Centro de Investigación y de Estudios
Avanzados del Instituto Politécnico Nacional

unidad zacatenco
departamento de matemáticas

Códigos σ-constacíclicos asociados a anillos de Frobenius

Tesis que presenta

German Vera Martinez

para obtener el título de

Maestría en ciencias con especialidad en Matemáticas

Directores de Tesis:

Dr. Rafael Heraclio Villarreal Rodríguez
Dr. Eliseo Sarmiento Rosales

Ciudad de México. Julio, 2019.

Agradecimientos

Hago una mención especial a mi padre Anselmo German Vera Meneses a quien le dedico la presente tesis, ya que durante el tiempo que estuvo conmigo siempre creyó en mí y me impulsó a seguir adelante, sus enseñanzas y su apoyo continuan aún conmigo.

A mi mamá Estela G. Martinez puesto que en todo momento estuvo apoyando mis decisiones y dandome ánimos para seguir adelante en el desarrollo de este proyecto y a mi hermano Gustavo Vera, ya que sus momentos de distracción también fueron fundamentales.

A mi ahora esposa Jessamyn Infante quien durante desde el inicio del grado me alentó a ingresar y estuvo conmigo en momentos cruciales desde el examen de ingreso hasta los últimos detalles de este trabajo final.

A mis asesores Dr. Rafael H. Villarreal y al Dr. Eliseo Sarmiento pues siempre se mostraron dispuestos a resolver mis dudas y asesorarme a lo largo de la maestría y de la culminación de la misma. Y mis sinodales por su tiempo revisando mi trabajo.

Agradezco al Consejo Nacional de Ciencia y Tecnología (CONACYT) por el apoyo brindado ya que sin el no habría sido posible la realización de este trabajo.

A mis amigos que sirvieron para darme ánimos en cada etapa de la maestría, desde el ingreso hasta el término de la misma.

Resumen

El objetivo central de la presente tesis será estudiar la estructura algebraica de los códigos σ-constancíclicos. Para llegar a este punto primero hablaremos sobre los fundamentos algebraicos y geométricos en los cuales nos apoyaremos para poder definir los diferentes tipos de códigos que veremos. Haremos un breve estudio de algunos tipos de códigos, obtendremos la matriz generadora y su correspondiente matriz chequeo de paridad, un interés principal será estudiar los códigos cíclicos, pues el objetivo central de la tesis será estudiar una generalización de estos códigos.

En el tercer capítulo estudiaremos los códigos σ-constancíclicos para ello tendremos que imponer a nuestro anillo R condiciones especiales que nos ayudarán a preservar algunas propiedades importantes que perdemos al pasar de un campo K a un anillo R. Finalmente el trabajo concluye dando la estructura algebraica de los códigos correspondiente a dichos anillos.

Abstract

The main objetive of this thesis will be study the algebraic structure of the -constancyclic codes. For this, we first talk about the algebraic and geometric fundaments that we will going to use to give the code definition and the different kinds of theme. We will make a little study of types of codes, we will compute the generator matrix and their parity check matrix, the cyclic codes will be the most important type because the central objetive will be make a generalization of these from fields to rings.

In the third chapter we will be study the -constancyclics codes, for this we have to impose special conditions for the ring R for help us to keep some important properties that we would lose from when going from field K to a ring R. Finally the conclusion of this thesis will be give the specific algebraic structure of this codes over the ring R.

Índice general

Introducción

El objetivo de este trabajo es describir la estructura algebraica de lo que llamaremos códigos σ-constancíclicos, los cuales se construyen con estructura de R-módulos, donde R es un anillo local de Frobenius finito, es decir, tiene un único ideal maximal y un único ideal minimal, lo anterior lo podemos interpretar como una red de anillos con nodos inicial y final no triviales, lo cual nos permitirá tener un mayor control sobre sus sub-anillos. Para poder llegar a este último punto es necesario hacer un estudio de las herramientas tanto algebraicas como geométricas que necesitamos para poder abordar de forma correcta el tema.

Durante el Capítulo 1 hacemos un estudio de las herramientas algebraicas y geométricas que necesitamos para hacer el estudio de los códigos. Comenzando con la teoría de las bases de Gröbner con la cual podemos dar una demostración del teorema de extensión que es muy útil para calcular invariantes algebraicos de variedades afines y proyectivas. Hacemos un estudio general de las principales propiedades de las variedades, pues como se demostrará los códigos tipo Reed-Muller son variedades. Los códigos lineales tienen estructura de espacio vectorial sobre un campo finito $\mathbb{F}_p$ para p número primo, como se verá el conjunto de vectores esta formado por una extensión de campo, motivo por el cual se hace un breve estudio de las principales propiedades de las extensiones de campos finitos.

Estas herramientas son usadas para poder abordar de forma correcta el estudio de los códigos lineales, lo cual se hace en el capítulo 2 de esta tesis para terminar en el tercer capítulo con una generalización, viendo que los códigos se pueden dotar de una estructura de módulos sobre anillos finitos.

En el segundo capítulo se realiza un estudio de varios tipos de códigos, comenzando con los códigos lineales y se dan distintos ejemplos de ellos. En cada caso se realiza el cálculo de su código ortogonal así como la construcción de su matriz generadora y su matriz chequeo de paridad. El orden del estudio de estos códigos es importante ya que como se verá la mayoria de las familias de códigos que se introducen resultan ser una

subclase de las familias que se estudian previamente, por decir:

$$\text{códigos residuo cuadrado} \hookrightarrow \text{ códigos cíclicos} \hookrightarrow \text{ códigos polinomiales} \hookrightarrow \text{ códigos lineales.}$$

De entre todos los tipos de código estudiados durante este capítulo los códigos cíclicos son los más trascendentes del capítulo, por lo tanto es importante comprender de forma clara su definición así como las dos distintas estructuras algebraicas con las que podemos describirlos. Por un lado podemos encajarlo en un cociente en el anillo de polinomios $K[X]$ y por otro lado lo podemos ver como el código generado por un polinomio $g(X)$ de grado menor o igual a cierto $n \in \mathbb{N}$.

En el tercer y último capítulo de la tesis se hace una generalización de los códigos cíclicos. Para ello comenzamos sustituyendo el alfabeto, en lugar de tomar un campo K finito, tomaremos un anillo R finito. Este primer y más significativo cambio nos presenta de entrada los problemas sobre la organización y la clasificación de sus subanillos. Recordemos que un código algebraico es un subespacio vectorial sobre cierto campo K finito. Con la finalidad de poder conservar algunas de las propiedades específicas de los campos se pide que el anillo R sea un anillo local, con lo cual conservamos la unicidad del subespacio más grande.

Teniendo esta idea en mente necesitamos *controlar* el subespacio más chico del anillo R, para ello es necesario apoyarnos en la definición de anillo de Frobenius, así como en la herramienta matemática formada alrededor de esta definición, como un primer resultado es posible demostrar que para un anillo local esto es equivalente a tener un único ideal minimal, más aún se sabe que este ideal minimal es el anulador de su ideal maximal.

En los trabajos del matemático Thomas Honold e Ivan Lanjev "Linear codes over finite chain rings"se hace el estudio de los códigos sobre anillos locales de Frobenius que son encadenados, es decir, la familia de subanillos forman una cadena, esto quiere decir que para cada par de subanillos están relacionados. En el trabajo mencionado se estudia la estructura algebraica del código lineal asociado a este tipo de anillos encadenados, después de ver los trabajos realizados por estos y otros matemáticos surge la pregunta natural, ¿Qué pasa con los anillos no encadenados? Responder esta pregunta es el trabajo principal de la presente tesis. Damos de forma explícita la estructura algebraica de un código lineal sobre un anillo R local, de Frobenius no encadenado.

Se exhibirán algunos de los resultados relacionados con módulos sobre anillos de Frobenius locales finitos no encadenados. Estos nos servirán para poder finalmente dar el resultado principal del capítulo, el cual describe de forma explícita la estructura algebraica de sus códigos lineales asociados.

Capítulo 1

Preliminares

En este primer capítulo se expondrá el marco teórico necesario para el desarrollo de esta tesis, hablaremos sobre códigos lineales y sus parámetros básicos como: la distancia mínima, la longitud y la dimensión, ya que éstos son importantes para su estudio. También hablaremos sobre: el espacio proyectivo $\mathbb{P}^n$, el espacio afín K^{n+1}, ideales anuladores y la función de Hilbert.

Las gráficas tienen una conexión muy importante con los códigos, por ello dedicaremos una sección de este primer capítulo al desarrollo de las nociones básicas de esta teoría.

1.1. Bases de Gröbner

Sabemos que el anillo de polinomios en una variable $K[x]$ es un dominio de ideales principales, es por ello que dado un polinomio $f \in K[x]$ y un ideal $I = \langle g \rangle$, para saber si f pertenence al ideal, basta con usar el algoritmo de la división para dividir a f por g, entonces $f \in I$ si y sólo si el residuo de dicha división es cero. Cuando intentamos generalizar al caso de varias variables nos encontramos con un problema fundamental, generar un análogo al algoritmo de la división. A eso nos dedicaremos en esta sección.

Para el desarrollo de las Bases de Gröbner llamaremos a $R = K[x_1, \ldots, x_n]$ el anillo de polinomios en n variables. Para cada $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$, se define $x^\alpha := \prod_i x_i^{\alpha_i}$. Con lo cual se identifica biunívocamente elementos de $\mathbb{Z}^n_{\geq 0}$ con monomios de R.

Definición 1.1.1 *Un orden monomial $\prec$ en R es una relación en $\mathbb{Z}^n_{\geq 0}$, o equivalentemente en los monomios de R, tal que:*

1. *$\prec$ es un orden total en $\mathbb{Z}^n_{\geq 0}$.*

2. *Si $\alpha \prec \beta$, entonces $\alpha + \gamma \prec \beta + \gamma$.*

3. $\prec$ es un buen orden.

Definición 1.1.2 *Sean $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Definimos el **orden lexicográfico** como; $\alpha \prec_{lex} \beta$ si $\alpha_i < \beta_i$ donde i es el menor entero $\in \mathbb{N}$ tal que $\alpha_i \neq \beta_i$.*

Como se dijo al inicio de la sección un elemento básico es el algoritmo de la división para el anillo de polinomios en n variables.

Definición 1.1.3 *Sea $f = \sum_\alpha a_\alpha x^\alpha$ un polinomio no cero en R y sea $\prec$ un orden monomial, entonces:*

1. *El **multigrado** de f se define como: $multideg(f) := \max\{\alpha \in \mathbb{Z}^n_{\geq 0} | a_\alpha \neq 0\}$.*
2. *El **coeficiente líder** de f: $LC(f) = a_{multideg(f)}$.*
3. *El **monomio líder** de f: $LM(f) = x^{multideg(f)}$.*
4. *El **término líder** de f: $LT(f) = LC(f)LM(f)$.*

Teorema 1.1.4 *(Algoritmo de la división en R) Sea $\prec$ orden monomial y sea $F = \{f_1, f_2, \ldots, f_s\}$ una s-tupla de polinomios en R, entonces todo $f \in R$ se puede escribir como:*

$$f = \sum_{i=1}^{s} q_i f_i + r.$$

donde $q_i, r \in R$, además $r = 0$ o es una combinación lineal de monomios, los cuales no son divisibles por ningún $LT(f_i)$. A r se le llama el residuo de f en la división por F, más aún, si $q_i f_i \neq 0$, entonces $multideg(f) \geq multideg(q_i f_i)$.

Definición 1.1.5 *Sea $I \subset R$ un ideal diremos que I es **ideal monomial** si existe $A \subset \mathbb{Z}^n_{\geq 0}$ tal que $I = \langle x^\alpha | \alpha \in A \rangle$.*

Lema 1.1.6 *Sea $I = \langle x^\alpha | \alpha \in A \rangle$ ideal monomial. Entonces un monomio $x^\beta \in I$ si y solamente si $x^\alpha | x^\beta$ para algún $x^\alpha \in I$.*

Demostración. Como primer punto es importante notar que $x^\beta = \sum_{i=1}^n h_i x^{\alpha(i)}$, con $h_i \in R$, pero cada h_i se puede expresar como la suma de monomios, resultando en la siguiente igualdad:

$$x^\beta = \sum_{i=1}^{s} (\sum_j c_{i,j} x^{\beta(i,j)}) x^{\alpha(i)} = \sum_{i,j} c_{i,j} x^{\beta(i,j)} x^{\alpha(i)}.$$

Entonces como cada término del lado derecho de la igualdad es divisible por algún $x^{\alpha(i)}$, siendo éste divisor de cada uno de los términos, es claro que x^β también debe serlo. ■

Corolario 1.1.7 *Sea I ideal monomial y sea $f \in R$ entonces, las siguientes condiciones son equivalentes:*

1. *$f \in I$.*
2. *Cada monomio de f esta en I.*
3. *f es combinación lineal de monomios de I.*

Demostración. Es inmediato del lema anterior. ■

Teorema 1.1.8 *(Lema de Dickson) Sea $I = \langle x^{\alpha} | \alpha \in A \rangle$ ideal monomial. Entonces I puede ser escrito como $I = \langle x^{\alpha(1)}, \ldots, x^{\alpha(s)} \rangle$, donde $\alpha(i) \in A \ \forall i$. Es decir, I admite una base finita.*

Demostración. [7][pag. 71] ■

Definición 1.1.9 *Sea $I \subset R \setminus \{0\}$ un ideal, entonces:*

1. *Denotamos por $LT(I)$ al conjunto de términos líder de elementos de I.*
2. *Denotamos por $\langle LT(I) \rangle$ al ideal generado por los elementos de $LT(I)$.*

Es claro que $\langle LT(I) \rangle$ es un ideal monomial, pues como los elementos de $LM(I)$ y $LT(I)$ difieren sólo por una constante no cero, entonces $\langle LT(I) \rangle = \langle LM(I) \rangle$. Además por el Lema de Dickson se tiene que $\langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_s) \rangle$ para algunos $g_i \in I$.

Definición 1.1.10 *Sea $\prec$ orden monomial fijo e I un ideal de R. Un subconjunto $G = \{g_1, \ldots, g_t\} \subset I$ se dice* ***base de Gröbner*** *si $\langle LT(g_1), \ldots, LT(g_t) \rangle = \langle LT(I) \rangle$.*

Notemos que de la definición anterior un subconjunto G es base de Gröbner si y sólo si el término lider de cualquier elemento de I es divisible por algún $LT(g_i)$.

La importancia de las bases de Gröbner radica en la posibilidad brindarle unicidad al residuo en el algoritmo de la división.

Proposición 1.1.11 *(Algoritmo de la división) Sea $G = \{g_1, \ldots, g_t\}$ una base de Gröbner para un ideal I y sea $f \in R$. Entonces, existe un único $r \in R$ con las siguientes propiedades.*

1. *Existe $g \in I$ tal que $f = g + r$.*
2. *Ningún término de r es divisible por ningún $LT(g_i)$.*

Demostración. Por el algoritmo de la división $f = a_1g_1 + \cdots + a_tg_t + r$, donde r cumple claramente las condiciones 1 y 2, tomando $g = \sum_{i=1}^{t} a_ig_i$.

Supongamos que existe r' y g' tales que $f = g+r = g'+r'$. Entonces $r-r' = g'-g \in I$, por lo tanto, se tiene que $LT(r-r') \in LT(I)$, como G es base de Gröbner para I, $LT(r-r')$ es divisible por algún $LT(g_i)$, lo cual es imposible dado que r, r' no son divisibles por ningún $LT(g_i)$. Por lo tanto, $r - r' = 0$ y se tiene la unicidad. ■

Corolario 1.1.12 *Sea G una base de Gröbner para un ideal I y sea $f \in R$, entonces $f \in I$ si y sólo si el residuo de la división de f por G es cero.*

Demostración. Sea $f \in R$, entonces, existe un único $r \in R$ tal que $f = g + r$ con $g \in I$ y ningún término de r es divisible por ningún $LT(g)$ para todo $g \in G$, es decir, como $f \in I$ entonces, si $r \in I$ implica que $f \in I$ si y sólamente si $r = 0$. ■

A continuación presentaremos un primer teorema con el cual podemos determinar si un conjunto $G \subset I$ es base de Gröbner para el ideal I.

Teorema 1.1.13 *Sea $I \subset K[x_1, \ldots, x_n]$ ideal no cero, sea $G = \{g_1, \ldots, g_s\}$ un conjunto de polinomios no cero, entonces las siguientes condiciones son equivalentes:*

1. *G es base de Gröbner para I.*
2. *$f \in I$ si y sólo si la la división de f por G es cero.*
3. *$f \in I$ si y sólo si $f = \sum h_ig_i$ con $LM(f) = \text{máx}_{1\leq i\leq s}(LM(h_i), LM(g_i))$.*
4. *$\langle LT(G)\rangle = \langle LT(I)\rangle$.*

Demostración.

1) $\Rightarrow$ 2) Es inmediato del corolario anterior.

2) $\Rightarrow$ 3) Es inmediato del algoritmo de la división.

3) $\Rightarrow$ 4) Por definición $LT(G) \subseteq LT(I)$. Sea $f \in I$, por hipótesis podemos escribir $LT(f) = \sum_{i=1}^{s} LT(h_i)LT(g_i)$ tal que $multideg(f) = multideg(g_i)multideg(f_i)$, por lo tanto, $LT(f) \in LT(G)$.

4) $\Rightarrow$ 1) Por definición de base de Gröbner. ■

Definición 1.1.14 *Sea $f, g \in R$ polinomios no cero, sea $multideg(f) = \alpha$ y $multideg(g) = \beta$, sea $\gamma_i := \text{máx}(\alpha_i, \beta_i)$, definimos el **minímo común multiplo** de $LM(f)$ y $LM(g)$ como $x^\gamma = LCM(LM(f), LM(g))$. El **S-polinomio** de f y g es la combinación:*

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

El siguiente resultado es el más usado para determinar cuando un conjunto G es base de Gröbner para algún ideal I, el cual se apoya fuertemente en la definición de $S-polinomio$.

Proposición 1.1.15 *(Criterio de Buchberger) Sea $I \subset R$ un ideal, sea $G = \{g_1, \ldots, g_t\}$ una base de de I, entonces G es una base de Gröbner de I si y sólo si la división de $S(g_i, g_j)$ por G es cero para todo $i \neq j$.*

Demostración. [7] [pag. 85] ■

Definición 1.1.16 *Sea $I = \langle f_1, \ldots, f_s \rangle \subseteq R$, se define el ℓ-**esimo ideal de eliminación** I_ℓ como:*

$$I_\ell = I \cap K[x_{\ell+1}, \ldots, x_n].$$

Notemos entonces que los elementos de I_ℓ polinomios en I en las variables $x_{\ell+1}, \ldots, x_n$, es decir, son polinomios en los cuales hemos eliminado las variables $x_1, \ldots, x_\ell$.

Teorema 1.1.17 *(Teorema de eliminación) Sea $I \subset R$ ideal y sea G base de Gröbner de I con respecto al orden lexicográfico. Entonces para todo $0 \leq \ell \leq n$, el conjunto $G_\ell = G \cap K[x_{\ell+1}, \ldots, x_n]$ es base de Gröbner para el ideal I_ℓ.*

Demostración. Sea $0 \leq \ell \leq n$. Por construcción claramente $G_\ell \subset I_\ell$, por lo tanto, $\langle LT(G_\ell) \rangle \subset \langle LT(I_\ell) \rangle$.

Para demostrar la contención recíproca es suficiente con mostrar que para cada $f \in I_\ell$ existe $g \in G_\ell$, tal que $LT(g) | LT(f)$.

Sea $f \in I_\ell \subset I$, luego como G es base de Gröbner para I, existe $g \in G$ tal que $LT(g) | LT(f)$. Como $x_n \prec \cdots \prec x_1$, entonces, cualquier monomio que contenga a las variables $x_1., \ldots, x_\ell$ es más grande que todos los monomios en $K[x_{\ell+1}, \ldots, x_n]$, es decir $LT(g) \in K[x_{\ell+1}, \ldots, x_n]$, implica que $g \in K[x_{\ell+1}, \ldots, x_n]$. Lo anterior demuestra que $g \in G_\ell$, por lo tanto, el teorema está demostrado. ■

A continuación se muestra el teorema de extensión el cual junto con el teorema de eliminación nos permite dar solución a sistemas de polinomios. Para ello comenzaremos dando unas definiciones.

Definición 1.1.18 *Sea $f \in K[x_1, x_2, \ldots, x_n]$, para cada $1 \leq j \leq n$, se define la x_j **representación de** f como:*

$$f = c_{fj}(x_1, x_2, \ldots, \hat{x}_j, \ldots, x_n) x_j^{N_j} + \sum_k g_{kj}.$$

Donde $N_j \geq 0$ y cada $c_{f,j} \in K[x_1, \ldots, \hat{x}_j, \ldots, x_n] \setminus \{0\}$ y cada g_{kj} es un polinomio tal que, el grado de x_j es menor a N_j.

Definición 1.1.19 *Sea $f \in K[x_1, x_2, \ldots, x_n]$ y considere la x_j representacón de f, se define el* ***grado de*** x_j ***en*** f *como:*

$$\deg(f, x_j) = N_j$$

Teorema 1.1.20 *(Teorema de extensión) Sea K un campo algebraicamente cerrado, $I = \langle f_1, \ldots, f_s\rangle \subset K[x_1 \ldots, x_n]$ y sea I_1 el primer ideal de eliminación. Entonces para cada $1 \leq i \leq s$, escribimos la x_1 representación de f_i, asumiento $c_i = c_{f_i}$:*

$$f_i = c_i(x_2, \ldots, x_n)x_i^{N_i} + \sum_k g_k.$$

Suponga que se tiene una solución parcial $a = (a_2, \ldots, a_n) \in V(I_1)$. Si $a \notin V(c_1, \ldots, c_n)$, entonces, existe $a_1 \in K$ tal que $(a_1, a_2, \ldots, a_n) \in V(I)$.

La demostración del teorema anterior se hará por partes, primero probaremos una versión para ideales con una base de Gröbner, y posteriormente adaptaremos la demostración al caso general.

Lema 1.1.21 *Sea $f = \sum A_j g_j$ representación estandar de orden léxicográfico, entonces :*

- $\deg(f, x_1) \geq \deg(A_j g_j, x_1) \quad \forall j.$
- $c_f = \sum_{\deg(A_j g_j, x_1) = N} c_{A_j} c_{g_j}.$

Demostración. El punto 1 es inmediato de la definición pues N es el grado máximo de x_1.

