* $l = \ell_{\mathrm{A}}(\mathrm{A})$*,* $\mathbb{T}$ *y* $\mathbb{T}_s$ *como hasta ahora,* n *un*

entero primo relativo con q y C *un código γ-constacíclico de longitud n sobre* A*. Sean* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$ *la representación de* $\mathrm{T}^n - \gamma$ *como producto de polinomios básicos irreducibles coprimos a pares en* $\mathrm{A}[\mathrm{T}]$ *y* $s_i = \deg(\tilde{\mathrm{f}}_i)$*. Entonces*

(*1*) *Existe una única partición de* $[1, \ldots, r]$, $\mathrm{U}_0, \mathrm{U}_1, \ldots, \mathrm{U}_l$, *donde* $\mathrm{U}_i = \{u \in [1, r] : \ell_{\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_u \rangle}(\mathrm{I}_u) = i\}$.

(*2*) *Para cada* $i \in \{2, \ldots, l-2\}$ *y cada* $u \in \mathrm{U}_i$, *existe una única* $(i-1) \times (l-2)$ *matriz en forma escalón reducida por filas sobre* $\mathbb{F}_{q^{s_u}}$, H_u, *tal que:*

$$\mathrm{C} = \langle \mathfrak{m}^2 \prod_{u \notin \mathrm{U}_1} \mathrm{f}_u, \mathfrak{m} \prod_{u \notin \mathrm{U}_{l-1}} \mathrm{f}_u, \prod_{u \notin \mathrm{U}_l} \mathrm{f}_u, (\mathrm{H}_u)_{\mathbb{T}_{s_u}}(\overline{\alpha})\widehat{\mathrm{f}}_u : u \in \cup_{i=2}^{l-2} \mathrm{U}_i \rangle.$$

$$|\mathrm{C}| = q^{\sum_{u \in \mathrm{U}_1} s_u + 2\sum_{u \in \mathrm{U}_2} s_u + \ldots + (l-1)\sum_{u \in \mathrm{U}_{l-1}} s_u + l \sum_{u \in \mathrm{U}_l} s_u}$$

Demostración.
Sea $\mathrm{B}_i = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_i \rangle$. Por el inciso (2) del Lema 3.1.1, existe una partición de $[1, \ldots, r]$, $\mathrm{U}_0, \mathrm{U}_1, \ldots, \mathrm{U}_l$, donde $\mathrm{U}_i = \{u \in [1, r] : \ell_{\mathrm{B}_u}(\mathrm{I}_u) = i\}$, tal que

$$\mathrm{C} \cong \bigoplus_{u \in \mathrm{U}_0} \mathrm{I}_u \oplus \bigoplus_{u \in \mathrm{U}_1} \mathrm{I}_u \oplus \ldots \oplus \bigoplus_{u \in \mathrm{U}_{l-1}} \mathrm{I}_u \oplus \bigoplus_{u \in \mathrm{U}_l} \mathrm{I}_u,$$

puesto que $\mathfrak{m}^2\mathrm{B}_i$ es el único ideal minimal de B_i y $\mathfrak{m}\mathrm{B}_i$ es el único ideal maximal de B_i, es decir $\mathfrak{m}^2\mathrm{B}_i$ es el único ideal de longitud 1 de B_i y $\mathfrak{m}\mathrm{B}_i$ es el único ideal de longitud $l-1$ de B_i,

$$\mathrm{C} \cong \mathfrak{m}^2 \bigoplus_{u \in \mathrm{U}_1} \mathrm{B}_u \oplus \bigoplus_{u \in \mathrm{U}_2} \mathrm{I}_u \oplus \ldots \oplus \bigoplus_{u \in \mathrm{U}_{l-2}} \mathrm{I}_u \oplus \mathfrak{m} \bigoplus_{u \in \mathrm{U}_{l-1}} \mathrm{B}_u \oplus \bigoplus_{u \in \mathrm{U}_l} \mathrm{B}_u,$$

donde $\mathrm{U}_i = \{u \in [1, r] : \ell_{\mathrm{B}_u}(\mathrm{I}_u) = i\}$.
Sean $i \in \{2, \ldots, l-2\}$ y $u \in \mathrm{U}_i$, por la Proposición 3.2.1, I_u es de la forma $(\mathrm{H}_u)_{\mathbb{T}_{s_u}}(\overline{\alpha})$ y es identificado en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$ por $(\mathrm{H}_u)_{\mathbb{T}_{s_u}}(\overline{\alpha})\widehat{\mathrm{f}}_u$, donde H_u es una $(i-1) \times (l-2)$ matriz en forma escalón reducida por filas sobre $\mathbb{F}_{q^{s_u}}$. También $\bigoplus_{u \in \mathrm{U}_i} \mathrm{B}_u$ es identificado en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$ con $\prod_{u \notin \mathrm{U}_i} \mathrm{f}_u$.
La última afirmación se sigue del inciso (c) del Lema 3.1.1.
Para probar la unicidad, supongamos que $\mathrm{W}_0, \mathrm{W}_1, \ldots, \mathrm{W}_l$ es una partición de $[1, r]$ y para cada $i \in \{2, \ldots, l-2\}$ y cada $u \in \mathrm{U}_i$, sea G_u una $(i-1) \times (l-2)$ matriz en forma escalón reducida por filas sobre $\mathbb{F}_{q^{s_u}}$, entonces:

$$\begin{aligned} \mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle &\cong \bigoplus_{u \in \mathrm{U}_0} \mathrm{B}_u \oplus \bigoplus_{u \in \mathrm{U}_1} \mathrm{B}_u \oplus \ldots \oplus \bigoplus_{u \in \mathrm{U}_{l-1}} \mathrm{B}_u \oplus \bigoplus_{u \in \mathrm{U}_l} \mathrm{B}_u \\ &= \bigoplus_{w \in \mathrm{W}_0} \mathrm{B}_w \oplus \bigoplus_{w \in \mathrm{W}_1} \mathrm{B}_w \oplus \ldots \oplus \bigoplus_{w \in \mathrm{W}_{l-1}} \mathrm{B}_w \oplus \bigoplus_{w \in \mathrm{W}_l} \mathrm{B}_w \end{aligned}$$

y

$$\begin{aligned} \mathrm{C} &\cong \bigoplus_{u \in \mathrm{U}_1} \mathfrak{m}^2 \mathrm{B}_u \oplus \bigoplus_{u \in \mathrm{U}_{l-1}} \mathfrak{m}\mathrm{B}_u \oplus \bigoplus_{u \in \mathrm{U}_l} \mathrm{B}_u \oplus \bigoplus_{u \in \cup_{i=2}^{l-2} \mathrm{U}_i} \langle (\mathrm{H}_u)_{\mathbb{T}_{s_u}}(\overline{\alpha}) \widehat{\mathrm{f}}_u \rangle \\ &= \bigoplus_{w \in \mathrm{W}_1} \mathfrak{m}^2 \mathrm{B}_w \oplus \bigoplus_{w \in \mathrm{W}_{l-1}} \mathfrak{m}\mathrm{B}_w \oplus \bigoplus_{w \in \mathrm{W}_l} \mathrm{B}_w \oplus \bigoplus_{w \in \cup_{i=2}^{l-2} \mathrm{W}_i} \langle (\mathrm{G}_w)_{\mathbb{T}_{s_w}}(\overline{\alpha}) \widehat{\mathrm{f}}_w \rangle. \end{aligned}$$

La afirmación se sigue de la Proposición 3.2.1.

En los siguientes ejemplos se ilustran las ideas del Teorema anterior.

EJEMPLO 3.2.4 *Sean* $\mathrm{A} = \mathbb{F}_2[\mathrm{X}, \mathrm{Y}, \mathrm{Z}, \mathrm{W}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{Z}^2, \mathrm{W}^2, \mathrm{XZ} - \mathrm{XY}, \mathrm{XW} - \mathrm{XY}, \mathrm{YZ} - \mathrm{XY}, \mathrm{YW} - \mathrm{XY}, \mathrm{ZW} - \mathrm{XY} \rangle$*, el anillo del ejemplo 3.2.2, y* γ *una unidad de* A.
Se tiene que $\mathrm{A} \in \mathfrak{F}_3$*,* $\ell_{\mathrm{A}}(\mathrm{A}) = 6$*,* $\{\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{w}\}$ *es un conjunto mínimo de generadores de* $\mathfrak{m}$*, el ideal maximal de* A*,* $\mathfrak{m}^2 = \langle \mathrm{xy} \rangle$ *y* $\mathbb{T} = \mathbb{F}_2$ *es un conjunto de representantes para el campo residual de* A.
Por el ejemplo 1.3.4, $\mathrm{T}^7 - \gamma$ *se factoriza en* $\mathrm{A}[\mathrm{T}]$ *como* $\mathrm{T}^7 - \gamma = \mathrm{f}_1\mathrm{f}_2\mathrm{f}_3$*, donde:*
$\mathrm{f}_1 = \lambda \mathrm{T} + 1$,
$\mathrm{f}_2 = \lambda \mathrm{T}^3 + \mathrm{T}^2 + 1$
$\mathrm{f}_3 = \mathrm{T}^3 + \mathrm{T} + \lambda$.
Entonces $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^7 - \gamma \rangle \cong \mathrm{A} \oplus \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_2 \rangle \oplus \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_3 \rangle$ *y* $\mathbb{T}_3 = \{a_1 + a_2\mathrm{T} + a_3\mathrm{T}^2 : a_i \in \mathbb{F}_2\}$ *es un conjunto de representantes para el campo residual de* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_i \rangle$*,* $i \in \{1, 2\}$*. Y se tiene:*

(*1*) *Si* $\mathrm{U}_0 = \mathrm{U}_1 = \mathrm{U}_2 = \mathrm{U}_4 = \mathrm{U}_5 = \mathrm{U}_6 = \emptyset, \mathrm{U}_3 = \{1, 2, 3\}$*, sean*

$$\mathrm{H}_1 = \begin{pmatrix} 1 & e_1 & 0 & e_2 \\ 0 & 0 & 1 & e_3 \end{pmatrix} \text{ sobre } \mathbb{F}_2,$$

$$\mathrm{H}_2 = \begin{pmatrix} 1 & \alpha_0 + \alpha_1\mathrm{T} + \alpha_2\mathrm{T}^2 & \beta_0 + \beta_1\mathrm{T} + \beta_2\mathrm{T}^2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ sobre } \mathbb{F}_8 \text{ y}$$

$\mathrm{H}_3 = \begin{pmatrix} 0 & 1 & 0 & \eta_0 + \eta_1\mathrm{T} + \eta_2\mathrm{T}^2 \\ 0 & 0 & 1 & \sigma_0 + \sigma_1\mathrm{T} + \sigma_2\mathrm{T}^2 \end{pmatrix}$ *sobre* $\mathbb{F}_8$.
El código asociado es:

$$\begin{aligned} &\langle \mathrm{x} + e_1\mathrm{y} + e_2\mathrm{w}, \mathrm{z} + e_3\mathrm{w}\rangle \quad \oplus \\ &\langle \mathrm{x} + (\alpha_0 + \alpha_1\mathrm{T} + \alpha_2\mathrm{T}^2)\mathrm{y} + (\beta_0 + \beta_1\mathrm{T} + \beta_2\mathrm{T}^2)\mathrm{z}, \mathrm{w}\rangle \quad \oplus \\ &\langle \mathrm{y} + (\eta_0 + \eta_1\mathrm{T} + \eta_2\mathrm{T}^2)\mathrm{w}, \mathrm{z} + (\sigma_0 + \sigma_1\mathrm{T} + \sigma_2\mathrm{T}^2)\mathrm{w}\rangle. \end{aligned}$$

El ideal correspondiente es:

$$\begin{aligned} &\langle (\mathrm{x} + e_1\mathrm{y} + e_2\mathrm{w})\mathrm{f}_2\mathrm{f}_3, (\mathrm{z} + e_3\mathrm{w})\mathrm{f}_2\mathrm{f}_3, \\ &(\mathrm{x} + (\alpha_0 + \alpha_1\mathrm{T} + \alpha_2\mathrm{T}^2)\mathrm{y} + (\beta_0 + \beta_1\mathrm{T} + \beta_2\mathrm{T}^2)\mathrm{z})\mathrm{f}_1\mathrm{f}_3, \mathrm{w}\mathrm{f}_1\mathrm{f}_3, \\ &(\mathrm{y} + (\eta_0 + \eta_1\mathrm{T} + \eta_2\mathrm{T}^2)\mathrm{w})\mathrm{f}_1\mathrm{f}_2, (\mathrm{z} + (\sigma_0 + \sigma_1\mathrm{T} + \sigma_2\mathrm{T}^2)\mathrm{w})\mathrm{f}_1\mathrm{f}_2\rangle. \end{aligned}$$

(*2*) *Si* $\mathrm{U}_0 = \mathrm{U}_2 = \mathrm{U}_5 = \mathrm{U}_6 = \emptyset, \mathrm{U}_1 = \{2\}, \mathrm{U}_3 = \{1\}, \mathrm{U}_4 = \{3\}$, *sean*
$\mathrm{H}_1 = \begin{pmatrix} 1 & e_1 & 0 & e_2 \\ 0 & 0 & 1 & e_3 \end{pmatrix}$ *sobre* $\mathbb{F}_2$,
$\mathrm{H}_3 = \begin{pmatrix} 1 & 0 & 0 & \alpha_0 + \alpha_1\mathrm{T} + \alpha_2\mathrm{T}^2 \\ 0 & 1 & 0 & \beta_0 + \beta_1\mathrm{T} + \beta_2\mathrm{T}^2 \\ 0 & 0 & 1 & \eta_0 + \eta_1\mathrm{T} + \eta_2\mathrm{T}^2 \end{pmatrix}$ *sobre* $\mathbb{F}_8$.
El código asociado es:

$$\langle \mathrm{x} + e_1\mathrm{y} + e_2\mathrm{w}, \mathrm{z} + e_3\mathrm{w}\rangle \oplus \langle \mathrm{xy}\rangle \oplus$$

$$\langle \mathrm{x} + (\alpha_0 + \alpha_1\mathrm{T} + \alpha_2\mathrm{T}^2)\mathrm{w}, \mathrm{y} + (\beta_0 + \beta_1\mathrm{T} + \beta_2\mathrm{T}^2)\mathrm{w}, \mathrm{z} + (\eta_0 + \eta_1\mathrm{T} + \eta_2\mathrm{T}^2)\mathrm{w}\rangle.$$

El ideal correspondiente es:

$$\langle (\mathrm{x} + e_1\mathrm{y} + e_2\mathrm{w})\mathrm{f}_2\mathrm{f}_3, (\mathrm{z} + e_3\mathrm{w})\mathrm{f}_2\mathrm{f}_3, \mathrm{xyf}_1\mathrm{f}_3, (\mathrm{x} + (\alpha_0 + \alpha_1\mathrm{T} + \alpha_2\mathrm{T}^2)\mathrm{w})\mathrm{f}_1\mathrm{f}_2,$$

$$(\mathrm{y} + (\beta_0 + \beta_1\mathrm{T} + \beta_2\mathrm{T}^2)\mathrm{w})\mathrm{f}_1\mathrm{f}_2, (\mathrm{z} + (\eta_0 + \eta_1\mathrm{T} + \eta_2\mathrm{T}^2)\mathrm{w})\mathrm{f}_1\mathrm{f}_2\rangle$$

EJEMPLO 3.2.5 *Sean* $\mathrm{A} = \mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X}\rangle$, *(ver el inciso (3) del Corolario 2.2.1), y* γ *una unidad de* A *(así* $\gamma = 1 + \mathrm{m}$, *donde* $\mathrm{m} = 2a + 4b + c\mathrm{x}$, $a, b, c \in \{0, 1\} \subset \mathbb{Z}_8$*). Se tiene que* $\mathrm{A} \in \mathfrak{F}_3$, $\ell_{\mathrm{A}}(\mathrm{A}) = 4$, $\{\mathrm{x}, 2\}$ *es un conjunto mínimo de generadores de* $\mathfrak{m}$, *el ideal maximal de* A, $\mathfrak{m}^2 = \langle 4\rangle$, $\mathbb{T} = \{0, 1\} \subset \mathbb{Z}_8$ *es un conjunto de representantes para el campo residual de* A.

Por el Ejemplo 1.3.5, $\mathrm{T}^7 - \gamma$ *se factoriza en* $\mathrm{A}[\mathrm{T}]$ *como* $\mathrm{T}^7 - \gamma = \mathrm{f}_1\mathrm{f}_2\mathrm{f}_3$*, donde:*
$\mathrm{f}_1 = \mathrm{m}^2\mathrm{T}^2 + \mathrm{T} + 7 + \mathrm{m}$,
$\mathrm{f}_2 = \mathrm{m}^2\mathrm{T}^4 + \mathrm{T}^3 + (3 + 4a + 3\mathrm{m})\mathrm{T}^2 + (2 + \mathrm{m}^2)\mathrm{T} + 7 + \mathrm{m}^2 + 3\mathrm{m}$,
$\mathrm{f}_3 = \mathrm{T}^3 + (6 + 4a)\mathrm{T}^2 + (5 + 4c)\mathrm{T} + 7 + 7\mathrm{m} \in \mathrm{A}[\mathrm{T}]$.
Entonces $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^7 - \gamma \rangle \cong \mathrm{A} \oplus \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_2 \rangle \oplus \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_3 \rangle$ *y* $\mathbb{T}_3 = \{a_1 + a_2\mathrm{T} + a_3\mathrm{T}^2 : a_i \in \{0, 1\}\}$ *es un conjunto de representantes para el campo residual de los anillos* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_i \rangle$, $i \in \{1, 2\}$. *Y se tiene:*

(*1*) *Si* $\mathrm{U}_0 = \mathrm{U}_3 = \mathrm{U}_4 = \emptyset, \mathrm{U}_1 = \{3\}, \mathrm{U}_2 = \{1, 2\}$*, sean*
$\mathrm{H}_1 = (1, 1)$ *sobre* $\mathbb{F}_2$,
$\mathrm{H}_2 = (1, a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2)$ *sobre* $\mathbb{F}_8$ (*es decir* $1, a_0, a_1, a_2 \in \mathbb{F}_2$).
El código asociado es:

$$\langle \mathrm{x} + 2 \rangle \oplus \langle \mathrm{x} + 2(a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2) \rangle \oplus \langle 4 \rangle.$$

El ideal correspondiente es:

$$\langle (\mathrm{x} + 2)\mathrm{f}_2\mathrm{f}_3, (\mathrm{x} + 2(a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2))\mathrm{f}_1\mathrm{f}_3, 4\mathrm{f}_1\mathrm{f}_2 \rangle.$$

En este caso se tiene $1, a_0, a_1, a_2 \in \{0, 1\} \subset \mathbb{Z}_8$.

