UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO CONJUNTO EN CIENCIAS MATEMÁTICAS

UNAM-UMSNH

CÓDIGOS DE CONVOLUCIÓN

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRA EN CIENCIAS MATEMÁTICAS

PRESENTA:

CAROLINA VENEGAS PÉREZ

TUTOR: MUSTAPHA LAHYANE

(INSTITUTO DE FÍSICA Y MATEMÁTICAS, UMSNH)

MORELIA, MICHOACAN, JUNIO 2011

Índice general

Agradecimientos

Esta tesis se la dedicó a mis Padres, a quienes agradezco de todo corazón por su amor y ser mis primeros maestros. Gracias por su esfuerzo, de toda una vida, para que yo me encuentre en el lugar que estoy. Agradezco a mi familia por el apoyo que me brindan. A ti Salvador, que me animaste día con día hasta lograrlo.

Agradezco al Dr. Mustapha Lahyane por haber confiado en mi persona, por su infinita paciencia y por la dirección de este trabajo. A mi mesa de sinodales: Dr. Rolando Jiménez Benítez, Dr. Janitzio Mejía Huguet, Dr. Israel Moreno Mejía y Dr. Osvaldo Osuna Castro, por su disposición, sus sugerencias y sus correcciones.

Estoy agradecida con la Universidad Nacional Autónoma de México y la Universidad Michoacana de San Nicolás de Hidalgo por acogerme en sus instituciones. Gracias a todos los del Posgrado Conjunto por su apoyo.

También agradezco los apoyos brindados por el CIC-UMSNH 2011 y por el CONCYTEG.

En sí, la presente tesis es un esfuerzo en el cual, directa o indirectamente, participaron varias personas leyendo, opinando, corrigiendo, teniéndome paciencia, dando ánimo, acompañando en los momentos de crisis y en los momentos de felicidad. Gracias a todos ustedes, en particular a la M.C. Brenda Leticia De La Rosa Navarro y a el M.C. Jesús Adrián Cerda Rodríguez.

Por último, y no por eso menos importante, agradezco a Dios por ser mi fortaleza y llenar mi vida de bendiciones.

Introducción

La información es una de las posesiones más valiosas de nuestra vida cotidiana. Sin embargo, los medios usados para transmitir y almacenar la información nunca son perfectos, dando cabida a errores, es por esto, que los códigos correctores, ver los trabajos (2; 8) y sus referencias, son un elemento clave en la transmisión y almacenaje de la información.

En las últimas seis décadas, la investigación en las áreas relacionadas con la información ha desarrollado una amplia gama de técnicas matemáticas sofisticadas que pretenden dar códigos correctores, para ser aplicados. Por ejemplo, se han planteado los códigos de convolución utilizados para las transmisiones de misiones espaciales, los códigos de barras (por ejemplo, el código ISBN para los libros), por tanto, hay una amplia gama de códigos por estudiar y mejorar.

Los códigos correctores abarcan diferentes clases de códigos, particularmente: los *códigos lineales clásicos*, ver la Observación 1.12, y los *códigos de convolución*, ver los trabajos (6; 11; 14; 4; 3).

Los códigos lineales clásicos se plantearon como subespacios vectoriales de espacios vectoriales sobre un campo finito. En este trabajo de tesis se presenta, en particular, una manera más general de considerarlos, tomándolos como submódulos de módulos libres de rango finito sobre un anillo finito, estos serán etiquetados simplemente como *códigos lineales*, ver la Definición 1.11.

Los códigos de convolución fueron introducidos en 1955 por P. Elias (5), quien los formuló como una alternativa a los códigos lineales clásicos.

En 1970, G. D. Forney, Jr. (6) plantea los códigos de convolución desde el punto de vista algebraico, al considerarlos como subespacios vectoriales sobre el campo de fracciones del anillo entero de polinomios en una variable con coeficientes en un campo finito. Luego en 1993, R. J. McEliece presenta su trabajo titulado “The Algebraic Theory of Convolutional Codes” (11), donde complementa el trabajo (6) de G. D. Forney, Jr.

En 1996, J. Rosenthal, J. M. Schumacher y E.V. York proponen una manera diferente de ver a los códigos de convolución, al tomarlos como submódulos de módulos libres de rango finito sobre un anillo de polinomios en una variable con coeficientes en un campo finito, ver (14, Introducción, párrafo 4, pág. 1881) .