Supongamos que $\{j_1, j_2, \ldots, j_r\}$ son todos los índices tales que $\deg(A_j g_j, x_1) = 1$, por lo tanto, podemos escribir a f como:

$$f = \sum_{k=1}^{r} A_{j_k} g_{j_k} + \sum_k g_k = \sum_{k=1}^{r} c_{A_{j_k}} c_{g_{j_k}} x_1^N + \sum_k g_k = (\sum_{k=1}^{r} c_{A_{j_k}} c_{g_{j_k}})x_1^N + \sum_k g_k.$$

Con lo cual queda demostrado. ■

Teorema 1.1.22 *Sea $G = \{g_1, g_2, \ldots, g_t\}$ una base de Gröbner de $I \subseteq K[x_1, x_2, \ldots, x_n]$, sea I_1 el primer ideal de elimininación. Para cada $1 \leq j \leq t$, sea $c_j = c_{g_j}$ y consideremos la x_1 representación de g_j. Y sea $a = (a_2, a_3, \ldots, a_n) \in V(I_1)$ tal que $a \notin V(c_1, \ldots, c_n)$, entonces:*

1. $\{f(x_1, a) | f \in I\} = \langle g_0(x_1, a)\rangle \subset K[x_1]$.
   Donde $g_0 \in G$ es tal que $\deg(g_0, x_1) = \min\{\deg(g_j, x_1) | g_j \in G \quad y \quad c_j(a) \neq 0\}$.

2. $\deg(g_0(x_1, a)) > 0$.

3. Si $g_0(x_1, a) = 0$ *entonces* $(a_1, a) \in V(I)$.

Demostración. La parte fundamental de esta demostración será probar la primera parte ya que los puntos 2 y 3 resultan inmediatos una vez probado 1.

Sea $a = (a_2, a_3, \ldots, a_n) \in V(I_1)$ tal que $a \notin V(c_1, \ldots, c_n)$. Consideremos el homomorfismo $\rho : K[x_1, x_2, \ldots, x_n] \to K[x_1]$, definido mediante:

$$\rho(f(x_1, \ldots, x_n)) = f(x_1, a).$$

Por ser un homomorfismo se tiene que $\rho(K[x_1, x_2, \ldots, x_n]) = \langle g_j(x_1, a)\rangle$.
Sea $d_0 = \deg(g_0, x_1)$. Veamos que $g_j(x_1, a) = 0$ si $\deg(g_j, x_1) < d_0$. Supongamos lo contrario, es decir, supongamos que existe $g_{j_0} \in G$ con $\deg(g_{j_0}, x_1) < d_0$ tal que $g_{j_0}(x_1, a) \neq 0$ y consideremos el siguiente conjunto:

$$A = \{\delta_j = \deg(g_j, x_1) - \deg(g_j(x_1, a)) | g_j(x_1, a) \neq 0\} \subset \mathbb{N}.$$

De la existencia de g_{j_0} es claro que $A \neq \emptyset$, por el principio del buen orden existe un primer elemento, sea g_b el polinomio tal que $\delta = \delta_b$ es el primer elemento de A, sea $d_b = \deg(g_b, x_1)$ por lo tanto, $\deg(g(x_1, a)) = d_b - \delta$, entonces consideremos:

$$\begin{aligned} S &= c_0 x_1^{d_0 - d_b} g_b - c_b g_0 \in I \\ &= c_0 x_1^{d_0 - d_b}(c_b x_1^{d_b} + \ldots) - c_b(c_0 x_1^{d_0} + \ldots). \end{aligned}$$

De la ecuación anterior es claro que $\deg(S, x_1) < d_0$. Al hacer le evaluación en a de S, como $c_b(a) = 0$ y $C_0(a) \neq 0$ se tiene que:

$$S(x_1, a) = c_0(a) x_1^{d_0 - d_b} g_b(x_1, a) - c_b(a) g_0(x_1, a) = c_0(a) x_1^{d_0 - d_b} g_b(x_1, a).$$

Por lo tanto, para obtner el grado de $S(x_1, a)$ es la suma de lo grados:

$$\deg(S(x_1, a)) = d_0 - d_b + \deg(g_b(x_1, a)) = d_0 - d_b + (d_b - \delta) = d_0 - \delta.$$

Por otro lado, si escribimos a S mediante la representación $S = \sum_{j=1}^{t} B_j g_j$. Por lo tanto, del lema anterior de obtiene:

$$\deg(B_j, x_1) + \deg(g_j, x_1) = \deg(B_j g_j, x_1) \leq \deg(S, x_1) < d_0.$$

Por otro lado, escribamos a S como suma de productos de elementos de G, es decir, $S = \sum_{j=1}^{t} B_j g_j$, por lo tanto, del lema anterior obtenemos lo siguiente:

$$\deg(B_j, x_1) + \deg(g_j, x_1) = \deg(B_j g_j, x_1) \leq \deg(S, x_1) < d_0$$

por lo tanto los $g_j s'$ que aparecen en la suma cumplen con que $\deg(g_j, x_1) < 0$, esto implica que $g_j(x_1, a) = 0$ o el grado de x_1 decrece en al menos δ, por lo tanto, se tiene lo siguiente:

$$\deg(B_j(x_1, a)) + deg(g_j(x_1, a)) \leq \deg(B_j, x_1) + \deg(g_j, x_1) - \delta < d_0 - \delta,$$

así finalmente:

$$\deg(S(x_1, a)) \leq \text{máx}\{\deg(B_j(x_1, a)) + \deg(g_j(x_1, a))\} < d_0 - \delta,$$

lo cual es una contradicción, lo cual demuestra que $g_j(x_1, a) = 0$ si $\deg(g_j, x_1) < d_0$

Nuestro objetivo ahora será probar que $g_j(x_1, a) \in \langle g_0(x_1, a)\rangle$ por medio de inducción sobre $\deg(g_j, x_1)$. Sea $g_j \in G$ tal que $\deg(g_j, x_1) < d_0$, por lo tanto, $g_j(x_1, a) = 0 \in \langle g_0(x_1, a)\rangle$. Fijemos $d \geq d_0$ y supongamos que la propiedad se cumple para todos los $g_j \in G$ tal que $deg(g_j, x_1) < d$. Y tomemos $g_j \in G$ con $\deg(g_j, x_1) = d$ y consideremos el polinomio siguiente:

$$\begin{aligned} S &= c_0 g_j - c_j x_1^{d-d_0} g_0 \in I \\ &= c_0(c_j x_1^d + \dots) - c_j x_1^{d-d_0}(c_0 x_1^d + \dots). \end{aligned}$$

Consideremos $S = \sum_{l=1}^{t} B_l g_l$, por lo argumentado anteriormente se tiene que $\deg(g_l, x_1) < d$, es decir cada $\deg(g_l, x_1) < d$ por lo tanto, por nuestra hipótesis de inducción se sigue que $g_l(x_1, a) \in \langle g_0(x_1, a)\rangle$ y $S(x_1, a) \in \langle g_0(x_1, a)\rangle$, por lo tanto, podemos concluir que $c_0(a)g_j(x_1, a) \in \langle g_0(x_1, a)\rangle$, como $c_0(a) \neq 0$, se sigue que $g_j(x_1, a) \in \langle g_0(x_1, a)\rangle$ tal como se queria demostrar, con lo cual se concluye la demostración del punto 1.

Para demostrar 2, supongamos lo contrario, es decir, supongamos que $\deg(g_0(x_1, a)) = 0$, como $c_0(a) \neq 0$ se sigue que $\deg(g_0, x_1) = 0$, por lo tanto, $g_0 \in I_1$ y $c_0 = g_0$, pero como $a \in V(I_1)$ implica que $c_0(a) = g_0(a) = 0$ lo cual contradice la elección de g_0, por lo tanto, $\deg(g_0(x_1, a)) > 0$. Por otro lado, si $a_1 \in K$ es tal que $g_0(a_1, a) = 0$ del punto 1, se sigue que $f(a_1, a) = 0$ para todo $f \in I$, es decir, $(a_1, a) \in V(I)$. ■

Ahora ya estamos en posición de poder demostrar el teorema de extensión.

Demostración. (Teorema de extensión)

Sea $G = \{g_1, \dots, g_t\}$ base de Gröbner de I y sea $a = (a_2, \dots, a_n)$ solución parcial. De la hipótesis se tiene que $c_i(a) \neq 0$ para algún i. Tomemos $f_i = \sum_{j=1}^{t} A_j g_j$. Luego del lema 1.1.21 se tiene que:

$$c_i = \sum_{\deg(A_j g_j, x_1) = N_i} c_{A_j} c_{g_j},$$

Por lo tanto al menos un $j \in \{1, \dots, t\}$ tal que $c_{g_j}(a) \neq 0$. Aplicando el teorema anterior, existe $g_0 \in$ con $\deg(g_0(x_1, a)) > 0$. Luego como K es algebraicamente cerrado existe $a_1 \in K$ tal que $g_0(a_1, a) = 0$, por lo tanto, $(a_1, a) \in V(I)$ y el teorema de extensión queda entonces demostrado. ■

.

1.2. Variedades afines

Sea K un campo se define el $n-$ésimo espacio afín sobre K como el conjunto de las $n-$tuplas de elementos de K, denotado por $\mathbb{A}^n$. Un elemento $p \in \mathbb{A}^n$ se llamará *punto*, y si $p = (a_1, \ldots, a_n)$ los elementos $a_i \in K$ se llamarán *coordenadas* de p. En algunos resultados necesitaremos la hipótesis adicional de que el campo K sea algebraicamente cerrado

Sea $A = K[x_1, x_2, \ldots, x_n]$ el anillo de polinomios en n variables sobre K. Notemos que podemos considerar a los elementos $f \in A$, como funciones $f : K^n \to K$ media nte la asignación $f(p) = f(a_1, \ldots, a_n)$. Sea f un polinomio, entonces podemos definir el ***conjunto de ceros de*** f ***sobre*** $\mathbb{A}^n$, el cual denotaremos por: $Z(f) = \{p \in \mathbb{A}^n | f(p) = 0\}$. Más generalmente si $T \subset A$, definimos el *conjunto de ceros de* T como:

$$Z(T) = \{p \in \mathbb{A}^n | f(p) = 0 \quad \forall f \in T\}.$$

Notemos que si $I = \langle T \rangle$, entonces $Z(I) = Z(T)$. Por otro lado, como A es anillo Noetheriano, todo ideal I de A es finitamente generado, es decir existe una colección finita de polinomios $f_1, \ldots, f_r \in I$ tal que $I = \langle f_1, \ldots, f_r \rangle$. Entonces $Z(T)$ puede ser expresado como el conjunto de lo ceros en común de una colección finita de polinomios.

Definición 1.2.1 *Sea $Y \subset \mathbb{A}^n$, diremos que es un* **conjunto algebraico***, si existe $T \subset A$, tal que $Y = Z(T)$.*

Proposición 1.2.2 *La unión finita de conjuntos algebraicos es un conjunto algebraico. La intersección arbitraria de conjuntos algebraicos vuelve a ser algebraica. El conjunto vacio y $\mathbb{A}^n$ son algebraicos.*

Demostración. Basta demostrarlo para un par de conjuntos, sean Y_1, Y_2 conjuntos algebraicos, entonces, existen $T_1, T_2 \in A$ tales que $Y_i = Z(T_i)$ para $i = 1, 2$.
Afirmación: $Y_1 \cup Y_2 = Z(T_1 T_2)$ donde $T_1 T_2 = \{fg | f \in T_1 \quad y \quad g \in T_2\}$.
En efecto: Sea $p \in Y_1 \cup Y_2$, entonces $p \in T_1$ o $p \in T_2$, por lo tanto, p es cero de cualquier polinomio en $T_1 T_2$. Por otro lado, si $p \in Z(T_1 T_2)$ supongamos que $p \notin Y_1$, es decir existe $f \in T_1$ tal que $f(p) \neq 0$. Sea $g \in T_2$ elemento arbitrario, consideremos el producto $fg \in T_1 T_2$, por lo tanto $f(p)g(p) = 0$, como $f(p) \neq 0$, se tiene que $g(p) = 0$, como g fue arbitrario $p \in T_2$. Sea $Y_\alpha = Z(T_\alpha)$ una familia de conjuntos algebraicos, entonces:

$$\begin{aligned} p \in \bigcap_\alpha Y_\alpha &\Leftrightarrow p \in Y_\alpha \quad \forall \alpha \\ &\Leftrightarrow \text{Para cada } \alpha \text{ p es cero para todo } f \in T_\alpha \\ &\Leftrightarrow p \text{ es cero para todo } f \in \bigcup_\alpha T_\alpha \\ &\Leftrightarrow p \in Z(\bigcup_\alpha T_\alpha). \end{aligned}$$

Finalmente $\emptyset = Z(a)$ para algún $a \in K \setminus \{0\}$ y $\mathbb{A}^n = Z(0)$. ■

Definición 1.2.3 *Sea $\tau = \{Y \subset \mathbb{A}^n | Y^c$ es conjunto algebraico$\}$ por la proposición anterior τ define una topología en $\mathbb{A}^n$, la cual llamaremos la* ***Topología de Zariski de*** $\mathbb{A}^n$.

Ejemplo 1.2.4 *Consideremos la topología de Zariski en la recta afin $\mathbb{A}^1$. Como $K[x]$ es un Domino de Ideales Principales (DIP), por lo tanto, para todo $I \subset A = K[x]$ es principal, es decir dado Y conjunto algebraico, existe $T \subset \mathbb{A}$ tal que $Z(< T >) = Y$, ahora como A es (DIP), existe un polinomio $f \in < T >$ tal que $< T >=< f >$, es decir, $Y = Z(f)$. Luego todo polinomio puede escribirse de la forma: $f(x) = c(x-a_1)\cdots(x-a_n)$ con $c, a_1, \ldots, a_n \in K$, por lo tanto, $Y = Z(f) = \{a_1, \ldots, a_n\}$. Es decir los conjuntos algebraicos de $\mathbb{A}^1$ están formado por conjuntos finitos, el conjunto vacío y el total. Por lo cual esta topología coincide con la de complementos finitos. Sean $x, y \in \mathbb{A}^1$ y supongamos que existen dos conjuntos abiertos $U, V \subset \mathbb{A}^1$ disjuntos tal que $x \in U, y \in V$, luego al tomar complementos $U^c \cup V^c = \mathbb{A}^1$, lo nos indica que $\mathbb{A}^1$ es finito, por lo tanto, en este caso, nuestra topología no es Hausdorff.*

Definición 1.2.5 *Sea X un espacio topológico, entonces un subconjunto $Y \subset X$ se llama* **irreducible**, *si no puede ser expresado como la unión de dos subconjuntos propios cada uno cerrado en Y. El vacío no es considerado como irreducible.*

Ejemplo 1.2.6 $\mathbb{A}^1$ *es un conjunto irreducible, ya que sus únicos cerrados distintos del total son todos conjuntos finitos, dado K es un campo algebraicamente cerrado, entonces $\mathbb{A}^1$ no puede ser expresado como unión de conjuntos finito.*

Proposición 1.2.7 *Todo subconjunto abierto no vacío de un espacio irreducible es denso e irreducible.*

Demostración. Sea X espacio irreducible, sea $U \subset X$ subconjunto propio abierto distinto del vacío.

1. U es irreducible:
   Supongamos que U no es irreducible, es decir existen F y G cerrados de X,tales que $U = (U \cap F) \cup (U \cap G)$, luego como X es irreducible $F \cup G \neq X$, por otro lado, U^c es un cerrado propio de X, es fácil ver que $X = (F \cup G) \cup U^c$, lo cual es una contradicción. Por lo tanto, U es irreducible.

2. U es denso:
   Sea V abierto de X distinto del vacío, si $V = X$ tenemos: $V \cap U \neq \emptyset$. Por otro lado, si $X \neq V$, como X es irreducible $U^c \cup V^c \neq X \Rightarrow (U^c \cup V^c)^c \neq \emptyset$, es decir U tiene interseccción no vacía con cualquier abierto de X, por lo tanto, U es denso en X.

■

Proposición 1.2.8 *Si Y es un subconjunto irreducible de X, entonces $\overline{Y}$ también es irreducible.*

Demostración. Sea $Y \subset X$ irreducible, y supongamos que $\overline{Y}$ no es irreducible, luego existen F y G cerrados de X, tales que si $U = F \cap \overline{Y}$ y $V = G \cap \overline{Y}$, entonces $Y \subset \overline{Y} = U \cup V$. Entonces notemos que podemos escribir a Y como: $Y = (U \cap Y) \cup (V \cap Y)$, los cuales son cerrados propios. Ahora falta ver que ambos cerrados son distintos del vacío. Supongamos que $U \cap Y = \emptyset$, por lo tanto, $Y \subset V$, como V es cerrado se tiene $\overline{Y} \subset V \subset G$, lo cual es una contradicción a la elección de G, así $U \cap Y \neq \emptyset$, análogamente se demuestra que $V \cap Y \neq \emptyset$. Lo cual implica una contradicción a la irreducibilidad de Y, por tanto $\overline{Y}$ es también irreducible. ■

Definición 1.2.9 *Una **variedad algebraica afín** o simplemente **variedad afín** es un subconjunto cerrado e irreducible de $\mathbb{A}^n$ con la topología inducida. Un subconjunto abierto de una variedad afín es una **variedad quasi-afín**.*

Ahora podemos obtener un mayor control de las relaciones entre subconjuntos de $\mathbb{A}^n$ e ideales de A. Para cualquier subconjunto $Y \subseteq \mathbb{A}^n$ definimos el *ideal anulador de Y en A* por:

$$I(Y) = \{f \in A | f(p) = 0 \quad \forall p \in Y\}.$$

Ahora tenemos una función Z, la cual mapea subconjuntos de A en conjuntos algebraicos y una función I la cual mapea subconjuntos de $\mathbb{A}^n$ en ideales. Sus propiedades quedarán expuestas en la siguiente proposición.

Teorema 1.2.10 *(Teorema de los Ceros de Hilbert) Sea K un campo algebraicamente cerrado, sean I un ideal de $A = K[x_1, x_2, \ldots, x_n]$ y $f \in A$ un polinomio que se anula en todos los puntos de $Z(I)$. Entonces $f^r \in I$ para algún $r \in \mathbb{N}$.*

Demostración. [3] pag 134. ■

Proposición 1.2.11

1. *Si $T_1 \subseteq T_2$ son subconjuntos de A, entonces $Z(T_2) \supseteq Z(T_1)$.*
2. *Si $Y_1 \subseteq Y_2$ son subconjuntos de $\mathbb{A}^n$, entonces $I(Y_1) \supseteq I(Y_2)$.*
3. *Sean $Y_1, Y_2 \subset \mathbb{A}^n$, entonces se cumple que $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$.*
4. *Sea $I \subseteq A$ un ideal y suponiendo K algebraicamente cerrado, entonces $I(Z(I)) = \sqrt{I}$.*

5. Sea $Y \subseteq \mathbb{A}^n$, entonces $Z(I(Y)) = \overline{Y}$.

Demostración. La demostración de los puntos 1, 2 y 3 son claros de las definiciones, el punto 4 es consecuencia inmediata del teorema de los Ceros de Hilbert.
Para demostrar el punto 5, notemos que $Y \subseteq Z(I(Y))$, el cual es un conjunto cerrado, por lo tanto, $\overline{Y} \subseteq Z(I(Y))$. Por otra parte sea W conjunto cerrado que contiene a Y, entonces $W = Z(a)$, para algún a ideal, luego por el inciso 2, se tiene que: $I(Z(a)) \subseteq I(Y)$, pero $a \subseteq I(Z(a))$ y usando el punto 1, obtenemos que $Z(I(Y)) \subseteq Z(I(Z(a))) \subseteq Z(a) = W$. ■

Corolario 1.2.12 *Supongamos que K es algebraicamente cerrado, entonces existe una correspondencia entre los conjuntos algebraicos de $\mathbb{A}^n$ e ideales radicales de A (Aquellos ideales tales que $a = \sqrt{a}$), dado por $Y \to I(Y)$ y $a \to Z(a)$. Además un conjunto algebraico en $\mathbb{A}^n$ es irreducible $\Leftrightarrow$ su ideal asociado en A es primo.*

Demostración. La existencia de la correspondecia entre los conjuntos esta dada, por las proposiciones anteriores, luego basta demostrar la última parte.

$\Rightarrow$) Sea Y subconjunto irreducible de $\mathbb{A}^n$, por demostrar que $I(Y)$ es primo. Sean $f, g \in I(Y)$, entonces $Y \subseteq Z(fg) = Z(f) \cup Z(g)$, podemos escribir a Y como unión de dos subconjuntos cerrados como: $Y = (Z(f) \cap Y) \cup (Z(g) \cap Y)$, por ser Y irreducible, se tiene que: $Y = Z(f) \cap Y$ o $Y = Z(g) \cap Y \Rightarrow Y \subset Z(f)$ o $Y \subset Z(g) \Rightarrow f \in I(Z(f)) \subset I(Y)$ o $g \in I(Z(g)) \subset I(Y)$. Por lo que efectivamente $I(Y)$ es ideal primo.

$\Leftarrow$ Sea p ideal primo, sean Y_1, Y_2 cerrados tales que $Z(p) = Y_1 \cup Y_2$, al tomar ideales $p = I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$ como p es ideal primo se tiene que $p = I(Y_1)$ o $p = I(Y_2)$ $\Rightarrow Z(p) = Y_1$ o $Z(p) = Y_2$, con lo cual $Z(p)$ es irreducible. ■

Ejemplo 1.2.13 *$\mathbb{A}^n$ es irreducible, ya que $\mathbb{A}^n = Z(0)$, el cual es primo en A.*

Ejemplo 1.2.14 *Sea f polinomio irreducible en $A = K[x, y]$, entonces el ideal generado por f es ideal primo en A, luego como A es dominio de factorización única el conjunto de ceros $Y = Z(f)$ es irreducible. Al conjunto de ceros Y lo llamaremos la **curva afín** definida por $f(x, y) = 0$. Si f tiene grado d diremos que Y es una curva de grado d.*

Ejemplo 1.2.15 *Generalizando el ejemplo anterior, si $f \in A = K[x_1, \ldots, x_n]$ es irreducible, obtenemos la variedad afín $Y = Z(f)$, la cual es llamada **superficie** si $n = 3$, o **hipersuperficie** si $n > 3$.*

Ejemplo 1.2.16 *Supongamos que K es algebraicamente cerrado y sea $\boldsymbol{m}$ ideal maximal de $A = K[x_1, \ldots, x_n]$, entonces $\boldsymbol{m}$ está en correspondencia con un conjunto cerrado e irreducible minimal de $\mathbb{A}^n$, veamos que este debe estar formado por un solo punto. Sean $p_1, p_2 \in Z(\boldsymbol{m}) \Rightarrow \boldsymbol{m} \subset I(p_1) \cap I(p_2) \Rightarrow \boldsymbol{m} \subset I(p_1)$ y $\boldsymbol{m} \subset I(p_2) \Rightarrow \boldsymbol{m} = I(p_1) = I(p_2) \Rightarrow p_1 = p_2$. Por lo tanto, $Z(\boldsymbol{m})$ está formado por un solo punto, digamos $p = (a_1, \ldots, a_n)$. Lo anterior demuestra que todo ideal maximal de A es de la forma $\boldsymbol{m} = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$, para algunos $a_1, \ldots, a_n \in K$.*

Definición 1.2.17 *Sea $Y \subseteq \mathbb{A}^n$ un conjunto algebraico afín, definimos el* ***anillo de coordenadas afín*** *$A(Y)$ de Y como el cociente $A(Y) = A/I(Y)$.*

Notemos que si Y es una variedad afín, entonces $I(Y)$ es ideal primo de A, por lo tanto, $A(Y)$ es dominio. Además $A(Y)$ es una K-álgebra finitamente generada. Recíprocamente, toda K-álgebra finitamente generada B, es el anillo de coordenadas afín de alguna variedad J. Más aún B se puede escribir como el cociente de algún anillo de polinomios $A = K[x_1, \ldots, x_n]$ y algún ideal primo a, entonces $J = Z(a)$.