(*2*) *Si* $\mathrm{U}_0 = \mathrm{U}_1 = \emptyset, \mathrm{U}_2 = \{1\}, \mathrm{U}_3 = \{2\}, \mathrm{U}_4 = \{3\}$*, sean*
$\mathrm{H}_1 = (1, a)$ *sobre* $\mathbb{F}_2$.
El código asociado es:

$$\langle \mathrm{x} + 2a \rangle \oplus \langle \mathrm{x}, 2 \rangle \oplus \langle 1 \rangle.$$

El ideal correspondiente es

$$\langle (\mathrm{x} + 2a)\mathrm{f}_2\mathrm{f}_3, \mathrm{x}\mathrm{f}_1\mathrm{f}_3, 2\mathrm{f}_1\mathrm{f}_3, \mathrm{f}_1\mathrm{f}_2 \rangle.$$

Capítulo 4

El dual de códigos constacíclicos sobre anillos en la familia $\mathfrak{L}_4$

Recordemos que $\mathfrak{F}_3$ denota la familia de anillos finitos de Frobenius que no son de cadena y cuyo ideal maximal tiene índice de nilpotencia 3 y que $\mathfrak{L}_4$ denota la familia de anillos finitos de Frobenius que no son de cadena y de longitud 4.
El objetivo de este capítulo es determinar el dual de un código γ-constacíclico, cuando el alfabeto del código es un anillo de la familia $\mathfrak{L}_4$ y la longitud del código no es divisible por la característica del campo residual del anillo. Una consecuencia de este resultado será obtener los códigos autoduales sobre este tipo de anillos.

4.1. Las extensiones no ramificadas de un anillo en la familia $\mathfrak{L}_4$

Los códigos γ-constacíclicos sobre anillos locales, cuando la longitud del código es prima relativa con la característica del campo residual, corresponden con una suma de ideales de algunas extensiones no ramificadas del anillo local, (ver Lema 3.1.1). Si C es un código constacíclico que corresponde con la suma de los ideales $\mathrm{I}_1, \ldots, \mathrm{I}_r$, el ideal que corresponde a su dual se puede escribir en términos de los ideales anuladores de los ideales $\mathrm{I}_1, \ldots, \mathrm{I}_r$, (ver Teorema 3.2.1). Por esta razón nos concentramos en describir las extensiones no ramificadas de un anillo en la familia $\mathfrak{L}_4$ y el ideal anulador de los ideales de un anillo en la familia $\mathfrak{L}_4$.

En el siguiente resultado se determinan las extensiones no ramificadas de los anillos de la familia $\mathfrak{L}_4$.

TEOREMA 4.1.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_{p^d})$ *un anillo en la familia* $\mathfrak{L}_4$, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$ *y* $\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f} \rangle$ *la extensión no ramificada de* A *determinada por* f. *En la siguiente tabla se presenta la relación entre el anillo local y su extensión no ramificada.*

$\mathrm{GR}(p^2, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$	$\mathrm{GR}(p^2, ds)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$
$\mathrm{GR}(p^2, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta\mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$	$\mathrm{GR}(p^2, ds)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$, s es par
	$\mathrm{GR}(p^2, ds)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta_1\mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$, s es impar
$\{0, 1, \ldots, \zeta^{p^d-2}\}$ es el conjunto de Teichmüller de $\mathrm{GR}(p^2, d)$	$\{0, 1, \ldots, \zeta_1^{p^{ds}-2}\}$ es el conjunto de Teichmüller de $\mathrm{GR}(p^2, ds)$
$\mathrm{GR}(p^2, d)[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$	$\mathrm{GR}(p^2, ds)[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$
$\mathrm{GR}(p^3, d)[\mathrm{X}]/\langle \mathrm{X}^2 - p^2, p\mathrm{X} \rangle$	$\mathrm{GR}(p^3, ds)[\mathrm{X}]/\langle \mathrm{X}^2 - p^2, p\mathrm{X} \rangle$
$\mathrm{GR}(p^3, d)[\mathrm{X}]/\langle \mathrm{X}^2 - \zeta p^2, p\mathrm{X} \rangle$	$\mathrm{GR}(p^3, ds)[\mathrm{X}]/\langle \mathrm{X}^2 - p^2, p\mathrm{X} \rangle$, s es par
	$\mathrm{GR}(p^3, ds)[\mathrm{X}]/\langle \mathrm{X}^2 - \zeta_1 p^2, p\mathrm{X} \rangle$, s es impar
$\{0, 1, \ldots, \zeta^{p^d-2}\}$ es el conjunto de Teichmüller de $\mathrm{GR}(p^3, d)$	$\{0, 1, \ldots, \zeta_1^{p^{ds}-2}\}$ es el conjunto de Teichmüller de $\mathrm{GR}(p^3, ds)$
$\mathbb{F}_{p^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$	$\mathbb{F}_{p^{ds}}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$
$\mathbb{F}_{p^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$	$\mathbb{F}_{p^{ds}}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$, s es par
	$\mathbb{F}_{p^{ds}}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta_1\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$, s es impar
ζ es un elemento primitivo de $\mathbb{F}_{p^d}$	ζ_1 es un elemento primitivo de $\mathbb{F}_{p^{ds}}$
$\mathrm{GR}(4, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - 2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y} \rangle$	$\mathrm{GR}(4, ds)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - 2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y} \rangle$
$\mathrm{GR}(4, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY} - 2, 2\mathrm{X}, 2\mathrm{Y} \rangle$	$\mathrm{GR}(4, ds)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY} - 2, 2\mathrm{X}, 2\mathrm{Y} \rangle$
$\mathrm{GR}(4, d)[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$	$\mathrm{GR}(4, ds)[\mathrm{X}]/\langle \mathrm{X}^2 \rangle$
$\mathrm{GR}(4, d)[\mathrm{X}]/\langle \mathrm{X}^2 - 2\mathrm{X} \rangle$	$\mathrm{GR}(4, ds)[\mathrm{X}]/\langle \mathrm{X}^2 - 2\mathrm{X} \rangle$
$\mathrm{GR}(8, d)[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X} \rangle$	$\mathrm{GR}(8, ds)[\mathrm{X}]/\langle \mathrm{X}^2 - 4, 2\mathrm{X} \rangle$
$\mathbb{F}_{2^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2 \rangle$	$\mathbb{F}_{2^{ds}}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2 \rangle$
$\mathbb{F}_{2^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$	$\mathbb{F}_{2^{ds}}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$

Demostración.
Por los Teoremas 2.1.1 y 2.1.2, el anillo B es local de Frobenius no de cadena. Por los Lemas 1.3.9, 1.3.10 y 1.3.11, el ideal maximal de B es $\mathfrak{m}\mathrm{B}$, el campo residual de B es $\mathbb{F}_{p^{ds}}$, $\mathrm{car}(\mathrm{A}) = \mathrm{car}(\mathrm{B})$, $\ell_{\mathrm{A}}(\mathrm{A}) = \ell_{\mathrm{B}}(\mathrm{B}) = 4$, $p \in \mathfrak{m}^2$ si y sólo si $p \in [\mathfrak{m}\mathrm{B}]^2 = \mathfrak{m}^2\mathrm{B}$ y un conjunto mínimo de generadores para $\mathfrak{m}$ es también un conjunto mínimo de

generadores para $\mathfrak{m}$B. Así, $\mathfrak{B} \in \mathfrak{L}_4$.
(1) Se denota por x y y a los elementos del anillo A que corresponden con X y Y. Entonces $\{x, y\}$ es un conjunto mínimo de generadores para $\mathfrak{m}$B. Por las observaciones hechas al inicio de esta demostración y el Teorema 2.2.1,

$$B \cong GR(p^2, ds)[X, Y]/\langle X^2 - Y^2, Y^2 - p, XY, Y^3, pX, pY\rangle$$

ó

$$B \cong GR(p^2, ds)[X, Y]/\langle X^2 - \zeta_1 Y^2, Y^2 - p, XY, Y^3, pX, pY\rangle,$$

donde $\{0, 1, \ldots, \zeta_1^{p^{ds}-2}\}$ es el conjunto de Teichmüller del anillo de Galois $GR(p^2, ds)$. La afirmación se sigue de la Observación 4.
(2) Sean x y y como en el inciso (1) y $\{0, 1, \ldots, \zeta^{p^d-2}\}$ el conjunto de Teichmüller del anillo de Galois $GR(p^2, d)$, entonces x y y satisfacen:

$$x^2 = \zeta y^2, y^2 = p, xy = y^3 = px = py = 0.$$

Por el Teorema 2.2.1,

$$B \cong GR(p^2, ds)[X, Y]/\langle X^2 - Y^2, Y^2 - p, XY, Y^3, pX, pY\rangle$$

ó

$$B \cong GR(p^2, ds)[X, Y]/\langle X^2 - \zeta_1 Y^2, Y^2 - p, XY, Y^3, pX, pY\rangle,$$

donde $\{0, 1, \ldots, \zeta_1^{p^{ds}-2}\}$ es el conjunto de Teichmüller del anillo de Galois $GR(p^2, ds)$. Sea $k = \frac{p^{ds}-1}{p^d-1} = p^{d(s-1)} + \ldots + p^d + 1$, entonces k es impar si y sólo si s es impar, ζ_1^k y ζ tiene orden multiplicativo $p^d - 1$, $\tilde{\zeta}_1^{ki} = \tilde{\zeta}$, para algún i con $(i, p^d - 1) = 1$, $\zeta_1^{ki} = \zeta + m_1$ y $\zeta_1^{-ki} = \zeta^{-1} + m_2$, donde $m_1, m_2 \in \mathfrak{m}$B.
Si s es par, k es par, $\{\alpha = \zeta_1^{-\frac{ki}{2}} x, \beta = y\}$ es un conjunto mínimo de generadores del ideal maximal $\mathfrak{m}$B y α y β satisfacen las relaciones de un conjunto mínimo de generadores del ideal maximal del anillo $GR(p^2, ds)[X, Y]/\langle X^2 - Y^2, Y^2 - p, XY, Y^3, pX, pY\rangle$. La afirmación se sigue de la observación 4.
Y si s es impar, k es impar, ki es impar, pues $(i, p^d - 1) = 1$, y $\{\alpha = \zeta_1^{\frac{1-ki}{2}} x, \beta = y\}$ es un conjunto mínimo de generadores del ideal maximal $\mathfrak{m}$B y α y β satisfacen las relaciones de un conjunto mínimo de generadores del ideal maximal del anillo $GR(p^2, ds)[X, Y]/\langle X^2 - \zeta_1 Y^2, Y^2 - p, XY, Y^3, pX, pY\rangle$. La afirmación se sigue de la Observación 4.

El resto de casos pueden ser tratados en forma similar al método aquí usado para los incisos (1) y (2).

En la Proposición 3.2.1 se describe la retícula de ideales de un anillo en la familia $\mathfrak{F}_3$. Recordando que la familia $\mathfrak{L}_4$ es parte de la familia $\mathfrak{F}_3$. El siguiente resultado es un caso especial de la Proposición 3.2.1, pues se describe la retícula de ideales de un anillo en la familia $\mathfrak{L}_4$.

LEMA 4.1.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$, $\{\alpha_1, \alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio básico irreducible,* $s = \deg(\tilde{\mathrm{f}})$, $(\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f} \rangle, \mathfrak{m}\mathrm{B}, \mathbb{F}_{q^s})$ *la extensión no ramificada de* A *determinada por* f, $\mathbb{T} \subset \mathrm{A}$ *un conjunto de representantes de* $\mathbb{F}_q$ *y* $\mathbb{T}_s := \{a_0 + a_1\mathrm{T} + \cdots + a_{s-1}\mathrm{T}^{s-1} : a_i \in \mathbb{T}\} \subset \mathrm{B}$ *el conjunto de representantes de* $\mathbb{F}_{q^s}$. *Entonces* B *tiene* $q^s + 5$ *ideales y estos son:*

$$\langle 0 \rangle \subset \mathfrak{m}^2\mathrm{B} \subset \langle \alpha_2 \rangle \mathrm{B}, \langle \alpha_1 + \lambda_1\alpha_2 \rangle \mathrm{B}, \langle \alpha_1 + \lambda_2\alpha_2 \rangle \mathrm{B}, \ldots, \langle \alpha_1 + \lambda_{q^s}\alpha_2 \rangle \mathrm{B} \subset \mathfrak{m}\mathrm{B} \subset \mathrm{B}, \text{ con } \lambda_i \in \mathbb{T}_s.$$

OBSERVACIÓN 6 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$ *y* B *como en el Lema 4.1.1. Los ideales del anillo* B *de longitud* 2 *están en correspondencia uno a uno con los elementos del conjunto* $\{(0,1), (1,\lambda) : \lambda \in \mathbb{T}_s\}$. *La correspondencia se define de la siguiente manera,* $\langle \alpha_2 \rangle \mathrm{B}$ *se corresponde con* $(0,1)$ *y* $\langle \alpha_1 + \lambda\alpha_2 \rangle \mathrm{B}$ *se corresponde con* $(1,\lambda)$.

En el resto de esta tesis, la siguiente notación será usada. Sean $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$, $q = p^d$, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ un polinomio básico irreducible, $s = \deg(\tilde{\mathrm{f}})$ y $(\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f} \rangle, \mathfrak{m}\mathrm{B}, \mathbb{F}_{q^s})$ la extensión no ramificada de A determinada por f.

(1) Un conjunto mínimo de generadores $\{\alpha_1, \alpha_2\}$ del ideal maximal $\mathfrak{m}$ será considerado de la siguiente manera:

   (i) Para alguno de los siguientes anillos:

      (a) $\mathrm{GR}(p^2, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$;

      (b) $\mathrm{GR}(p^2, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta\mathrm{Y}^2, \mathrm{Y}^2 - p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y} \rangle$,
      donde $\{0, 1, \ldots, \zeta^{p^d-2}\}$ es el conjunto de Teichmüller de $\mathrm{GR}(p^2, d)$;

      (c) $\mathbb{F}_{p^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$;

      (d) $\mathbb{F}_{p^d}[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3 \rangle$,
      ζ es un elemento primitivo de $\mathbb{F}_{p^d}$;

      (e) $\mathrm{GR}(4, d)[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2 - \mathrm{Y}^2, \mathrm{Y}^2 - 2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y} \rangle$;

(f) $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2,\mathrm{Y}^2,\mathrm{XY}-2,2\mathrm{X},2\mathrm{Y}\rangle$;

(g) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2,\mathrm{Y}^2\rangle$;

(h) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2,\mathrm{XY},\mathrm{Y}^3\rangle$;

se tomará $\{\alpha_1,\alpha_2\}=\{\mathrm{x},\mathrm{y}\}$.

(ii) Para alguno de los siguientes anillos:

(a) $\mathrm{GR}(p^2,d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$;

(b) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-p^2,p\mathrm{X}\rangle$;

(c) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-\zeta p^2,p\mathrm{X}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ es el conjunto de Teichm*üller* de $\mathrm{GR}(p^3,d)$,

se tomará $\{\alpha_1,\alpha_2\}=\{\mathrm{x},p\}$.

(iii) Para alguno de los siguientes anillos:

(a) $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$;

(b) $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2-2\mathrm{X}\rangle$;

(c) $\mathrm{GR}(8,d)[\mathrm{X}]/\langle \mathrm{X}^2-4,2\mathrm{X}\rangle$,

se tomará $\{\alpha_1,\alpha_2\}=\{\mathrm{x},2\}$.

Cuando trabajemos con un conjunto mínimo de generadores para $\mathfrak{m}$ entenderemos que $\{\alpha_1,\alpha_2\}$ es el conjunto mínimo de generadores para $\mathfrak{m}$ que se acaba de mencionar.

(2) Se usa la siguiente notación:

(i) $\overline{\alpha}$ para $\{\alpha_1,\alpha_2\}$;

(ii) $(0,1)_{\overline{\alpha}}$ para el elemento $\alpha_2\in \mathrm{B}$;

(iii) $(1,\lambda)_{\overline{\alpha}}$ para el elemento $\alpha_1+\lambda\alpha_2\in \mathrm{B}$;

(iv) $(0,1)^{\mathrm{B}}_{\overline{\alpha}}$ para el ideal de B generado por α_2;

(v) $(1,\lambda)^{\mathrm{B}}_{\overline{\alpha}}$ para el ideal de B generado por $\alpha_1+\lambda\alpha_2$, donde $\lambda\in\mathbb{T}_s$.

(3) La relación $\ell_{\mathrm{A}}(\mathrm{I})+\ell_{\mathrm{A}}(\mathrm{ann}_{\mathrm{A}}(\mathrm{I}))=\ell_{\mathrm{A}}(\mathrm{A})$, del Lema 2.1.7, implica que si I es un ideal del anillo A, entonces la longitud de I es 2 si y sólo si la longitud de

$\mathrm{ann_A(I)}$ es 2.
Por lo tanto, se induce la permutación

$$(*)^{\perp} : \{(0,1),(1,\lambda) : \lambda \in \mathbb{T}_s\} \to \{(0,1),(1,\lambda) : \lambda \in \mathbb{T}_s\}$$

dada por

$$\vec{u}_{\overline{\alpha}} \mapsto \vec{v}_{\overline{\alpha}} := \vec{u}_{\overline{\alpha}}^{\perp} \quad \text{si} \quad \mathrm{ann_B}(\vec{u}_{\overline{\alpha}}^{\mathrm{B}}) = \vec{v}_{\overline{\alpha}}^{\mathrm{B}}.$$

En los siguientes resultados se calcula el ideal anulador de los ideales de un anillo de la familia $\mathfrak{L}_4$.

LEMA 4.1.2 *Sea* A *alguno de los siguientes anillos:*

(*1*) $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$*;*

(*2*) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-p^2, p\mathrm{X}\rangle$*;*

(*3*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$*;*

(*4*) $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y}\rangle$*;*

(*5*) $\mathrm{GR}(8,d)[\mathrm{X}]/\langle \mathrm{X}^2-4, 2\mathrm{X}\rangle$*;*

(*6*) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$*;*

$\mathfrak{m}$ *su ideal maximal,* $\overline{\alpha} = \{\alpha_1, \alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$ *y* $\mathbb{T}$ *como hasta ahora. Entonces* $\mathrm{ann_A}(\mathfrak{m}) = \mathfrak{m}^2 = \langle \alpha_1^2 \rangle = \langle \alpha_2^2 \rangle$ *y*

$$(0,1)_{\overline{\alpha}}^{\perp} = (1,0)_{\overline{\alpha}}, \;\; (1,0)_{\overline{\alpha}}^{\perp} = (0,1)_{\overline{\alpha}}, \;\; (1,\lambda_1)_{\overline{\alpha}}^{\perp} = (1,\lambda_2)_{\overline{\alpha}}, \text{ donde } \lambda_1,\lambda_2 \in \mathbb{T}, \; \tilde{\lambda}_1\tilde{\lambda}_2 = -1.$$

Demostración.
La primer afirmación se sigue de los Lemas 2.1.5 y 2.2.3, Las otras afirmaciones se siguen de las siguientes relaciones:
(*i*) $(0,1)_{\overline{\alpha}}(1,0)_{\overline{\alpha}} = \alpha_2\alpha_1 = 0$,
(*ii*) Si $\tilde{\lambda}_1\tilde{\lambda}_2 = -1$ entonces $\lambda_1\lambda_2 = -1 + m$, donde $m \in \mathfrak{m}$, y $(1,\lambda_1)_{\overline{\alpha}}(1,\lambda_2)_{\overline{\alpha}} = (\alpha_1 + \lambda_1\alpha_2)(\alpha_1 + \lambda_2\alpha_2) = \alpha_1^2 + \lambda_1\lambda_2\alpha_2^2 = (1+\lambda_1\lambda_2)\alpha_2^2 = m\alpha_2^2 = 0$.