Esta tesis presenta también una generalización de los códigos de convolución al considerarlos como submódulos de módulos libres de rango finito sobre un dominio de ideales principales, y se pretende en la medida de lo posible extender sus *parámetros fundamentales*, ver las Definiciones 2.1 y 2.3, así, como sus *matrices generadoras*, ver la Definición 2.6.

A continuación presentaremos el esquema de investigación planteado en este trabajo de tesis:

En el primer capítulo se dan de una manera general el concepto de un código sobre un conjunto finito no vacío, ver la Definición 1.4, y algunos de sus parámetros intrínsecos, a saber, la *longitud* y el *tamaño*, ver las Definiciones 1.5 y 1.8 respectivamente. En particular, cuando el conjunto finito no vacío tiene una estructura algebraica de un anillo, daremos una clase de códigos llamados *códigos lineales*. A cada código lineal se le asocia el parámetro *distancia mínima* (Definición 1.18) dada por la distancia de Hamming, la cual entre otras propiedades permite determinar el número de errores que puede detectar y corregir nuestro código, ver (2).

Una aportación de este texto, es la generalización del concepto de *dimensión* de un código lineal, ver la Definición 1.14. La dimensión de un codigo lineal puede ser mayor que la longitud de este codigo, ver la Proposición 1.18, hecho que nunca ocurre en los códigos lineales clásicos ni tampoco en los códigos lineales definidos por J. Walker en (17). Otro aporte de este texto (ver la Proposición 1.27) es la generalización de la cota de Singleton para códigos lineales clásicos, la cual da una cota superior a la dimensión de un código lineal en términos de la longitud y distancia mínima del mismo. Así mismo se muestra la existencia de códigos que satisfacen la igualdad en dicha cota.

En este mismo capítulo, se incluirá la *matriz generadora* y la *matriz de control* de un código lineal, ver las Definiciones 1.20 y 1.21 respectivamente, las cuales permiten exponer al código en términos de estas de manera natural. Por otro lado, una matriz de control de un código lineal C es una matriz generadora de un código lineal llamado *código dual* de C. Se mostrará una relación existente entre las dimensiones de un código lineal con su código dual, ver la Proposición 1.40.

En el segundo capítulo se propone una generalización de los códigos de convolución, construyéndolos sobre dominios de ideales principales, ver la Definición 2.1. Esta generalización engloba las propuestas dadas por G.D. Forney, Jr. en (6) y por J. Rosenthal, J. M. Schumacher y E.V. York en (14). Los códigos de convolución se utilizan para proteger la información añadiendo redundancia a la misma, de manera que las palabras del código tengan la distancia mínima necesaria. Además de que estos códigos no sólo dependen del mensaje actual sino también de una cantidad finita de mensajes anteriores, así estos códigos tienen una memoria, lo que los hace más seguros. Es por ello el interés de estudiar a tales códigos.

Resulta ser que los códigos de convolución sobre un campo finito son exactamente los códigos lineales clásicos, debido a esto se quisiera dotar a los códigos de convolución del parámetro dimensión, sin embargo esto no es posible, pues no se podría aseverar que la dimensión estuviera bien definida. Por lo tanto damos el concepto de *rango* de un código de convolución (Definición 2.3), que es el equivalente a la dimensión en los códigos lineales clásicos. Sin embargo, el rango y la dimensión no coinciden salvo en el caso de los códigos de convolución sobre un campo finito.

En este mismo capítulo, se define a las *matrices generadoras* de los códigos de convolución, Definición 2.6. Además, se aporta una caracterización al conjunto de todas las matrices generadoras de un código convolucional, enunciada en la Proposición 2.11. Después, se da el concepto de *matriz de control* de un código de convolución (Definición 2.7). Y también, se aporta una caracterización al conjunto de todas las matrices de control de un código convolucional, ver la Proposición 2.19. Más aún, a partir de una matriz de control de un código de convolución C, se construye un código de convolución, llamado *código dual* de C, y se da la relación entre los parámetros de C y de su código dual, ver la Proposición 2.18.