Definición 1.2.18 *Un espacio topológico X es llamado* ***Noetheriano****, si satisface la condición de cadena descendente para subconjuntos cerrados, es decir, para toda sucesión de conjuntos $Y_1 \supseteq Y_2 \supseteq \ldots$, existe $r \in \mathbb{N}$, tal que $Y_r = Y_{r+1} = Y_{r+2} = \ldots$*

En forma de ejemplo y para aterrizar ideas sobre esto. Veamos que $\mathbb{A}^n$ es un espacio topológico noetheriano. Sea $Y_1 \supseteq Y_2 \supseteq \ldots$ cadena descendiente de conjunto cerrados, entonces al tomar los ideales anuladores, tenemos formada la cadena ascendente de ideales $I(Y_1) \subseteq I(Y_2) \subseteq \ldots$ en A. Como A es un anillo Noetheriano, existe $r \in \mathbb{N}$ tal que, $I(Y_r) = I(Y_{r+i})$ para todo i. Finalmente, $Y_r = Z(I(Y_r)) = Z(I(Y_{r+ii})) = Y_{r+i}$ para todo i.

Proposición 1.2.19 *Sea X un espacio topológico Noetheriano, entonces todo cerrado Y no vacío puede ser expresado como una unión finita $Y = Y_1 \cup \cdots \cup Y_r$ de subconjuntos cerrados irreducibles. Si además imponemos la condición que $Y_j \nsubseteq Y_i$ siempre que $i \neq j$, entonces la representación es única. A cada Y_i le llamaremos* ***compontente irreducible*** *de Y.*

Demostración. Sea Γ el conjunto de los subconjuntos cerrados de X, que no pueden ser escritos como unión finita de conjuntos cerrados irreducibles. Si $\Gamma \neq \emptyset$, como X es Noetheriano, existe elemento minimal en Γ, digamos Y. Por construcción de Γ, Y no puede ser irreducible, entonces podemos escribir Y como unión de subconjuntos cerrados propios $Y = Y \cup\ Y''$. Luego por la minimalidad de Y, Y' y Y'' pueden ser escritos como unión finita de conjuntos cerrados irreducibles, por lo que también Y se puede escribir como una unión finita, lo cual es una contradicción. Por lo tanto, $\Gamma = \emptyset$, es decir, todo subconjunto cerrado no vacío puede descomponerse en sus factores irreducibles.

Ahora vemos que si se pide que $Y_j \nsubseteq Y_i$ si $i \neq j$, entonces la representación es única. Supongamos que existen dos representaciones para Y, $Y_1' \cup \cdots \cup Y_s' = Y = Y_1 \cup \cdots \cup Y_r$, fijándonos en Y_1', se que $Y_1' = \bigcup(Y_1' \cap Y_i)$, pero como es irreducible, entonces se tiene que $Y_1' = Y_1' \cap Y_i \subseteq Y_i$ para algún i, sin pérdida de generalidad supongamos $i = 1$, entonces $Y_1' \subseteq Y_1$, similarmente $Y_1 \subset Y_j'$, por transitividad de la contención, se tiene que $Y_1' \subseteq Y_j'$, por hipótesis $Y_1' = Y_j'$, por lo tanto, $Y_1 = Y_1'$. Definiendo $Z := (Y \setminus Y_1) = (Y \setminus Y_1')$, con lo que se obtiene la siguiente igualdad $Z = Y_2' \cup \cdots \cup Y_s' = Y = Y_2 \cup \cdots \cup Y_r$, procediendo por inducción se obtiene la unicidad de los Y_i. ■

Corolario 1.2.20 *Todo conjunto algebraico en $\mathbb{A}^n$ puede ser expresado de manera única como unión de variedades, de tal forma que ninguna variedad contenga a otra.*

Definición 1.2.21 *Sea X espacio topológico, definimos la **dimensión de** X (denotado por $\dim X$) como el supremo de todos los enteros n tales que exista una cadena $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ de subconjuntos cerrados irreducibles distintos de X. Definimos la dimensión de una variedad afín o quasi-afín mediante la definición anterior tomando a la variedad como el espacio topológico.*

Ejemplo 1.2.22 *La dimensión de $\mathbb{A}^1$ es 1, ya que los únicos conjuntos cerrados irreducibles no triviales son los conjuntos unipuntuales.*

Definición 1.2.23 *Sea A un anillo la **altura** de un ideal primo p, es el supremo sobre todas las n tales que existe una cadena $p_0 \subset p_1 \subset \cdots \subset p_n = p$ de ideales primos distintos. Definimos la **dimensión o dimensión de Krull** de A, como el supremo de las alturas sobre todos los ideales primos.*

Proposición 1.2.24 *Si Y es un conjunto algebraico afín, entonces la dimensión de Y es igual a la dimensión de su anillo de coordenadas afín $A(Y)$.*

Demostración. Sea Y conjunto algebraico afín de $\mathbb{A}^n$, entonces los subconjuntos cerrados irreducibles se corresponden con ideales primos de A contenidos en $I(Y)$, y estos por el teorema de correspondencia, están relacionados directamente con los ideales primos de $A(Y)$. Luego la dimensión de Y es la longitud de la cadena de primos más grande en $A(Y)$, es decir su dimensión. ■

La proposición anterior es sumamente útil, ya que nos permite aplicar los resultados de la teoría de la dimensión para anillos Noetherianos en la geometría algebraica.

Teorema 1.2.25 *Sea K un campo y sea B un dominio finitamente generado como una K-álgebra. Entonces:*

- *La dimensión de B es igual al grado de transcendencia del campo de cocientes $K(B)$ de B sobre K.*
- *Para cualquier ideal primo p en B se tiene:*

$$\text{altura}(p) + \dim B/p = \dim B$$

Demostración. [13] [Cap. 5, 14] ■

Proposición 1.2.26 *La dimensión de $\mathbb{A}^n$ es n.*

Demostración. Sabemos que la dimensión de $\mathbb{A}^n$ es la misma que la de su anillo afín de coordenadas $A = K[x_1, \ldots, x_n]$, por otro lado el anillo A se puede ver como una k-álgebra finitamente generada. Luego por el teorema anterior se tiene que la dimensión es n. ■

Proposición 1.2.27 *Si Y es una variedad quasi-afín, entonces* $\dim Y = \dim \overline{Y}$

Demostración. Dada la sucesión $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ de conjuntos distintos cerrados e irreducibles de Y, entonces al tomar cerradura, obtenemos la sucesión $\overline{Z_0} \subset \overline{Z_1} \subset \cdots \subset \overline{Z_n}$ de conjuntos distintos cerrados e irreducibles de $\overline{Y}$, entonces $\dim Y \leq \dim \overline{Y}$. Lo cual nos dice que $\dim Y$ es finita, entonces podemos elegir una cadena maximal tal que $Z_0 \subset Z_1 \subset \cdots \subset Z_n$, donde $\dim Y = n$. En este caso Z_0 debe consistir de un solo punto $p \in \mathbb{A}^n$, luego es claro que $\overline{Z_0} \subset \overline{Z_1} \subset \cdots \subset \overline{Z_n}$ es también cadena maximal, por otro lado, p tiene correspondencia con un ideal maximal $\boldsymbol{m}$ del anillo afín de coordenadas $A(\overline{Y})$ de $\overline{Y}$. Luego los primos que se corresponden con los $\overline{Z_i}$ están contenidos en $\boldsymbol{m}$, por lo que su altura será n. Pero como p es un solo punto, entonces $A(\overline{Y})/\boldsymbol{m} \cong K$, es decir $n = \dim A(\overline{Y}) = \dim \overline{Y}$ ■

Teorema 1.2.28 *Sea A un anillo Noetheriano y sea $f \in A$ el cual no es divisor de cero ni unidad. Entonces todo ideal primo minimal que contenga a f tiene altura 1.*

Demostración. [3] [p. 122] ■

Proposición 1.2.29 *Sea A anillo Noetheriano y dominio entero, entonces A es dominio de factorización única $\Leftrightarrow$ todo ideal primo de altura 1 es principal.*

Demostración. [13] [p. 141] ■

Proposición 1.2.30 *Una variedad Y en $\mathbb{A}^n$ tiene dimensión $n-1$ si y solo si es el conjunto de ceros $Z(f)$ de un polinomio irreducible no constante en $A = K[x_1, \ldots, x_n]$.*

Demostración. $\Rightarrow$) Sea Y una variedad de $\mathbb{A}^n$ con dimensión $n-1$, sabemos que este se debe corresponder con un ideal p primo de A. Como A es de factorización única, entonces por la proposición anterior, p es necesariamente principal, el cual debe ser generado por un polinomio irreducible f, por lo tanto, $Y = Z(f)$.

$\Leftarrow$) Sea f polinomio irreducible, claramente $Z(f)$ es una variedad. Considerando el ideal primo generado por f, $p = \langle f \rangle$, por la proposición anterior tiene altura 1, por lo tanto, su variedad correspondiente $Z(f)$ debe tener dimensión $n-1$. ■

1.3. Variedades proyectivas

A continuación haremos las construcciones para poder definir las variedades proyectivas. Obviaremos las partes que sean repetitivas.

Sea K un campo, consideremos el $(n+1)-$espacio afín $\mathbb{A}^{n+1}$, definamos la siguiente relación de equivalencia; $(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n) \Leftrightarrow$ existe $\lambda \in K \setminus \{0\}$, tal que $(b_0, b_1, \ldots, b_n) = (\lambda a_0, \lambda a_1, \ldots, \lambda a_n)$. Entonces definimos el n-espacio proyectivo $\mathbb{P}^n$, como el cociente $\mathbb{A}^{n+1} \setminus \{0\}/\sim$. Luego el conjunto de las $(n+1)-$entradas que pertenecen a P es llamado *el conjunto de coordenadas homogéneas de P*.

Un anillo R es graduado si se puede descomponer como la suma directa de grupos abelianos R_d, es decir: $R = \oplus_{d\geq 0} R_d$, tal que para todo $d, e \geq 0$ se tiene que $R_e R_d \subseteq R_{e+d}$. Luego un elemento de R_d es llamado un *elemento homogéneo de grado d*. Más aún todo elemento de R puede ser escrito de una forma única como suma de elementos homogéneos. Un ideal $I \subseteq R$ es ideal homogéneo si $I = \oplus_{d\geq 0}(I \cap R_d)$. Recordemos también algunos resultados sobre ideales homogéneos.

- Un ideal es homogéneo si y solo si es generado por elementos homogéneos.
- Sea I, J ideales homogéneos, entonces $I + J$ es homogéneo.
- Sea I, J ideales homogéneos, entonces $I \cap J$ es homogéneo.
- Sea I, J ideales homogéneos, entonces IJ es homogéneo.
- Sea I ideal homogéneo, entonces $\sqrt{I}$ es homogéneo
- Sea I ideal homogéneo, entonces I es primo si para cualesquiera dos elementos homogéneos f y g tales que $fg \in I \Rightarrow f \in I$ o $g \in I$.

Ahora tomemos a $R = K[x_0, x_1, \ldots, x_n]$, y tomemos la siguiente graduación, cada R_d será el conjunto de combinaciones lineales finitas de monomios en R de grado d. Lo anterior toma importancia, para poder definir una evaluación en los puntos de una variedad proyectiva. Si $f \in R$, entonces es claro que el hecho que f se anule en alguno de los puntos de la clase de equivalencia no implica que se anule en todos ellos. En cambio, si f es un polinomio homogéneo de grado d, entonces claramente $f(\lambda a_0, \lambda a_1, \ldots, \lambda a_n) = \lambda^d f(a_0, a_1, \ldots, a_n)$, lo que significa que si f se anula en un punto, entonces se anulará en toda la clase de equivalencia. Así f dará una función entre el espacio $\mathbb{P}^n$ y el conjunto formado por el cero y el uno mediante la siguiente asignación. $f(P) = 0$ si $f(a_0, a_1, \ldots, a_n) = 0$, y $f(P) = 1$ si $f(a_0, a_1, \ldots, a_n) \neq 0$.

Tomando en consideración lo anterior, estamos en posibilidades de hablar sobre los ceros de un polinomio homogéneo, denotado por $Z(f) = \{P \in \mathbb{P}^n | f(P) = 0\}$. Como en el

caso afín, si T es un conjunto de polinomios homogéneos, definimos los ceros de T como:

$$Z(T) = \{P \in \mathbb{P}^n | f(P) = 0, \quad \forall f \in T\}$$

Si I es un ideal homogéneo de R, al igual que en el caso afín, como R es un anillo noetheriano, entonces existe una colección finita de polinomios $f_1, f_2, \ldots, f_r$, tales que $I = \langle f_1, f_2, \ldots, f_r \rangle$, que por ser I homogéneo cada f_i también lo es, más aún:

$$Z(I) = Z(f_1, f_2, \ldots, f_r).$$

Definición 1.3.1 *$Y \subseteq \mathbb{P}^n$ se llamará conjunto algebraico si existe un conjunto T de elementos homogéneos de R, tal que $Y = Z(T)$.*

Proposición 1.3.2 *La unión de dos conjuntos algebraicos es algebraico. La intersección de cualquier familia de conjuntos algebraicos es algebraico. El conjunto vacío y el espacio total son conjuntos algebraicos.*

Definición 1.3.3 *Se define la Topología de Zariski en $\mathbb{P}^n$ tomando a los abiertos como los complementos de los conjuntos algebraicos.*

Siguiendo con la analogía, ahora daremos las definiciones de irreducibilidad y de dimensión en el caso proyectivo.

Definición 1.3.4 *Una variedad algebraica proyectiva (o simplemente variedad proyectiva) es un conjunto algebraico irreducible en $\mathbb{P}^n$ con la topología inducida. Un conjunto abierto es una variedad quasi-proyectiva. La dimensión de una variedad proyectiva o quasi-proyectiva es su dimensión como espacio topológico.*

Si Y es cualquier subconjunto de $\mathbb{P}^n$, definimos el ideal homogéneo de Y en R, como el ideal generado por $\{f \in R |\ f$ es homogéneo y $f(P) = 0\ \forall P \in Y\}$. Si Y es un conjunto algebraico, definimos el anillo homogéneo de coordenadas de Y por $R(Y) = R/I(Y)$.

Veremos la conexión que tiene el espacio proyectivo $\mathbb{P}^n$ con los espacios afines. Ya que el n-esimo espacio proyectivo tiene una cubierta abierta de n-espacios afines, más aún cada variedad proyectiva tiene cubierta abierta de variedades afines.

Si $f \in R$ es un polinomio lineal homogéneo, entonces el conjunto de ceros de f es llamado un *hiperplano*. En particular denotamos al conjunto de ceros del polinomio x_i por H_i, para $i = 0, \ldots, n$, sea U_i el conjunto abierto $\mathbb{P}^n \setminus H_i$. Entonces $\mathbb{P}^n$ está cubierto por los conjuntos abiertos U_i, ya que si $P = (a_0, a_1 \ldots, a_n)$ es un punto, entonces existe al menos un $a_i \neq 0$, por lo tanto $P \in U_i$. Consideremos el mapeo $\varphi_i : U_i \to \mathbb{A}^n$ como sigue: Si $P = (a_0, a_1, \ldots, a_n) \in U_i$, entonces $\varphi_i(P) = Q$, donde Q es un punto con coordenadas

$$\left(\frac{a_0}{a_i}, \ldots, \frac{a_n}{a_i}\right),$$

omitiendo el término a_i/a_i. Notemos que φ_i está bien definida ya que las coordenadas $\frac{a_j}{a_i}$ son independientes de las coordenadas homogéneas que elijamos.

Proposición 1.3.5 *El mapeo φ_i es un homeomorfismo dotando a U_i con la topología inducida y $\mathbb{A}^n$ con la topología de Zariski.*

Demostración. Claramente φ_i es biyectiva, entonces basta con demostrar que φ_i manda cerrados en U_i en conjuntos cerrados en $\mathbb{A}^n$.

Sea $A = K[y_1, y_2, \ldots, y_n]$, definimos un mapeo α del conjunto de polinomios homogéneos R^h hacia A, y un mapeo β de A hacia R^h, definidos mediante las siguientes reglas de asignación. Sea $f \in R^h$, entonces $\alpha(f) = f(1, y_1, \ldots, y_n)$, por otro lado, si $g \in A$, sea $e = \deg g$, entonces $\beta(g) = x_0^e g(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$ que es un polinomio homogéneo de grado e y que está en R^h.

Sin perdida de generalidad supondremos que $i = 0$ y por facilidad de notación escribiremos U en lugar de U_0 y similarmente φ en lugar de φ_0. Sea $Y \subseteq U$ subconjunto cerrado, y sea $\overline{Y}$ su cerradura en $\mathbb{P}^n$, luego existe $T \subseteq R^h$ tal que $Z(T) = \overline{Y}$, entonces podemos escribir a T de la siguiente manera: $T = I(Y)$. Usando el hecho de que R es un anillo Noetheriano, entonces existe una colección finita de polinomios tales que $I(Y) = \langle f_1, f_2, \ldots, f_r \rangle$, consideremos $T' = \alpha(T) = \alpha(\langle f_1, f_2, \ldots, f_r \rangle)$ y $g_j := \alpha(f_j)$. $P \in \varphi(Y) \Leftrightarrow f_j(1, a_1, \ldots, a_n) = 0 \ \forall j \Leftrightarrow g_j(a_1, \ldots, a_n) = 0 \ \forall j$, por lo tanto, $\varphi(Y) = Z(g_1, \ldots, g_r) = Z(T')$.

Sea $W \subset \mathbb{A}^n$, luego existe $T' \subset A$ tal que $W = Z(T') = Z(f_1, \ldots, f_k)$. Sean $g_j := \beta(f_j)$, veamos que $\varphi^{-1}(W) = Z(g_1, \ldots, g_k) \cap U$. Tomemos $P \in \varphi^{-1}(W)$, entonces existe $w \in W$ tal que $P = \varphi^{-1}(w)) = (1, w_1, \ldots, w_n)$, claramente $P \in U$, por otro lado, $g_j(P) = 1^{\deg f_j} f(x_1, \ldots, x_n) = 0$, por lo tanto $P \in Z(g_1, \ldots, g_k) \cap U$. Por otro lado, sea $P \in Z(g_1, \ldots, g_k) \cap U$, sin perdida de generalidad podemos considerar $P = (1, p_1, \ldots, p_n)$, por la elección de P, para cada j se tiene $0 = g_j(P) = f(p_1, \ldots, p_n)$, es decir si tomamos $P' = (p_1, \ldots, p_n) \Rightarrow P' \in Z(f_1, \ldots, f_k) = W$, por lo tanto, $\varphi^{-1}(P') = P \in \varphi^{-1}(W)$. Con lo cual tenemos que W es cerrado en U. En resumen φ y φ^{-1} son funciones cerradas, con lo que se concluye que φ es homeomorfismo. ■

Corolario 1.3.6 *Si Y es una variedad proyectiva (quasi-proyectiva), entonces Y puede ser cubierto por conjunto abiertos $\{Y \cap U_i\}_{i=0}^n$, los cuales son homeomorfos a variedades afines (quasi-afines), vía el homeomorfismo φ_i definido anteriormente.*

1.4. Gráficas

Definición 1.4.1 *Una **gráfica** $G = (V_G, A_G)$ es una dupla formada por un conjunto finito no vacío V_G, cuyos elementos son llamados **vértices** y un subconjunto A_G de parejas*

no ordenadas de elementos de V_G, los cuales son llamados ***aristas****, y serán denotados como a,$\{x, y\}$,xy.*

Definición 1.4.2 *Sea G una gráfica, si $\{u, w\} \in A_G$, entonces diremos que $u, w \in V_G$* ***están unidos****.*

En este momento tenemos los elementos básicos para poder dar definiciones de tipos de aristas, subgráficas, grado de un vértice, así como sus propiedades fundamentales.

Definición 1.4.3 *Si dos o más aristas están unidas al mismo par de vértices son llamadas* ***aristas múltiples****, si una arista une a un vértice consigo mismo esta es llamada* ***bucle o loop****. Una gráfica sin bucles ni aristas múltiples es llamamada* ***gráfica simple****.*

De aquí en adelante consideraremos únicamente gráficas simples a menos que especifiquemos lo contrario.

Definición 1.4.4 *Sea $G = (V_G, A_G)$ una gráfica con vértices V_G y aristas A_G, a la pareja $H = (V_H, A_H)$ se le llamará* ***subgráfica*** *de G si $V_H \subseteq V_G$ y $A_H \subseteq A_G$.*

Definición 1.4.5 *Sea $G = (V_G, A_G)$ una una gráfica, y sea $u \in V_G$ un vértice de G. El* ***grado*** *de u es la cantidad de aristas que contienen a u, denotado por $\deg u$. Un vértice v con $\deg v = 0$ se llamará aislado.*

De aquí en adelante, por simplicidad dada una gráfica G llamaremos V al conjunto V_G y A al conjunto A_G, así diremos que $G = (V, A)$, a menos que tengamos la necesidad de especificar.