El mismo argumento que el usado en el Lema 4.1.2 se puede usar para probar los siguientes resultados.

LEMA 4.1.3 *Sea* A *alguno de los siguientes anillos:*

(*1*) $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^2,d)$*;*

(*2*) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-\zeta p^2, p\mathrm{X}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^3,d)$*;*

(*3*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$,
donde ζ *es un elemento primitivo de* $\mathbb{F}_{p^d}$*;*

$\mathfrak{m}$ *su ideal maximal,* $\overline{\alpha}=\{\alpha_1,\alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$ *y* $\mathbb{T}$ *como hasta ahora. Entonces* $\mathrm{ann}_{\mathrm{A}}(\mathfrak{m})=\mathfrak{m}^2=\langle\alpha_1^2\rangle=\langle\alpha_2^2\rangle$ *y*

$$(0,1)_{\overline{\alpha}}^{\perp}=(1,0)_{\overline{\alpha}},\quad (1,0)_{\overline{\alpha}}^{\perp}=(0,1)_{\overline{\alpha}},\quad (1,\lambda_1)_{\overline{\alpha}}^{\perp}=(1,\lambda_2)_{\overline{\alpha}},\ \text{donde } \tilde{\lambda}_1\tilde{\lambda}_2=-\tilde{\zeta},$$

donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller del anillo de Galois* $\mathrm{GR}(p^2,d)$*, en el caso del anillo* $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$.
$\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller del anillo de Galois* $\mathrm{GR}(p^3,d)$*, en el caso del anillo* $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-\zeta p^2, p\mathrm{X}\rangle$.
Y ζ *es un elemento primitivo de* $\mathbb{F}_q$*, en el caso del anillo* $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$.

LEMA 4.1.4 *Sea* A *alguno de los siguientes anillos:*

(*1*) $\mathrm{GR}(p^2,d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$

(*2*) $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY}-2, 2\mathrm{X}, 2\mathrm{Y}\rangle$

(*3*) $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$

(*4*) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$

$\mathfrak{m}$ *su ideal maximal,* $\overline{\alpha}=\{\alpha_1,\alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$ *y* $\mathbb{T}$ *como hasta ahora. Entonces* $\mathrm{ann}_{\mathrm{A}}(\mathfrak{m})=\mathfrak{m}^2=\langle\alpha_1\alpha_2\rangle$ *y*

$$(0,1)_{\overline{\alpha}}^{\perp}=(0,1)_{\overline{\alpha}},\qquad (1,\lambda_1)_{\overline{\alpha}}^{\perp}=(1,\lambda_2)_{\overline{\alpha}},\ \text{donde } \tilde{\lambda}_1=-\tilde{\lambda}_2.$$

LEMA 4.1.5 *Sea* $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2-2\mathrm{X}\rangle$ *el anillo,* $\mathfrak{m}$ *su ideal maximal,* $\overline{\alpha}=\{\alpha_1,\alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$ *y* $\mathbb{T}$ *como hasta ahora. Entonces* $\mathrm{ann}_{\mathrm{A}}(\mathfrak{m})=\mathfrak{m}^2=\langle \mathrm{x}^2\rangle=\langle 2\mathrm{x}\rangle$ *y*

$$(0,1)_{\overline{\alpha}}^{\perp}=(0,1)_{\overline{\alpha}},\quad (1,\lambda_1)_{\overline{\alpha}}^{\perp}=(1,\lambda_2)_{\overline{\alpha}},\quad \text{donde } \tilde{\lambda}_2=\tilde{\lambda}_1+\tilde{1}$$

Al combinar el Teorema 4.1.1 y los Lemas 4.1.2, 4.1.3, 4.1.4, 4.1.5 se tiene:

COROLARIO 4.1.1 *Sea* A *alguno de los siguientes anillos:*

(*1*) $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$*;*

(*2*) $\mathrm{GR}(p^2,d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$*;*

(*3*) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-p^2, p\mathrm{X}\rangle$*;*

(*4*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$*;*

(*5*) $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{Y}^2-2, \mathrm{XY}, \mathrm{Y}^3, 2\mathrm{X}, 2\mathrm{Y}\rangle$*;*

(*6*) $\mathrm{GR}(4,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2, \mathrm{XY}-2, 2\mathrm{X}, 2\mathrm{Y}\rangle$*;*

(*7*) $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2\rangle$*;*

(*8*) $\mathrm{GR}(4,d)[\mathrm{X}]/\langle \mathrm{X}^2-2\mathrm{X}\rangle$*;*

(*9*) $\mathrm{GR}(8,d)[\mathrm{X}]/\langle \mathrm{X}^2-4, 2\mathrm{X}\rangle$*;*

(*10*) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$*;*

(*11*) $\mathbb{F}_{2^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2, \mathrm{XY}, \mathrm{Y}^3\rangle$*;*

$\mathfrak{m}$ *el ideal maximal de* A, $\overline{\alpha}=\{\alpha_1,\alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$, $\mathrm{f}\in \mathrm{A}[\mathrm{T}]$ *un polinomio básico irreducible,* $s=\deg(\tilde{\mathrm{f}})$, $(\mathrm{B}=\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle, \mathfrak{m}\mathrm{B}, \mathbb{F}_{q^s})$ *la extensión no ramificada de* A *determinada por* f, $\mathbb{T}$ *y* $\mathbb{T}_s$ *como hasta ahora. Entonces el ideal anulador de los ideales del anillo* B *tiene la misma expresión que el ideal anulador de los ideales del anillo* A *pero con los coeficientes* λ_1,λ_2 *in* $\mathbb{T}_s$.

COROLARIO 4.1.2 *Sea* A *alguno de los siguientes anillos:*

(*1*) $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2, \mathrm{Y}^2-p, \mathrm{XY}, \mathrm{Y}^3, p\mathrm{X}, p\mathrm{Y}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^2,d)$*;*

(*2*) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-\zeta p^2, p\mathrm{X}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^3,d)$*;*

(*3*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2,\mathrm{XY},\mathrm{Y}^3\rangle$,
donde ζ *es un elemento primitivo de* $\mathbb{F}_{p^d}$*;*

$\mathfrak{m}$ *el ideal maximal de* A, $\overline{\alpha}=\{\alpha_1,\alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$, $\mathrm{f}\in\mathrm{A}[\mathrm{T}]$ *un polinomio básico irreducible,* $s=\deg(\tilde{\mathrm{f}})$, $(\mathrm{B}=\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle,\mathfrak{m}\mathrm{B},\mathbb{F}_{q^s})$ *la extensión no ramificada de* A *determinada por* f, $\mathbb{T}$ *y* $\mathbb{T}_s$ *como hasta ahora y* $\mathrm{g}\in\mathbb{T}_s$ *tal que* $\mathrm{g}+\langle\tilde{\mathrm{f}}\rangle\in\mathbb{F}_q[\mathrm{T}]/\langle\tilde{\mathrm{f}}\rangle\cong\mathbb{F}_{q^s}$ *es un elemento primitivo de* $\mathbb{F}_{q^s}$.

(*a*) *Si* s *es par, el ideal anulador de los ideales de* B *tiene la misma expresión que el ideal anulador de los ideales de los anillos*

(*1*) $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2,\mathrm{Y}^2-p,\mathrm{XY},\mathrm{Y}^3,p\mathrm{X},p\mathrm{Y}\rangle$*;*

(*2*) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-p^2,p\mathrm{X}\rangle$*;*

(*3*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\mathrm{Y}^2,\mathrm{XY},\mathrm{Y}^3\rangle$*;*

respectivamente, (ver Lema 4.1.2) pero con los coeficientes λ_1,λ_2 *en* $\mathbb{T}_s$.

(*b*) *Si* s *es impar, el ideal anulador de los ideales de* B *tiene la misma expresión que el ideal anulador de los ideales de los anillos*

(*2*) $\mathrm{GR}(p^2,d)[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2,\mathrm{Y}^2-p,\mathrm{XY},\mathrm{Y}^3,p\mathrm{X},p\mathrm{Y}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^2,d)$

(*5*) $\mathrm{GR}(p^3,d)[\mathrm{X}]/\langle \mathrm{X}^2-\zeta p^2,p\mathrm{X}\rangle$,
donde $\{0,1,\ldots,\zeta^{p^d-2}\}$ *es el conjunto de Teichmüller de* $\mathrm{GR}(p^3,d)$*;*

(*7*) $\mathbb{F}_{p^d}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2-\zeta\mathrm{Y}^2,\mathrm{XY},\mathrm{Y}^3\rangle$,
donde ζ *es un elemento primitivo de* $\mathbb{F}_{p^d}$*;*

respectivamente, (ver Lema 4.1.3) pero con los coeficientes λ_1,λ_2 *en* $\mathbb{T}_s$ *y* $\zeta=\mathrm{g}$.

4.2. El dual de códigos constacíclicos sobre anillos en la familia $\mathfrak{L}_4$

Sea A un anillo, el producto escalar sobre A^n es definido como $(a_1,\ldots,a_n)\cdot(b_1,\ldots,b_n)=a_1b_1+\ldots+a_nb_n$. Dos vectores $\vec{a}=(a_1,\ldots,a_n)$ y $\vec{b}=(b_1,\ldots,b_n)$ son llamadas ortogonales si $\vec{a}\cdot\vec{b}=0$. Sea $\mathrm{C}\subset\mathrm{A}^n$ un código lineal sobre A de longitud

n, el dual de C, denotado por $\mathrm{C}^{\perp}$, es el conjunto de palabras de A^n que son ortogonales a toda parabra de C, es decir, $\mathrm{C}^{\perp} = \{\vec{a} \in \mathrm{A}^n : \vec{a} \cdot \vec{b} = 0,\ \forall\ \vec{b} \in \mathrm{C}\}$. Un código C es llamado *autodual* si $\mathrm{C} = \mathrm{C}^{\perp}$.

En esta Sección la estructura del dual de un código constacíclico sobre anillos en la familia $\mathfrak{L}_4$, de longitud prima relativa con la característica del campo residual del anillo, es determinada.

Sea $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$, $q = p^d$, γ una unidad de A, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ un polinomio básico irreducible, $s = \deg(\tilde{\mathrm{f}})$, $(\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f} \rangle, \mathfrak{m}\mathrm{B}, \mathbb{F}_{q^s})$ la extensión no ramificada de A determinada por f y $\mathbb{T} \subset \mathrm{A}$ un conjunto de representantes de $\mathbb{F}_q$. En lo que resta de este trabajo se usará la siguiente notación:

(1) La longitud del código será denotada por n, y no será divisible por p.

(2) Puesto que $(n, p) = 1$, entonces $\mathrm{T}^n - \gamma$ es producto de una única familia de polinomios mónicos básicos irreducibles coprimos a pares en $\mathrm{A}[\mathrm{T}]$, por el Lema 1.3.17. $\mathrm{f}_1, \ldots, \mathrm{f}_r$ serán dichos polinomios.

(3) $\mathbb{T}_s = \{a_0 + a_1\mathrm{T} + \cdots + a_{s-1}\mathrm{T}^{s-1} : a_i \in \mathbb{T}\} \subset \mathrm{B}$ denotará el conjunto de representantes de $\mathrm{B}/\mathfrak{m}\mathrm{B} = \mathbb{F}_{q^s}$.

(4) El elemento $a_0 + a_1\mathrm{T} + \ldots + a_{n-1}\mathrm{T}^{n-1} + \langle \mathrm{T}^n - \gamma \rangle$ de $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$ será denotada simplemente por $a_0 + a_1\mathrm{T} + \ldots + a_{n-1}\mathrm{T}^{n-1}$.

(5) El homomorfismo natural $\tilde{}\colon \mathrm{A}[\mathrm{T}] \to \mathbb{F}_q[\mathrm{T}]$ es el que está dado por

$$\mathrm{f} = a_0 + a_1\mathrm{T} + \ldots + a_k\mathrm{T}^k \mapsto \tilde{\mathrm{f}} = (a_0 + \mathfrak{m}) + (a_1 + \mathfrak{m})\mathrm{T} + \ldots + (a_k + \mathfrak{m})\mathrm{T}^k.$$

(6) Si H es un factor de $\mathrm{T}^n - \gamma$ o de $\mathrm{T}^n - \gamma^{-1}$ nosotros simplemente escribiremos $\widehat{\mathrm{H}} = \frac{\mathrm{T}^n - \gamma}{\mathrm{H}}$ o $\widehat{\mathrm{H}} = \frac{\mathrm{T}^n - \gamma^{-1}}{\mathrm{H}}$, de acuerdo al caso.

El siguiente resultado no estará acompañado de una demostración, su demostración se puede consultar por ejemplo en [18].

LEMA 4.2.1 *Sean* A *un anillo,* γ *una unidad de* A, σ_γ *la permutación* γ*-constacíclica,* $\mathrm{f} = a_0 + a_1\mathrm{T} + \ldots + a_{n-2}\mathrm{T}^{n-2} + a_{n-1}\mathrm{T}^{n-1}$ *y* $\mathrm{g} = b_{n-1} + b_{n-2}\mathrm{T} + \ldots + b_1\mathrm{T}^{n-2} + b_0\mathrm{T}^{n-1}$. *Entonces el producto* fg *en* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$ *está dado por* $\mathrm{fg} = c_0 + c_1\mathrm{T} + \ldots + c_{n-1}\mathrm{T}^{n-1}$, *donde*

$$c_i = [\sigma_\gamma^{n-1-i}(a_0, \ldots, a_{n-1})] \cdot (b_0, \ldots, b_{n-1}) = \gamma(a_0, \ldots, a_{n-1}) \cdot [\sigma_{\gamma^{-1}}^{i+1}(b_0, \ldots, b_{n-1})].$$

Bajo las condiciones del Lema 4.2.1, se tiene $\mathrm{fg} = 0$ en $\mathrm{A[T]}/\langle \mathrm{T}^n - \gamma \rangle$ si y sólo si $(b_0, \ldots, b_{n-1})$ es ortogonal a $(a_0, \ldots, a_{n-1})$ y a todos sus corrimientos γ-constacíclicos si y sólo si $(a_0, \ldots, a_{n-1})$ es ortogonal a $(b_0, \ldots, b_{n-1})$ y a todos sus corrimientos γ^{-1}-constacíclicos.

Para un polinomio $\mathrm{f} = a_0 + a_1\mathrm{T} + \cdots + a_{l-1}\mathrm{T}^{l-1} + a_l\mathrm{T}^l \in \mathrm{A[T]}$, $a_l \neq 0$, el polinomio reverso del polinomio f es definido como $\mathrm{f}^* = \mathrm{T}^l\mathrm{f}(\frac{1}{\mathrm{T}}) = a_l + a_{l-1}\mathrm{T} + \ldots + a_1\mathrm{T}^{l-1} + a_0\mathrm{T}^l$. Es fácil verificar las siguientes propiedades:

(1) Si $a_0 \neq 0$, entonces $(\mathrm{f}^*)^* = \mathrm{f}$;

(2) Si a_l es una unidad, entonces $\tilde{\mathrm{f}}^* = (\tilde{\mathrm{f}})^*$;

(3) Si A es un campo y f es irreducible, entonces f^* es irreducible;

(4) Si f es un polinomio mónico básico irreducible, entonces f^* es básico irreducible;

(5) Si f, g son coprimos, entonces f^* y g^* son coprimos;

(6) Si $\deg(\mathrm{f}) \geq \deg(\mathrm{g})$, entonces $(\mathrm{f} + \mathrm{g})^* = \mathrm{f}^* + \mathrm{T}^{\deg(\mathrm{f})-\deg(\mathrm{g})}\mathrm{g}^*$;

(7) Si a_l es una unidad de A, entonces $(\mathrm{fg})^* = \mathrm{f}^*\mathrm{g}^*$, para todo $\mathrm{g} \in \mathrm{A[T]}$.

El siguiente resultado es consecuencia directa de las relaciones $\mathrm{T}^n - \gamma = \mathrm{g}_1 \cdots \mathrm{g}_r$, $(\mathrm{T}^n - \gamma)^* = 1 - \gamma\mathrm{T}^n = \mathrm{g}_1^* \cdots \mathrm{g}_r^*$, $\mathrm{T}^n - \gamma^{-1} = -\gamma^{-1}\mathrm{g}_1^* \cdots \mathrm{g}_r^*$, donde $\mathrm{g}_1 \cdots \mathrm{g}_r$ son polinomios mónicos.

COROLARIO 4.2.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$, γ *una unidad de* A, $\overline{\alpha} = \{\alpha_1, \alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$, $\mathrm{g}_1, \ldots, \mathrm{g}_k$ *polinomios mónicos tales que* $\mathrm{T}^n - \gamma = \mathrm{g}_1 \cdots \mathrm{g}_k$ *y* $\lambda = \lambda_0 + \lambda_1\mathrm{T} + \ldots + \lambda_h\mathrm{T}^h \in \mathrm{A[T]}$, *entonces:*

(*1*) *El término constante de* g_i *es una unidad,* $\deg(\mathrm{g}_i) = \deg(\mathrm{g}_i^*)$, $(\mathrm{g}_i^*)^* = \mathrm{g}_i$ *y* $(\widehat{\mathrm{g}_i}^*)^* = \widehat{\mathrm{g}_i}$, *para* $1 \leq i \leq k$.

(*2*) *Si* $a_{0,i}$ *es el término constante de* g_i, *entonces* $\mathrm{h}_1 = \frac{1}{a_{0,1}}\mathrm{g}_1^*, \ldots, \mathrm{h}_k = \frac{1}{a_{0,k}}\mathrm{g}_k^*$ *son polinomios mónicos tales que* $\mathrm{T}^n - \gamma^{-1} = \mathrm{h}_1 \cdots \mathrm{h}_k$.
En particular, si $\mathrm{f}_1, \ldots, \mathrm{f}_r$ *son los únicos polinomios mónicos básicos irreducible coprimos a pares tales que* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$ *entonces* $\mathrm{h}_1, \ldots, \mathrm{h}_r$ *son los únicos polinomios mónicos básicos irreducibles coprimos a pares tales que* $\mathrm{T}^n - \gamma^{-1} = \mathrm{h}_1 \cdots \mathrm{h}_r$.