En el tercer capítulo, nos especializamos en los códigos de convolución sobre el anillo polinomios en una variable con coeficientes en un campo finito y los códigos de convolución sobre el campo de fracciones de un anillo de polinomios en una variable con coeficientes en un campo finito, para más detalle de estos últimos, véase la Definición 3.5. Se dan las definiciones y propiedades necesarias para definir un parámetro fundamental, llamado *grado*, ver la Definición 2.12. Es por ello que se definen los *índices de Forney* (ver la Definición 3.12) para dar de manera más sencilla tal parámetro. Para determinar los índices de Forney es necesario elegir una matriz generadora *minimal* (ver la Definición 3.9), la cual cumple ser *básica* y *reducida*, (ver las Definiciones 3.7 y 3.8 y la Proposición 3.22). Un último aporte de esta tesis es dar dos caracterizaciones de las matrices básicas usando herramientas de geometría algebraica, ver el Teorema 3.12, incisos 3 y 4. Además se extienden todas estas propiedades a los códigos de convolución sobre un anillo de polinomios en una variable con coeficientes en un campo finito.

Finalmente, hemos agregado una lista de problemas abiertos de investigación, que nos gustaría resolver. Ver página 49.

Por último, desarrollamos una serie de apéndices que contienen en breve algunos conceptos y resultados relevantes que hemos utilizado a lo largo de este trabajo de tesis. Damos también un índice alfabetico y la bibliografía empleada.

Morelia, Michoacán. A 13 de Junio de 2011.

C. Venegas Pérez.

Notación y Terminología

A lo largo de este texto se considerará que un anillo siempre es conmutativo y con unidad. Los anillos y módulos se denotarán por letras mayúsculas, mientras que sus elementos por letras minúsculas. Un anillo se acostumbra denotar por A, tomaremos la notación $\mathbb{A}$ para indicar que es un anillo finito. Análogamente, F denotará un campo y $\mathbb{F}$ un campo finito. Por otro lado, un Dominio de Ideales Principales (DIP) será denotado por $\mathcal{A}$. Y el grupo multiplicativo de las matrices invertibles de tamaño $k \times k$ con entradas en $\mathcal{A}$ es denotado por $GL_k(\mathcal{A})$.

$\mathbb{N}$ y $\mathbb{Z}$ son asignados a los conjuntos de los números naturales y enteros respectivamente. Así mismo $\mathbb{Z}_+$ se refiere al conjunto de los enteros positivos, esto es, a $\mathbb{N} \cup \{0_{\mathbb{Z}}\}$.

Además la notación a usar para el campo de q elementos, con q un entero natural primo, es $\mathbb{F}_q$.

CAPíTULO 1

Códigos

Con los avances tecnológicos de esta era, la transmisión adecuada de la información es de suma importancia pues tales avances no podrían surgir sin ella. Esto sugiere una buena codificación de la información para que las alteraciones que ocurran por el ruido existente en los canales durante la transmisión puedan ser detectadas y corregidas.

En este capítulo, daremos principalmente las herramientas matemáticas de un código lineal definido sobre un anillo finito, que es una generalización de los códigos lineales definidos sobre un campo finito.

1. Concepto General de los Códigos

En esta sección introduciremos el concepto de los códigos y algunos de sus parámetros. En particular, a cada código *bloque* le asociaremos su longitud y su tamaño.

DEFINICIÓN 1.1. Un *alfabeto* Σ es un conjunto finito no vacío. Un *dígito* de Σ es un elemento del alfabeto Σ. Una *palabra* sobre Σ es una yuxtaposición de un número finito de dígitos de Σ.

EJEMPLO 1.1. El abecedario es el conjunto finito no vacío $\{a, b, c, \ldots, x, y, z\}$. Las palabras sobre este alfabeto son las palabras usuales.

EJEMPLO 1.2. El alfabeto binario $\mathbb{F}_2$ tiene por dígitos a 0 y 1. Las palabras sobre el alfabeto binario, llamadas *palabras binarias*, son secuencias finitas de 0 y 1.

Una palabra es una yuxtaposición de un número finito de dígitos, sin embargo este número puede variar dependiendo de la palabra, esto sugiere la siguiente definición.

DEFINICIÓN 1.2. La *longitud* de una palabra sobre un alfabeto es el número de dígitos que aparecen en la palabra.