Definición 1.4.6 *Una gráfica se llamará* ***regular*** *si todos los vértices de G tienen el mismo grado. Si dicho grado es $n \in \mathbb{N}$, diremos que G es $n-$**regular**.*

Lema 1.4.7 *Sea G una gráfica, entonces se cumple la siguiente igualdad: $2|A| = \sum_{u \in V} \deg u$.*

Demostración. Sea $a = \{u, v\} \in A_G$, notemos que este vértice se cuenta dos veces en la suma de los grados, uno en u y otro en v, por tanto se concluye el resultado. ■

Observación 1.4.8 *Del lema anterior es claro que la suma de todos los grados es un número par, además, la cantidad de vértices con grado impar siempre es par.*

Definición 1.4.9 *Sean $G = (V, A)$ y $G' = (V', A')$ dos gráficas. Diremos que G y G' son* ***isomorfas*** *lo que detonaremos mediante $G \cong G'$, si existe una biyección $\varphi : V \to V'$ tal que $xy \in A \Leftrightarrow \varphi(x)\varphi(y) \in A'$ para todo $x, y \in V$.*

Definición 1.4.10 *Sean u y w dos vértices de una gráfica. Diremos que estos son* ***adjacentes*** *si existe $a \in A$ tal que a=$\{u,w\}$. Además se dirá que u y w son* ***incidentes*** *con a; y a se dirá incidente con u y w.*

Definición 1.4.11 *Sea G gráfica con n vértices $V = \{v_1, v_2, \ldots, v_n\}$. Se define la* ***matriz de adyacencia*** *como la matriz $M_G = (a_{ij})$, donde a_{ij} es el número de aristas que unen a v_i y v_j. Si v_i tiene un bucle, entonces $a_{ii} := 2$.*

Definición 1.4.12 *Sea G una gráfica con n vértices $v_1, v_2, \ldots, v_n$ y m aristas $a_1, a_2, \ldots, a_m$. Se define la* ***matriz de incidencia*** *como la matriz $I_G = (b_{ij}) \in M_{n\times m}$, donde b_{ij} es el número de ocasiones en que el vértice v_i incide con la arista a_j.*

Definición 1.4.13 *Una gráfica G se llamará* ***gráfica completa*** *si cada vértice esta unido con los $n-1$ vértices restantes. Las gráficas completas con n vértices serán denotadas por K_n.*

Observación 1.4.14 *Notemos que una gráfica completa tiene* $\binom{n}{2} = \dfrac{n(n-1)}{2}$ *aristas.*

Definición 1.4.15 *Sea $G = (V, A)$ una gráfica, diremos que es una* ***gráfica nula*** *si $A = \emptyset$. Si $|V| = n$ entonces denotaremos por N_n a la gráfica nula de n vértices.*

Definición 1.4.16 *Una* ***gráfica bipartita*** *es una gráfica cuyo conjunto de vértices V, admite una partición $\{R, B\}$, tal que para toda arista $a = \{u, v\} \in A$, se cumple que $u \in R$ y $v \in B$.*

Definición 1.4.17 *Una* ***gráfica bipartita completa*** *es una gráfica bipartita en la que cada vértice del conjunto R es unido con cada vértice del conjunto B. Una gráfica bipartita completa que cumple $|R| = r$ y $|S| = s$ se denotará como $K_{r,s}$.*

Notemos que una gráfica bipartita completa $K_{r,s}$ tiene exactamente $r + s$ vértices, y rs aristas. Por otro lado, su matriz de adjayencia $M_G \in M_{r+s}$ y $I_G \in M_{(r+s)\times rs}$.

Ahora nos encaminaremos a dar la definición de árboles, para ello daremos unas definiciones previas.

Definición 1.4.18 *Un* ***camino*** *es una gráfica no vacía $C = (V, A)$ tal que si $V = \{v_0, v_2, \ldots, v_n\}$ entonces $A = \{v_0v_2, v_2v_3, \ldots, v_{n-1}v_n\}$. Note que C une a v_0 y a v_n y estos elementos son llamados* ***vértices extremos*** *de C. La longitud de C está dado por $|A|$, y el camino de longitud n será denotado por C^n.*

Ahora vamos a incluir un poco de notación.

Notación 1.4.19 *Bajo las condiciones de la definición anterior escribiremos* $C = v_0v_2 \dots v_n$ *y diremos que* C *es el camino de* v_0 *a* v_n*.*

Para $1 \leq i \leq j \leq n$ definimos:

$$Px_i := x_1 \dots x_i$$
$$x_iP := x_i \dots x_n$$
$$x_iPx_j := x_i \dots x_j$$

$$\mathring{P} := x_2 \dots x_{n-1}$$
$$P\mathring{x}_i := x_1 \dots x_{i-1}$$
$$\mathring{x}_iP := x_{i+1} \dots x_n$$
$$\mathring{x}_iP\mathring{x}_j := x_{i+1} \dots x_{j-1}$$

Definición 1.4.20 *Sea* $P = v_0v_1 \dots v_{n-1}$ *un camino, un* ***ciclo*** *es un camino de la forma* $C = v_0v_1 \dots v_{n-1}v_0$*. La* ***longitud*** *de un ciclo está dado por la cantidad de aristas que tenga. Al ciclo de longitud n será llamado un* $n-$*ciclo y se denotará por medio de* C_n*.*

Definición 1.4.21 *Sea* $G \neq \emptyset$ *una gráfica, se dirá que* G *es conexa si para cualesquiera dos vértices* $v_1, v_2 \in V$ *existe un camino en* G*, con* v_1 *y* v_2 *como esquinas.*

Proposición 1.4.22 *Sea* G *una gráfica conexa, si* $V = \{v_1, v_2 \dots, v_n\}$*, entonces* $G_i = G[v_1, v_2 \dots, v_i]$ *la subgráfica inducida por los vértices* $v_1, \dots, v_i$ *es conexa.*

Demostración. [9] pag.10 ■

Definición 1.4.23 *Sea* G *una gráfica, diremos que* G *es un* ***bosque*** *si es acíclica, es decir que no contenga ningún ciclo. Un bosque conexo se llamará* ***árbol****.*

A continuación daremos una caracterización básica de árbol.

Teorema 1.4.24 *Sea* T *una gráfica, las siguientes condiciones son equivalentes:*

1. T *es arbol.*
2. *Cualesquiera dos vértices* $x, y \in V$ *están unidos por un único camino en* T*.*
3. T *es conexa, pero* $T - a := (V, A \setminus \{a\})$ *es disconexa para cualquier arista* $a \in A$*.*
4. T *es acíclica, pero* $T + xy := (V, A \cup \{xy\})$ *contiene al menos un ciclo, para cualesquiera dos vértices* $x, y \in V$ *que no sean adjacentes.*

Demostración. 1) $\Rightarrow$ 2) Sea T arbol, sean $x, y \in V$ dos vértices cualquiera, como T es conexa, existe un camino $C_1 = (v_0 = x)v_1, \ldots, v_{k-1}(y = v_k$, luego si suponemos que existe otro camino distinto, digamos $C_2 = (v'_0 = x), v'_1 \ldots, v_{r-1}(v'_r = y)$. Como C_1 y C_2 son caminos distintos entonces, tomemos $i > 0$ como el mínimo tal que $v_i = v'_i$, es decir $v_j \neq v'_j$ para todo $0 < j < i$, luego entonces consideremos el ciclo $C = v_0v_1 \ldots v_iv'_{i-1} \ldots v'_1v'_0$. Por lo tanto, el camino que une a x con y, debe ser único.

2) $\Rightarrow$ 3) Sea $a \in A$, supongamos que $a = xy$, luego como $T - a$ es conexa, existe un camino C en $T - a$ que une a x y y, notemos que el camino C también esta contenido en T. Por otro lado, como $a \in A$, entonces a es un camino de longitud 1 entre x, y, lo cual contradice a la unicidad de los caminos en T. Por lo tanto, $T - a$ debe ser disconexa para todo $a \in A$.

3) $\Rightarrow$ 4) Supongamos que existe un ciclo $C = v_0v_1 \ldots v_{k-1}v_0$ en T. Consideremos la siguiente gráfica $T - v_0v_1$. Sean $x, y \in T - v_0v_1$ dos vértices cualesquiera, en T existe un camino $P = (x_0 = x)x_1 \ldots (x_k = y)$, si $x_ix_{i+1} = v_0v_1$ para algún i, basta considerar el camino $(Px_i)v_0v_{k-1} \ldots v_1(x_{i+1}P)$, el cual es un camino en $T - v_0v_1$ que une a x con y, lo cual contradice nuestra hipótesis. Por lo tanto, T es acíclica.
Por otro lado, sean $x, y \in V$ cualesquiera dos vértices en T que no sean adyacentes, luego existe un camino P en T que los une, entonces $C = P + xy$ es un ciclo en $T + xy$.

4) $\Rightarrow$ 1) Por hipótesis T es acíclica, para ver que T es conexa tomemos dos vértices cualesquiera $x, y \in V$ que no sean adyacentes y consideremos la gráfica $T + xy$ la cual por hipótesis contiene un ciclo C, por lo tanto, existe el camino $P := C - xy$ en T que une a X con y. Por lo tanto, T es un árbol. ■

1.5. Extensiones de campo

En esta sección daremos las definiciones y resultados básicos de extensiones de campos necesarias, haciendo mención de resultados principales sobre los campos finitos, puesto que los códigos lineales tiene su alfabeto sobre campos de este estilo.

Definición 1.5.1 *Sean F y K dos campos, si $F \subseteq K$. Entonces diremos que K es una extensión de F, lo cual será denotado como K/F*

De la definición anterior es claro notar que K tiene estructura de F-espacio vectorial, por lo tanto, podemos hablar de su dimensión, lo cual nos abre el camino para dar la definición del grado de una extensión.

Definición 1.5.2 *Sea F/K extensión, entonces definimos el **grado de la extensión** como $[F : K] := \dim_F(K)$. Si $[F : K] < \infty$, diremos que K/F es extensión finita.*

Definición 1.5.3 *Sea K/F una extensión, diremos que un elemento $k \in K$ es algebraico sobre F si existe $f(x) \in F[x] \setminus \{0\}$ tal que $f(k) = 0$. El polinomio mónico $m(x)$ de menor grado tal que $m(k) = 0$, se llamára el polinomio mínimo.*

Proposición 1.5.4 *El orden de un campo finito F es p^n para algún primo p y algún $n \in \mathbb{N}$.*

Demostración. Como F es finito, se tiene que $char(F) < \infty$, es decir $char(F) = p$ para p número primo, luego el campo mínimal de F es $\mathbb{F}_p$. Por otro lado, por la finitud de F se tiene que debe tener una base finita β como $\mathbb{F}_p$ espacio vectorial, digamos $|\beta| = n$. Luego $F \cong \times_{i=1}^{n} \mathbb{F}_p$, por lo tanto, $|F| = p^n$. ■

Teorema 1.5.5 *Sea F campo finito, entonces el grupo multiplicativo $F^* = F \setminus \{0\}$ es cíclico.*

Demostración. Es claro que F^* es grupo abeliano de orden $q - 1$, para q potencia de un número primo. Supongamos que no fuera cíclico, entonces, existe $1 < r < q - 1$ tal que $a^r = 1$ para todo $a \in F$, es decir $Z(x^{r+1} - x) = F$, por lo tanto:

$$\prod_{a \in F} (x - a) | x^{r+1} - x,$$

lo cual es una contradicción pues $\deg(\prod_{a \in F} (x - a)) = q$. ■

Capítulo 2

Códigos lineales

En este capítulo desarrollaremos la teoría de códigos lineales, presentaremos los resultados relevantes de los códigos lineales, haremos la descripción de tipos de códigos lineales, como son los códigos polinomiales, los códigos de Hamming entre otros, serán de particular importancia los códigos cíclicos ya que en el tercer capítulo se dará una generalización de estos códigos sobre estructuras bases que no necesariamente son campos.

2.1. Códigos Lineales

Recordemos que si $\mathbb{F}$ es un campo finito, entonces $\text{char}(\mathbb{F}) < \infty$, luego al ser campo se sigue que $\text{char}(\mathbb{F}) = p$, para $p \in \mathbb{N}$ primo. Por lo tanto, el campo primitivo base de $\mathbb{F}$ será $\mathbb{F}_p$ que es el campo de p elementos, del hecho que $\mathbb{F}$ es campo finito entonces $[\mathbb{F} : \mathbb{F}_p] < \infty$, luego entonces $|\mathbb{F}| = p^r$ para algún $r \in \mathbb{N}$. En lo que sigue K denotará al campo $K = \mathbb{F}_{p^r} = \mathbb{F}_q$.

Consideremos el siguiente espacio vectorial sobre K:

$$K^n = \{(a_1, a_2, \ldots, a_n) | a_i \in K \quad \forall i = 1, \ldots, n\}.$$

Definición 2.1.1 *Sea $C \subset K^n$ un subconjunto, diremos que C es un **código lineal** de longitud n, si C es subespacio de K^n, y a cada elemento $a \in C$ le llamaremos una palabra código.*

Por simplicidad nos referiremos a C, como un $[n, k]$-*código lineal*, donde k es la dimensión de C como K espacio vectorial.

Definición 2.1.2 *Sean $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n) \in C$, definimos la función distancia de Hamming $\rho : K^n \times K^n \longrightarrow \mathbb{R}$ como:*

$$\rho(a, b) = \sum_{i=1}^{n} x_i \qquad \textit{donde} \quad x_i = \begin{cases} x_i = 1 & \textit{Si } a_i \neq b_i \\ x_i = 0 & \textit{En otro caso} \end{cases}$$

Definición 2.1.3 *Sea $a = (a_1, a_2, \ldots, a_n) \in C$, definimos el peso de Hamming como:*

$$wt(a) = \sum_{i=1}^{n} b_i \qquad donde \quad b_i = \begin{cases} b_i = 1 & Si\ a_i \neq 0 \\ b_i = 0 & En\ otro\ caso \end{cases}$$

Observación 2.1.4 Notemos que las definiciones anteriormente expuestas tienen una relación muy estrecha, algunas de ellas son:

1. $wt(a) = \rho(a, 0) \quad \forall a \in C$
2. $\rho(a, b) = \rho(a - b, 0) = wt(a - b) \quad \forall a, b \in C$

En la definición anterior, se dio a ρ como una distancia, y a continuación lo justificaremos.

Lema 2.1.5 *Sea C un $[n, k, -]$-código lineal y sean $a, b \in C$, entonces:*

$$wt(a + b) \leq wt(a) + wt(b) \tag{2.1}$$

Demostración. Sean $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in C$, sean $I, J \subset \{1, \ldots, n\}$ tal que $a_i, b_j \neq 0 \quad \forall i \in I, j \in J$, ahora note que si $J \cap I = \emptyset$ se tiene la igualdad en Ec.(2.1). En caso contrario, sea $i_0 \in J \cap I$ elemento arbitrario, entonces hay dos casos:

- $a_{i_0} + b_{i_0} = 0$
- $a_{i_0} + b_{i_0} \neq 0$

Es decir observando la entrada i_0:

$$wt((0, \ldots, a_{i_0} + b_{i_0}, \ldots, 0)) < wt((0, \ldots, a_{i_0}, \ldots, 0)) + wt((0, \ldots, b_{i_0}, \ldots, 0)).$$

Como i_0 se eligió de manera arbitraria, finalmente se tiene que;

$$wt(a + b) \leq wt(a) + wt(b)$$

■

Corolario 2.1.6 *Sea C un $[n, k]$-código lineal, entonces la función $\rho : K^n \times K^n \longrightarrow \mathbb{R}$, es una métrica.*

Demostración. De la definción de distancia, es inmediato la condición de positividad y de simetría, por lo que nos enfocaremos a demostrar la desigualdad del triángulo. Sean $a, b, c \in C$, por el lema 2.1.5 y la observación anterior tenemos lo siguiente:

$$\begin{aligned} \rho(a,b) &= \rho(a-b,0) \\ &= wt(a-b) \\ &= wt(a-b+c-c) \\ &\leq wt(a-c)+wt(c-b) \\ &= \rho(a,c)+\rho(b,c) \end{aligned}$$

Es decir:

$$\rho(a,b) \leq \rho(a,c)+\rho(c,b) \quad \forall a,b,c \in C$$

■

Definición 2.1.7 *Sea C un $[n,k]$-código lineal, se define la distancia mínima, denotada por $\delta(C)$ o simplemente d como:*

$$\delta(C) = min\{\rho(a,b)|a,b \in C\}.$$

De acuerdo con la relación entre la distancia y el peso de una palabra, como C es subespacio de K^n, se sigue que el mínimo de los pesos de las palabras en C coincide con $\delta(C)$. En adelante, a un código de longitud n, dimensión k y distancia mínima $d := \delta(C)$, lo llamaremos un $[n,k,d]$-*código lineal*.

A continuación daremos una primera cota a la distancia mínima, la cual se conoce como la cota de *Singleton*.

Teorema 2.1.8 *Sea C un $[n,k,d]$-código lineal, entonces se tiene que:*

$$d \leq n+1-k. \tag{2.2}$$

Demostración. Considere el siguiente subespacio vectorial:

$$V = \{(a_1,\ldots,a_{d-1},0,\ldots,0)|a_i \in K\}$$

, se tiene que $dim(V) = d-1$, además $V \cap C = \emptyset$, ya que en caso contrario existiría una palabra con peso menor o igual a $d-1$, por lo tanto, se sigue:

$$\begin{aligned} n &\geq dim(C)+dim(V) \\ &= k+d-1. \end{aligned}$$

■

A continuación expondremos lo que conoceremos como vectores error, y cuando es posible que nuestro código detecte el error y lo corrija, en este punto se muestra una característica fundamental del código en el cual la distancia mínima juega un papel indispensable.

Definición 2.1.9 *Sea C un código lineal un vector error e es **detectable** si para todo $a \in C$ se tiene que $a + e \notin C$. En caso contrario diremos que el error es indetectable.*

Un vector error, puede tener una o más entradas erróneas, por lo que si un vector tiene r entradas erróneas, diremos que ocurrio un r-error. Dado e un r-error podemos asociarle el vector tal que tiene 1 en las posiciones error y cero en el resto de entradas, dando un vector con peso r.

Teorema 2.1.10 *Para $K = \mathbb{F}_2$, sea C un $[n, k, d]$-código lineal, tomemos $\ell \in \mathbb{N}$, entonces, todos los r-erroes con $r \leq \ell$ son detectables si y sólo si $d \geq 1 + \ell$.*

Demostración. $\Rightarrow$) Sea $l \in \mathbb{N}$, supongamos que el código C es capaz de detectar todos los $r - errores$, es decir, para todo $e \in \mathbb{F}_2^n$ con $wt(e) \leq l$ y $b \in C$ se tiene que $(b+e) \notin C$. Sean $b, b' \in C$ supongamos que $\rho(b, b') \leq l$, consideremos $e := b + b'$, entonces es claro que $wt(e) \leq l$, además, $b + e = b + b + b' = b'$, lo cual es una contradicción, por lo tanto:

$$\rho(b, b') \geq l + 1 \quad \forall b, b' \in C$$

$\Leftarrow$) Supongamos que existe un l-error con $l \leq r$ que sea indetectable, es decir existe $b \in C$ tal que $e + b \in C$. Además notemos que $\rho(b + e, b) = wt(e) \leq r$, por lo tanto $d \leq r$, lo cual es una contradicción. Por lo tanto todo l error es detectable. ■

Para un código C con distancia mínima d y tomemos $t := [\frac{d-1}{2}]$. Si para $a \in K^n$ se tiene que $\rho(a, c) \leq t$ para algún $c \in C$, entonces claramente c es la única palabra con esta propiedad, si suponemos que existe otra palabra $s \in C$ con la misma propiedad entonces:

$$\rho(c, s) \leq \rho(c, a) + \rho(s, a) = d - 1 < d$$

Lo cual es una contradicción, por lo tanto, c es la única palabra código con $\rho(a, c) \leq t$. Entonces si al transmitir información, se recibe un vector a con las propiedades anteriores, se acepta a c como la palabra transmitida. A lo anterior diremos que C ***corrige*** el error a o que la palabra a es un error corregible.

Corolario 2.1.11 *Bajo las condiciones anteriores, C es capaz de detectar y corregir t errores.*

A continuación daremos la construcción de las matrices generadoras de un código así como su matriz de chequeo de paridad.

Sea C un $[n, k, d]$-código lineal, entonces podemos tomar una base para C, digamos $\beta = \{x_1, \ldots, x_k\}$, para cualquier $c \in C$ este se puede escribir como una conbinación lineal

de elementos de β, lo cual podemos escribir de forma matricial como:

$$c = \sum_{i=1}^{k} a_i x_i = a_1(x_{11}, \ldots, x_{1n}) + \cdots + a_k(x_{k1}, \ldots, x_{kn}) =$$

$$= (a_1, \ldots, a_k) \begin{pmatrix} x_{11} \ldots x_{1n} \\ \vdots \\ x_{k1} \ldots x_{kn} \end{pmatrix} = (a_1, \ldots, a_n)G.$$

Donde G es la matriz con filas $x_1, \ldots, x_k$.

Definición 2.1.12 *Bajo las condiciones anteriores, a la matriz G se le llamará la* ***matriz generadora*** *del código C.*

Sea S_n el grupo símetrico y sea $\sigma \in S_n$, si tomamos un vector $a = (a_1, \ldots, a_n)$ entonces $\sigma(a) := (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$, además si $U \subset K^n$ entonces $\sigma(U) = \{\sigma(u) | u \in U\}$.

Definición 2.1.13 *Sean C y C' dos códigos de longitud n, entonces diremos que son* ***equivalentes****. Si existe $\sigma \in S_n$ tal que $\sigma(C) = C'$.*

Notemos que si C y C' son dos códigos equivalentes entonces el mínimo de los pesos de palabras no cero es el mismo, por lo tanto, tienen la misma distancia mínima así mantendrán las mismas propiedades de detección y corrección de errores.

Definición 2.1.14 *Sea $\sigma \in S_n$, se define la* ***matriz de permutación*** *$P \in M_n$ asociada a σ como; $P_{\sigma(j)j} = 1$ para todo $1 \leq j \leq n$ y cero en otro caso.*

Notemos que si P es una matriz de permutación, al tomar un vector $a \in K^n$ y considerar el vector aP, entonces la j-ésima entrada de este es de la siguiente forma:

$$a_1 p_{1j} + a_2 p_{2j} + \cdots + a_{\sigma(j)} p_{\sigma(j)j} + \cdots + a_n + p_{nj} = a_{\sigma(j)}$$

Por lo tanto, se tiene que $aP = \sigma(a)$.