(*3*) $\alpha_1 + \lambda_0\alpha_2 \neq 0$ *y* $((\alpha_1 + \lambda\alpha_2)^*)^* = \alpha_1 + \lambda\alpha_2$.

(*4*) $\widehat{\mathrm{g}_i^*} = -\gamma^{-1}\prod_{j\neq i}\mathrm{g}_j^* = -\gamma(\prod_{j\neq i}\mathrm{g}_j)^* = -\gamma\widehat{\mathrm{g}_i}^*$, $1 \leq i \leq r$.

(*5*) *Se tienen las siguientes relaciones en el anillo* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma^{-1}\rangle$:

- (*a*) $\mathrm{T}^{-i} = \mathrm{T}^{n-i}\gamma$,
- (*b*) $(\alpha_2)^* = \alpha_2$,
- (*c*) $(\alpha_1 + \lambda\alpha_2)^* = \alpha_1\mathrm{T}^{\deg(\lambda)} + \lambda^*\alpha_2 = \mathrm{T}^{\deg(\lambda)}[\alpha_1 + \lambda^*\mathrm{T}^{n-\deg(\lambda)}\gamma\alpha_2]$,
- (*d*) *Sea* $\lambda_1 \in \mathrm{A}[\mathrm{T}]$ *el residuo de la división de* $\lambda^*\mathrm{T}^{n-\deg(\lambda)}\gamma$ *por* g_i^*, *es decir* $\lambda^*\mathrm{T}^{n-\deg(\lambda)}\gamma = \mathrm{g}_i^*\mathrm{Q} + \lambda_1$, *donde* $\deg(\lambda_1) \leq \deg(\mathrm{g}_i^*) = \deg(\mathrm{g}_i)$, *entonces:*

$$\langle(\alpha_1 + \lambda\alpha_2)^*\widehat{\mathrm{g}_i}^*\rangle = \langle(\alpha_1 + \lambda^*\mathrm{T}^{n-\deg(\lambda)}\gamma\alpha_2)\widehat{\mathrm{g}_i}^*\rangle =$$

$$\langle(\alpha_1 + (\mathrm{g}_i^*\mathrm{Q} + \lambda_1)\alpha_2)\widehat{\mathrm{g}_i^*}\rangle = \langle(\alpha_1 + \lambda_1\alpha_2)\widehat{\mathrm{g}_i}^*\rangle.$$

En el Teorema 3.2.1 se describe la estructura de los códigos γ-constacíclicos sobre anillos de la familia $\mathfrak{F}_3$, de longitud prima relativa con la característica del campo residual del anillo local. Puesto que la familia de anillos $\mathfrak{L}_4$ es una subfamilia de $\mathfrak{F}_3$ entonces las afirmaciones del Teorema 3.2.1 son ciertas para los anillos de la familia $\mathfrak{L}_4$. Presentamos el siguiente resultado que es un caso particular del Teorema 3.2.1, cuando los códigos tienen por alfabeto un anillo de la familia $\mathfrak{L}_4$, y se hacen algunas modificaciones en la notación.

Teorema 4.2.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$, γ *una unidad de* A, $\overline{\alpha} = \{\alpha_1, \alpha_2\}$ *un conjunto mínimo de generadores de* $\mathfrak{m}$, $\mathrm{f}_1, \ldots, \mathrm{f}_r$ *los únicos polinomios mónicos básicos irreducibles coprimos a pares tales que* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$, $\mathbb{T} \subseteq \mathrm{A}$ *y* $\mathbb{T}_s \subseteq \mathrm{B}$ *conjuntos de representantes del campo residual de* A *y de* B *respectivamente. Sea* C *un código* γ*-constacíclico de longitud* n, *entonces existe un único subconjunto* U *de* $\{1, \ldots, r\}$, $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_3, \mathrm{F}_4$ *únicos polinomios mónicos y para cada* $u \in \mathrm{U}$, *existe un único* $\vec{\mathrm{v}}_u \in \{(0,1), (1,\lambda) : \lambda \in \mathbb{T}_{\deg(\mathrm{f}_u)}\}$, *tales que*

(*1*) $\mathrm{T}^n - \gamma = \mathrm{F}_0\mathrm{F}_1\mathrm{F}_3\mathrm{F}_4\prod_{u\in\mathrm{U}}\mathrm{f}_u$,

(*2*) $\mathrm{C} = \langle \mathfrak{m}^2\widehat{\mathrm{F}}_1, \mathfrak{m}\widehat{\mathrm{F}}_3, \widehat{\mathrm{F}}_4, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}}_u : u \in \mathrm{U}\rangle$,

(*3*) $|\mathrm{C}| = q^{4\deg(\mathrm{F}_4)+3\deg(\mathrm{F}_3)+\deg(\mathrm{F}_1)+2\sum_{u\in\mathrm{U}}\deg(\mathrm{f}_u)}$.

Demostración. Aplicando el Teorema 3.2.1, considerando que la longitud del anillo es 4, sea $\mathrm{U}_0, \mathrm{U}_1, \mathrm{U}_2, \mathrm{U}_3, \mathrm{U}_4$ la única partición de $\{1, \ldots, r\}$ y para cada $u \in \mathrm{U}_2$ sea H_u la única 1×2 matriz en forma escalón reducida por filas sobre $\mathbb{F}_{q^{s_u}}$ tal que: $|\mathrm{C}| = q^{\sum_{u\in \mathrm{U}_1} s_u + 2\sum_{u\in \mathrm{U}_2} s_u + 3\sum_{u\in \mathrm{U}_3} s_u + 4\sum_{u\in \mathrm{U}_4} s_u}$ y

$$\mathrm{C} = \langle \mathfrak{m}^2 \prod_{u\notin \mathrm{U}_1} \mathrm{f}_u, \mathfrak{m} \prod_{u\notin \mathrm{U}_{l-1}} \mathrm{f}_u, \prod_{u\notin \mathrm{U}_l} \mathrm{f}_u, (\mathrm{H}_u)_{\mathbb{T}_{s_u}}(\overline{\alpha})\widehat{\mathrm{f}}_u : u \in \mathrm{U}_2 \rangle.$$

Resta definir $\mathrm{F}_i = \prod_{u\in \mathrm{U}_i} \mathrm{f}_u$, para $i \in \{0, 1, 3, 4\}$, y $\mathrm{U} = \mathrm{U}_2$.

Para el siguiente resultado observar que si C es un código γ-constacíclico sobre el anillo A, entonces C se identifica con un ideal del anillo $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$, $\mathrm{C}^\perp$ es código γ^{-1}-constacíclico y se identifica con un ideal del anillo $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma^{-1} \rangle$.
Además recordar que si C es un código lineal de longitud n sobre un anillo local finito de Frobenius A, entonces $|\mathrm{C}||\mathrm{C}^\perp| = |\mathrm{A}|^n$, ([31]).

Teorema 4.2.2 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$, γ, $\overline{\alpha} = \{\alpha_1, \alpha_2\}$, $\mathrm{f}_1, \ldots, \mathrm{f}_r$, $\mathbb{T}$ *y* $\mathbb{T}_s$ *como en el Teorema 4.2.1. Sean* C *un código* γ*-constacíclico,* $\mathrm{U} \subseteq \{1, \ldots, r\}$, $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_3, \mathrm{F}_4$ *y* $\{\vec{\mathrm{v}}_u : u \in \mathrm{U}\}$ *como en el Teorema 4.2.1. Sean* $\mathrm{G}_i = \frac{1}{a_{0,i}}\mathrm{F}_i$, $\mathrm{g}_u = \frac{1}{b_{0,u}}\mathrm{f}_u$, *donde* $a_{0,i}$ *y* $b_{0,u}$ *son los coeficientes constantes de* F_i *y* f_u *respectivamente,* $i \in \{0, 1, 3, 4\}$ *y* $u \in \mathrm{U}$, *entonces:*

(1) $|\mathrm{C}^\perp| = q^{4\deg(\mathrm{F}_0)+3\deg(\mathrm{F}_1)+\deg(\mathrm{F}_3)+2\sum_{u\in \mathrm{U}} \deg(\mathrm{f}_u)}$.

(2) $\mathrm{U} \subseteq \{1, \ldots, r\}$, $\mathrm{G}_0, \mathrm{G}_1, \mathrm{G}_3, \mathrm{G}_4$, $\{\mathrm{g}_u : u \in \mathrm{U}\}$, $\{(\vec{\mathrm{v}}_u^\perp)^* : u \in \mathrm{U}\}$ *son los únicos objetos asociados al código* γ^{-1}*-constacíclico* $\mathrm{C}^\perp$*, como en el Teorema 4.2.1, y el ideal correspondiente de* $\mathrm{C}^\perp$ *es*

$$\langle \mathfrak{m}^2\widehat{\mathrm{G}}_3^*, \mathfrak{m}\widehat{\mathrm{G}}_1^*, \widehat{\mathrm{G}}_0^*, (\vec{\mathrm{v}}_u^\perp)_{\overline{\alpha}}^*\widehat{\mathrm{g}}_u^* : u \in \mathrm{U}\rangle = \langle \mathfrak{m}^2\widehat{\mathrm{F}}_3^*, \mathfrak{m}\widehat{\mathrm{F}}_1^*, \widehat{\mathrm{F}}_0^*, (\vec{\mathrm{v}}_u^\perp)_{\overline{\alpha}}^*\widehat{\mathrm{f}}_u^* : u \in \mathrm{U}\rangle.$$

Demostración.
(1) La relación del Lema 1.3.4, $|\mathrm{M}| = |\mathbb{F}_q|^{\ell_{\mathrm{A}}(\mathrm{M})}$, donde M es un A-módulo, implica que $|\mathrm{A}| = q^4$. Puesto que $n = \deg(\mathrm{F}_0) + \deg(\mathrm{F}_1) + \deg(\mathrm{F}_3) + \deg(\mathrm{F}_4) + \sum_{u\in \mathrm{U}} \deg(\mathrm{f}_u)$, entonces por el inciso (3) del Teorema 4.2.1,

$$|\mathrm{C}^\perp| = \frac{|\mathrm{A}|^n}{|\mathrm{C}|} = \frac{q^{4n}}{|\mathrm{C}|} = \frac{q^{4\deg(\mathrm{F}_0)+4\deg(\mathrm{F}_1)+4\deg(\mathrm{F}_3)+4\deg(\mathrm{F}_4)+4\sum_{u\in \mathrm{U}} \deg(\mathrm{f}_u)}}{q^{\deg(\mathrm{F}_1)+3\deg(\mathrm{F}_3)+4\deg(\mathrm{F}_4)+2\sum_{u\in \mathrm{U}} \deg(\mathrm{f}_u)}} =$$

$$q^{4\deg(\mathrm{F}_0)+3\deg(\mathrm{F}_1)+\deg(\mathrm{F}_3)+2\sum_{u\in \mathrm{U}}\deg(\mathrm{f}_u)}.$$

(2) La segunda igualdad entre los ideales es fácil de verificar. Por el inciso (2) del Corolario 4.2.1, el producto de los polinomios mónicos $\mathrm{G}_0^*, \mathrm{G}_1^*, \mathrm{G}_3^*, \mathrm{G}_4^*, \{\mathrm{g}_u^* : u \in \mathrm{U}\}$ es $\mathrm{T}^n - \gamma^{-1}$, $\deg(\mathrm{F}_i^*) = \deg(\mathrm{F}_i)$, $i \in \{0,1,3,4\}$, y $\deg(\mathrm{f}_u^*) = \deg(\mathrm{f}_u)$, $u \in \mathrm{U}$.
Entonces, por el inciso (3) del Teorema 4.2.1 y el inciso $(5d)$ del Corolario 4.2.1, el número de elementos del código γ^{-1}-constacíclico

$$\mathrm{D} = \langle \mathfrak{m}^2\widehat{\mathrm{F}}_3^*, \mathfrak{m}\widehat{\mathrm{F}}_1^*, \widehat{\mathrm{F}}_0^*, (\vec{\mathrm{v}}_u^{\perp})_{\overline{\alpha}}^*\widehat{\mathrm{f}}_u^* : u \in \mathrm{U}\rangle$$

es $|\mathrm{D}| = q^{4\deg(\mathrm{F}_0^*)+3\deg(\mathrm{F}_1^*)+\deg(\mathrm{F}_3^*)+2\sum_{u\in \mathrm{U}}\deg(\mathrm{f}_u^*)} = q^{4\deg(\mathrm{F}_0)+3\deg(\mathrm{F}_1)+\deg(\mathrm{F}_3)+2\sum_{u\in \mathrm{U}}\deg(\mathrm{f}_u)}$.
Finalmente, de los incisos (1) y (3) del Corolario 4.2.1 y las relaciones:

(1) $\mathfrak{m}^3 = \langle 0\rangle$,

(2) $(\vec{\mathrm{v}}_u)_{\overline{\alpha}}(\vec{\mathrm{v}}_u^{\perp})_{\overline{\alpha}}\widehat{\mathrm{f}}_u = 0$, en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma\rangle$, $u \in \mathrm{U}$.

(3) $\widehat{\mathrm{F}}_i\widehat{\mathrm{F}}_j = 0$, en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma\rangle$, $i, j \in \{0,1,3,4\}$, $i \neq j$.

(4) $\widehat{\mathrm{f}}_i\widehat{\mathrm{f}}_j = 0$, en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma\rangle$, $i \neq j$.

(5) $\widehat{\mathrm{F}}_i\widehat{\mathrm{f}}_u = 0$, en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma\rangle$, $i \in \{0,1,3,4\}$ y $u \in \mathrm{U}$.

se obtiene $\mathrm{D} \subseteq \mathrm{C}^{\perp}$. La afirmación se sigue del inciso (1).

Observación 7 *Para determinar $\vec{u}_{\overline{\alpha}}^{\perp}$ en el Teorema 3.2.1, los Corolarios 4.1.1 y 4.1.2 se deben usar. Después para determinar $(\vec{u}_{\overline{\alpha}}^{\perp})^*\widehat{\mathrm{f}_u}^*$, el inciso $(5d)$ del Corolario 4.2.1 se debe usar.*

En los siguientes ejemplos se ilustran las ideas del Teorema anterior.

Observar que cada unidad del anillo $\mathrm{A} = \mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$ tiene la propiedad $\gamma = \gamma^{-1}$, (ver Proposición 3.2, [21]), cada elemento de A se puede escribir de manera única como $a + b\mathrm{x} + c\mathrm{y} + d\mathrm{xy}$, donde $a, b, c, d \in \mathbb{F}_2$, $\overline{\alpha} = \{\mathrm{x}, \mathrm{y}\}$ es un conjunto mínimo de generadores del ideal maximal de A, $\mathfrak{m}^2 = \langle \mathrm{xy}\rangle$. Si $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ es un polinomio básico irreducible con $s = \deg(\tilde{\mathrm{f}})$, entonces $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$ es isomorfo a $\mathbb{F}_{2^s}[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$, por el Teorema 4.1.1, y $\mathbb{T}_s = \{a_0 + a_1\mathrm{T} + \ldots + a_{s-1}\mathrm{T}^{s-1} : a_i \in \mathbb{F}_2\}$ es un conjunto de representantes del campo residual de $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$. Por el Lema 4.1.4, $(0,1)_{\overline{\alpha}}^{\perp} = (0,1)_{\overline{\alpha}}$ y $(1,\lambda)_{\overline{\alpha}}^{\perp} = (1,\lambda)_{\overline{\alpha}}$ en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$, $\lambda \in \mathbb{T}_{\deg(\tilde{\mathrm{f}})}$.

EJEMPLO 4.2.1 *Sean* $\mathrm{A} = \mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$, *el anillo* (13) *del Teorema 2.2.1, y* γ *una unidad de* A.
Por el Lema de Hensel, $\mathrm{T}^{15}-\gamma$ *se factoriza en* $\mathrm{A}[\mathrm{T}]$ *como* $\mathrm{T}^{15}-\gamma = \mathrm{f}_1\mathrm{f}_2\mathrm{f}_3\mathrm{f}_4\mathrm{f}_5$, *donde:*
$\mathrm{f}_1 = \mathrm{T}^4 + \gamma\mathrm{T} + 1$,
$\mathrm{f}_2 = \mathrm{T}^4 + \gamma\mathrm{T}^3 + \mathrm{T}^2 + \gamma\mathrm{T} + 1$,
$\mathrm{f}_3 = \mathrm{T}^4 + \gamma\mathrm{T}^3 + 1$,
$\mathrm{f}_4 = \mathrm{T}^2 + \gamma\mathrm{T} + 1$,
$\mathrm{f}_5 = \mathrm{T} + \gamma$.
Y se cumple $\mathrm{f}_1^* = \mathrm{f}_3$, $\mathrm{f}_2^* = \mathrm{f}_2$, $\mathrm{f}_3^* = \mathrm{f}_1$, $\mathrm{f}_4^* = \mathrm{f}_4$, $\mathrm{f}_5^* = \gamma\mathrm{f}_5$, *entonces:*

(*1*) *Si* $\mathrm{F}_0 = \mathrm{f}_1$, $\mathrm{F}_1 = \mathrm{f}_2$, $\mathrm{F}_3 = \mathrm{f}_3$, $\mathrm{F}_4 = \mathrm{f}_4\mathrm{f}_5$ *y* $\mathrm{U} = \emptyset$, *el código correspondiente es:*

$$\mathrm{C} = \langle \mathfrak{m}^2\widehat{\mathrm{F}_1}, \mathfrak{m}\widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} : u \in \mathrm{U}\rangle =$$

$$\langle \mathfrak{m}^2\widehat{\mathrm{f}_2}, \mathfrak{m}\widehat{\mathrm{f}_3}, \widehat{\mathrm{f}_4\mathrm{f}_5}\rangle = \langle \mathfrak{m}^2\mathrm{f}_1\mathrm{f}_3\mathrm{f}_4\mathrm{f}_5, \mathfrak{m}\mathrm{f}_1\mathrm{f}_2\mathrm{f}_4\mathrm{f}_5, \mathrm{f}_1\mathrm{f}_2\mathrm{f}_3\rangle.$$

Su código dual es

$$\mathrm{C}^{\perp} = \langle \mathfrak{m}^2\widehat{\mathrm{F}}_3^*, \mathfrak{m}\widehat{\mathrm{F}}_1^*, \widehat{\mathrm{F}}_0^*, (\vec{\mathrm{v}}_u^{\perp})_{\overline{\alpha}}^*\widehat{\mathrm{f}}_u^* : u \in \mathrm{U}\rangle =$$

$$\langle \mathfrak{m}^2\widehat{\mathrm{F}_3}^*, \mathfrak{m}\widehat{\mathrm{F}_1}^*, \widehat{\mathrm{F}_0}^*\rangle = \langle \mathfrak{m}^2\widehat{\mathrm{f}_3}^*, \mathfrak{m}\widehat{\mathrm{f}_2}^*, \widehat{\mathrm{f}_1}^*\rangle = \langle \mathfrak{m}^2\widehat{\mathrm{f}_3^*}, \mathfrak{m}\widehat{\mathrm{f}_2^*}, \widehat{\mathrm{f}_1^*}\rangle =$$

$$\langle \mathfrak{m}^2\widehat{\mathrm{f}_1}, \mathfrak{m}\widehat{\mathrm{f}_2}, \widehat{\mathrm{f}_3}\rangle = \langle \mathfrak{m}^2\mathrm{f}_2\mathrm{f}_3\mathrm{f}_4\mathrm{f}_5, \mathfrak{m}\mathrm{f}_1\mathrm{f}_3\mathrm{f}_4\mathrm{f}_5, \mathrm{f}_1\mathrm{f}_2\mathrm{f}_4\mathrm{f}_5\rangle.$$