EJEMPLO 1.3. La palabra "*hola*" sobre el abecedario es de longitud cuatro, mientras que la palabra "*supercalifragilisticoespialidoso*" sobre el abecedario es de longitud 32.

DEFINICIÓN 1.3. Sea Σ un alfabeto. Σ^n denota el conjunto de todas las palabras sobre Σ de longitud n con $n \in \mathbb{N}$. El conjunto de todas las palabras sobre Σ es $\cup_{n\in\mathbb{N}}\Sigma^n$ y es denotado por Σ^*.

A partir de un conjunto finito de palabras sobre un mismo alfabeto, se puede dar el concepto de código. Tal concepto se da a continuación:

DEFINICIÓN 1.4. Un *código* sobre un alfabeto Σ es un subconjunto finito no vacío de Σ^*.

EJEMPLO 1.4. Sea C el conjunto $\{al, buen, entendedor, pocas, palabras\}$. C es un código sobre el abecedario.

EJEMPLO 1.5. Un código sobre el alfabeto binario es llamado *código binario*. Sea B el conjunto $\{000, 011, 101, 110\}$. B es un código binario.

No necesariamente las palabras de un código tienen que ser de la misma longitud. Esto justifica la definición siguiente:

DEFINICIÓN 1.5. Un código C sobre un alfabeto Σ que tiene palabras de diferentes longitudes es un código de *longitud variable* . En caso contrario, el código es de *longitud fija* y la *longitud* de dicho código es la longitud de cualquiera de sus palabras.

DEFINICIÓN 1.6. Sea Σ un alfabeto. Un *código bloque* sobre Σ es un código de longitud fija.

EJEMPLO 1.6. Del Ejemplo 1.4, C es un código cuyas palabras sobre el abecedario tienen diferentes longitudes. Así, C es un código sobre el abecedario de longitud variable. Mientras que el código binario B del Ejemplo 1.5 es un código bloque de longitud 3.

PROPOSICIÓN 1.7. *Sea C un código bloque sobre un alfabeto Σ. Existe un único entero positivo n tal que C es un subconjunto de Σ^n.*

DEMOSTRACIÓN. Basta considerar a n como la longitud de dicho código bloque. □

Así, a cada código bloque le asociamos de manera natural el parámetro n, donde n es la longitud del código.

De aquí en adelante sólo consideraremos códigos bloque, así cuando se mencione código nos referimos a un código bloque.

DEFINICIÓN 1.7. Las palabras pertenecientes a un código dado son llamadas *palabras código*.

EJEMPLO 1.8. Las palabras *al, buen, entendedor, pocas* y *palabras*, son palabras código pues pertenecen al código del Ejemplo 1.4. Mientras que el resto de las palabras sobre el abecedario no son palabras código respecto a este código.

Otro parámetro relevante de los códigos es el tamaño, definido a continuación:

Definición 1.8. El *tamaño* de un código C sobre un alfabeto Σ es el número de palabras sobre Σ que pertenecen a C, es decir, la cardinalidad de C. Y se denota por $|C|$.

Ejemplo 1.9. El código C sobre el abecedario del Ejemplo 1.4 tiene tamaño $|C|$ igual a 5. Mientras que el código binario B del Ejemplo 1.5 tiene tamaño $|B|$ igual a 4.

Observación 1.9. El tamaño $|C|$ de cualquier código C sobre cualquier alfabeto es finito.

2. Tasa de Información

Un valor relevante para un código sobre un alfabeto es la *tasa de información* que definiremos enseguida:

Definición 1.10. Sea C un código sobre un alfabeto Σ de longitud n. La *tasa de información* de C es el valor

$$\frac{1}{n}\log_{|\Sigma|}|C|.$$

Y se denota por $R(C)$.

Ejemplo 1.10. La tasa de información del código binario B del Ejemplo 1.5 es

$$R(B) = \frac{1}{3}\log_2 4 = \frac{2}{3}.$$

El siguiente Lema da un acotamiento a la tasa de información de un código.