Proposición 2.1.15 *Sean C y C' dos códigos cualesquiera, C y C' son equivalentes si y sólo si existe una matriz de permutación P tal que $C' = \{cP | c \in C\}$.*

Demostración. La demostración es inmediata de las definiciones de equivalencia y de matriz de permutación. ■

Teorema 2.1.16 *Sea C un $[n, k, d]$-código lineal, existe un código C' equivalente cuya matriz generadora es de la forma $(I_k A)$ donde $A \in M_{k \times n-k}$.*

Demostración. [22] pag 85. ■

Definición 2.1.17 *Sea C un código lineal se define la matriz* ***chequeo de paridad*** *$H \in M_{n-k,k}$ como la matriz tal que:*

$$Hu^t = 0 \qquad \forall u \in C.$$

En el siguiente resutado expondremos la fuerte relación que guardan la matriz chequeo de paridad con la matriz generadora de un código C.

Proposición 2.1.18 *Sea C un $[n,k,d]$-código lineal con matriz generadora G y matriz chequeo de paridad H. Si $G = (I_k \quad A)$ entonces $H = (-A^t \quad I_{n-k})$.*

Demostración. Sea $c \in C$, por demostrar que $(-A^t I_{n-k})u^t = 0$. Como G es matriz generadora entonces, existe $a \in K^k$ tal que $c = aG = a(I_k A) = a(aA)$, por lo tanto, se tiene:

$$(-A^t I_{n-k})c^t = (-A^t I_{n-k}) \begin{pmatrix} a^t \\ (aA)^t \end{pmatrix} = -A^t a^t + (aA)^t = 0.$$

Como $c \in C$ fue arbitrario se tiene el resultado. ■

Daremos la construcción de nuevos códigos apartir de un código dado, un primer ejemplo de ello es el código dual $C^\perp$. Para ello daremos la definición del producto interno canónico.

Definición 2.1.19 *Sean $x, y \in K^n$, se define el producto interno canónico entre ambos vectores como:*

$$\langle x, y\rangle = \langle (x_1, \ldots, x_n), (y_1, \ldots, y_n)\rangle = \sum_{i=1}^{n} x_i y_i.$$

Notemos que la función anterior no es un producto interno pues en $\mathbb{F}_2$, se tiene:

$$\langle (1,1), (1,1)\rangle = 1 + 1 = 0.$$

Definición 2.1.20 *Sea C un $[n,k,d]$-código lineal, se define el* ***código dual*** *asociado a C, denotado por $C^\perp$, como sigue:*

$$C^\perp = \{u \in K^n | \, \langle u, v\rangle = 0 \quad \forall v \in C\}.$$

Si $C^\perp = C$, se dirá que C es un código ***auto dual****.*

Teorema 2.1.21 *Sea C un $[n,k,d]$-código con matriz generadora G y matriz chequeo de paridad H. Entonces $C^\perp$ es un $[n, n-k, d']$-código con matriz generadora H y matriz chequeo de paridad G.*

Demostración. Es claro que $C^{\perp}$ es subespacio vectorial de K^n. Ahora veamos que en efecto G es la matriz chequeo de paridad del código $C^{\perp}$. Sea $w \in C^{\perp}$ elemento arbitrario, por lo tanto, $vw^t = 0 \; \forall v \in C$, luego como G es la matriz generadora del código C, se sigue que $(aG)w^t = 0$ para todo $a \in K^k$, por lo tanto, se sigue inmediatamente que $Gw^t = 0$. Recíprocamente si $w \in K^n$ tal que $Gw^t = 0$, entonces se tiene que $vw^t = 0$ para todo $v \in C$, es decir:

$$C^{\perp} = \{w \in K^n | Gw^t = 0\}.$$

Lo cual prueba que G es la matriz chequeo de paridad de $C^{\perp}$.

Ahora calculemos $\dim C^{\perp}$, consideremos la siguiente transformación lineal:

$$\theta : K^n \to K^n$$
$$\theta(x) = Gx^t.$$

Claramente θ es una transformación lineal, cuyo nucleo es $ker\theta = C^{\perp}$, además por la definición se sigue que $rank(\theta) = rank(G) = k$. Del teorema de la dimensión se sigue que:

$$\dim C^{\perp} = n - rank(\theta) = n - k.$$

Por otro lado, sea C' el código lineal con matriz generadora H, como H es una matriz $(n-k) \times n$ con $n-k$ columnas linealmente independientes, se sigue que $\dim C' = n-k$, por otro lado, como H es la matriz chequeo de paridad de C, se sigue que cada $u \in C$ es ortogonal con cada fila de H, es decir $C' \subseteq C^{\perp}$. Por lo tanto, $C' = C^{\perp}$ y H es la matriz generadora de $C^{\perp}$. ■

2.2. Códigos polinomiales

Los códigos polinomiales nos proporcionan una nueva manera de ver a los códigos lineales sobre un campo finito K como el anillo de polinomios en la variable x sobre el campo K.

Consideremos el espacio vectorial K^n y el anillo de polinomios en una variable $K[x]$ el cual recordemos que es un espacio vectorial sobre el mismo campo. Sabemos que K^n es isomorfo a $K[x]_n = \{f \in K[x] | \deg f < n\}$, bajo el isomorfismo:

$$\psi((a_0, a_1, \ldots, a_{n-1})) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.$$

Por lo tanto, si C es un $[n, k, d]$-código sobre el campo K bajo dicho isomorfismo, podemos identificar a los elementos de C como un polinomio de grado menor a n, por lo tanto identificaremos a un elemento del código como un vector ordenado o como un polinomio, según la situación.

Definición 2.2.1 *Sea $g(x) = g_0 + g_1x + \cdots + g_kx^k$ un polinomio de grado a lo más k. El **código polinomial** con polinomio generador $g(x)$ es $C_{g(x)} = \langle g(x) \rangle$. Y cada mensaje de longitud m; $a(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$ lo codifica en la palabra $b(x) = b_0 + b_1x + \cdots + b_{m+k-1}x^{m+k-1} = a(x)g(x)$.*

Proposición 2.2.2 *El código polinomial de longitud $n = m + k$ con polinomio generador $g(x)$ es subespacio de K^n.*

Demostración. La demostración es inmediata bajo el isomorfismo ψ. ■

De esta forma notemos que la distancia minima de un código polinomial con polinommio generador $g(x)$, similarmente que en el caso de los códigos lineales es el mínimo de los pesos $wt(a(x)g(x))$ de polinomios no cero.

Proposición 2.2.3 *Un polinomio con coeficientes en $\mathbb{F}_2$ es divisible por $1 + x$ si y solo si tiene un número par de términos.*

Demostración. $\Rightarrow$) Sea $f(x) = a_0 + a_1x + \cdots + a_nx^n$, $a_i \in \mathbb{F}_2$ un polinomio divisible por $1 + x$, entonces existe un polinomio $b(x) \in \mathbb{F}_2[x]$, tal que:

$$f(x) = (1 + x)b(x)$$

Al evaluar $a_0 + a_1 + \cdots + a_n = f(1) = 0$, lo cual solo es posible si hay un cantidad par de coeficientes.

$\Leftarrow$) Recíprocamente sea $f(x)$ un polinomio con una cantidad par de términos, digamos $f(x) = x^{i_1} + x^{i_2} + \cdots + x^{i_{2k}}$ tales que $i_1 < \ldots < i_{2k}$, agrupando los términos $f(x) = (x^{i_1}+x^{i_2})+\cdots+(x^{i_{2k-1}}+x^{i_{2k}})$. Ahora notemos que si $i < j$, entonces $x^i+x^j = x^i(1+x^{j-i}) = x^i(1 + x)(1 + x + \cdots + x^{j-i-1})$, realizando esto en cada uno de las agrupaciones de $f(x)$ se tiene el resultado. ■

Teorema 2.2.4 *Sea $g(x) \in \mathbb{F}_2[x]$, si $g(x)$ no divide a ningún polinomio de la forma $x^k - 1$ con $k < n$, entonces el código polinomial generado por $g(x)$ tiene distancia minima al menos 3.*

Demostración. [22] pag 29. ■

Proposición 2.2.5 *Sea $e = (e_0, e_1, \ldots, e_{n-1})$ un vector de error de un código polinomial con polinomio generador $g(x)$, entonces e es indetéctable $\Leftrightarrow g(x)|e(x)$.*

Demostración. $\Rightarrow$) Supongamos que $e(x)$ es indetectable, es decir existe $f(x) \in \langle g \rangle$ tal que $e(x) + f(x) \in \langle g \rangle$, luego $e(x) \in \langle g \rangle$.

$\Leftarrow$) Recíprocamente si $g(x)|e(x)$, podemos escribir a $e(x) = h(x)g(x)$, luego basta tomar $h_1, h_2 \in K[X]$ tal que $h_1 + h_2 = h$. ■

Teorema 2.2.6 *Sea C código polinomial con polinomio generador $g(x)$, si $g(x) = g_0 + g_1x + \cdots + g_kx^k$, entonces tiene matriz generadora $G \in M_{(n-k)\times n}$:*

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_k & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{k-1} & g_k & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_k \end{pmatrix}.$$

***Demostración*.** Es claro ver que la matriz G, tomando la submatriz formada por las primeras $n-k$ columnas, se tiene una matriz cuadrada en cuya diagonal esta formada por términos g_0, es decir, al calcular el determinante de esta submatriz se obtiene $g_0^{n-k} \neq 0$, es decir se forma una matriz no singular, por lo tanto, G tiene rango $n-k$. Ahora solo resta ver que efectivamente el código generado por G coincide con C. Sea $b = (b_0, b_1, \dots, b_{n-k-1})$ y calculemos la multiplicación por G.

$$(b_0, b_1, \dots, b_{n-k-1}) \begin{pmatrix} g_0 & g_1 & \dots & g_k & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{k-1} & g_k & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_k \end{pmatrix} =$$

$$= (b_0g_0, b_0g_1 + b_1g_0, \textstyle\sum_{i+j=2} b_ig_j, \dots, b_{n-k-1}g_k).$$

El cual corresponde a hacer la multiplicación de g por un polinomio de grado menor o igual a $n-k-1$. ■

2.3. Códigos de Hamming

Los códigos de Hamming son un ejemplo clasico de los códigos binarios, es decir en esta sección trabajaremos con $K = \mathbb{F}_2$, demostraremos que para todo C código de Hamming la distancia mínima es siempre la misma, más aún $\delta(C) = 3$, además existe una relación biunívoca entre los naturales $\mathbb{N}$ y los códigos Hamming.

Para poder realizar la construcción de estos códigos es necesario hacer las siguientes observaciones.

1. Sea $r \in \mathbb{N}$ entonces las *palabras código* tendrán $n = 2^r - 1$ dígitos y el mensaje tendrá $m = 2^r - r - 1$ dígitos. Para cada $b = (b_1 \dots, b_n)$ la correspondiente *mensaje* es $a = (b_3, b_5, b_6.b_7. \dots, b_{2^k+1}, \dots, b_{2^{k+1}-1}, \dots, b_{2^r-1})$ y los restantes $b_0, b_2, \dots, b_{2^{r-1}}$ son los símbolos de chequeo, las cuales consideraremos desconocidas hasta el momento.

2. Sea $M \in M_{r\times 2^r-1}$ la matriz tal que el $i-esimo$ renglón es la representación binaria de i.

   Si $r=3$, entonces $M \in M_{7\times 3}$ con $M^t = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

3. Al tomar la multiplicación de matrices e igualarla con cero $bM = 0$ obtenemos un sistema de r ecuaciones lineales con r incógnitas, las cuales son $b_0, b_{2^1}, \ldots, b_{2^{r-1}}$.

   Siguiendo con el ejemplo cuando $r=3$, las ecuaciones que se producen son:

$$\begin{aligned} b_4 + b_5 + b_6 + b_7 &= 0 \\ b_2 + b_3 + b_6 + b_7 &= 0 \\ b_1 + b_3 + b_5 + b_7 &= 0 \end{aligned}$$

Lema 2.3.1 *De acuerdo a la notación anterior en cada una de las r ecuaciones lineales aparece exactamente uno de los* b_{2^i}.

Demostración. Suponga que b_{2^i} aparece en la ecuación que resulta al multiplicar b por la k-ésima columna de la matriz M, es decir la entrada $(2^i, k)$ de M es 1, la cual se encuentra en el renglón 2^i, la cual es la representación binaria de 2^i esto solo ocurre en la $(r-i)$ columna entonces $k = r-i$. Entonces si b_{2^i}, b_{2^j} son tales que aparecen en la misma ecuación de la relación anterior se tiene que $j = i$. ■

Definición 2.3.2 *El código que se genera en el algoritmo anterior se llama el* $(2^r - r - 1, 2^r - 1)$ ***código de Hamming***

Notemos entonces que por definición, los códigos de Hamming tiene a M como su matriz chequeo de paridad y por lo tanto, apartir de ella es posible encontrar su matriz generadora.

Teorema 2.3.3 *Sea C un código de Hamming, entonces* $\delta(C) = 3$.

Demostración. Sea C código de Hamming con $n = 2^r - 1$ y $m = 2^r - r - 1$. Sea $a \in \mathbb{F}_2^m$ con $wt(a) = 1$ y $b = b_1 b_2 \ldots b_n$ su correspondiente palabra código. Supongamos que la i-ésima entrada de a es no cero, entonces $i \neq 2^j$ para algún j, es decir en la representación binaria de i hay al menos dos entradas no cero, sean s y t dos entradas no cero de la representación binaria.

Sean $M_1, M_2, \ldots, M_r$ las columnas de la matriz M, en la ecuación $bM_s = 0$. Sea b_{2^k} el símbolo de chequeo presente en la ecuación, entonces tenemos que $b_{2^k} + b_i = 0$, por lo

tanto, $b_{2^k} \neq 0$, similarmente si b_{2^l} es el símbolo de chequeo de bM_t se prueba que $b_{2^l} \neq 0$. Por lo tanto, es claro que $wt(b) \geq 3$.

Sea $a \in \mathbb{F}_2^m$ con $wt(a) = 2$ y $b = b_1 b_2 \dots b_n$ su correspondiente palabra código. Supongamos que las entradas no cero están en las posiciones i, j, de nuevo entonces i, j no son potencias de dos, por otro lado, como $i \neq j$ entonces sus representaciones binarias difieren en al menos una posiciones, supongamos entonces que la entrada s de la representación binaria de i es 1, mientras que la de j es 0. Sea b_{2^k} el símbolo de chequeo que aparece en la ecuación $bM_s = 0$, es claro entonces que $b_{2^k} + b_i = 0$, es decir $b_{2^k} \neq 0$, es decir en b al menos existe un simbolo de chequeo no cero, por lo tanto, $wt(b) \geq 3$.

Sea $a \in \mathbb{F}_2^m$ y $b = b_1 b_2 \dots b_n$ su correspondiente palabra código, donde $a_1 = 1$ y $a_i = 0$ $\forall 2 \leq i \leq m$. ■

2.4. Códigos Bose-Chaudhuri-Hocquenghem

Sea C un $[n, k, d]$-código lineal sobre el campo $\mathbb{F}$ cuyo orden $|\mathbb{F}| = q$ es potencia de un primo. Sea $r \in \mathbb{N}$ el natural más pequeño tal que $q^r \geq n + 1$. Sea K extensión de $\mathbb{F}$ de grado r, como K es finito existe elemento primitivo, por decir α. Sea $m_i(X)$ el polinomio mínimo de α^i sobre $\mathbb{F}$, para $1 \leq i \leq d - 1$.

Definición 2.4.1 *Bajo la notación anterior, un código BCH es el generado por el polinomio* $g(X) = LCM(m_1(X), m_2(X), \dots, m_{d-1}(X))$

Teorema 2.4.2 *Sea C un $[n, k, d]$-código lineal entonces su código BCH tiene distancia mínima al menos d.*

Demostración. Supongamos que existe $c(X) \in \langle g(x) \rangle$ cuyo peso sea menos que d, digamos:

$$c(X) = c_1 x^{n_1} + c_2 x^{n_2} + \cdots + c_{d-1} x^{n_{d-1}} \qquad n_1 > n_2 > \cdots > c_{d-1} \geq 0$$

Como el código tiene longitud n, entonces todo polinomio debe tener grado a lo más $n-1$, es decir $n_1 \leq n - 1$.

Por otro lado, por definición se tiene que $\alpha, \alpha^2, \dots, \alpha^{d-1}$ son raíces de $c(x)$, así tenemos el siguiente sistema de ecuaciones.

$$\begin{array}{rcl} c_1\alpha^{n_1} + \cdots + c_{d-1}\alpha^{n_{d-1}} & = & 0 \\ c_1\alpha^{2n_1} + \cdots + c_{d-1}\alpha^{2n_{d-1}} & = & 0 \\ \vdots & \vdots & \vdots \\ c_1\alpha^{(d-1)n_1} + \cdots + c_{d-1}\alpha^{(d-1)n_{d-1}} & = & 0 \end{array}$$

La matriz A asociada a este sistema lineal es conocida como la matriz de *Vandermonde*, cuyo determinante es conocido:

$$\det A = \prod_{i>j}(\alpha^{n_i} - \alpha^{n_j}) \neq 0.$$

De lo anterior se tiene que la única solución al sistema lineal es la homogénea, es decir $c(x) = 0$.

Por lo tanto, para toda polinomio $c(x) \neq 0$ se tiene $wt(c(x) \geq d$, lo cual implica que la distancia miníma del código sea al menos d.

■

2.5. Código cíclicos

En esta sección veremos un tipo muy particular de los códigos polinomiales, aunque en su definición no aparenten tener relación alguna con ellos, existe una caracterización que relaciona fuertemente los códigos cíclicos con los códigos polinomiales. Sea $q = |K|$, durante esta sección vamos a tomar longitudes n tal que $(n, q) = 1$.

Definición 2.5.1 *Sea C un $[n, k, d]$-código lineal, C es llamado* ***ciclíco*** *si para cada $(a_0, a_1, \ldots, a_{n-1}) \in C$ se tiene que $(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in C$.*

Definamos un mapeo de K^n al cociente $K[x]/\langle x^n - 1\rangle$, mediante,

$$\varphi : K^n \to K[x]/\langle x^n - 1\rangle$$
$$\varphi((a_0, a_1, \ldots, a_{n-1})) = a_0 + a_1x + \cdots + a_{n-1}x^{x-1} + \langle x^n - 1\rangle$$

Claramente φ es una transformación lineal entre ambos espacios, por lo tanto, $\varphi(C)$ es subespacio de $K[X]/\langle x^n - 1\rangle$. Por otro lado, si $(a_0, a_1, \ldots, a_{n-1}) \in C$, entonces $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C \Leftrightarrow a_{n-1} + a_0x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle = x^n a_{n-1} + a_0x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle = x(a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) + \langle x^n - 1\rangle \in \varphi(C)$. Es decir un código C es cíclico si y sólo si $\varphi(C)$ es un ideal.

En consecuencia de lo anterior, trataremos a un código cíclico como un ideal en el cociente del anillo de polinomios con el ideal generado por $x^n - 1$.

En adelante y por simplicidad escribiremos solo el polinomio $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ pensado como clase de equivalencia en lugar de $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$. De igual manera nos referiremos a C o $\varphi(C)$ sin distinción alguna a menos que se especifique lo contrario.

Teorema 2.5.2 *Sea C un código cíclico sobre K, entonces:*

1. *Existe un único polinomio mónico $g(x)$ de grado mínimo en C que lo genera.*
2. *$g(x)$ es factor de $x^n - 1$.*
3. *Si $\deg g(x) = r$. Entonces $\dim C = n - r$ y cualquier $a(x) \in C$ tiene representación única de la forma $a(x) = g(x)b(x)$, donde $\deg b(x) < n - r$.*
4. *Si $g(x) = g_0 + g_1x + \cdots + g_rx^r$, entonces la matriz $(n-r) \times n$*

$$G = \begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & g_r & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & g_0 & g_1 & \dots & g_r \end{pmatrix},$$

es la matriz generadora de C.

Demostración. Sea $N := \{\deg a(x) | a(x) \in C\} \subset \mathbb{N}$, claramente $N \neq \emptyset$ por lo tanto por el principio del buen orden existe un elemento minimal. Así sea $g(x) \in K[x]$ el polinomio de menor grado tal que pertence a C, sin pérdida de generalidad podemos suponer a $g(x)$ polinomio mónico.
Para ver que $g(x)$ genera a C, sea $a(x) \in C$ elemento arbitrario, y aplicando el algoritmo de la división en el anillo $K[X]$, existen polinomios $r(x), s(x) \in K[X]$, tales que:

$$a(x) = s(x)g(x) + r(x) \quad \text{donde} \quad \deg r(x) < \deg g(x) \text{ o } r(x) = 0.$$

Si suponemos que $r(x) \neq 0$, entonces se tiene que $r(x) = a(x) - g(x)s(x)$, como C es cíclico se tiene que visto en el anillo de polinomios es un ideal, así se tiene $r(x) \in C$, lo cual contradice a la minimalidad de $g(x)$, es decir $a(x) = s(x)g(x)$, por lo tanto $g(x)$ genera al código C.

Por otro lado, si suponemos que existe otro polinomio mónico $g'(x)$ de grado mínimo tal que $g'(x) \in C$, tomando $h(x) := g(x) - g'(x)$, es claro que $h(x) \in C$ y además $\deg h(x) < \deg g(x)$, lo cual es una contradicción a la elección de $g(x)$.

Ahora, de nuevo usando el algoritmo de la división se tiene que existen $r(x), s(x) \in K[x]$ tales que :

$$x^n - 1 = g(x)s(x) + r(x).$$

De nuevo, si $r(x) \neq 0$, se tiene que $\deg r(x) < \deg g(x)$ y además $r(x) \in C$, por lo tanto, $x^n - 1 = g(x)s(x)$.