(*2*) *Si* $\mathrm{F}_0 = 1$, $\mathrm{F}_1 = 1$, $\mathrm{F}_3 = \mathrm{f}_1$, $\mathrm{F}_4 = \mathrm{f}_2$, $\mathrm{U} = \{3,4,5\}$, $\vec{\mathrm{v}}_3 = (1, 1+\mathrm{T}+\mathrm{T}^2)$, $1+\mathrm{T}+\mathrm{T}^2 \in \mathbb{T}_{\deg(\mathrm{f}_3)}$, $\vec{\mathrm{v}}_4 = (1, 1+\mathrm{T})$, $1+\mathrm{T} \in \mathbb{T}_{\deg(\mathrm{f}_4)}$, *y* $\vec{\mathrm{v}}_5 = (1,1)$, $1 \in \mathbb{T}_{\deg(\mathrm{f}_5)}$, *el código correspondiente es:*

$$\mathrm{C} = \langle \mathfrak{m}^2\widehat{\mathrm{F}_1}, \mathfrak{m}\widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} : u \in \mathrm{U}\rangle =$$

$$\langle \mathfrak{m}\widehat{\mathrm{f}_1}, \widehat{\mathrm{f}_2}, [\mathrm{x} + (1+\mathrm{T}+\mathrm{T}^2)\mathrm{y}]\widehat{\mathrm{f}_3}, [\mathrm{x} + (1+\mathrm{T})\mathrm{y}]\widehat{\mathrm{f}_4}, [\mathrm{x}+\mathrm{y}]\widehat{\mathrm{f}_5}\rangle.$$

Puesto que:
(*a*) $(1,\lambda)^{\perp} = (1,\lambda)$ *en* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_i\rangle$, $i \in \{1,2,3\}$,
(*b*) *el residuo de la división de* $(1+\mathrm{T}+\mathrm{T}^2)^*\mathrm{T}^{15-2}\gamma = (\mathrm{T}^{13}+\mathrm{T}^{14}+\mathrm{T}^{15})\gamma$ *por* $\mathrm{f}_3^* = \mathrm{f}_1$ *es* $(1+\gamma)\mathrm{T}^3 + \mathrm{T}^2 + \gamma$,
(*c*) *el residuo de la división de* $(1+\mathrm{T})^*\mathrm{T}^{15-1}\gamma = (\mathrm{T}^{14}+\mathrm{T}^{15})\gamma$ *por* $\mathrm{f}_4^* = \mathrm{f}_4$ *es*

$\mathrm{T}+1+\gamma$.
El código dual de C *es:*

$$\mathrm{C}^{\perp}=\langle \mathfrak{m}^2\widehat{\mathrm{F}}_3^*, \mathfrak{m}\widehat{\mathrm{F}}_1^*, \widehat{\mathrm{F}}_0^*, (\vec{\mathrm{v}}_u^{\perp})_{\overline{\alpha}}^*\widehat{\mathrm{f}}_u^* : u\in \mathrm{U}\rangle =$$

$$\langle \mathfrak{m}^2\widehat{\mathrm{f}_1}^*, [\mathrm{x}+((1+\gamma)\mathrm{T}^3+\mathrm{T}^2+\gamma)\mathrm{y}]\widehat{\mathrm{f}_3}^*, [\mathrm{x}+(\mathrm{T}+1+\gamma)\mathrm{y}]\widehat{\mathrm{f}_4}^*, [\mathrm{x}+\mathrm{y}]\widehat{\mathrm{f}_5}^*\rangle =$$

$$\langle \mathfrak{m}^2\widehat{\mathrm{f}_3}, [\mathrm{x}+(\mathrm{T}^2+1)\mathrm{y}]\widehat{\mathrm{f}_1}, [\mathrm{x}+\mathrm{Ty}]\widehat{\mathrm{f}_4}, [\mathrm{x}+\mathrm{y}]\widehat{\mathrm{f}_5}\rangle =$$

$$\langle \mathfrak{m}^2\mathrm{f}_1\mathrm{f}_2\mathrm{f}_4\mathrm{f}_5, [\mathrm{x}+(\mathrm{T}^2+1)\mathrm{y}]\mathrm{f}_2\mathrm{f}_3\mathrm{f}_4\mathrm{f}_5, [\mathrm{x}+\mathrm{Ty}]\mathrm{f}_1\mathrm{f}_2\mathrm{f}_3\mathrm{f}_5, [\mathrm{x}+\mathrm{y}]\mathrm{f}_1\mathrm{f}_2\mathrm{f}_3\mathrm{f}_4\rangle.$$

Sean $\mathrm{A}=\mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2-4, 2\mathrm{X}\rangle$ el anillo (12) del Teorema 2.2.1 y γ una unidad de A. γ tiene orden multiplicativo 1, 2 ó 4, (ver Proposición 3.8, [21]). Cada elemento de A se puede escribir en la forma $a+b\mathrm{x}$, donde $a\in\mathbb{Z}_8$ y $b\in\{0,1\}\subset\mathbb{Z}_8$, las unidades de A se pueden escribir como $1+2a+4b+c\mathrm{x}$, donde $a,b,c\in\{0,1\}$, $\overline{\alpha}=\{\mathrm{x},2\}$ es un conjunto mínimo de generadores del ideal maximal de A, $\mathfrak{m}^2=\langle 4\rangle$, $\mathbb{T}=\{0,1\}\subset\mathbb{Z}_8$ es un conjunto de representantes para el campo residual de A. Y si f es un polinomio básico irreducible sobre el anillo A con $s=\deg(\tilde{\mathrm{f}})$, entonces $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$ es isomorfo a $\mathrm{GR}(8,s)[\mathrm{X}]/\langle \mathrm{X}^2-4, 2\mathrm{X}\rangle$, por el Teorema 4.1.1, y $\mathbb{T}_s=\{a_0+a_1\mathrm{T}+\ldots+a_{s-1}\mathrm{T}^{s-1} : a_i\in\{0,1\}\subset\mathbb{Z}_8\}$ es un conjunto de representantes del campo residual de A. Por el Lema 4.1.2, se tiene en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$, $(0,1)_{\overline{\alpha}}^{\perp}=(1,0)_{\overline{\alpha}}$, $(1,0)_{\overline{\alpha}}^{\perp}=(0,1)_{\overline{\alpha}}$ y $(1,\lambda_1)_{\overline{\alpha}}^{\perp}=(1,\lambda_2)_{\overline{\alpha}}$, donde $\lambda_1,\lambda_2\in\mathbb{T}_s$, con $\tilde{\lambda}_1\tilde{\lambda}_2=-1=1$ en $\mathbb{F}_{2^s}$.

Ejemplo 4.2.2 *Sean* $\mathrm{A}=\mathbb{Z}_8[\mathrm{X}]/\langle \mathrm{X}^2-4, 2\mathrm{X}\rangle$*, el anillo del inciso* (12) *en el Teorema 2.2.1, y* γ *una unidad de* A*, entonces* $\gamma=1+\mathrm{m}$, $\mathrm{m}=2a+4b+c\mathrm{x}$ *y* $a,b,c\in\{0,1\}\subset\mathbb{Z}_8$. *Por el Lema de Hensel,* $\mathrm{T}^7-\gamma$ *se factoriza en* $\mathrm{A}[\mathrm{T}]$ *como* $\mathrm{T}^7-\gamma=\mathrm{f}_1\mathrm{f}_2\mathrm{f}_3$*, donde:*
$\mathrm{f}_1=\mathrm{T}^3+(3+\mathrm{m}+\mathrm{m}^2)\mathrm{T}^2+2\mathrm{T}+7+3\mathrm{m}$,
$\mathrm{f}_2=\mathrm{T}^3+(6+2\mathrm{m})\mathrm{T}^2+(5+\mathrm{m}^2+2\mathrm{m})\mathrm{T}+7+3\mathrm{m}$,
$\mathrm{f}_3=\mathrm{T}+7+\mathrm{m}+\mathrm{m}^2\in\mathrm{A}[\mathrm{T}]$.
Entonces:

(*1*) *Si* $\mathrm{F}_0=\mathrm{f}_1, \mathrm{F}_1=1, \mathrm{F}_3=\mathrm{f}_3, \mathrm{F}_4=1$, $\mathrm{U}=\{2\}$ *y* $\vec{\mathrm{v}}_2=(1,\mathrm{T})$, $\mathrm{T}\in\mathbb{T}_{\deg(\mathrm{f}_2)}$, *el código correspondiente es:*

$$\mathrm{C}=\langle \mathfrak{m}^2\widehat{\mathrm{F}_1}, \mathfrak{m}\widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} : u\in\mathrm{U}\rangle=\langle \mathfrak{m}\widehat{\mathrm{f}_3}, [\mathrm{x}+2\mathrm{T}]\widehat{\mathrm{f}_2}\rangle=\langle \mathfrak{m}\mathrm{f}_1\mathrm{f}_2, [\mathrm{x}+2\mathrm{T}]\mathrm{f}_1\mathrm{f}_3\rangle.$$

Puesto que:
(*a*) $(1,\mathrm{T})_{\overline{\alpha}}^{\perp}=(1,\mathrm{T}^2+1)_{\overline{\alpha}}$ *en* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_2\rangle$,

(*b*) *el residuo de la división de* $(\mathrm{T}^2+1)^*\mathrm{T}^{7-2}\gamma = (\mathrm{T}^7+\mathrm{T}^5)\gamma$ *por* f_2^* *es* $2\gamma^2\mathrm{T}^2 + 7\gamma\mathrm{T} + \gamma^3 + 7\gamma$.
El código dual de C *es:*

$$\mathrm{C}^\perp = \langle \mathfrak{m}^2\widehat{\mathrm{F}}_3^*, \mathfrak{m}\widehat{\mathrm{F}}_1^*, \widehat{\mathrm{F}}_0^*, (\vec{\mathrm{v}}_u^\perp)_{\overline{\alpha}}^*\widehat{\mathrm{f}}_u^* : u \in \mathrm{U}\rangle =$$

$$\langle \mathfrak{m}^2\widehat{\mathrm{f}_3}^*, \widehat{\mathrm{f}_1}^*, [\mathrm{x} + (2\gamma^2\mathrm{T}^2 + 7\gamma\mathrm{T} + \gamma^3 + 7\gamma)2]\widehat{\mathrm{f}_2}^*\rangle = \langle \mathfrak{m}^2\widehat{\mathrm{f}_3^*}, \widehat{\mathrm{f}_1^*}, [\mathrm{x}+2\mathrm{T}]\widehat{\mathrm{f}_2^*}\rangle =$$

$$\langle \mathfrak{m}^2\mathrm{f}_1^*\mathrm{f}_2^*, \mathrm{f}_2^*\mathrm{f}_3^*, [\mathrm{x}+2\mathrm{T}]\mathrm{f}_1^*\mathrm{f}_3^*\rangle.$$

(*2*) *Si* $\mathrm{F}_0 = \mathrm{F}_1 = \mathrm{F}_3 = \mathrm{F}_4 = 1$, $\mathrm{U} = \{1,2,3\}$, $\vec{\mathrm{v}}_1 = (1, \mathrm{T})$, $\mathrm{T} \in \mathbb{T}_{\deg(\mathrm{f}_1)}$, $\vec{\mathrm{v}}_2 = (1,0)$, $0 \in \mathbb{T}_{\deg(\mathrm{f}_2)}$ *y* $\vec{\mathrm{v}}_3 = (1,1)$, $1 \in \mathbb{T}_{\deg(\mathrm{f}_3)}$, *el código correspondiente es:*

$$\mathrm{C} = \langle \mathfrak{m}^2\widehat{\mathrm{F}_1}, \mathfrak{m}\widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} : u \in \mathrm{U}\rangle = \langle [\mathrm{x}+2\mathrm{T}]\widehat{\mathrm{f}_1}, \mathrm{x}\widehat{\mathrm{f}_2}, [\mathrm{x}+2]\widehat{\mathrm{f}_3}\rangle =$$

$$\langle [\mathrm{x}+2\mathrm{T}]\mathrm{f}_2\mathrm{f}_3, \mathrm{x}\mathrm{f}_1\mathrm{f}_3, [\mathrm{x}+2]\mathrm{f}_1\mathrm{f}_2\rangle.$$

Puesto que:
(*a*) $(1,\mathrm{T})_{\overline{\alpha}}^\perp = (1, \mathrm{T}+\mathrm{T}^2)$, *en* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_1\rangle$,
(*b*) $(1,0)_{\overline{\alpha}}^\perp = (0,1)$, *en* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_2\rangle$,
(*c*) $(1,1)_{\overline{\alpha}}^\perp = (1,1)$, *en* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}_3\rangle$.
(*d*) *el residuo de la división de* $(\mathrm{T}^2+\mathrm{T})^*\mathrm{T}^{7-2}\gamma = (1+\mathrm{T})\mathrm{T}^5\gamma = (\mathrm{T}^6+\mathrm{T}^5)\gamma$ *por* f_1^* *es* $(\gamma^3+\gamma^2+4\gamma)\mathrm{T}^2 + (2\gamma^2+3\gamma)\mathrm{T} + \gamma^3 + 3\gamma^2$.
El código dual de C *es:*

$$\mathrm{C}^\perp = \langle \mathfrak{m}^2\widehat{\mathrm{F}}_3^*, \mathfrak{m}\widehat{\mathrm{F}}_1^*, \widehat{\mathrm{F}}_0^*, (\vec{\mathrm{v}}_u^\perp)_{\overline{\alpha}}^*\widehat{\mathrm{f}}_u^* : u \in \mathrm{U}\rangle =$$

$$\langle [\mathrm{x} + 2\big((\gamma^3+\gamma^2+4\gamma)\mathrm{T}^2 + (2\gamma^2+3\gamma)\mathrm{T} + \gamma^3 + 3\gamma^2\big)]\widehat{\mathrm{f}_1}^*, 2\widehat{\mathrm{f}_2}^*, [\mathrm{x}+2]\widehat{\mathrm{f}_3}^*\rangle =$$

$$\langle [\mathrm{x}+2\mathrm{T}]\widehat{\mathrm{f}_1}^*, 2\widehat{\mathrm{f}_2}^*, [\mathrm{x}+2]\widehat{\mathrm{f}_3}^*\rangle = \langle [\mathrm{x}+2\mathrm{T}]\mathrm{f}_2^*\mathrm{f}_3^*, 2\mathrm{f}_1^*\mathrm{f}_3^*, [\mathrm{x}+2]\mathrm{f}_1^*\mathrm{f}_2^*\rangle.$$

4.3. Códigos constacíclicos autoduales sobre anillos en la familia $\mathfrak{L}_4$

En esta Sección se describen los códigos γ-constacíclicos autoduales, cuando el alfabeto de los códigos es un anillo de la familia $\mathfrak{L}_4$, la longitud del código es prima relativa con la característica del campo residual del anillo y $\gamma = \gamma^{-1}$. Recordar que un polinomio f sobre el anillo finito A es llamado auto-reverso si f^* y f son asociados.

En esta parte se usará la siguiente notación: dado un anillo $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ en la familia $\mathfrak{L}_4$ y $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ un polinomio básico irreducible, con $s = \deg(\tilde{\mathrm{f}})$. $\overline{\alpha} = \{\alpha_1, \alpha_2\}$ será un conjunto mínimo de generadores del ideal maximal de A, γ denotará una unidad del anillo A y tendrá la propiedad $\gamma = \gamma^{-1}$, $\mathbb{T}$ será un conjunto de representantes para $\mathbb{F}_q$ y $\mathbb{T}_s = \{a_0 + a_1\mathrm{T} + \ldots + a_{s-1}\mathrm{T}^{s-1}\}$ será el conjunto de representantes para el campo residual del anillo local $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f} \rangle$

PROPOSICIÓN 4.3.1 *Sea* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$, γ, $\overline{\alpha} = \{\alpha_1, \alpha_2\}$, $\mathbb{T}$ *y* $\mathbb{T}_s$ *como hasta ahora. Sea* C *un código* γ*-constacíclico,* $\mathrm{U} \subseteq \{1, \ldots, r\}$, $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_3, \mathrm{F}_4$, $\{\mathrm{f}_u : u \in \mathrm{U}\}$ *y* $\{\vec{\mathrm{v}}_u : u \in \mathrm{U}\}$*, como en el Teorema 4.2.1, tales que*

$$\mathrm{C} = \langle \mathfrak{m}^2\widehat{\mathrm{F}_1}, \mathfrak{m}\widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} : u \in \mathrm{U} \rangle.$$

Entonces C *es autodual si y sólo si se cumplen las siguientes condiciones:*

(*1*) F_1 *es asociado a* F_3^*,

(*2*) F_4 *es asociado a* F_0^*,

(*3*) *para cada* $u \in \mathrm{U}$ *existe* $u_1 \in \mathrm{U}$ *tal que* f_u *es asociado a* $\mathrm{f}_{u_1}^*$ *y* $\langle (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} \rangle = \langle (\vec{\mathrm{v}}_{u_1}^{\perp})_{\overline{\alpha}}^*\widehat{\mathrm{f}_u} \rangle$ *en* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$.