Lema 1.11. *Sea C un código sobre un alfabeto Σ de longitud n. Se sigue que $R(C)$ está dentro del rango entre 0 y 1.*

Demostración. Es una consecuencia de las desigualdades naturales, a saber $1 \leq |C| \leq |\Sigma|^n$. □

3. Códigos Lineales

En esta sección veremos una clase particular de códigos llamados *códigos lineales*, estos tienen la propiedad de que para cualquier *combinación lineal* de un número finito de palabras código es una palabra código. Para ello será necesario dotar al alfabeto de una estructura algebraica, por lo que consideraremos de aquí en adelante a los alfabetos como anillos finitos.

Usualmente se estudian a los códigos lineales sobre un campo finito, sin embargo la aportación de este texto es generalizar este concepto, tomando un anillo finito en lugar de un campo finito.

Además, en esta sección asociaremos una matriz a un código lineal y veremos como esta matriz determina completamente al código. Más aún, definiremos el código dual de un código lineal dado y algunos parámetros de este.

Para el resto del capítulo, $\mathbb{A}$ será un alfabeto que tiene una estructura algebraica de un anillo finito. En ocaciones solamente escribiremos código en lugar de código sobre $\mathbb{A}$.

Definición 1.11. Un conjunto C es un *código lineal* sobre $\mathbb{A}$ si C es un $\mathbb{A}$-submódulo de $\mathbb{A}^n$, para algún $n \in \mathbb{N}$, dicho n es la longitud de C.

Observación 1.12. Con respecto a la definición anterior, si el anillo $\mathbb{A}$ es un campo, entonces los códigos lineales sobre $\mathbb{A}$ son llamados usualmente *códigos lineales clásicos*. Para mayor información sobre dichos códigos y algunas construcciones geométricas de ellos, ver el trabajo (2).

Ejemplo 1.12. Consideremos el anillo finito $\mathbb{Z}/6\mathbb{Z}$, se cumple que $\mathbb{Z}/6\mathbb{Z}$ es un código lineal sobre $\mathbb{Z}/6\mathbb{Z}$. Además, dicho código lineal tiene longitud 1 y tamaño 6.

Ejemplo 1.13. El código binario B del Ejemplo 1.5 genera el código lineal dado por

$$\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\},$$

pues es un $\mathbb{F}_2$-submódulo de $\mathbb{F}_2^3$. Más aún su longitud es 3 y su tamaño es 4.

Ejemplo 1.14. Sea B' el conjunto

$$\{(0,0,0,1,1),(1,1,0,0,1),(1,0,1,0,1),(1,1,1,1,1)\}.$$

B' es un código binario de longitud 5 y tamaño 4, sin embargo B' no es un código lineal, pues $(0,0,0,0,0)$ no pertenece a B'.

Observación 1.13. Si C es un código lineal sobre $\mathbb{A}$ de longitud n, entonces $|C| \leq |\mathbb{A}|^n$.

La siguiente proposición nos da una caracterización de los códigos lineales.

Proposición 1.15. *Sea C un código sobre $\mathbb{A}$. C es un código lineal si, y sólo si, existe $m \in \mathbb{N}$ tal que $C \subseteq \mathbb{A}^m$ y para cualesquiera palabras código $u, v \in C$ y dígito $\lambda \in \mathbb{A}$, las palabras $u + v$ y $\lambda \cdot u$ también están en C.*

Demostración. Su prueba es elemental. □

Así, los códigos lineales son conjuntos de palabras que son cerrados bajo la adición de palabras y la multiplicación por un dígito. En particular, la palabra cero siempre pertenece a cualquier código lineal.

El concepto de longitud de un módulo es el concepto de dimensión en espacios vectoriales. Usualmente, se define la dimensión de un espacio vectorial como el número de vectores de una base. En los $\mathbb{A}$-módulos pueden no existir bases, por lo tanto, no podemos utilizar esta definición en término de bases.

Ahora, definiremos la dimensión de un código lineal.

Definición 1.14. Sea C un código lineal sobre $\mathbb{A}$. La *dimensión* de C es la longitud del módulo C sobre $\mathbb{A}$ y se denota por $\mathrm{k}(C)$.

Ejemplo 1.16. El código lineal del Ejemplo 1.12 es de dimensión $\mathrm{k}(\mathbb{Z}/6\mathbb{Z}) = 2$, pues una serie de composición del $\mathbb{Z}/6\mathbb{Z}$-módulo $\mathbb{Z}/6\mathbb{Z}$ es $\{6\mathbb{Z}\} \subsetneq 2\mathbb{Z}/6\mathbb{Z} \subsetneq \mathbb{Z}/6\mathbb{Z}$.