Sea $\beta = \{g(x), xg(x), \dots, x^{n-r-1}g(x)\}$, claramente β es un conjunto linealmente independiente, basta ver que genera a todo elemento del código. Sea $a(x) \in C$, luego podemos escribir a $a(x)$ como:

$$a(x) = g(x)b(x) + c(x)(x^n - 1)$$

Pero como $g(x)|x^n-1$ obtenemos que $a(x) = g(x)b(x) + c(x)h(x)g(X) = d(x)g(x)$, notemos que lo anterior implica que $\deg d(x) < n-r$, entonces podemos escribir a $a(x)$ como combinación lineal de elementos de β. Por lo tanto, β es una base para C, es decir; $\dim C = n-r$. La última parte es inmediato por lo visto en códigos polinomiales. ■

Definición 2.5.3 *Sea C código cíclico con polinomio generador $g(x)$, sea $h(x)$ el polinomio tal que $x^n-1 = h(x)g(x)$, entonces $h(x)$ se llamará el* ***Polinomio de Chequeo*** *de C.*

La definición anterior tiene sentido, pues cada $a(x) \in C$, se puede escribir de la siguiente manera $a(x) = g(x)b(x)$, por lo tanto, $a(x)h(x) = (x^n-1)b(x) = 0$

Si $h(x) = h_0 + xh_1 + \cdots + h_{n-r}x^{n-r}$, entonces una palabra $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ pertenece a C si y sólo si se cumple que $c(x)h(x) = 0$, es decir para cada $j = 0, 1, \ldots, n-1$ se tiene que $\sum_{i=0}^{n-1} c_i h_{j-i} = 0$ donde los subíndices son tomados mód n y bajo la convención $h_k = 0$ para todo $k > n-r$. Lo anterior lo podemos poner en forma matricial como:

$$(c_0, c_1, \ldots, c_{n-1}) \begin{pmatrix} 0 & 0 & \ldots & 0 & h_{n-r} & \ldots & h_1 & h_o \\ 0 & & & h_{n-r} & h_{n-r-1} & \ldots & h_0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & & \vdots \\ h_0 & 0 & \ldots & \ldots & \ldots & \ldots & h_2 & h_1 \end{pmatrix} = 0.$$

Notemos que H es una matriz simétrica con lo que $H^t = H$, por lo que $cH = 0 \Leftrightarrow Hc^t = 0$. Por lo tanto, es claro que el código generado por H está contenido en $C^\perp$, sabemos que $\dim C^\perp = n - \dim C = n - (n-r) = r$. Por otro lado, es claro que los primeros r renglones de H son linealmente independientes por lo tanto, el código generado por H es precisamente $C^\perp$. Sea H_1 la matriz formada por los primeros r renglones de H, por lo anterior es claro que H_1 genera a $C^\perp$, además por el teorema anterior se sigue que el dual es también código cíclico.

Consideremos la permutacón $\sigma = (1 \quad r)(2 \quad r-1)(3 \quad r-2)\cdots$, entonces sabemos que el código generado por $\sigma(H_1)$ será equivalente a $C^\perp$. Por el Teorema 2.5.2 se tiene que $C^\perp$ tiene polinomio generador de la siguiente forma:

$$k(x) = h_{n-r} + h_{n-r-1}x + \cdots + h_0x^{n-r} = x^{n-r}(h_0 + h_1x^{-1} + \cdots + h_{n-r}x^{-(n-r)}) = x^{n-r}h(x^{-1}).$$

Teorema 2.5.4 *Sea C un código cíclico de longitud n con polinomio generador $g(x)$ de grado r y polinomio de chequeo $h(x)$, entonces:*

1. *$C^\perp$ es también código cíclico con polinomio generador $x^{n-r}h(x^{-1})$.*
2. *$C^\perp$ es equivalente al código generado por $h(x)$.*

Demostración. La demostración es inmediata de la construcción anterior. ■

El teorema anterior nos permite dar una condición suficiente y necesaria para que un código cíclico sea auto dual.

Teorema 2.5.5 *Sea C código cíclico de longitud n con polinomio generador $g(x)$ tal que $\deg g(x) = r$, entonces C es auto dual si y sólo si $x^r g(x)g(x^{-1}) = x^n - 1$.*

Demostración. Sea $h(x)$ el polinomio de chequeo de C de la definición se tiene $x^n - 1 = g(x)h(x)$, por el teorema anterior $k(x) = x^{n-r}h(x^{-1})$ es el polinomio generador de $C^{\perp}$. Luego $x^n - 1 = x^r g(x^{-1})x^{n-r}h(x^{-1}) = x^r g(x^{-1})k(x)$, por lo tanto, $k(X) = \dfrac{x^n - 1}{x^r g(x^{-1})}$, luego:

$$\begin{array}{rcl} C \text{ es auto dual} & \Leftrightarrow & g(x) = k(x) \\ & \Leftrightarrow & g(x) = \frac{x^n-1}{x^r g(x^{-1})} \\ & \Leftrightarrow & x^r g(x)g(x^{-1}) = x^n - 1 \end{array}$$

Lo cual termina la demostración. ■

Teorema 2.5.6 *Sea C un código cíclico de longitud n, entonces, existe un único elemento $c(x) \in C$ tal que:*

1. *$c(x) = c^2(x)$.*
2. *$\langle c(x) \rangle = C$.*
3. *$\forall f(x) \in C$ se cumple que $f(x)c(x) = f(x)$, es decir $c(x)$ es una identidad en C.*

Demostración. Sean $g(x)$ y $h(x)$ el polinomio generador y de chequeo de C, entonces se tiene que $g(X)h(X) = x^n - 1$, como $(n, q) = 1$, entonces $x^n - 1$ no tiene ceros múltiples, es decir $(h(x), g(x)) = 1$, por lo tanto, existen polinomios $r(x), s(x) \in K[X]$, tales que:

$$r(x)g(x) + s(x)h(x) = 1 \tag{2.3}$$

Tomando $c(x) := a(X)b(x)$, y multiplicando la ecuación anterior por $c(x)$ se tiene que :

$$\begin{array}{rcl} c^2(x) + g(x)h(x)r(x)s(x) & = & c(x) \\ c^2(x) & = & c(x). \end{array}$$

Por otro lado, como $g(x)|c(x)$ se tiene que $\langle c(x) \rangle \subset \langle g(x) \rangle$ multiplicando la ecuación 2.3 por $g(x)$ obtenemos que $g(x)c(x) = g(x)$, con lo cual se tiene la contención contraria y por lo tanto, $\langle g(x) \rangle = \langle c(x) \rangle = C$.
El punto 3 se obtiene inmediatamente de 1 y 2. Sea $d(x)$ otro polinomio que cumple con los puntos 1,2 y 3, por lo tanto; $d(x) = c(x)d(x) = c(x)$. Con lo cual se demuestra la unicidad. ■

Definición 2.5.7 *El elemento $c(x)$ del teorema anterior se le llamará el* ***elemento idempotente*** *de C.*

2.6. Códigos residuo cuadrático

En esta sección hablaremos sobre un tipo especial de códigos cíclicos, para ello veremos que dado un conjunto de números se puede particionar en dos clases de equivalencia, los que son residuos cuadráticos y los que no, posteriormente definiremos los códigos residuos cuadráticos como los generados por unos polinomios formados por medio de las particiones, aunque ambos códigos son generados por dos clases de equivalencia distintos, se demostrará que ambos son equivalentes. Por otro lado y como hemos hecho con los códigos anteriores daremos la forma que tiene su matriz generadora.

Definición 2.6.1 *Sea p número primo, entonces diremos que un entero a es* ***residuo cuadrático*** *módulo p, si existe $x \in \mathbb{N}$ tal que $x^2 \equiv a \mod p$.*

Podemos extender la definición anterior al caso de campos finitos los cuales son objeto de nuestro estudio. Sea K campo finito, con $char(K) = p$, entonces se tiene que existe un elemento primitivo, digamos λ, luego $a \in K$ es residuo cuadrático módulo p, si $a = \lambda^{2k}$ para algún $k \in \mathbb{Z}$. Sea Q el conjunto de los elementos que son residuos cuadráticos, y N el conjunto de los que no lo son.
Para poder hacer la construcción de los tipos de código que estudiaremos en esta sección, daremos un resultado básico para los conjuntos Q y N.

Proposición 2.6.2 *Sea p número primo, si Q y N denotan el conjunto de los residuos cuadráticos y los no residuos cuadráticos, entonces:*

1. $|Q| = |N| = \dfrac{p-1}{2}$.
2. $ab \in Q$, *si* $a, b \in Q$ *o* $a, b \in N$.
3. $ab \in N$, *si* $a \in Q$ *y* $b \in N$, *o* $a \in N$ *y* $b \in Q$.
4. *Si* $p = 4k + 1$, *entonces* $-1 \in Q$.
5. *Si* $p = 4k - 1$, *entonces* $-1 \in N$.

Demostración. Los puntos 1,2 y 3 son inmediatos, basta demostrar los puntos 4 y 5.
Sea λ elemento primitivo, definiendo $\beta = \lambda^{(p-1)/2}$. Entonces $\beta^2 = 1$. Por lo tanto, $(\beta + 1)(\beta - 1) = 0$, como λ es elemento primitivo $\beta \neq 1$, es decir $\beta = -1$ ■

Sea p número primo, n entero positivo no divisible por p. Por el pequeño teorema de Fermat, se tiene que existe m número entero tal que $p^m \equiv 1 \mod n$. Sea $S = \{0, 1, \ldots, n-1\}$, definimos en S la siguiente relación de equivalencia $\sim$; Sean $a, b \in S$ diremos que $a \sim b$

si $a \equiv bp^i \mod n$ para algún i, claremente es relación de equivalencia, por lo tanto, S se puede partir por medio de las clases de equivalencia descritos por $\sim$, notemos que estas tienen la siguiente forma:

$$C_s = \{a \in S | a \equiv sq^i \mod n\} = \{s, qs, \ldots, q^{m_s-1}s\}$$

Donde m_s es el menor entero tal que $sq^{m_s} \equiv s \mod n$.

Sea $\mathbb{F}_{p^m}$ extensión del campo $\mathbb{F}_p$ y sea α una raiz n-ésima primitiva de la unidad, tal que $\alpha \in \mathbb{F}_{p^m}$. Daremos un resutado fundamental para poder proceder a la construcción de los códigos residuos cuadrático.

Proposición 2.6.3 *Si C_s es la clase equivalencia bajo la relación de equivalencia $\sim$. entonces:*

$$\prod_{i \in C_s} (x - \alpha^i),$$

es el polinomio mínimo de α^s sobre $\mathbb{F}_p$.

Demostración. [22] Pag. 144. ■

Ahora procederemos a la construcción de los códigos residuo cuadrático. Sea $p \neq 2$ número primo, sea $s \in Q$ también número primo. Por el teorema de Euler, existe $m \in \mathbb{N}$ tal que $s^m \equiv 1 \mod p$. Consideremos la extensión de campo $\mathbb{F}_{s^m}/\mathbb{F}_s$, es claro que el grado de dicha extensión es m. Sea $\rho \in \mathbb{F}_{s^m}$ elemento primitivo de la extensión.
Tomando $\alpha = \rho^{(s^m-1)/p}$, claramente se tiene que α es raiz p-ésima primitiva de la unidad.

Por la elección de s se tiene que tal tomar la relación de equivalencia $\sim$ con la multiplicación de s, los conjuntos Q y N son particionados en clases. Por lo tanto, los siguientes polinomios tienen coeficientes en $\mathbb{F}_s$.

$$q(x) = \prod_{i \in Q} (x - \alpha^i) \qquad n(x) = \prod_{j \in N} (x - \alpha^j)$$

Lema 2.6.4 *Bajo las condiciones anterior y las definiciones de $n(x)$ y $q(x)$ se tiene que:*

$$x^p - 1 = (x - 1)n(x)q(x)$$

Demostración. La demostración es evidente. ■

Definición 2.6.5 *Bajo las condiciones anteriores, definimos los **códigos residuo cuadrático** F, N ,$\bar{F}$ y $\bar{N}$ de longitud p sobre el campo $\mathbb{F}_s$, como los códigos cíclicos generados por los polinomios $q(X)$,$n(x)$,$(x-1)q(x)$ y $(x-1)n(x)$ respectivamente.*

De acuerdo con la definición de código residuo cuadrático, los polinomios seguirán siendo pensados como clases de equivalencia del cociente del anillo de polinomios en una variable con coeficientes en $\mathbb{F}_s$ con el anillo generado por $x^p - 1$. Ahora haremos algunas observaciones respecto a la definición anterior.

1. $\bar{F} \subset F$ y $\bar{N} \subset N$. Lo cual es inmediato de la definición.
2. $\deg q(x) = \deg n(x) = \dfrac{p-1}{2}$. Se sigue del hecho que $|Q| = |N| = \dfrac{p-1}{2}$.
3. $\dim F$=$\dim N = \dfrac{p+1}{2}$. Esto se sigue del hecho que dado C un código cíclico de longitud n con polinomio generador $g(x)$ con $\deg g(x) = r$, entonces $\dim C = n - r$.
4. $\dim \bar{F} = \dim \bar{N} = \dfrac{p-1}{2}$.

Teorema 2.6.6 *Los códigos residuo cuadráticos F y N ($\bar{F}$ y $\bar{N}$) son equivalentes.*

Demostración. Sea $n \in N$, como p es primo entonces, existe r entero positivo tal que $nr \equiv 1 \mod p$. Como $1 \in Q$, entonces se tiene que $r \in N$. Por otro lado $q(x^n) = \prod_{i \in Q}(x^n - \alpha^i)$, del hecho que $\alpha^i = (\alpha^{ri})^n$, se tiene que $\alpha^{ri}(\ ri \in N)$ es raiz del polinomio $q(x^n)$. De lo anterior es claro que $n(x)|q(x^n)$.

Sea $\theta \in End(\mathbb{F}_s[X]/\langle x^p - 1\rangle)$, definido mediante $\theta(f(x)) = f(x^n)$. Veamos que al tomar la restricción en F se tiene una biyección con N.

Tomemos $f(x) \in F$ el cual lo podemos escribir como $f(x) = q(x)s(x)$ para algún $s(x) \in \mathbb{F}_s[X]$, entonces $\theta(f(x)) = q(x^n)s(x^n) = n(x)t(x)s(x^n)$, es decir $\theta(F) \subset N$. Por otro lado, se tiene que $1 = nr + pq$ para algún $q < 0$, notemos que se tiene la siguiente relación.

$$x = (x^{nr+pt})(1) = (x^{nr+pt})((x^p)^{-q}) = (x^n)^r.$$

De lo anterior se tiene que $\theta \in End(\mathbb{F}_s[X]/\langle x^p - 1\rangle)$, por lo tanto del teorema de la dimensión se tiene que también debe ser inyectiva. Por lo tanto, $\theta|_F$ es también biyeeción con N pues ambos espacios tienen la misma dimensión. Con lo cual se demuestra que ambos códigos son isomorfos.

Por otro lado, θ también define una permutación σ en el conjunto $\{0, 1, \ldots, p-1\}$ dado por:

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & \cdots & p-1 \\ \bar{0} & \bar{1} & \bar{2} & \cdots & \overline{p-1} \end{pmatrix}$$

Donde $\bar{i}$ es el residuo de dividir ni por p. Con lo cual se muestra que F y N son códigos equivalentes. El caso de $\bar{F}$ equivalente con $\bar{N}$ es análogo. ■

Ahora procederemos a calcular el código dual de los códigos residuo cuadrático.

Teorema 2.6.7 *Sean F, $\bar{F}$, N, $\bar{N}$ los código residuo cuadrático. Entonces:*

1.
$$\begin{array}{llll} F^{\perp} = \bar{F} & y & N^{\perp} = \bar{N} & Si \quad p = 4k-1. \\ F^{\perp} = \bar{N} & y & N^{\perp} = \bar{F} & Si \quad p = 4k+1. \end{array}$$

2. $F = \langle \bar{F}, \sum_{i=0}^{p-1} x^i \rangle$ *y* $N = \langle \bar{N}, \sum_{i=0}^{p-1} x^i \rangle$.

***Demostración*.** Sea $h(x)$ el polinomio de chequeo del código F, entonces su código dual esta generado por el polinomio $k(x) = x^{p-\frac{p-1}{2}} h(x^{-1})$, ahora haremos unas factorizaciones para expresar a $k(x)$ de una forma conveniente.

$$k(x) = x^{-1}(1-x)x^{-\frac{p-1}{2}} \prod_{j \in N} (1-\alpha^j x) = c(x-1) \prod_{j \in N} (x - \alpha^{-j})$$

$$\text{Donde } c = (-1)^{-\frac{p+1}{2}} \prod_{j \in N} \alpha^j$$

Ahora se dividirá en dos casos.

1. Si $p = 4k+1$.

   Por las propiedades que dimos al inicio de la sección se tiene que $-1 \in Q$, por lo tanto, $-j \in N$, es decir $k(x) = (x-1)\prod_{j \in N}(x - \alpha^{-j}) = (x-1)n(x)$, por lo tanto, $F^{\perp} = \bar{N}$.

2. si $p = 4k-1$.

   Del hecho que $-1 \in N$, entonces se tiene que $k(x) = (x-1)q(x)$, es decir $F^{\perp} = \bar{F}$.

El cálculo de $N^{\perp}$ es análogo.

Por otro lado, notemos que $\sum_{i=0}^{p-1} x^i = n(x)q(x)$, entonces sigue que:

$$\langle (x-1)q(x), \sum_{i=0}^{p-1} x^i \rangle \subset \langle q(x) \rangle.$$

Del hecho que $(x-1, n(x)) = 1$ existen polinomios $a(x), b(x)$ tal que $1 = (x-1)a(x) + n(x)b(x)$, entonces multiplicando lo anterior por $q(x)$, obtenemos:

$$\begin{aligned} q(x) &= (x-1)q(x)a(x) + q(x)n(x)b(x), \\ &= (x-1)q(x)a(x) + \left(\sum_{i=0}^{p-1} x^i \right) b(x). \end{aligned}$$

Lo cual demuestra la contención recíproca y por lo tanto, $\langle (x-1)q(x), \sum_{i=0}^{p-1} x^i \rangle = \langle q(x) \rangle$. Análogamente se demuestra que $\langle (x-1)n(x), \sum_{i=0}^{p-1} x^i \rangle = \langle n(x) \rangle$. ■

Del teorema anterior se puede observar claramente la relación que guardan las matrices generadoras de los códigos residuo cuadráticos.

Corolario 2.6.8 *Bajo las condiciones del teorema anterior se tienen las siguientes relaciones:*

1. *Si $\bar{G}_F$ es matriz generadora de $\bar{F}$, entonces:*

$$G_F = \left(\begin{array}{c|c} \bar{G} & \\ \hline 1 \quad 1 \cdots 1 & \end{array} \right),$$

   es la matriz generadora de F.

2. *Si $\bar{G}_N$ es matriz generadora de $\bar{N}$, entonces:*

$$G_N = \left(\begin{array}{c|c} \bar{N} & \\ \hline 1 \quad 1 \cdots 1 & \end{array} \right),$$

   es la matriz generadora de N.

Demostración. La demostración es inmediata del teorema anterior. ■

2.7. Códigos Reed-Muller

Sea $K = \mathbb{F}_q$ y $A := K[x_0, \ldots, x_n] = \oplus_{d \geq 0} A_d$ el anillo de polinomios en $n+1$ variables con coeficientes en K, con la graduación estandar.

Definición 2.7.1 *Sea X un subconjunto no vacío de $\mathbb{P}^n(K)$, se define* ***el ideal anulador graduado*** *como $I_X := \langle f \in A | f \text{ es homogéneo y } f(P) = 0 \quad \forall P \in X \rangle$. Además se define* ***la parte homogénea de grado*** *d* ***de*** *I_x como $I_X(d)$.*

Bajo las condiciones anteriores y de la definición se sigue que $I_X = \oplus_{d \geq 0} I_X(d)$.

Definición 2.7.2 *Sea X un conjunto no vacío de $\mathbb{P}^n(K)$ se define la* ***función de Hilbert*** *del anillo coordenado $R = A/I_X$ como:*

$$H_X : \mathbb{N} \cup 0 \to \mathbb{N} \cup 0$$
$$H_X(d) := \dim_K A_d/I_X(d) = \dim_K A_d - \dim_K I_X(d)$$

A continuación se expone un resultado fundamental de la función de Hilbert la cual nos ayuda determinar los parámetros básicos de los códigos tipo Reed-Muller.

Proposición 2.7.3 *Sea X subconjunto no vacío de $\mathbb{P}^n(K)$ y sea $\gamma_X := \min\{d \geq 0 | I_X(d) \neq 0\}$, entonces existe $a_X \in \mathbb{N}$ tal que:*

1. $H_X(d) = \dim_K A_d = \binom{n+d}{d}$ *si y sólo si* $d < \gamma_X$.
2. $H_X(d) < H_X(d+1) < |X|$ *si* $0 \leq d \leq a_x$.
3. $H_X(d) = |X|$ *para* $d \geq a_X + 1$

Demostración. [12] pag 166. ■

Definición 2.7.4 *Bajo la notación de la proposición anterior, se define el* ***a-invariante*** *de R, como el entero a_X.*

Definición 2.7.5 *Sean $d \in \mathbb{N} \cup \{0\}$ y $X = \{P_1, \ldots, P_m\} \subseteq \mathbb{P}^n(K)$, se define el* ***mapeo evaluación*** *mediante la siguiente asignación:*

$$ev_d : A_d \to K^m$$

$$ev_d(f) = (f(P_1), \ldots, f(P_m)).$$

Claramente el mapeo evaluación es una lineal y además, se tiene que $\ker(ev_d) = I_X(d)$.

Definición 2.7.6 *Sea X subconjunto no vacío de $\mathbb{P}^n(K)$, se define el código* ***Reed-Muller de orden d sobre X*** *como $ev_d(A_d)$, es decir, la imagen del mapeo evaluación.*

Por el primer teorema de isomorfismo se sigue que $C_X(d) = ev_d(A_d) \cong A_d/I_X(d)$, por lo tanto de la proposición anterior:

$$\dim C_X(d) = \dim A_d/I_X(d) = H_X(d)$$

A forma de ejemplo consideremos el mapeo de Segre, el cual está definido como:

$$\phi : \mathbb{P}^n(K) \times \mathbb{P}^m(K) \to \mathbb{P}^N(K),$$

$$\phi(\overline{x}, \overline{y}) = (x_0y_0, \ldots, x_0y_m, x_1y_0, \ldots, x_ny_0, \ldots, x_ny_m),$$

donde:

$$\overline{x} = (x_0, \ldots, x_n) \quad \overline{y} = (y_0, \ldots, y_m)$$

$$N = (n+1)(m+1) - 1$$

Claramente el mapeo de Segre está bien definido, es decir, dos elementos de la misma clase tienen como imagen una misma clase en $\mathbb{P}^N(K)$. Y la imagen de dicho mapeo es decir $\phi(\mathbb{P}^n(K) \times \mathbb{P}^m(K))$ se llama la ***variedad de Segre***.

$$S = \phi(\mathbb{P}^n(K) \times \mathbb{P}^m(K)) = \{\phi(P_i, Q_j) = P_{ij} \in \mathbb{P}^N(K) | P_I \in \mathbb{P}^n(K) \quad Q_j \in \mathbb{P}^m(K)\}$$

Notemos que $i \in \{1, \ldots, \ell_1\}$ y $j \in \{1, \ldots, \ell_2\}$, con $\ell_1 = |\mathbb{P}^n(K)| = \frac{q^{n+1}-1}{q-1}$ y $\ell_2 = |\mathbb{P}^m(K)| = \frac{q^{m+1}-1}{q-1}$

Por lo tanto en este caso el código tipo Reed-Muller de grado d $C_S(d)$ asociado a S es la imagen del mapeo evaluación:

$$K[Z_{00}, \ldots, Z_{ij}, \ldots, Z_{nm}] \to K^{k_1 k_2},$$

$$f \to (f(P_{11}), \ldots, f(P_{ij}), \ldots, f(P_{nm}))$$

2.8. Código generado por una gráfica bipartita completa

En el Capítulo 1 vieron las propiedades principales de una gráfica y se dio la definición de una gráfica bipartita completa, ahora veremos que existe una forma de relacionar las propiedades de la gráfica con la teoría de códigos mediante su matriz de incidencia, asociando a esta última una variedad y terminando así siendo un código de tipo de Reed-Muller asociado a una variedad que viene de una gráfica bipartita.