Demostración.
Sea $\mathrm{G}_0 = \frac{1}{a_{0,0}}\mathrm{F}_0, \mathrm{G}_1 = \frac{1}{a_{0,1}}\mathrm{F}_1, \mathrm{G}_3 = \frac{1}{a_{0,3}}\mathrm{F}_3, \mathrm{G}_4 = \frac{1}{a_{0,4}}\mathrm{F}_4$, $\{\mathrm{g}_u = \frac{1}{b_{0,u}}\mathrm{f}_u : u \in \mathrm{U}\}$ y $\{(\vec{\mathrm{v}}_u^{\perp})^* : u \in \mathrm{U}\}$ como en el Teorema 4.2.2, donde $a_{0,i}$ y $b_{0,u}$ son los términos constantes de F_i and f_u respectivamente, $i \in \{0, 1, 3, 4\}$ y $u \in \mathrm{U}$. Entonces,

$$\mathrm{C} = \mathrm{C}^{\perp} = \langle \mathfrak{m}^2\widehat{\mathrm{F}_1}, \mathfrak{m}\widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} : u \in \mathrm{U} \rangle = \langle \mathfrak{m}^2\widehat{\mathrm{G}_3}^*, \mathfrak{m}\widehat{\mathrm{G}_1}^*, \widehat{\mathrm{G}_0}^*, (\vec{\mathrm{v}}_u^{\perp})_{\overline{\alpha}}^*\widehat{\mathrm{g}_u}^* : u \in \mathrm{U} \rangle$$

si y sólo si $\mathrm{F}_1 = \mathrm{G}_3^*$, $\mathrm{F}_3 = \mathrm{G}_1^*$, $\mathrm{F}_4 = \mathrm{G}_0^*$, y para cada $u \in \mathrm{U}$ existe $u_1 \in \mathrm{U}$ tal que $\mathrm{f}_u = \mathrm{g}_{u_1}^*$ y $\langle (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} \rangle = \langle (\vec{\mathrm{v}}_{u_1}^{\perp})_{\overline{\alpha}}^*\widehat{\mathrm{f}_u} \rangle$, en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$; por la unicidad en el Teorema 4.2.1, si y sólo si F_1 es asociado de F_3^*, F_4 es asociado de F_0^*, para cada $u \in \mathrm{U}$ existe $u_1 \in \mathrm{U}$ tal que f_u es asociado a $\mathrm{f}_{u_1}^*$ y $\langle (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} \rangle = \langle (\vec{\mathrm{v}}_{u_1}^{\perp})_{\overline{\alpha}}^*\widehat{\mathrm{f}_u} \rangle$, en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma \rangle$.

LEMA 4.3.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* λ *una unidad de* A, $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ *un polinomio mónico tal que los ceros de* $\tilde{\mathrm{f}} \in \mathbb{F}_q[\mathrm{T}]$ *son distintos en alguna cerradura algebraica de* $\mathbb{F}_q$ *y* $\mathrm{f}^* = \lambda\mathrm{f}$*. Por el Lema 1.3.17, sean* $\mathrm{f}_1, \ldots, \mathrm{f}_r$ *los únicos polinomios básicos irreducibles tal que* $\mathrm{f} = \mathrm{f}_1 \cdots \mathrm{f}_r$*. Entonces existen* r_1, r_2 *enteros no negativos tales que* $r = 2r_1 + r_2$ *y, después de renumerar,* f_i *es un asociado de* f_{r_1+i}, $1 \leq i \leq r_1$ *y* f_{2r_1+i} *es auto-reverso,* $1 \leq i \leq r_2$.

Demostración.
Es suficiente verificar que para cada $i \in \{1, \ldots, r\}$ el polinomio f_i^* es un asociado de f_j, para algún $j \in \{1, \ldots, r\}$. Puesto que $\mathrm{f} = \mathrm{f}_1 \cdots \mathrm{f}_r$, $\mathrm{f}^* = \lambda \mathrm{f} = \mathrm{f}_1^* \cdots \mathrm{f}_r^*$, y cada f_i^* es básico irreducible, entonces f_i^* es asociado a algún f_j, para algún $j \in \{1, \ldots, r\}$, por el Lema 1.3.17.

COROLARIO 4.3.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$ *un anillo local finito,* γ *una unidad de* A *con la propiedad* $\gamma = \gamma^{-1}$, $\mathrm{f}_1, \ldots, \mathrm{f}_r$ *los únicos polinomios mónicos básicos irreducibles tales que* $\mathrm{T}^n - \gamma = \mathrm{f}_1 \cdots \mathrm{f}_r$, *lema 1.3.17. Existen* r_1, r_2 *enteros no negativos tales que* $r = 2r_1 + r_2$ *y, después de renumerar,* f_i *es un asociado de* f_{r_1+i}, $1 \leq i \leq r_1$ *y* f_{2r_1+i} *es auto-reverso,* $1 \leq i \leq r_2$.

Demostración.
La afirmacion se sigue de la relación $(\mathrm{T}^n - \gamma)^* = 1 - \gamma \mathrm{T}^n = -\gamma(\mathrm{T}^n - \gamma)$.

En el resto de este trabajo se usará la notación del Corolario 4.3.1.

DEFINICIÓN 4.3.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$, γ, $\mathrm{f}_1, \ldots, \mathrm{f}_r$ r_1,r_2 *como en el Corolario 4.3.1. Y sea* W *un subconjunto de* $\{1, \ldots, r\}$.

(*1*) *Se denota* $\mathrm{W}^* = \{i \in \{1, \ldots, r\} : \mathrm{f}_i^*$ *es asociado* a f_j, *para algún* $j \in \mathrm{W}\}$. *Esto es, los polinomios asociados de los polinomios en el conjunto* $\{\mathrm{f}_w : w \in \mathrm{W}\}$ *son los polinomios* $\{\mathrm{f}_\alpha : \alpha \in \mathrm{W}^*\}$.

(*2*) W *es llamado especial si para cada* $w_1 \in \mathrm{W}$ *el polinomio* $\mathrm{f}_{w_1}^*$ *no es asociado de* f_w, *para todo* $w \in \mathrm{W}$. *Es decir* $\mathrm{W} \cap \mathrm{W}^* = \emptyset$.

Observar que $\{1, \ldots, 2r_1 + 1\}^* = \{1, \ldots, 2r_1 + 1\}$, y si X es un conjunto especial entonces $\mathrm{X} \subseteq \{1, \ldots, 2r_1\}$ y X^* es un conjuto especial también. $\emptyset$ se considera un conjunto especial y $\emptyset^* = \emptyset$

TEOREMA 4.3.1 *Sean* $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{L}_4$, γ, $\overline{\alpha} = \{\alpha_1, \alpha_2\}$, $\mathbb{T}$, $\mathbb{T}_s$, $\mathrm{f}_1, \ldots, \mathrm{f}_r$ *y* r_1, r_2 *como hasta ahora. Sea* C *un código* γ*-constacíclico,* $\mathrm{U} \subseteq \{1, \ldots, r\}$, $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_3, \mathrm{F}_4$, $\{\mathrm{f}_u : u \in \mathrm{U}\}$ *y* $\{\vec{\mathrm{v}}_u : u \in \mathrm{U}\}$ *como en el Teorema 4.2.1 tal que:*

$$\mathrm{C} = \langle \mathfrak{m}^2 \widehat{\mathrm{F}_1}, \mathfrak{m} \widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}} \widehat{\mathrm{f}_u} : u \in \mathrm{U} \rangle.$$

Entonces C *es código autodual si y sólo si se cumplen las siguientes condiciones:*

(*1*) $[2r_1+1, r] \subseteq \mathrm{U}$, $\mathrm{U} = \mathrm{U}^*$;

(*2*) *para cada* $u \in \mathrm{U}$ *existe* $u_1 \in \mathrm{U}$ *tal que* f_u *es asociado a* $\mathrm{f}^*_{u_1}$ *y* $\langle(\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u}\rangle = \langle(\vec{\mathrm{v}}^{\perp}_{u_1})^*_{\overline{\alpha}}\widehat{\mathrm{f}_u}\rangle$, *en* $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma\rangle$;

(*3*) *existen conjuntos especiales* U_0 *y* U_1 *tal que,* $\mathrm{U}, \mathrm{U}_0, \mathrm{U}_0^*, \mathrm{U}_1, \mathrm{U}_1^*$ *es una partición de* $\{1, \ldots, r\}$ *y* $\mathrm{F}_i = \prod_{u\in \mathrm{U}_i} \mathrm{f}_u$, $i \in \{0,1,3,4\}$, *donde* $\mathrm{U}_3 = \mathrm{U}_1^*$, $\mathrm{U}_4 = \mathrm{U}_0^*$.

Demostración.
$\Rightarrow$) Puesto que $\mathrm{T}^n - \gamma = \mathrm{F}_0\mathrm{F}_1\mathrm{F}_3\mathrm{F}_4 \prod_{u\in \mathrm{U}} \mathrm{f}_u$, y $\mathrm{F}_0, \mathrm{F}_1, \mathrm{F}_3, \mathrm{F}_4$ y $\prod_{u\in \mathrm{U}} \mathrm{f}_u$ son polinomios mónicos, existe una partición $\mathrm{U}_0, \mathrm{U}_1, \mathrm{U}_3, \mathrm{U}_4$ de $\{1, \ldots, r\} \setminus \mathrm{U}$ tal que $\mathrm{F}_i = \prod_{u\in \mathrm{U}_i} \mathrm{f}_u$, $i \in \{0,1,3,4\}$, por el Lema 1.3.17.
Por la Proposición 4.3.1, $\mathrm{F}_1 = \prod_{u\in \mathrm{U}_1} \mathrm{f}_u$ es asociado de $\mathrm{F}_3^* = \prod_{u\in \mathrm{U}_3} \mathrm{f}^*_u$, $\mathrm{F}_4 = \prod_{u\in \mathrm{U}_4} \mathrm{f}_u$ es asociado de $\mathrm{F}_0^* = \prod_{u\in \mathrm{U}_0} \mathrm{f}^*_u$, para cada $u \in \mathrm{U}$ existe $u_1 \in \mathrm{U}$ tal que f_u es asociado a $\mathrm{f}^*_{u_1}$ y $\langle(\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u}\rangle = \langle(\vec{\mathrm{v}}^{\perp}_{u_1})^*_{\overline{\alpha}}\widehat{\mathrm{f}_u}\rangle$, en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{T}^n - \gamma\rangle$. Entonces $\mathrm{U} = \mathrm{U}^*$, y por el Lema 1.3.17, $\mathrm{U}_4 = \mathrm{U}_0^*$, $\mathrm{U}_3 = \mathrm{U}_1^*$, en consecuencia U_0 y U_1 son conjuntos especiales. Finalmente, puesto que $\mathrm{U}_0 \cup \mathrm{U}_1 \cup \mathrm{U}_3 \cup \mathrm{U}_4 \cup \mathrm{U} = \{1, \ldots, r\}$ y $\mathrm{U}_0 \cup \mathrm{U}_1 \cup \mathrm{U}_3 \cup \mathrm{U}_4 \subseteq \{1, \ldots, 2r_1\}$ entonces $[2r_1+1, r] \subseteq \mathrm{U}$.
$\Leftarrow$) Se sigue de la Proposición 4.3.1.

En las siguientes líneas algunos ejemplos son presentados para ilustrar los resultados del Teorema anterior.

Ejemplo 4.3.1 *Sea* $\mathrm{A} = \mathbb{F}_2[\mathrm{X}, \mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle$ *el anillo del Ejemplo 4.2.1,* γ *una unidad de* A *y* C *un código* γ*-constacíclico autodual de longitud* 7 *sobre* A.
Por el Lema de Hensel, $\mathrm{T}^7 - \gamma$ *se factoriza en* $\mathrm{A}[\mathrm{T}]$ *como* $\mathrm{T}^7 - \gamma = \mathrm{f}_1\mathrm{f}_2\mathrm{f}_3$, *donde:*
$\mathrm{f}_1 = \mathrm{T}^3 + \gamma\mathrm{T}^2 + \gamma$,
$\mathrm{f}_2 = \mathrm{T}^3 + \mathrm{T} + \gamma$,
$\mathrm{f}_3 = \mathrm{T} + \gamma$.
Así $r_1 = 1$, $r_2 = 1$, *los conjutos especiales de* $\{1,2,3\}$ *son* $\{1\}, \{2\}, \emptyset$. *Los subconjuntos de* $\{1,2,3\}$ *con la propiedad* $\{3\} \subseteq \mathrm{U}$ *y* $\mathrm{U} = \mathrm{U}^*$ *son* $\{3\}$ *y* $\{1,2,3\}$.
Por el Lema 4.1.4, $\vec{\mathrm{v}}^{\perp}_{\overline{\alpha}} = \vec{\mathrm{v}}_{\overline{\alpha}}$, *para* $\vec{\mathrm{v}}_{\overline{\alpha}} \in \{(0,1)_{\overline{\alpha}}, (1,\lambda)_{\overline{\alpha}} : \lambda \in \mathbb{T}_s\}$.
Entonces $\mathrm{C} = \langle \mathfrak{m}^2\widehat{\mathrm{F}_1}, \mathfrak{m}\widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} : u \in \mathrm{U}\rangle$ *es alguno de los siguientes:*

(*1*) *Cuando* $\mathrm{U} = \{3\}$, $\mathrm{U}_0 = \emptyset, \mathrm{U}_4 = \mathrm{U}_0^* = \emptyset$, $\mathrm{U}_1 = \{1\}$, $\mathrm{U}_3 = \mathrm{U}_1^* = \{2\}$.

  (*a*) $\langle \mathfrak{m}^2\widehat{\mathrm{f}_1}, \mathfrak{m}\widehat{\mathrm{f}_2}, \mathrm{x}\widehat{\mathrm{f}_3}\rangle$,

(*b*) $\langle \mathfrak{m}^2\widehat{\mathrm{f}_1}, \mathfrak{m}\widehat{\mathrm{f}_2}, (\mathrm{x}+\mathrm{y})\widehat{\mathrm{f}_3}\rangle$,

(*c*) $\langle \mathfrak{m}^2\widehat{\mathrm{f}_1}, \mathfrak{m}\widehat{\mathrm{f}_2}, \mathrm{y}\widehat{\mathrm{f}_3}\rangle$.

(*2*) *Cuando* $\mathrm{U} = \{3\}$, $\mathrm{U}_0 = \emptyset, \mathrm{U}_4 = \mathrm{U}_0^* = \emptyset$, $\mathrm{U}_1 = \{2\}$, $\mathrm{U}_3 = \mathrm{U}_1^* = \{1\}$.

(*a*) $\langle \mathfrak{m}^2\widehat{\mathrm{f}_2}, \mathfrak{m}\widehat{\mathrm{f}_1}, \mathrm{x}\widehat{\mathrm{f}_3}\rangle$,

(*b*) $\langle \mathfrak{m}^2\widehat{\mathrm{f}_2}, \mathfrak{m}\widehat{\mathrm{f}_1}, (\mathrm{x}+\mathrm{y})\widehat{\mathrm{f}_3}\rangle$,

(*c*) $\langle \mathfrak{m}^2\widehat{\mathrm{f}_2}, \mathfrak{m}\widehat{\mathrm{f}_1}, \mathrm{y}\widehat{\mathrm{f}_3}\rangle$.

(*3*) *Cuando* $\mathrm{U} = \{3\}$, $\mathrm{U}_1 = \emptyset, \mathrm{U}_3 = \mathrm{U}_1^* = \emptyset$, $\mathrm{U}_0 = \{1\}$, $\mathrm{U}_4 = \mathrm{U}_0^* = \{2\}$.

(*a*) $\langle \widehat{\mathrm{f}_2}, \mathrm{x}\widehat{\mathrm{f}_3}\rangle$,

(*b*) $\langle \widehat{\mathrm{f}_2}, (\mathrm{x}+\mathrm{y})\widehat{\mathrm{f}_3}\rangle$,

(*c*) $\langle \widehat{\mathrm{f}_2}, \mathrm{y}\widehat{\mathrm{f}_3}\rangle$.

(*4*) *Cuando* $\mathrm{U} = \{3\}$, $\mathrm{U}_1 = \emptyset, \mathrm{U}_3 = \mathrm{U}_1^* = \emptyset$, $\mathrm{U}_0 = \{2\}$, $\mathrm{U}_4 = \mathrm{U}_0^* = \{1\}$.

(*a*) $\langle \widehat{\mathrm{f}_1}, \mathrm{x}\widehat{\mathrm{f}_3}\rangle$,

(*b*) $\langle \widehat{\mathrm{f}_1}, (\mathrm{x}+\mathrm{y})\widehat{\mathrm{f}_3}\rangle$,

(*c*) $\langle \widehat{\mathrm{f}_1}, \mathrm{y}\widehat{\mathrm{f}_3}\rangle$.

(*5*) *Cuando* $\mathrm{U} = \{1,2,3\}$, *entonces* $\mathrm{U}_1 = \mathrm{U}_1^* = \mathrm{U}_3 = \mathrm{U}_0 = \mathrm{U}_0^* = \mathrm{U}_4 = \emptyset$.

(*a*) $\langle \vec{\mathrm{v}}_{\overline{\alpha}}^*\widehat{\mathrm{f}_1}, \vec{\mathrm{v}}_{\overline{\alpha}}\widehat{\mathrm{f}_2}, \mathrm{x}\widehat{\mathrm{f}_3}\rangle$, $\vec{\mathrm{v}}_{\overline{\alpha}} \in \{(0,1)_{\overline{\alpha}}, (1,\lambda)_{\overline{\alpha}} : \lambda \in \mathbb{T}_3\}$.

(*b*) $\langle \vec{\mathrm{v}}_{\overline{\alpha}}^*\widehat{\mathrm{f}_1}, \vec{\mathrm{v}}_{\overline{\alpha}}\widehat{\mathrm{f}_2}, \mathrm{y}\widehat{\mathrm{f}_3}\rangle$, $\vec{\mathrm{v}}_{\overline{\alpha}} \in \{(0,1)_{\overline{\alpha}}, (1,\lambda)_{\overline{\alpha}} : \lambda \in \mathbb{T}_3\}$.

(*c*) $\langle \vec{\mathrm{v}}_{\overline{\alpha}}^*\widehat{\mathrm{f}_1}, \vec{\mathrm{v}}_{\overline{\alpha}}\widehat{\mathrm{f}_2}, (\mathrm{x}+\mathrm{y})\widehat{\mathrm{f}_3}\rangle$, $\vec{\mathrm{v}}_{\overline{\alpha}} \in \{(0,1)_{\overline{\alpha}}, (1,\lambda)_{\overline{\alpha}} : \lambda \in \mathbb{T}_3\}$.

En consecuencia, si $\phi : \left[\mathbb{F}_2[\mathrm{X},\mathrm{Y}]/\langle \mathrm{X}^2, \mathrm{Y}^2\rangle\right]^7 \to \mathbb{F}_2^{28}$ *está dado por*

$$\vec{a} + \vec{b}\mathrm{x} + \vec{c}\mathrm{y} + \vec{d}\mathrm{xy} \mapsto (\vec{a}+\vec{b}+\vec{c}+\vec{d}, \vec{c}+\vec{d}, \vec{b}+\vec{d}, \vec{d}), \text{ donde } \vec{a}, \vec{b}, \vec{c}, \vec{d} \in \mathbb{F}_2^7.$$

El mapeo de Gray definido en [14], entonces $\phi(\mathrm{C}^\perp) = \phi(\mathrm{C}) = \phi(\mathrm{C})^\perp$ *es un código binario autodual de longitud* 28, $|\phi(\mathrm{C})||\phi(\mathrm{C})^\perp| = |\phi(\mathrm{C})|^2 = 2^{28}$, $|\phi(\mathrm{C})| = 2^{14}$ *y* $\phi(\mathrm{C})$ *tiene dimensión* 14.