Ejemplo 1.17. Sea B el código binario $\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$. B es de dimensión $\mathrm{k}(B) = 2$.

Proposición 1.18. *Sea C un código lineal sobre $\mathbb{A}$ de longitud n y dimensión $\mathrm{k}(C)$. Se cumple que $\mathrm{k}(C) \leq n\,\mathrm{k}(\mathbb{A})$.*

Demostración. Dado que C es de longitud n, se tiene que $C \subseteq \mathbb{A}^n$. Por la Proposición A.16, se satisface que $\mathrm{k}(C) \leq \mathrm{k}(\mathbb{A}^n)$ y además por el Lema A.21 se cumple que $\mathrm{k}(\mathbb{A}^n) = n\,\mathrm{k}(\mathbb{A})$. Por lo tanto, $\mathrm{k}(C) \leq n\,\mathrm{k}(\mathbb{A})$. □

Corolario 1.19. *Sea C un código lineal sobre $\mathbb{A}$ de longitud n. La dimensión $\mathrm{k}(C)$ de C es finita.*

El Ejemplo 1.16 muestra claramente que si es posible dar un código lineal que satisface la igualdad en la cota de la Proposición 1.18. Más aún, tal código lineal satisface que su dimensión es mayor estrictamente que su longitud, en oposición a la propiedad que tienen los códigos lineales clásicos, en los cuales se afirma que la dimensión siempre es menor o igual que la longitud.

4. Peso y Distancia de Hamming

De una manera natural surgen las siguientes preguntas:

- ¿Qué característica podemos adjudicar a cada una de las palabras de un código lineal?,
- ¿Cómo se comparan entre ellas?

Para dar respuesta a estas preguntas introduciremos el peso de Hamming.

Definición 1.15. El *peso de Hamming* sobre $\mathbb{A}$ es la siguiente función:

$$\begin{array}{rccl} \mathrm{wt}: & \mathbb{A} & \longrightarrow & \mathbb{Z}_+ \\ & a & \longmapsto & \mathrm{wt}(a) = \begin{cases} 0_{\mathbb{Z}} \text{ si } a = 0_{\mathbb{A}}, \\ 1_{\mathbb{Z}} \text{ si } a \neq 0_{\mathbb{A}}. \end{cases} \end{array}$$

Se dice que el *peso del dígito a* de $\mathbb{A}$ es $\mathrm{wt}(a)$.

Una de las propiedades fundamentales del peso de Hamming sobre un anillo es el siguiente resultado:

LEMA 1.20. *Sea* wt *el peso de Hamming sobre* $\mathbb{A}$. *Para cualesquiera* a_1 *y* a_2 *dígitos de* $\mathbb{A}$, *se cumple que*

$$\mathrm{wt}(a_1 + a_2) \leq \mathrm{wt}(a_1) + \mathrm{wt}(a_2).$$

DEMOSTRACIÓN. Se observa que $\mathrm{wt}(b) \geq 0_{\mathbb{Z}}$ para todo $b \in \mathbb{A}$. Sean $a_1, a_2 \in \mathbb{A}$.

- Si $a_1 + a_2 = 0_{\mathbb{A}}$, entonces $\mathrm{wt}(a_1 + a_2) = 0_{\mathbb{Z}}$ y por lo tanto, $\mathrm{wt}(a_1 + a_2) \leq \mathrm{wt}(a_1) + \mathrm{wt}(a_2)$.
- Si $a_1 + a_2 \neq 0_{\mathbb{A}}$, se tiene que $a_1 \neq 0_{\mathbb{A}}$ o $a_2 \neq 0_{\mathbb{A}}$. Así, $\mathrm{wt}(a_1 + a_2) = 1 \leq \mathrm{wt}(a_1) + \mathrm{wt}(a_2)$.

□

El peso de Hamming se puede extender a cualquier $\mathbb{A}$-módulo libre de rango finito como se muestra en la siguiente definición.