Sea $K_{m,n}$ una gráfica bipartita completa y sea $M = I_{K_{m,n}}$ su matriz de incidencia, como ya vimos $M \in M_{(n+m)\times(nm)}$. Por otro lado hagamos un reacomodo de los vértices de la siguiente manera $V = \{v_1, v_2, \ldots, v_m, v_{m+1}, v_{m+2}, \ldots, v_{m+n}\}$ y al conjunto de aristas lo ordenaremos de la siguiente manera:

- Las aristas $\{a_1, \ldots, a_n\}$ serán las aristas que se conectan con v_1 con los vértices de la otra partición mediante la asignación, a_1 será la arista que conecta v_1 con v_{m+1}, a_2 conecta a v_1 con v_{m+2} sucesivamente a_n conecta a v_1 con v_{m+n}.
- Las arista $\{a_{n+1}, \ldots, a_{2n}\}$ serán las aristas que se conectan con v_2 con los vértices de la otra partición mediante la asignación, a_{n+1} será la arista que conecta v_2 con v_{m+1}, a_{n+2} conecta a v_2 con v_{m+2} sucesivamente a_{2n} conecta a v_2 con v_{m+n}

Operando de esta forma ordenamos al conjunto de aristas como:

$$A = \{a_1, \ldots, a_n, a_{n+1}, \ldots, a_{2n}, \ldots, a_{nm}\},$$

por lo tanto la matriz de incidencia tiene la siguiente representación:

$$M = \begin{pmatrix} & a_1 & a_2 & a_3 & \ldots & a_{n+1} & a_{n+2} & a_{n+3} & \ldots \\ v_1 & 1 & 1 & 1 & \ldots & 0 & 0 & 0 & \ldots \\ v_2 & 0 & 0 & 0 & \ldots & 1 & 1 & 1 & \ldots \\ v_3 & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ v_{m+1} & 1 & 0 & 0 & \ldots & 1 & 0 & 0 & \ldots \\ v_{m+2} & 0 & 1 & 0 & \ldots & 0 & 1 & 0 & \ldots \\ v_{m+3} & 0 & 0 & 1 & \ldots & 0 & 0 & 1 & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix}$$

A la matriz de incidencia anterior podemos asociarle una variedad, así la variedad X derivada de la matriz de incidencia de la gráfica bipartida $K_{m,n}$ está dada por:

$$X = \{(t_1t_{m+1}, t_1t_{m+2}, \ldots, t_1t_{m+n}, t_2t_{m+1}, t_2t_{m+2}, \ldots, t_2t_{m+n}, \ldots, \\ t_mt_{m+1}, t_mt_{m+2}, \ldots, t_mt_{m+n}) | t_i \in K^* \text{ para toda } i = 1, \ldots, m+n\}$$

La representación anterior de la variedad asociada a la matriz de incidencia puede resultar un poco complicada, por lo que haremos una adaptación de lo anterior a una representación un poco más accesible, primeramente al multiplicar cada elemento por su correspondiente $t_1^{-1}t_{m+1^{-1}}$ obtener lo siguiente:

$$X = \{(1, t_{m+1}^{-1}t_{m+2}, \ldots, t_{m+1}^{-1}t_{m+n}, t_1^{-1}t_2, t_1^{-1}t_2t_{m+1}^{-1}t_{m+2}, \ldots, t_1^{-1}t_2t_{m+1}^{-1}t_{m+n},$$
$$\ldots, t_1^{-1}t_m, t_1^{-1}t_mt_{m+1}^{-1}t_{m+2}, \ldots, t_1^{-1}t_mt_{m+1}^{-1}t_{m+n} | t_i \in K^*$$
$$\text{para toda } i = 1, \ldots, m+n)\}$$

observe que el término t_{m+1}^{-1} y t_1^{-1} aparece de forma recurrente en las expresiones de nuestros vectores, por ello podemos realizar los siguientes cambios de variables:

$$t_{m+1}^{-1}t_{m+2} = x_1$$
$$t_{m+1}^{-1}t_{m+3} = x_2$$
$$\ldots$$
$$t_{m+1}^{-1}t_{m+n} = x_{n-1}$$
$$t_1^{-1}t_2 = y_1$$
$$t_1^{-1}t_3 = y_2$$
$$\ldots$$
$$t_1^{-1}t_m = y_{m-1},$$

por lo tanto podemos ver nuestra variedad como:

$$X = \{(1, x_1, x_2, \ldots, x_{n-1}, y_1, x_1y_1, x_2y_1, \ldots, x_{n-1}y_1,$$
$$y_2, x_1y_2, x_2y_2, \ldots, x_{n-1}y_2, \ldots, y_{m-1}, x_1y_{m-1}, x_2y_{m-1}, \ldots, x_{n-1}y_{m-1})$$
$$| x_1, \ldots, x_{n-1}, y_1, \ldots, y_{m-1} \in K^*\}$$

Sea $X = \{P_1, P_2, \ldots, P_r\}$ y consideremos siguiente mapeo evaluación:

$$\phi : K[Z_{00}, \ldots, Z_{(m-1)(n-1)}]_d \to K^r$$

$$\phi(f) = (f(P_1), \ldots, f(P_r))$$

Finalmente el código tipo Reed-Muller de orden d, $C_X(d)$, asociado a la matriz de incidencia de la gráfica bipartita completa $K_{n,m}$ es la imagen del mapeo evaluación anterior.

Capítulo 3

Códigos sobre anillos finitos locales de Frobenius

Es sabido que una forma de generalizar la idea de un espacio vectorial V sobre un campo K es por medio de la noción de M módulo sobre un anillo R. Por otro lado, en el segundo capítulo de la presente tesis estudiamos a los códigos cíclicos, ahora veremos una generalización de un código cíclico, para ello tomaremos γ una unidad de R y definiremos un código γ-constacíclico, en este capítulo nos enfocaremos al estudio de los anillos finitos locales de Frobenius.

A lo largo de este capítulo asumiremos que R es un anillo finito conmutativo con identidad.

3.1. Antecedentes

Definición 3.1.1 *Sean R y A anillos y M un R-módulo.*

1. *Diremos que A es **extensión** de R si $R \subseteq A$.*

2. *Sea A extensión de R y sea $I \subset R$ ideal, entonces diremos que el ideal IA es la **expansión** de I hacia A.*

3. *El ideal aniquilador de M en R se definine como:*
   $ann_R(M) := \{r \in R | rm = 0 \quad \forall m \in M\}$.

4. *Un elemento $r \in R$ se llama **regular** si no es divisor de cero.*

5. *$\mathcal{L}_R(M)$ denotará el conjunto de todos los R-submódulos de M.*

6. *Sea $M = M_0 \supset M_1 \supset \cdots \supset M_{l-1} \supset M_l = \langle 0 \rangle$ una cadena, un* ***refinamiento*** *es una cadena tal que se le agrega uno o más submódulos.*

7. *Sean dos $M = C_0 \supset C_1 \supset \cdots \supset C_{r-1} \supset C_r = \langle 0 \rangle$ y $M = D_0 \supset D_1 \supset \cdots \supset D_{s-1} \supset D_s = \langle 0 \rangle$ dos cadenas de M, entonces, son* ***cadenas isomorfas*** *si:*

   - $r = s$
   - *Existe una permutación $\sigma \in S_r$ tal que :*

   $$C_{i-1}/C_i \cong D_{\sigma(i)-1}/D_{\sigma(i)}.$$

8. *Una serie de composición de M es una cadena de R-submódulos $M = M_0 \supset M_1 \supset \cdots \supset M_{l-1} \supset M_l = \langle 0 \rangle$ tal que cada $\mathcal{L}_R(M_i/M_{i+1}) = \{M_i/M_{i+1}, \langle 0 \rangle\}$. Al número l lo llamaremos la* ***longitud*** *de M y la denotaremos por $\ell_R(M) = l$ y $l = \infty$ si no existe serie de composición con un número finito de elementos en la cadena.*

Sea R un anillo y sea $I \subset R$ ideal de de R, entonces es claro de la definición de ideal aniquilador que $I \subset ann(ann(I))$ para cualquier ideal I, por otro lado, si I es ideal trivial, es decir, $I = R$ o $I = \langle 0 \rangle$, si $I = R$ es claro que $R \subset ann(ann(R)) = R$, ahora si $I = \langle 0 \rangle$ se tiene que $ann(ann(\langle 0 \rangle)) = ann(R) = \langle 0 \rangle$, ahora supongamos que I no es ideal trivial, entonces sea $r \in ann(ann(I))$ no cero, se cumple que $rx = 0$ para todo $x \in ann(I)$ donde $xa = 0$ para todo $a \in I$, por lo tanto, se sigue que $r \in I$, con lo cual podemos concluir que $ann(ann(I)) = I$.

Teorema 3.1.2 *(Teorema de Jordan-Holder-Schreir) Sea M R-módulo, entonces cuales para quiera dos cadenas de submódulos de M, existen refinamiento de cada cadena que son isomorfos.*

Del teorema de Jordan-Holder-Schreir la longitud $\ell_R(M)$ es independiente de la serie de composición que se elija. Además si $R = K$ un campo y $M = V$ un espacio vectorial su longitud coincide con la dimensión como e.v, supongamos que $l = \dim V$ sea $\beta = \{v_1.v_2, \ldots, v_l\}$, $V = \langle v_1.v_2, \ldots, v_l \rangle \supset \langle v_1.v_2, \ldots, v_{l-1} \rangle \supset \langle v_1.v_2, \ldots, v_{l-2} \rangle \supset \langle v_1 \rangle \supset \langle 0 \rangle$, es claro que para cada i $\langle v_1.v_2, \ldots, v_{l-i} \rangle / \langle v_1.v_2, \ldots, v_{l-i-1} \rangle \cong \langle v_{l-i} \rangle$, por lo tanto, es una serie de composición, por lo tanto, $\ell_K(V) = \dim V$.

Sea R un anillo, entonces si $\mathfrak{m}$ es un ideal maximal, sabemos que $k_{\mathfrak{m}} := R/\mathfrak{m} \cong \mathbb{F}_q$ para $q = p^d$ alguna potencia de un primo p.

Proposición 3.1.3 *Sea R un anillo y M un R-módulo no cero, entonces M es módulo simple si y sólo si $M \cong R/\mathfrak{n}$ para algún $\mathfrak{n}$ ideal maximal de R.*

Demostración.
$\Rightarrow$) Sea M un R-módulo no cero, luego existe $m \in M \setminus \{0\}$, consideremos el siguiente homomorfismo de R-módulos:

$$\begin{array}{rccc} \phi: & R & \to & M \\ & r & \to & rm \end{array}$$

Claramente $m \in \phi(R)$, luego como M es módulo simple $\phi(R) = M$, por lo tanto, del primer teorema de isomorfismos $M \cong R/\ker(\phi)$, es decir $R/\ker(\phi)$ es también módulo simple, por el teorema de correspondencia se sigue que $\ker(\phi)$ es ideal maximal de R.
$\Leftarrow$) Si $M \cong R/\mathfrak{n}$, con $\mathfrak{n}$ ideal maximal de R, del teorema de correspondencia es inmediato ver que M es módulo simple.
■

Definición 3.1.4 *Sea R un anillo diremos que es **anillo local** si existe un único ideal maximal $\mathfrak{m}$.*
En dado caso escribiremos k en lugar de $k_{\mathfrak{m}}$. Y denotaremos al anillo local R como el triplete $(R, \mathfrak{m}, \mathbb{F}_q)$.

Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local finito, por lo tanto, existe $t \in \mathbb{N}$ tal que $\mathfrak{m}^t = \langle 0 \rangle$ y $\mathfrak{m}^{t-1} \neq \langle 0 \rangle$, donde t es llamado el ***índice de nilpotencia*** de $\mathfrak{m}$. Por el lema de Nakayama en R podemos formar la cadena $R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^{t-1} \supset \mathfrak{m}^t = \langle 0 \rangle$, por lo tanto, $\ell_R(R) \geq t$. Además si M es un R-módulo y $M = M_0 \supset M_1 \supset \cdots \supset M_{l-1} \supset M_l = \langle 0 \rangle$ una serie de composición, entonces como cada M_i/M_{i+1} es un R-módulo simple se tiene que $M_i/M_{i+1} \cong R/\mathfrak{m} \cong \mathbb{F}_q$. De lo anterior se concluye que $|M| = |M/M_1||M_1/M_2| \ldots |M_{l-2}/M_{l-1}||M_l| = |\mathbb{F}_q|^l = p^{dl}$.

Proposición 3.1.5 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local y M un R-módulo, entonces G genera a M si y sólo si $\bar{G}$ (la imagen de G) genera a $M/\mathfrak{m}M$ como $\mathbb{F}_q$-espacio vectorial.*

Demostración. La demostración es inmediata de la definición del isomorfismo natural de $M \to M/\mathfrak{m}M$. ■
Esta proposición nos permite definir un conjunto R-generador minimal, como veremos a continuación.

Definición 3.1.6 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo y M un R-módulo, sea $\bar{\beta}$ base para $M/\mathfrak{m}M$, entonces β es llamado un **conjunto R-generador minimal**. Denotaremos por $v_R(M) := |\bar{\beta}|$.*

De la definición anterior notemos que como $M/\mathfrak{m}M$ es un $\mathbb{F}_q$ espacio vectorial, entonces $v_R(M) = \dim_{\mathbb{F}_q}(M/\mathfrak{m}M) = \ell_{\mathbb{F}_q}(M/\mathfrak{m}M)$.

Definición 3.1.7 *Sea R un anillo finito, diremos que R es un **anillo encadenado**, si $\mathcal{L}_R(R)$ es una cadena, bajo el orden de contención usual de conjuntos.*

Proposición 3.1.8 *Sea R un anillo finito, entonces R es anillo encadenado si y sólo si R es local y su ideal maximal es local.*

Demostración.
$\Rightarrow$) Sea R anillo finito tal que es un anillo encadenado, claramente es un anillo local, pues si $\mathfrak{m}, \mathfrak{n}$ son dos ideales maximales, como R es encadenado se tiene que $\mathfrak{m} \subset \mathfrak{n}$ o $\mathfrak{m} \supset \mathfrak{n}$, lo cual implica que $\mathfrak{m} = \mathfrak{n}$. Ahora para ver que es local, supongamos que $\mathfrak{m}$ es generado por al menos dos elementos $x, y \in \mathfrak{m}$, es decir $\langle x \rangle \nsubseteq \langle y \rangle$ y $\langle y \rangle \nsubseteq \langle x \rangle$ lo cual contradice al hecho de ser encadenado, por lo tanto, $\mathfrak{m}$ es principal.
$\Leftarrow$) Recíprocamente, supongamos que R es anillo local con ideal maximal $\mathfrak{m} = \langle m \rangle$, sean I, J dos ideales cualquiera, entonces, existen $r, s \in \mathbb{N}$ tales que $I = \langle m^r \rangle$ y $J = \langle m^s \rangle$. Sin perdida de generalidad supongamos que $s \leq r$, entonces $I \subset J$, por lo tant R es anillo encadenado. ■

Definición 3.1.9 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ un anillo local finito, diremos que R es anillo de **Frobenius** si $ann_R(\mathfrak{m})$ es el único ideal minimal.*

Proposición 3.1.10 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ un anillo local finito, entonces es anillo de Frobenius si y sólo si $ann_R(\mathfrak{m})$ es un ideal simple de R.*

Demostración. La demostración se encuentra en [24]. ■

Proposición 3.1.11 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local de Frobenius, entonces $ann_R(\mathfrak{m}) = \mathfrak{m}^{t-1}$ donde t es el índice de nilpotencia de $\mathfrak{m}$.*

Demostración. La demostración es inmediata del hecho que $\mathfrak{m}^{t-1}$ es un ideal minimal. ■

Por lo tanto, observemos que si un anillo R es anillo encadenado, entonces el único ideal minimal de R es $\mathfrak{m}^{t-1}$, por lo tanto, es anillo de Frobenius.

Definición 3.1.12 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ un anillo local, y sea $^-$: $R[x] \to \mathbb{F}_q[x]$ el homomorfismo natural de anillos tal que $r \to r + \mathfrak{m}$ y $T \to T$*

1. *Un polinomio $f \in R[x]$ se dirá básico irreducible si $\bar{f}$ es irreducible en $\mathbb{F}_q[x]$.*
2. *Dos polinomios $f, g \in R[x]$ se dicen coprimos si $\langle f \rangle + \langle g \rangle = R[x]$.*

Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local, $f \in R[x]$ un polinomio básico irreducible mónico tal que $\deg(\bar{f}) = s$, entonces podemos construir el siguiente anillo $B = R[x]/\langle f \rangle = \{a_0 + a_1 T + \cdots + a_{s-1} T^{s-1} | a_i \in R\}$, notemos que claramente B es una extensión separable de R.

Proposición 3.1.13 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local, entonces la extensión B de R es anillo local con ideal maximal $\mathfrak{m}B$ y campo de cocientes $\mathbb{F}_{q^s}$.*

Demostración. Ver Teorema XVI.8 en [14] ■

Sea $\mathbb{T} \subset R$ conjunto de representantes de $\mathbb{F}_q$, entonces el conjunto $\mathbb{T}_s = \{a_0 + a_1T + \cdots + a_{s-1}T^{s-1} | a_i \in \mathbb{T}\} \subset B$ es un conjunto de representantes de $\mathbb{F}_{q^s}$.

Proposición 3.1.14 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local, sea $I \subset R$ entonces $l(I) = l(IB)$ y $(ann(I))B = ann(IB)$.*

Demostración. Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local, sea $I \subset R$ ideal y supongamos $l(I) = n$, sea $I = I_0 \supset I_1 \supset \cdots \supset I_n = \langle 0 \rangle$ serie de composición, es decir, para cada i $I_i/I_{i+1} \cong R/\mathfrak{m}$, consideremos la siguiente cadena $IB = I_0B \supset I_1B \supset \cdots \supset I_nB = \langle 0 \rangle$, para cada i se tiene que $I_i/I_{i+1} \cong R/\mathfrak{m}$ por lo tanto, i $I_iB/I_{i+1}B \cong B/\mathfrak{m}B$, como B es local con ideal maximal $\mathfrak{m}B$ se tiene que la cadena anterior es serie de composición para el anillo IB, por lo tanto, $l(IB) = l(I)$.

Por otro lado, sea $r \in (ann(I))B$, entonces $r = xb$ con $x \in ann(I)$ y $b \in B$, consideremos $s \in ann(IB)$ con $s = xb'$ elemento arbitrario, por lo tanto, al tomar su multiplicacion $rs = (ix)bb' = 0$, por lo tanto, $r \in ann(IB)$. Para ver la contención contraria, tomemos $r \in ann(IB)$, supongamos que r no pertenece al ideal $(ann(I))B$, es decir $r \neq jb'$ para todo $j \in ann(I), b' \in B$, entonces se tiene que $r(ib) \neq (jb')(ib)$ para todo $i \in I, j \in ann(I), byb' \in B$, es decir, $0 = r(ib) \neq 0$, por lo tanto, existen $j_0 \in ann(I), b_0 \in B$, tal que $r = j_0b_0 \in (ann(I))B$, con lo cual se concluye finalmente que $(ann(I))B = ann(IB)$. ■

Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local, de la proposición anterior se tiene que $\ell(ann(\mathfrak{m})) = \ell(ann(\mathfrak{m}B))$, $v_R(\mathfrak{m}) = \ell(\mathfrak{m}/\mathfrak{m}^2) = \ell(\mathfrak{m}B/\mathfrak{m}^2B) = v_B(\mathfrak{m}B)$. Es decir R es anillo de Frobenius si y sólo si $1 = \ell(ann(\mathfrak{m})) = \ell(ann(\mathfrak{m}B)) = 1$ si y sólo si B es anillo de Frobenius, más aún si $\beta = \{\alpha_1, \ldots, \alpha_r\}$ es conjunto R-generador minimal para $\mathfrak{m}$ entonces $\bar{\beta} = \{\bar{\alpha}_1, \ldots, \bar{\alpha}_r\}$ es conjunto B-generador minimal de $\mathfrak{m}B$.

Lema 3.1.15 (Lema de Hansel) *Sea R un anillo, sea $u \in R^*$ y $f \in R[x]$ tal que*

$$uf = \bar{g}_1 \ldots \bar{g}_r.$$

Para $\bar{g}_i$ polinomios coprimos a pares, entonces, existen $g_1, \ldots, g_r \in R[x]$ tales que:

1. *$g_1, \ldots, g_r$ son coprimos a pares.*
2. *$ug_i = \bar{g}_i$ para cada $1 \leq i \leq r$.*

3. $f = g_1 \dots g_r$.

Del lema anterior podemos concluir que una factorización en producto de elementos coprimos a pares en $\mathbb{F}_q[x]$ se puede entender como una factorización sobre R.

Lema 3.1.16 *Sea $(R, \mathfrak{m}, \mathbb{F}_q))$ un anillo local, $f \in R[x]$ polinomio mónico tal que $\bar{f} \in \mathbb{F}_q[x]$ es de ceros simples en la cerradura algebraica de $\mathbb{F}_q$, entonces:*

1. *Existe una familia única de polinomios básicos irreducibles coprimos a pares $f_1, f_2, \dots, f_r \in R[x]$ tal que $f = f_1 f_2 \dots f_r$.*

2. *Si $g_1, g_2, \dots, g_s \in R[x]$ son polinomios mónicos tales que $f = \prod_{i=1}^{s} g_i$, entonces $r \geq s$ y existe una partición $\{U_i\}_{i=1}^{s} \subset \{1, 2, \dots, r\}$ tal que $g_i = \prod_{j \in U_i} f_j$. Es decir, los polinomios g_i son coprimos a pares.*

3. *Si $g_1, \dots, g_k$ son polinomios basicos irreducibles tales que f es un asociado de $\prod_{i=1}^{k} g_i$, entonces $r = k$ y existe una permutación σ tal que para cada $1 \leq i \leq r$ f_i es asociado con $g_{\sigma(i)}$.*

Demostración. Sea $f \in R[x]$ polinomio mónico, sea $\bar{f_1} \dots, \bar{f_r}$ la descomposición en factores irreducibles de $\bar{f} \in \mathbb{F}_q)$, como $\bar{f}$ tiene ceros simples en la cerradura algebraica de $\mathbb{F}_q$, $\bar{f_i}$ son polinomios coprimos a pares, por lo tanto, del lema de Hansel, existe una familia $f_1, \dots, f_r \in R[x]$ de polinomios coprimos a pares, tales que $f = \prod_{i=1}^{r} f_i$. La unicidad de esta familia es consecuencia de la unicidad de la descomposición unica en factores irreducibles de $\bar{f}$, lo cual demuestra 1).