Recordar que las unidades del anillo $\mathrm{A} = \mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2 + 2\mathrm{X}\rangle$ tienen la propiedad $\gamma = \gamma^{-1}$, (ver Proposición 3.4, [21]), y cada elemento de A se puede escribir de manera única como $a + b\mathrm{x}$, donde $a, b \in \mathbb{Z}_4$, $\overline{\alpha} = \{\mathrm{x}, 2\}$ es un conjunto mínimo de generadores del ideal maximal de A, $\mathfrak{m}^2 = \langle 2\mathrm{x}\rangle$, $\mathbb{T} = \{0, 1\} \subset \mathbb{Z}_4$ es un conjunto de representantes del campo residual de A. Adicionalmente si $\mathrm{f} \in \mathrm{A}[\mathrm{T}]$ es un polinomio básico irreducible sobre el anillo A con $s = \deg(\tilde{\mathrm{f}})$, entonces $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$ es isomorfo a $\mathrm{GR}(4, s)[\mathrm{X}]/\langle \mathrm{X}^2 + 2\mathrm{X}\rangle$, por el Teorema 4.1.1, $\mathbb{T}_s = \{a_0 + a_1\mathrm{T} + \ldots + a_{s-1}\mathrm{T}^{s-1} : a_i \in \{0, 1\} \subset \mathbb{Z}_4\}$ es un conjunto de representantes del campo residual de $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$. Por el Lema 4.1.5, se tienen las relaciones en $\mathrm{A}[\mathrm{T}]/\langle \mathrm{f}\rangle$: $(0, 1)_{\overline{\alpha}}^{\perp} = (0, 1)_{\overline{\alpha}}$ y $(1, \lambda_1)_{\overline{\alpha}}^{\perp} = (1, \lambda_2)_{\overline{\alpha}}$, donde $\lambda_1, \lambda_2 \in \mathbb{T}_s$ y $\tilde{\lambda}_2 = \tilde{\lambda}_1 + 1$ en $\mathbb{F}_{2^s}$.

Ejemplo 4.3.2 *Sean* $\mathrm{A} = \mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2 + 2\mathrm{X}\rangle$ *el anillo (11) del Teorema 2.2.1,* γ *una unidad del anillo* A *y* C *un código* γ*-constacíclico de longitud* 9 *sobre* A.
Por el Lema de Hensel, $\mathrm{T}^9 - \gamma$ *se factoriza en* $\mathrm{A}[\mathrm{T}]$ *como* $\mathrm{T}^9 - \gamma = \mathrm{f}_1\mathrm{f}_2\mathrm{f}_3$*, donde:*
$\mathrm{f}_1 = \mathrm{T}^6 + \gamma\mathrm{T}^3 + 1$,
$\mathrm{f}_2 = \mathrm{T}^2 + \gamma\mathrm{T} + 1$,
$\mathrm{f}_3 = \mathrm{T} + 3\gamma$.
Así, $r_1 = 0$, $r_2 = 3$ *y* $\emptyset$ *es el único conjunto especial. En el Teorema 4.3.1,* $\mathrm{U} = \{1, 2, 3\}$.
Y se tienen las siguientes relaciones

(*a*) *Si* $\lambda = a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2 + a_3\mathrm{T}^3 + a_4\mathrm{T}^4 + \mathrm{T}^5$, *entonces* $(1, \lambda)_{\overline{\alpha}}^{\perp} = (1, 1 + \lambda)_{\overline{\alpha}}$ *y el residuo de la división de* $(1 + \lambda)^*\mathrm{T}^{9-5}\gamma$ *por* f_1 *es*

$$3a_3\gamma + 1 + a_0 + 3a_2\gamma\mathrm{T} + 3a_1\gamma\mathrm{T}^2 + 3a_3\mathrm{T}^3 + (\gamma + 3a_2)\mathrm{T}^4 + (a_4\gamma + 3a_1)\mathrm{T}^5.$$

Así

$$\begin{aligned}
&\langle((1, \lambda)_{\overline{\alpha}}^{\perp})^*\mathrm{f}_1\rangle = \langle(1, \lambda)_{\overline{\alpha}}\mathrm{f}_1\rangle \\
\Leftrightarrow\ & \tilde{a}_0 + \tilde{a}_1\mathrm{T} + \tilde{a}_2\mathrm{T}^2 + \tilde{a}_3\mathrm{T}^3 + \tilde{a}_4\mathrm{T}^4 + \mathrm{T}^5 = \\
& \tilde{a}_0 + 3\tilde{a}_3\tilde{\gamma} + 1 + 3\tilde{a}_2\tilde{\gamma}\mathrm{T} + 3\tilde{a}_1\tilde{\gamma}\mathrm{T}^2 + 3\tilde{a}_3\mathrm{T}^3 + (\tilde{\gamma} + 3\tilde{a}_2)\mathrm{T}^4 + (\tilde{a}_4\tilde{\gamma} + 3\tilde{a}_1)\mathrm{T}^5 \\
\Leftrightarrow\ & \tilde{a}_3 = 1, \tilde{a}_2 = \tilde{a}_1, \tilde{a}_4 = \tilde{a}_1 + 1 \\
\Leftrightarrow\ & \lambda = a_0 + a_1\mathrm{T} + a_1\mathrm{T}^2 + \mathrm{T}^3 + (1 + a_1)\mathrm{T}^4 + \mathrm{T}^5, \\
& \textit{para algunos } a_0, a_1 \in \{0, 1\}.
\end{aligned}$$

(*b*) *Si* $\lambda = a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2 + a_3\mathrm{T}^3 + \mathrm{T}^4$, *entonces* $(1,\lambda)^{\perp}_{\overline{\alpha}} = (1, 1+\lambda)_{\overline{\alpha}}$ *y el residuo de la división de* $(1+\lambda)^*\mathrm{T}^{9-4}\gamma$ *por* f_1 *es*

$$3a_3\gamma + 1 + a_0 + 3\gamma a_2\mathrm{T} + 3\gamma a_1\mathrm{T}^2 + 3a_3\mathrm{T}^3 + 3a_2\mathrm{T}^4 + (\gamma + 3a_1)\mathrm{T}^5.$$

Así

$$\begin{aligned}
& \langle((1,\lambda)^{\perp}_{\overline{\alpha}})^*\mathrm{f}_1\rangle = \langle(1,\lambda)_{\overline{\alpha}}\mathrm{f}_1\rangle \\
\Leftrightarrow\ & \tilde{a}_0 + \tilde{a}_1\mathrm{T} + \tilde{a}_2\mathrm{T}^2 + \tilde{a}_3\mathrm{T}^3 + \mathrm{T}^4 = \\
& 3\tilde{a}_3\tilde{\gamma} + 1 + \tilde{a}_0 + 3\tilde{\gamma}\tilde{a}_2\mathrm{T} + 3\tilde{\gamma}\tilde{a}_1\mathrm{T}^2 + 3\tilde{a}_3\mathrm{T}^3 + 3\tilde{a}_2\mathrm{T}^4 + (\tilde{\gamma} + 3\tilde{a}_1)\mathrm{T}^5 \\
\Leftrightarrow\ & \tilde{a}_1 = \tilde{a}_2 = \tilde{a}_3 = 1 \\
\Leftrightarrow\ & \lambda = a_0 + \mathrm{T} + \mathrm{T}^2 + \mathrm{T}^3 + \mathrm{T}^4, a_0 \in \{0,1\}.
\end{aligned}$$

(*c*) *Si* $\lambda = a_0 + a_1\mathrm{T} + a_2\mathrm{T}^2 + \mathrm{T}^3$, *entonces* $(1,\lambda)^{\perp}_{\overline{\alpha}} = (1, 1+\lambda)_{\overline{\alpha}}$ *y el residuo de la división de* $(1+\lambda)^*\mathrm{T}^{9-3}\gamma$ *por* f_1 *es*

$$3\gamma + a_0 + 1 + 3a_2\gamma\mathrm{T} + 3a_1\gamma\mathrm{T}^2 + 3\mathrm{T}^3 + 3a_2\mathrm{T}^4 + 3a_1\mathrm{T}^5.$$

Así

$$\begin{aligned}
& \langle((1,\lambda)^{\perp}_{\overline{\alpha}})^*\mathrm{f}_1\rangle = \langle(1,\lambda)_{\overline{\alpha}}\mathrm{f}_1\rangle \\
\Leftrightarrow\ & \tilde{a}_0 + \tilde{a}_1\mathrm{T} + \tilde{a}_2\mathrm{T}^2 + \mathrm{T}^3 = \\
& 3\tilde{\gamma} + \tilde{a}_0 + 1 + 3\tilde{a}_2\tilde{\gamma}\mathrm{T} + 3\tilde{a}_1\tilde{\gamma}\mathrm{T}^2 + 3\mathrm{T}^3 + 3\tilde{a}_2\mathrm{T}^4 + 3\tilde{a}_1\mathrm{T}^5 \\
\Leftrightarrow\ & \tilde{a}_1 = \tilde{a}_2 = 0 \\
\Leftrightarrow\ & \lambda = a_0 + \mathrm{T}^3, a_0 \in \{0,1\}.
\end{aligned}$$

(*d*) *Si* $\lambda = a_0 + a_1\mathrm{T} + \mathrm{T}^2$, *entonces* $(1,\lambda)^{\perp}_{\overline{\alpha}} = (1, 1+\lambda)_{\overline{\alpha}}$ *y el residuo de la división de* $(1+\lambda)^*\mathrm{T}^{9-2}\gamma$ *por* f_1 *es*

$$\gamma(a_0 + 1) + 3\mathrm{T} + 3a_1\mathrm{T}^2 + 3\gamma\mathrm{T}^4 + 3\gamma a_1\mathrm{T}^5.$$

Así

$$\begin{aligned}
& \langle((1,\lambda)^{\perp}_{\overline{\alpha}})^*\mathrm{f}_1\rangle = \langle(1,\lambda)_{\overline{\alpha}}\mathrm{f}_1\rangle \\
\Leftrightarrow\ & \tilde{a}_0 + \tilde{a}_1\mathrm{T} + \mathrm{T}^2 = \\
& \tilde{\gamma}(\tilde{a}_0 + 1) + 3\mathrm{T} + 3\tilde{a}_1\mathrm{T}^2 + 3\tilde{\gamma}\mathrm{T}^4 + 3\tilde{\gamma}\tilde{a}_1\mathrm{T}^5 \\
\Leftrightarrow\ & 0 = 1.
\end{aligned}$$

(*e*) *Si* $\lambda = a_0 + \mathrm{T}$, *entonces* $(1,\lambda)^{\perp}_{\overline{\alpha}} = (1, 1+\lambda)_{\overline{\alpha}}$ *y el residuo de la división de* $(1+\lambda)^{*}\mathrm{T}^{9-1}\gamma$ *por* f_1 *es*

$$a_0 + 1 + 3\gamma\mathrm{T}^2 + 3\mathrm{T}^5.$$

Así

$$\begin{aligned} & \langle((1,\lambda)^{\perp}_{\overline{\alpha}})^{*}\mathrm{f}_1\rangle = \langle(1,\lambda)_{\overline{\alpha}}\mathrm{f}_1\rangle \\ \Leftrightarrow\ & \tilde{a}_0 + \mathrm{T} = \tilde{a}_0 + 1 + 3\tilde{\gamma}\mathrm{T}^2 + 3\mathrm{T}^5 \\ \Leftrightarrow\ & 0 = 1. \end{aligned}$$

(*f*) *Si* $\lambda = a_0$, *entonces* $(1,\lambda)^{\perp}_{\overline{\alpha}} = (1, 1+\lambda)_{\overline{\alpha}}$ *y el residuo de la división de* $(1+\lambda)^{*}\mathrm{T}^{9-0}\gamma$ *por* f_i, $i \in \{1,2,3\}$, *es*

$$1 + \lambda = 1 + a_0.$$

Así

$$\begin{aligned} & \langle((1,\lambda)^{\perp}_{\overline{\alpha}})^{*}\mathrm{f}_i\rangle = \langle(1,\lambda)_{\overline{\alpha}}\mathrm{f}_i\rangle \\ \Leftrightarrow\ & \tilde{a}_0 = 1 + \tilde{a}_0 \\ \Leftrightarrow\ & 0 = 1. \end{aligned}$$

(*g*) *Para* $i \in \{1,2,3\}$, *se tiene*

$$\langle((0,1)^{\perp}_{\overline{\alpha}})^{*}\mathrm{f}_i\rangle = \langle 2\mathrm{f}_i\rangle = \langle(0,1)_{\overline{\alpha}}\mathrm{f}_i\rangle.$$

(*h*) *Si* $\lambda = a_0 + \mathrm{T}$, *entonces* $(1,\lambda)^{\perp}_{\overline{\alpha}} = (1, 1+\lambda)_{\overline{\alpha}}$ *y el residuo de la división de* $(1+\lambda)^{*}\mathrm{T}^{9-1}\gamma$ *por* f_2 *es*

$$a_0 + 1 + 3\gamma + 3\mathrm{T}.$$

Así

$$\begin{aligned} & \langle((1,\lambda)^{\perp}_{\overline{\alpha}})^{*}\mathrm{f}_2\rangle = \langle(1,\lambda)_{\overline{\alpha}}\mathrm{f}_2\rangle \\ \Leftrightarrow\ & \tilde{a}_0 + \mathrm{T} = \tilde{a}_0 + 1 + 3\tilde{\gamma} + 3\mathrm{T} \\ \Leftrightarrow\ & \lambda = a_0 + \mathrm{T}, a_0 \in \{0,1\}. \end{aligned}$$

Por lo tanto $\mathrm{C} = \langle \mathfrak{m}^2\widehat{\mathrm{F}_1}, \mathfrak{m}\widehat{\mathrm{F}_3}, \widehat{\mathrm{F}_4}, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}_u} : u \in \mathrm{U}\rangle$ *es alguno de los siguientes:*

(*a*) $\left\langle [\mathrm{x}+2(a_0+a_1\mathrm{T}+a_1\mathrm{T}^2+\mathrm{T}^3+(1+a_1)\mathrm{T}^4+\mathrm{T}^5)]\widehat{\mathrm{f}_1}, 2\widehat{\mathrm{f}_2}, 2\widehat{\mathrm{f}_3}\right\rangle$, $a_0, a_1 \in \{0,1\}$.

(*b*) $\left\langle [\mathrm{x}+2(a_0+\mathrm{T}+\mathrm{T}^2+\mathrm{T}^3+\mathrm{T}^4)]\widehat{\mathrm{f}_1}, 2\widehat{\mathrm{f}_2}, 2\widehat{\mathrm{f}_3}\right\rangle$, $a_0 \in \{0,1\}$.

(*c*) $\left\langle [\mathrm{x}+2(a_0+\mathrm{T}^3)]\widehat{\mathrm{f}_1}, 2\widehat{\mathrm{f}_2}, 2\widehat{\mathrm{f}_3}\right\rangle$, $a_0 \in \{0,1\}$.

(*d*) $\left\langle 2\widehat{\mathrm{f}_1}, 2\widehat{\mathrm{f}_2}, 2\widehat{\mathrm{f}_3}\right\rangle = \left\langle 2\right\rangle$.

(*e*) $\left\langle [\mathrm{x}+2(a_0+a_1\mathrm{T}+a_1\mathrm{T}^2+\mathrm{T}^3+(1+a_1)\mathrm{T}^4+\mathrm{T}^5)]\widehat{\mathrm{f}_1}, [\mathrm{x}+2(a_2+\mathrm{T})]\widehat{\mathrm{f}_2}, 2\widehat{\mathrm{f}_3}\right\rangle$, $a_0, a_1, a_2 \in \{0,1\}$.

(*f*) $\left\langle [\mathrm{x}+2(a_0+\mathrm{T}+\mathrm{T}^2+\mathrm{T}^3+\mathrm{T}^4)]\widehat{\mathrm{f}_1}, [\mathrm{x}+2(a_1+\mathrm{T})]\widehat{\mathrm{f}_2}, 2\widehat{\mathrm{f}_3}\right\rangle$, $a_0, a_1 \in \{0,1\}$.

(*g*) $\left\langle [\mathrm{x}+2(a_0+\mathrm{T}^3)]\widehat{\mathrm{f}_1}, [\mathrm{x}+2(a_1+\mathrm{T})]\widehat{\mathrm{f}_2}, 2\widehat{\mathrm{f}_3}\right\rangle$, $a_0, a_1 \in \{0,1\}$.

(*h*) $\left\langle 2\widehat{\mathrm{f}_1}, [\mathrm{x}+2(a_0+\mathrm{T})]\widehat{\mathrm{f}_2}, 2\widehat{\mathrm{f}_3}\right\rangle$, $a_0 \in \{0,1\}$.

En consecuencia si $\phi : \left[\mathbb{Z}_4[\mathrm{X}]/\langle \mathrm{X}^2+2\mathrm{X}\rangle\right]^9 \to \mathbb{Z}_4^{18}$ *está dado por*

$$\vec{a}+\vec{b}\mathrm{x} \mapsto (\vec{a}+\vec{b}, \vec{b}), \text{ donde } \vec{a}, \vec{b}, \in \mathbb{Z}_4^9.$$

El mapeo de Gray definido en [21]. Entonces $\phi(\mathrm{C}^{\perp}) = \phi(\mathrm{C}) = \phi(\mathrm{C})^{\perp}$ *es un código cuaternario autodual de longitud* 18, $|\phi(\mathrm{C})||\phi(\mathrm{C})^{\perp}| = |\phi(\mathrm{C})|^2 = |\mathbb{Z}_4|^{18} = 4^{18}$, $|\phi(\mathrm{C})| = 4^9$.

Conclusiones

Recordemos que $\mathfrak{F}_3$ denota la familia de anillos locales finitos de Frobenius no de cadena y cuyo ideal maximal tiene índice de nilpotencia 3, $\mathfrak{L}_4$ denota la familia de anillos locales finitos de Frobenius no de cadena con longitud 4 y que $\mathfrak{L}_4 \subset \mathfrak{F}_3$.
En esta tesis, los códigos mencionados sobre anillos locales son de longitud prima relativa con la característica del campo residual del anillo.

1. Los anillos locales finitos de Frobenius no de cadena y con longitud 4

En este trabajo se han descrito todos los anillos de la familia $\mathfrak{L}_4$, y por las siguientes contenciones, (ver Lemas 2.2.2 y 2.2.3),

$$\left\{\begin{array}{c}\text{Anillos locales}\\ \text{finitos de Frobenius}\\ \text{no de cadena con}\\ p^4 \text{ elementos}\end{array}\right\} \subset \left\{\begin{array}{c}\text{Anillos locales}\\ \text{finitos de Frobenius}\\ \text{no de cadena con}\\ \text{longitud 4}\end{array}\right\} \subset \left\{\begin{array}{c}\text{Anillos locales}\\ \text{finitos de Frobenius}\\ \text{no de cadena cuyo}\\ \text{ideal maximal}\\ \text{tiene índice de}\\ \text{nilpotencia 3}\end{array}\right\}$$

se han determinado todos los anillos locales de Frobenius no de cadena con p^4 elementos.