Supongamos que $f = g_1 g_2 \dots g_s$, por lo tanto, al tomar sus imagenes en $\mathbb{F}_q$, se tiene que $\bar{f} = \bar{g_1}\bar{g_2} \dots \bar{g_s}$, como los polinomios $\{\bar{f_i}\}$ son la descomposición irreducible de $\bar{f}$, implica que $r \geq s$. Por otro lado, sea para cada $1 \leq i \leq s$ sea $\bar{f_1^i}, \bar{f_2^i}, \dots, \bar{f_{l_i}^i}$ la descomposición en factores irreducibles de $\bar{g_i}$ en $\mathbb{F}_q$, tal que $\bar{g_i} = \bar{f_1^i}\bar{f_2^i} \dots \bar{f_{l_i}^i}$, entonces:

$$\bar{f_1}\bar{f_2} \dots \bar{f_r} = \bar{f} = \bar{f_1^1}\bar{f_2^1} \dots \bar{f_{l_1}^1}\bar{f_1^2}\bar{f_2^2} \dots \bar{f_{l_2}^2} \dots \bar{f_1^s}\bar{f_2^s} \dots \bar{f_{l_s}^s}$$

Además como $\bar{f}$ tiene ceros simples, todos los $\bar{f_{j_i}^i}$ son distintos para cada $1 \leq i \leq s$ y $1 \leq j \leq l_i$. Como la factorización en factores irreducibles es única, para cada $1 \leq i \leq s$ el conjunto $\{1, 2, \dots, l_i\}$ se corresponde con un subconjunto de $\{1, 2, \dots, r\}$ digamos U_i. Luego es claro que $\{U_i\}_{i=1}^{s}$ forma una partición de $\{1, 2, \dots, r\}$ tal que $g_i = \prod_{j \in U_i} \bar{f_j}$.

El último punto es inmediato del punto anterior y de la definición de polinomio básico irreducible.

■

Del lema anterior, sea $(R, \mathfrak{m}, \mathbb{F}_q)$ anillo local y tomemos $n \in \mathbb{N}$ tal que $(n, q) = 1$. Si $\gamma \in R^*$, entonces el polinomio $x^n - \gamma$ tiene raíces simples en la cerradura algebraica de $\mathbb{F}_q$ por lo tanto, se cumple el lema, pues como $(n, q) = 1$ no puede tener dos raíces de la unidad iguales pues $\mathbb{F}_q^*$ es grupo cíclico. Es decir podemos descomponer a $x^n - \gamma$ como producto de polinomios básicos irreducibles coprimos a pares en el anillo $R[x]$.

Notación 3.1.17 *1. Si h es un factor de $x^n - \gamma$ o de $x^n - \gamma^{-1}$ entonces $\hat{h} := \frac{x^n-\gamma}{h}$ o $\hat{h} := \frac{x^n-\gamma^{-1}}{h}$, según sea el caso.*

2. Para cada $a \in \mathbb{F}_{q^s}$, $a^{\mathbb{T}_s}$ denotára la representación de a en $\mathbb{T}_s$. Para cada $h = a_0 + a_1T + \cdots + a_lT^l \in \mathbb{F}_{q^s}[T]$ el polinomio $a_0^{\mathbb{T}_s} + a_1^{\mathbb{T}_s}T + \cdots + a_l^{\mathbb{T}_s}T^l \in B[T]$ será denotado por $h^{\mathbb{T}_s}$

3. El $GR(A, s)$-submódulo de M, $\langle \sum_{i=1}^{l} a_{1_i}^{\mathbb{T}_s}\alpha_i, \ldots, \sum_{i=1}^{l} a_{k_i}^{\mathbb{T}_s}\alpha_i$, será denotado por $H_{\bar{\alpha}}^{\mathbb{T}_s}$.

En este punto estamos en condiciones de poder describir la estructura algebraica de los códigos constacíclicos sobre un anillo finito de $\mathfrak{F}_3$ de longitud primo relativo con la característica del campo residual del anillo.

Teorema 3.1.18 *Sea $(R, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{F}_3$, $\gamma \in R^*$, $l\ell_R(R)$, $\bar{\alpha} = \{\alpha_1, \ldots, \alpha_{l-2}\}$ un conjunto minimal R-generador de $\gtrsim$, $\mathbb{T}$ y $\mathbb{T}_s$ definidos anterioremente. C un código γ-constacíclico de longitud n sobre R con $(n, q) = 1$. Sea $f_1, \ldots, f_r$ la descomposición única en factores mónicos básicos irreducibles coprimos a pares de $x^n - \gamma$ y sea $s_i = \deg(f_i)$. Entonces, existen una colección única de polinomios mónicos F_0, F_1, F_3, F_4, y únicos subconjuntos $U_2, U_3, \ldots, U_{l-2}$ de $[1, \ldots, r]$, y para cada $i \in \{2, \ldots, l-2\}$ y cada $u \in U_i$, una única matriz $(i-1) \times (l-2)$ sobre $\mathbb{F}_{q^{s_u}}$, tal que:*

1. $x^n - \gamma = F_0F_1F_3F_4 \prod_{u\in U_2} f_u \cdots \prod_{u\in U_{l-2}} f_u$.

2. $C = \langle \mathfrak{m}^2\hat{F}_1, \mathfrak{m}\hat{F}_3, \hat{F}_4, (H_u)_{\bar{\alpha}}^{\mathbb{T}_{s_u}} \hat{f}_u : u \in \cup_{i=2}^{l-2} U_i \rangle$.

3. $|C| = q^{l\deg(F_4)+(l-1)\deg(F_3)+\deg(F_1)+2\sum_{u\in U_2} s_u+\cdots+(l-2)\sum_{u\in U_{l-2}} s_u}$.

3.2. Códigos constacíclicos sobre anillos finitos de Frobenius locales no encadenados

Hasta ese punto hemos preparado lo necesario para poder hacer un estudio adecuado de los códigos γ-constacíclicos sobre anillos. Ahora procederemos a calcular el código dual de algunos de estos códigos.

Definición 3.2.1 *Sea R un anillo finito, $\gamma \in R^*$ y $\sigma_\gamma : R^n \to R^n$ dado por $\sigma_\gamma((a_0, a_1, \ldots, a_{n-1})) = (\gamma a_{n-1}, a_0, a_2, \ldots, a_{n-2})$. Un código γ-constacíclico de longitud n es un R-submódulo de R^n invariante bajo σ_γ.*

Es facil ver que C es código constacíclico si y sólo si su imagen en el anillo cociente $R[x]/\langle x^n - \gamma\rangle$ es un ideal. Por otra parte, denotaremos por $\mathcal{F}_3$ a la familia de anillos finitos de Frobenius locales no encadenados con índice de nilpotencia 3.

Proposición 3.2.2 *Sea $(R, \mathfrak{m}, \mathbb{F}_q)$ un anillo local, sea $\mathbb{T} \subset R$ conjunto de representantes de $\mathbb{F}_q$, M un R-módulo y $\{\alpha_1 \ldots, \alpha_l\}$ conjunto R-generador mínimal de M. Entonces para cada $0 < k < l = \dim_{\mathbb{F}_q}(M/\mathfrak{m}M)$ los R-submódulos de M entre M y $\mathfrak{m}M$ de longitud $k + \ell_R(\mathfrak{m}M)$ están en correspondencia 1-1 con las matrices $H \in M_{k\times l}(\mathbb{F}_q)$ reducidas. Más aún la matriz $H = (\bar{a_{ij}})$ se corresponde con el submódulo $\langle \sum_{i=1}^n a_{1i}\alpha_i, \ldots, \sum_{i=1}^n a_{ki}\alpha_i\rangle + \mathfrak{m}M$.*

Demostración. La matriz $H = (\bar{a_{ij}})$ se corresponde con $\langle \sum_{i=1}^l \bar{a}_{1i}\bar{\alpha}_i, \ldots, \sum_{i=1}^l \bar{a}_{ki}\bar{\alpha}_i\rangle$ como $\mathbb{F}_q$-subespacio vectorial de $M/\mathfrak{m}M$, entonces $\langle \sum_{i=1}^l a_{1i}\bar{\alpha}_i, \ldots, \sum_{i=1}^l a_{ki}\bar{\alpha}_i\rangle$ es un R-módulo de $m/\mathfrak{m}M$, y por el teorema de correspondencia existe una relación biounívoca con $\langle \sum_{i=1}^l a_{1i}\alpha_i, \ldots, \sum_{i=1}^l a_{ki}\alpha_i\rangle + \mathfrak{m}M$. ■

Sea $(R, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{F}_3$, por lo tanto, como R es anillo de Frobenius su único ideal minimal esta dado por $\mathfrak{m}^2$, es decir, para todo I ideal no trivial de R se tiene que $\mathfrak{m}^2 \subseteq I \subseteq \mathfrak{m}$, la proposición anteior nos permite calcular de manera explícita todos los ideales de R.

Corolario 3.2.3 *Sea $(R, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{f}_3$, $l = \ell_R(R)$, $\overline{\alpha} = \{\alpha_1, \ldots, \alpha_{l-2}\}$ conjunto R-generador minimal de $\mathfrak{m}$, $f \in R[x]$ polinomio básico irreducible mónico tal que $\deg f = s$, sea B la extensión separable de R generado por f. Entonces para cada $k \in \{2, \ldots, l-2\}$ están en correspondencia 1-1 con las $(k-1) \times (k-1)$ matrices irreducibles escalonadas sobre $\mathbb{F}_{q^s}$.*

Demostración. Sea $(R, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{F}_3$, sea $f \in R[x]$ polinomio mónico básico irreducible de grado s, sea B la extensión separable generada por f, en la proposición anterior tomemos $M = \mathfrak{m}B$ como B-módulo, los ideales de longitud $a + \ell(\mathfrak{m}^2B) = a + 1$ para cada $0 < a < l - 2$ están en correspondencia 1-1 con las matrices $a \times (l-2)$. Es decir los ideales de longitud $k \in \{2, \ldots, l-2\}$ están en correspondencia 1-1 con las matrices $(k-1) \times (l-2)$ sobre $\mathbb{F}_{q^s}$ ■

Ahora consideremos B como la extensión separable de $R \in \mathfrak{F}_3$ con $l = \ell_R(R)$, sea I ideal de longitud $k \in \{2, \ldots, l-2\}$ y sea $H \in M_{(k-1)\times(l-2)}[\mathbb{F}_{q^s}]$ la matriz en correspondencia con I. Como $\ell(R) = \ell(I) + \ell(ann(I))$, entonces el ideal $ann(I)$ se corresponde con una matriz $(\ell(R) - k - 1) \times (l-2)$, en este caso denotaremos por $H^\perp$.

A forma de ejemplo consideremos el siguiente anillo $R = GF(2)[X, Y, Z, W]/\langle XZ - XY, XW - XY, YZ - XY, YW - XY, ZW - XY, X^2, Y^2, Z^2.W^2\rangle$ claramente es anillo local con $\{x, y, z, w\}$ como su conjunto R-generador minimal del maximal $\mathfrak{m}$. Además se sabe que $\ell(R) = 6$. Es decir por el corolario de la proposición anterior basta con calcular las $(1 \times 4), (2 \times 4), (3 \times 4)$, son las siguientes:

1. Matrices (1×4):

   $(1, a_1, a_2, a_3), (0, 1, b_1, b_2), (0, 0, 1, c), (0, 0, 0, 1)$

2. Matrices (2×4):

   $$\begin{pmatrix} 1 & 0 & d_1 & d_2 \\ 0 & 1 & d_3 & d_4 \end{pmatrix}, \begin{pmatrix} 1 & e_1 & 0 & e_2 \\ 0 & 0 & 1 & e_3 \end{pmatrix}, \begin{pmatrix} 1 & f_1 & f_2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & g_1 \\ 0 & 0 & 1 & g_2 \end{pmatrix},$$
   $$\begin{pmatrix} 0 & 1 & h & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

3. Matrices (3×4):

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

Por lo tanto y de acuerdo con la proposición anterior los ideales del anillo R son, $\langle 0\rangle$, $\mathfrak{m}^2 = \langle xy\rangle$, $\mathfrak{m} = \langle x, y, z, w\rangle$, R, y los ideales que se encuentran entre $\mathfrak{m}^2$ y $\mathfrak{m}$.

1. Ideales de longitud 1: $\langle x + a_1y + a_2z + a_3w\rangle$, $\langle y + b_1z + b_2w\rangle$, $\langle z + cw\rangle$, $\langle w\rangle$

2. Ideales de longitud 2: $\langle x + d_1z + d_2w, y + d_3z + d_4w\rangle$, $\langle x + e_1y + e_2w, z + e_3w\rangle$, $\langle x + f_1y + f_2z, w\rangle$, $\langle y + g_1w, z + g_2w\rangle$, $\langle y + hz, w\rangle$, $\langle z, w\rangle$.

3. Ideales de longitud 3: $\langle x, m_1w, y+m_2w, z+m_3w\rangle$, $\langle x+n_1z, y+n_2z, w\rangle$, $\langle x+oy, z, w\rangle$, $\langle y, z, w\rangle$.

De esta forma hemos desarrollado las herramientas necesarias para poder describir la estructura de un código sobre el anillo de Frobenius.

Teorema 3.2.4 *Sea $(R, \mathfrak{m}, \mathbb{F}_q) \in \mathfrak{f}_3$, $\gamma \in R^*$, $\ell = \ell_R(R)$, $\overline{(\alpha)} = \{\alpha_1, \ldots, \alpha_{l-2}\}$ conjunto mínimal R-generador de $\mathfrak{m}$, luego entonces sea C un código γ-constacíclico sobre R de longitud n con $(n, q) = 1$. $f_1, \ldots, f_r$ polinomios mónicos irreducicles coprimos a pares tales que $t^n - \gamma = f_1, \ldots, f_r$ y $s_i = \deg(f_i)$. Entonces, existen únicos polinomios*

mónicos F_0, F_1, F_3, F_4. *y únicos subconjuntos* $U_2, U_3, \ldots . U_{l-2}$ *de* $[1, \ldots, r]$, *y para cada* $i \in \{2, \ldots, l-2\}$ *y cada* $u \in U$, *una única matriz* $(i-1) \times (l-2)$ *matriz reducida escalonada sobre* $\mathbb{F}_{q^{s_u}}$, *tal que:*

- $t^n - \gamma = F_0 F_1 F_3 F_4 \prod_{u \in U} f_u \cdots \prod_{u \in U_{l-2}} f_u$.
- $C = \langle \mathfrak{m}^2 \hat{F}_1, \mathfrak{m} \hat{F}_3, \hat{F}_4, (H_u)_{\bar{\alpha}}^{\mathbb{T}_{s_u}} \hat{f}_u : u \in \cup_{i=2}^{l-2}$.
- $|C| = q^{l \deg(F_4) + (l-1)\deg(F_3) + \deg(F_1) + 2\sum_{u \in U_2} s_u + \cdots + 2\sum_{u \in U_{l-2}} s_u}$.

Demostración. De lo visto anteriormente existe $\{U_0, U_1, \ldots, U_l\}$ partición de $[1, \ldots, r]$. Para cada $i \in \{2, \ldots, l-2\}$ y para cada $u \in U_i$, podemos construir entonces la correspondiente matriz reducida $(i-1) \times (l-2)$, tales que:

$$C = \langle \mathfrak{m}^2 \prod_{u \notin U_1} f_u, \mathfrak{m} \prod_{u \in U_{l-1}} f_u, \prod_{u \in U_l} f_u, (H_u)_{\mathbb{T}_{s_u}}(\bar{\alpha}) \bar{f}_u : u \in U_{i=2}^{l-2} \rangle.$$

Luego basta con tomar $F_i := \prod_{u \in U_i} f_u$ para $i \in \{0, 1\}$, $F_3 := \prod_{u \in U_{l-1}} f_u$ y $F_4 := \prod_{u \in U_l} f_u$, y la existencia queda entonces demostrada.

Por otro lado para la unicidad, sea $V_2, \ldots, V_{l-2} \subseteq [1, r]$ partición y G_0, G_1, G_3, G_4 polinomios mónicos tales que $x^n - \gamma = G_0 G_1 G_3 G_4 \prod_{v \in V_2} f_v \cdots \prod_{v \in V_{l-2}} f_v$ y $C = \langle \mathfrak{m}^2 \hat{G}_0, \mathfrak{m} \hat{G}_3, \hat{G}_4, (H_w)_{\bar{\alpha}}^{\mathbb{T}_{sp}} \hat{f}_p :$ $w \in \cap_{i=2}^{l-2} W_i$, luego existe una partición Y_0, Y_1, Y_3, Y_4 del intervalo $[1, n] \setminus [V_2 \cap \cdots \cap V_{l-2}]$, tal que $G_i = \prod_{y \in Y_i} f_{y_i}$ y los polinomios G_0, G_1, G_3, G_4 y $\{f_v | v \in \cap_{i=2}^{l-2} V_i\}$ son coprimos a pares.

Por lo tanto se tiene que:

$$R[x]/\langle x^n - \gamma \rangle \cong \langle \hat{G}_0 \rangle \oplus \langle \hat{G}_1 \rangle \oplus \langle \hat{G}_3 \rangle \oplus \langle \hat{G}_4 \rangle \oplus \oplus_{v \in V_2} \langle \hat{f}_v \rangle \oplus \cdots \oplus \oplus_{v \in V_{l-2}} \langle \hat{f}_v \rangle.$$

Además:

$$C = \langle \mathfrak{m}^2 \hat{G}_1 \rangle \oplus \langle \mathfrak{m} \hat{G}_3 \rangle \oplus \hat{G}_4 \oplus \oplus_{v \in V_2} \langle (H_v)_{\bar{\alpha}}^{\mathbb{T}_{s_v}} \hat{f}_v \rangle \oplus \cdots \oplus \oplus_{v \in V_{l-2}} \langle (H_v)_{\bar{\alpha}}^{\mathbb{T}_{s_v}} \hat{f}_v \rangle =$$

$$= \oplus_{y \in Y_1} \langle \mathfrak{m}^2 \hat{f}_y \rangle \oplus \oplus_{y \in Y_3} \langle \mathfrak{m} \hat{f}_y \rangle \oplus \oplus_{y \in Y_4} \langle \hat{f}_y \rangle \oplus \oplus_{v \in V_2} \langle (H_v)_{\bar{\alpha}}^{\mathbb{T}_{s_v}} \hat{f}_v \rangle \oplus \cdots \oplus \oplus_{v \in V_{l-2}} \langle (H_v)_{\bar{\alpha}}^{\mathbb{T}_{s_v}} \hat{f}_v \rangle$$

Lo cual muestra la unicidad. ■

Bibliografía

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, GSM **3**, American Mathematical Society, 1994.

[2] N. Alon, Combinatorial Nullstellensatz, Recent trends in combinatorics (Maŕaháza, 1995), Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29.

[3] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.

[4] E. Ballico and C Fontanari, The Horace method for error-correcting codes, Appl. Algebra Engrg. Comm. Comput. **17** (2006), no. 2, 135–139.

[5] C.A Castillo Guillen, C. Renteria-Márquez, H.Tapia-Recillas *Constacyclic codes over finite local Frobenius non-chain rings with nilpotency index 3*

[6] C.A Castillo Guillen, R. Renteria-Márquez, E. Sarmiento- Rosales, H. Tapia- Recillas *The dual of a constacyclic code, self-dual, reversible and complementary constacyclic codes over finite local Frobenius non-chain rings with nilpotency index 3*

[7] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, 1992.

[8] D. Cox, J. Little and D. O'Shea, *Using Algebraic Geometry*, Graduate Texts in Mathematics **185**, Springer-Verlag, 1998.

[9] Reinhard Diestel *Graph Theory*, Springer-Verlag, 2000 no.1-14

[10] D. Eisenbud, *The geometry of syzygies: A second course in commutative algebra and algebraic geometry*, Graduate Texts in Mathematics **229**, Springer-Verlag, New York, 2005.

[11] D. Eisenbud, D. R. Grayson, and M. Stillman, eds., *Computations in algebraic geometry with Macaulay 2*, Algorithms and Computation in Mathematics **8**, Springer-Verlag, Berlin, 2002.

[12] A.V Geramita, M. Kreuzer and L.Robbiano. *Cayley-Bacharach schemes and their canonical modules*. Transactions of the AMS, Vol.339, number 1, sept.(1993)

[13] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, Cambridge, 1986.

[14] B.R McDonald, Finite rings with identity, Marcel Dekker, New York, 1974

[15] R. Stanley, Hilbert functions of graded algebras, Adv. Math. **28** (1978), 57–83.

[16] T. Honold, Linear codes over finite chain rings, Munich Germany, 1998

[17] H. Stichtenoth, *Algebraic function fields and codes*. Universitext, Springer-Verlag, Berlin, 1993.

[18] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, University Lecture Series **8**, American Mathematical Society, Rhode Island, 1996.

[19] S. Tohăneanu, Lower bounds on minimal distance of evaluation codes, Appl. Algebra Engrg. Comm. Comput. **20** (2009), no. 5-6, 351–360.

[20] M. Tsfasman, S. Vladut and D. Nogin, *Algebraic geometric codes*: *basic notions*, Mathematical Surveys and Monographs **139**, American Mathematical Society, Providence, RI, 2007.

[21] J. H. van Lint, *Introduction to coding theory*, Third edition, Graduate Texts in Mathematics **86**, Springer-Verlag, Berlin, 1999.

[22] Lekh R. Vermani, *Elements or Algebraic Coding Theory*, Springer-Sciense+Business B.V, 1996

[23] R. H. Villarreal, *Monomial Algebras*, Monographs and Textbooks in Pure and Applied Mathematics **238**, Marcel Dekker, New York, 2001.

[24] J. Wood, Duality for modules over finite rings and applications to coding theory, Am. J. Math. 121 (1999).