2. Sobre la estructura de los códigos γ-constacíclicos sobre anillos de la familia $\mathfrak{F}_3$.

En este trabajo se ha descrito la estructura de los códigos γ-constacíclicos sobre anillos de la familia $\mathfrak{F}_3$, donde la longitud del código es prima relativa con la característica del campo residual del anillo.
Para obtener los códigos C, sobre el anillo $(\mathrm{A}, \mathfrak{m}, \mathbb{F}(q)) \in \mathfrak{F}_3$, se deben seguir los siguientes pasos:

(1) Factorizar sobre el anillo A el binomio $\mathrm{T}^n - \gamma$ como producto de únicos polinomios básicos irreducibles. Esto se hace primero factorizando el binomio $\mathrm{T}^n - \tilde{\gamma}$ sobre el campo residual del anillo A, posteriormente aplicar el Lema de Hensel y finalmente aplicar el Lema 1.3.2.

(2) Si l es la longitud del anillo y $\mathrm{T}^n - \gamma = \mathrm{f}_1\mathrm{f}_2\cdots\mathrm{f}_r$ es la factorización de $\mathrm{T}^n - \gamma$ como producto de únicos polinomios básicos irreducibles, obtener una partición con $l+1$ subconjuntos del conjunto $\{1, 2, \ldots, r\}$, $\mathrm{U}_0, \mathrm{U}_1, \ldots, \mathrm{U}_l$.

(3) Para cada $i \in \{2, \ldots, l-2\}$ y cada $u \in \mathrm{U}_i$ elegir una matriz en forma escalón reducida por filas sobre $\mathbb{F}_{q^{s_u}}$, $s_u = \deg(\tilde{\mathrm{f}}_u)$.

(4) Finalmente, obtener el código de acuerdo a la fórmula:

$$\mathrm{C} = \langle \mathfrak{m}^2 \prod_{u \notin \mathrm{U}_1} \mathrm{f}_u, \mathfrak{m} \prod_{u \notin \mathrm{U}_{l-1}} \mathrm{f}_u, \prod_{u \notin \mathrm{U}_l} \mathrm{f}_u, (\mathrm{H}_u)_{\mathbb{T}_{s_u}}(\overline{\alpha})\widehat{\mathrm{f}}_u : u \in \cup_{i=2}^{l-2} \rangle.$$

donde $\widehat{\mathrm{f}}(\mathrm{T}) = \frac{\mathrm{T}^n - \gamma}{\mathrm{f}(\mathrm{T})}$.

3. El dual de códigos γ-constacíclicos sobre anillos en la familia $\mathfrak{L}_4$

La descripción dada para un código γ-constacíclico sobre anillos de la familia $\mathfrak{F}_3$ fue útil para calcular el código dual de un código constacíclico sobre anillos en la familia $\mathfrak{L}_4$, (ver [4]).
Para presentar el método para obtener el dual de un código γ-constacíclico, cuando

el alfabeto del código es un anillo en la familia $\mathfrak{L}_4$, primero presentamos el método para obtener códigos γ-constacíclico sobre anillos en la familia $\mathfrak{L}_4$, lo cual es un caso especial de la conclusión anterior.
Para la descripción de los códigos γ-constacíclicos sobre anillos en la familia $\mathfrak{L}_4$ se deben seguir los siguientes pasos:

(1) Una vez factorizado el binomio $\mathrm{T}^n - \gamma$ como producto de polinomios básicos irreducibles, $\mathrm{T}^n - \gamma = \mathrm{f}_1\mathrm{f}_2 \cdots \mathrm{f}_r$. Obtener una partición con 5 subconjuntos del conjunto $\{1, 2, \ldots, r\}$, $\mathrm{U}_0, \mathrm{U}_1, \mathrm{U}_2, \mathrm{U}_3, \mathrm{U}_4$. Definir $\mathrm{F}_i = \prod_{u \in \mathrm{U}_i} \mathrm{f}_u$, para $i \in \{0, 1, 3, 4\}$ y $\mathrm{U} = \mathrm{U}_2$.

(2) Para cada $u \in \mathrm{U}$ elegir $\vec{\mathrm{v}}_u \in \{(0, 1), (1, \lambda) : \lambda \in \mathbb{T}_{\deg(\mathrm{f}_u)}\}$, ver Observación 7

(3) Finalmente, obtener el código de acuerdo a la fórmula:

$$\mathrm{C} = \langle \mathfrak{m}^2\widehat{\mathrm{F}}_1, \mathfrak{m}\widehat{\mathrm{F}}_3, \widehat{\mathrm{F}}_4, (\vec{\mathrm{v}}_u)_{\overline{\alpha}}\widehat{\mathrm{f}}_u : u \in \mathrm{U}\rangle$$

Ahora para obtener el dual del código C, se deben seguir los siguientes pasos:

(1) Para cada $u \in \mathrm{U}$ obtener $(\vec{\mathrm{v}}_u^{\perp})^*$, ver Observación 7.

(2) Finalmente, obtener el código dual de acuerdo a la fórmula:

$$\mathrm{C}^{\perp} = \langle \mathfrak{m}^2\widehat{\mathrm{F}}_3^*, \mathfrak{m}\widehat{\mathrm{F}}_1^*, \widehat{\mathrm{F}}_0^*, (\vec{\mathrm{v}}_u^{\perp})_{\overline{\alpha}}^*\widehat{\mathrm{f}}_u^* : u \in \mathrm{U}\rangle.$$

4. Códigos autoduales sobre anillos de la familia $\mathfrak{L}_4$

La caracterización de los códigos autoduales sobre anillos de la familia $\mathfrak{L}_4$ se presentó en el Teorema 4.3.1.

Índice de símbolos

$a(\mathbb{T}_s)$	Elemento de $\mathbb{T}_s \subset$ B que representa al elemento $a \in \mathbb{F}_{q^s}$
A[T]	Anillo de polinomios en una variable con coeficientes en el anillo A
$\mathrm{A}[\mathrm{X}_1, \ldots, \mathrm{X}_r]$	Anillo de polinomios en las variables $\mathrm{X}_1, \ldots, \mathrm{X}_r$ con coeficientes en el anillo A
$\mathrm{Ann}_{\mathrm{A}}(\mathrm{M})$	Anulador del A-módulo M
A^*	Grupo de unidades del anillo A
$(\mathrm{A}, \mathfrak{m}, \mathrm{k})$	Anillo local A con ideal maximal $\mathfrak{m}$ y campo residual k
$\mathrm{B} = \mathrm{A}[\mathrm{T}]/\langle \mathrm{f}(\mathrm{T}) \rangle$	La extensión no ramificada de A determinada por f(T), f(T) es un polinomio básico irreducible de grado s
$\mathrm{C}^{\perp}$	Dual del código lineal C
car(A)	Característica del anillo A
$\dim_{\mathrm{k}}(\mathrm{V})$	Dimensión del k-espacio vectorial V
det(A)	Determinante de la matriz A

deg(f)	Grado del polinomio f
f^*	Polinomio reverso de f
$\mathfrak{F}_3$	Familia de anillos locales finitos de Frobenius no de cadena y cuyo ideal maximal tiene índice de nilpotencia 3
$\mathbb{F}_q$	Campo finito con q elementos, $q = p^d$, p es un número primo y d es un natural
$(\mathbb{F}_q^*)^2$	Los cuadrados de las unidades del campo finito $\mathbb{F}_q$
$\widehat{f}$	Cociente de la división de $\mathrm{T}^n - \gamma$ con f
$\mathrm{GR}(p^k, d)$	Anillo de Galois
$\mathrm{G}(n, q)$	Número de Galois sobre el campo finito $\mathbb{F}_q$
$\mathrm{H}_{\mathbb{T}_s}(\overline{\alpha})$	Ideal de B dado por $\langle \sum_{i=1}^{l} a_{1i}(\mathbb{T}_s)\alpha_i, \ldots, \sum_{i=1}^{l} a_{ki}(\mathbb{T}_s)\alpha_i \rangle$, H es la matriz (a_{ij}) sobre el campo finito $\mathbb{F}_{q^s}$
I + J	Suma de los ideales I y J
IJ	Producto de los ideales I y J
I^k	Potencia del ideal I
I[T]	Polinomios con coeficientes en el ideal I
LM(G)	Monomios lideres de los polinomios del conjunto G
$\ell_{\mathrm{A}}(\mathrm{M})$	Longitud del A-módulo M
$\mathcal{L}_{\mathrm{A}}(\mathrm{M})$	Retícula de A-submódulos de M

$\mathfrak{L}_4$	Familia de anillos locales finitos de Frobenius no de cadena de longitud 4
Rad(A)	Radical de Jacobson
Soc(M)	Zoclo de M
s_u	Grado del polinomio f_u
$\mathbb{T}$	Conjunto de representantes del campo residual del anillo local finito $(\mathrm{A}, \mathfrak{m}, \mathbb{F}_q)$
$\mathbb{T}_s$	Conjunto de representantes del campo residual de B, el campo residual es $\mathrm{B}/\mathfrak{m}\mathrm{B} = \mathbb{F}_{q^s}$ y $\mathbb{T}_s$ está dado por $\{a_0 + \ldots + a_{s-1}\mathrm{T}^{s-1} : a_i \in \mathbb{T}\}$
t	Índice de nilpotencia del ideal maximal del anillo local A
$\vec{v}_{\overline{\alpha}}^{\perp}$	Denota al ideal $\mathrm{ann}_{\mathrm{B}}(\vec{u}_{\overline{\alpha}}^{\mathrm{B}})$
$\mathrm{v}_{\mathrm{A}}(\mathrm{M})$	Número mínimo de generadores del A-módulo M
$\lvert\mathrm{X}\rvert$	Cardinalidad del conjunto X
$\mathbb{Z}_n$	Anillo de enteros módulo m
γ	Unidad del anillo A
σ_γ	Permutación γ-constacíclica
ρ_γ	La representación polinomial de A^n.
$\binom{n}{k}_q$	Coeficiente binomial Gaussiano

$\overline{\alpha} = \{\alpha_1, \ldots, \alpha_l\}$	Conjunto mínimo de generadores del ideal maximal del anillo local A
$\tilde{}$	La proyección natural
$\langle m_1, \ldots, m_s \rangle$	A-submódulo de M generado por $m_1, \ldots, m_s$
$\{0, 1, \ldots, \zeta^{p^d-2}\}$	Conjunto de Teichmüller del anillo de Galois $\mathrm{GR}(p^k, d)$
$(0,1)_{\overline{\alpha}}$	El elemento α_2 (cuando $\mathrm{A} \in \mathfrak{L}_4$)
$(1,\lambda)_{\overline{\alpha}}$	El elemento $\alpha_1 + \lambda\alpha_2$ (cuando $\mathrm{A} \in \mathfrak{L}_4$)
$(0,1)^{\mathrm{B}}_{\overline{\alpha}}$	El ideal de B generado por α_2 (cuando $\mathrm{A} \in \mathfrak{L}_4$)
$(1,\lambda)^{\mathrm{B}}_{\overline{\alpha}}$	El ideal de B generado por $\alpha_1 + \lambda\alpha_2$, $\lambda \in \mathbb{T}_s$ (cuando $\mathrm{A} \in \mathfrak{L}_4$)

Bibliografía

[1] F. W. Anderson and K. R. Fuller, *Rings and Categories of Modules*, Springer-Verlag, vol. **13**, (1973).

[2] A. R. Calderbamk, and N. J. A Sloane, *Modular and p-adic codes*, Des. Codes and Cryptogr., vol **6**, (21-35), (1995).

[3] C. A. Castillo-Guillén, C. Rentería-Marquéz and H. Tapia-Recillas, *Constacyclic Codes over finite Frobenius non-chain rings with nilpotency index* 3, Finite Fields and Their Applications, vol. **43**, (1-21), (2017).

[4] C. A. Castillo-Guillén, C. Rentería-Marquéz and H. Tapia-Recillas, *Duals of constacyclic codes over finite local non-chain Frobenius rings of lenght* 4, Discrete Mathematics vol. **43**, (33-55), (2018).

[5] H. Q. Dinh, *Constacyclic Codes of length p^s over $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$*, Journal of Algebra, vol. **324**, (940-950), (2010).

[6] H. Q. Dinh and S. R. López-Permouth, *Cyclic Codes Over the integers modulo p^m*, Finite Fields and Their Applications, vol. **3**, (334-352), (1997).

[7] H. Q. Dinh and S. R. López Permouth, *Cyclic and Negacyclic Codes Over Finite Chain Rings*, IEEE Trans. Inform. Theory, vol. **50**, (1728-1744), (2004).

[8] S. T. Dougherty, J. Kim, H. Kulosman, H. Liu, *Self-dual codes over commutative Frobenius rings*, Finite Fields and Their Applications, vol. **16**, (14-26), (2010).

[9] S. T. Dougherty, S. Karadeniz, B. Yildiz, *Cyclic codes over* R_k, Des. Codes and Cryptogr., vol. **63**, (113-126), (2012).

[10] S. T. Dougherty, P. Gaborit, M. Harada and Patrick Solé, *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, vol. **45**, (32-45), (1999).

[11] S. T. Dougherty, S. Karadeniz, B. Yildiz, *Codes over* R_k*, Gray maps and their binary images*, Finite Fields and Their Applications, vol. **17**. (205-219), (2011).

[12] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbamk, N. J. A Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory, vol. **50**, (301-319), (1994).

[13] T. Honold, *Characterization of finite Frobenius rings*, Arch. Math. (Basel), vol. **76(6)**, $(406 - 415)$, (2001).

[14] S. Karadeniz and B. Yildiz, *Cyclic codes over* $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes and Cryptogr., vol. **58**, (221-234), (2011).

[15] S. Karadeniz, B. Yildiz, *Linear codes over* $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$, Des. Codes and Cryptogr., vol. **54**, (61-81), (2010).

[16] T. Y. Lam, *Lectures on modules and rings*, Graduate Texts in Mathematics Springer- Verlag, New York, vol. **189**, (1999).

[17] S. Lang, *Algebra*, Graduate Texts in Mathematics Springer- Verlag, New York, (2002).

[18] F. J. MacWilliams and N. J. A Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, (1977).

[19] H. Matsumura, *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics, (1986).

[20] B. R. McDonald, *Finite rings with identity*, Pure and Applied Mathematics. New York: Marcel Dekker, vol. **28**, (1974).

[21] E. Martínez-Moro and S. Szabo, *On Codes over Local Frobenius Non-Chain Rings of Order* 16, Contemporary Mathematics, vol. **684**, (227-241), (2015).

[22] T. Nakayama, *On Frobenius algebras I*, Annals of Math. (2) vol. **40**, (611-633), (1939).

[23] T. Nakayama, *On Frobenius algebras II*, Annals of Math. (2) vol. **42**, (1-21), (1941).

[24] A. Nijenhuis, A. E. Solow and H. S. Wilf, *Bijective Methods in the Theory of Finite Vector Spaces*, Journal of Combinatorial Theory, vol. **37**, (80-84), (1984).

[25] J. J. Rotman, *An introduction to homological Algebra*, Academic press, inc, (1979).

[26] C. E. Shannon, *A Mathematical theory of communication*, Bell Syst. Tech. J.27, 379-423, 623-656, (1948).

[27] H. Tapia-Recillas and G. Vega, *Some Constacyclic Codes Over $\mathbb{Z}_{2^k}$ and Binary Quasi-Cyclic Codes*, Discrete Appl. Math., vol. **128**, (305-316), (2003).

[28] H. Tapia-Recillas, *On the Gray image of linear cyclic codes over Galois rings*, UAM-I, México D.F., MEXICO, Merseille-Luminy, France, $(26-30)$ September, (2005).

[29] J. Wolfmann, *Negacyclic and cyclic codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory, Vol. **45**, $(2527-2532)$, (1999).

[30] J. Wolfmann, *Binary images of cyclic codes over $\mathbb{Z}_4$*, IEEE Trans. Inform. Theory, Vol. **47**(5), $(1773-1779)$, (2001).

[31] J. Wood, *Duality for modules over finite rings and applications to coding theory.* Amer. J. Math. vol. **121**(3), (555-575), (1999).

[32] O. Zariski and P. Samuel, *Commutative Algebra*, Van Nostrand, New York, vol. **1**, (1958).

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA
METROPOLITANA
Unidad Iztapalapa
DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

CÓDIGOS γ-CONSTACÍCLICOS Y SUS DUALES SOBRE ANILLOS LOCALES FINITOS DE FROBENIUS NO DE CADENA Y CUYO IDEAL MAXIMAL TIENE ÍNDICE DE NILPOTENCIA 3

TESIS QUE PRESENTA

M. en C. Carlos Alberto Castillo Guillén

para obtener el grado de
Doctor en Ciencias (Matemáticas)

Asesores de tesis:
Dr. Horacio Tapia Recillas
Dr. Carlos Rentería Márquez

Sinodales
Dr. Carlos Rentería Márquez
Dr. Guillermo Benito Morales Luna
Dr. Felipe de Jesús Zaldívar Cruz
Dr. Rogelio Fernández Alonso González
Dr. José Noé Gutiérrez Herrera

Ciudad de México
30 de Octubre de 2019
Salón EP 101

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE DISERTACIÓN PÚBLICA

No. 00067
Matrícula: 2121800862

Códigos γ-constacíclicos y sus duales sobre anillos locales finitos de Frobenius no de cadena y cuyo ideal maximal tiene índice de nilpotencia 3

En la Ciudad de México, se presentaron a las 12:00 horas del día 30 del mes de octubre del año 2019 en la Unidad Iztapalapa de la Universidad Autónoma Metropolitana, los suscritos miembros del jurado:

DR. FELIPE DE JESUS ZALDIVAR CRUZ
DR. JOSE NOE GUTIERREZ HERRERA
DR. GUILLERMO BENITO MORALES LUNA
DR. CARLOS RENTERIA MARQUEZ
DR. ROGELIO FERNANDEZ ALONSO GONZALEZ

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron a la presentación de la Disertación Pública cuya denominación aparece al margen, para la obtención del grado de:

DOCTOR EN CIENCIAS (MATEMATICAS)

DE: CARLOS ALBERTO CASTILLO GUILLEN

y de acuerdo con el artículo 78 fracción IV del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

CARLOS ALBERTO CASTILLO GUILLEN
ALUMNO

REVISÓ

MTRA. ROSALIA SERRANO DE LA PAZ
DIRECTORA DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JESUS ALBERTO OCHOA TAPIA

PRESIDENTE

DR. FELIPE DE JESUS ZALDIVAR CRUZ

VOCAL

DR. JOSE NOE GUTIERREZ HERRERA

VOCAL

DR. GUILLERMO BENITO MORALES LUNA

VOCAL

DR. CARLOS RENTERIA MARQUEZ

SECRETARIO

DR. ROGELIO FERNANDEZ ALONSO GONZALEZ