DEFINICIÓN 1.16. Sea $n \in \mathbb{N}$. El *peso de Hamming* sobre $\mathbb{A}^n$ es la función wt dada por:

$$\begin{array}{rccl} \mathrm{wt}: & \mathbb{A}^n & \longrightarrow & \mathbb{Z}_+ \\ & v & \longmapsto & \mathrm{wt}(v) = \Sigma_{i=1}^{n} \mathrm{wt}(v_i). \end{array}$$

donde $v = (v_1, \ldots, v_n)$ con $v_i \in \mathbb{A}$ y $\mathrm{wt}(v_i)$ es el peso del dígito v_i, para toda $i \in \{1, \ldots, n\}$.

El siguiente resultado es una consecuencia inmediata de las propiedades del peso de Hamming sobre un anillo. Su demostración es elemental.

PROPOSICIÓN 1.21. *Sea* wt *el peso de Hamming sobre* $\mathbb{A}^n$ *con* $n \in \mathbb{N}$. *Se satisfacen las siguientes propiedades:*

1. *Para toda* $x \in \mathbb{A}^n$, $\mathrm{wt}(x) \geq 0_{\mathbb{Z}}$.
2. *Para toda* $x \in \mathbb{A}^n$, $\mathrm{wt}(x) = 0_{\mathbb{Z}}$ *si, y sólo si,* $x = 0_{\mathbb{A}^n}$.
3. *Para toda* $x, y \in \mathbb{A}^n$, $\mathrm{wt}(x + y) \leq \mathrm{wt}(x) + \mathrm{wt}(y)$.

A partir del peso de Hamming consideremos la siguiente función:

$$\begin{array}{rccl} \delta: & \mathbb{A}^n \times \mathbb{A}^n & \longrightarrow & \mathbb{Z}_+ \\ & (v, w) & \longmapsto & \delta(v, w) = \mathrm{wt}(v - w). \end{array}$$

δ dará una estructura métrica a $\mathbb{A}^n$, pues es una consecuencia del resultado siguiente.

PROPOSICIÓN 1.22. *Con la notación anterior,* δ *cumple las siguientes propiedades. Sean* u, v *y* w *elementos de* $\mathbb{A}^n$.

1. $\delta(v, w) \geq 0_{\mathbb{Z}}$.
2. $\delta(v, w) = 0_{\mathbb{Z}}$, *si y sólo, si* $v = w$.
3. $\delta(v, w) = \delta(w, v)$.
4. $\delta(v, w) \leq \delta(v, u) + \delta(u, w)$.

En particular, $(\mathbb{A}^n, \delta)$ *es un espacio métrico.*

Definición 1.17. Con la notación anterior, δ es la *distancia de Hamming* sobre $\mathbb{A}^n$.

Si v y w son elementos de $\mathbb{A}^n$, se observa que $\delta(v, w)$ es el número de posiciones en que v difiere de w.

Por otro lado, con la distancia de Hamming se induce un parámetro al código que se llamará distancia mínima del código y se definirá como sigue:

Definición 1.18. Sea C un código lineal sobre $\mathbb{A}$ de longitud n. La *distancia mínima* de C es 0_Z si C es nulo, si no, es el entero

$$min\{\delta(u, v) \mid u, v \in C,\ u \neq v\}$$

donde δ es la distancia de Hamming sobre $\mathbb{A}^n$. La distancia mínima de C se denotará por $d(C)$.

Ejemplo 1.23. La distancia mínima del código lineal $\mathbb{Z}/6\mathbb{Z}$ del Ejemplo 1.12 es $d(\mathbb{Z}/6\mathbb{Z}) = 1$.

Ejemplo 1.24. La distancia mínima del código binario lineal B del Ejemplo 1.13 es $d(B) = 2$.

Observación 1.19. El peso de Hamming sobre $\mathbb{A}^n$ se puede expresar a través de la distancia de Hamming sobre $\mathbb{A}^n$ mediante la fórmula $\mathrm{wt}(x) = \delta(x, 0)$, para toda $x \in \mathbb{A}^n$. Más aún, para cualquier código lineal C sobre $\mathbb{A}$, se cumple que $d(C) = \mathrm{wt}(C)$ donde $\mathrm{wt}(C) = 0_{\mathbb{Z}}$ si C es nulo, o sino

$$\mathrm{wt}(C) = min\{\mathrm{wt}(u) \mid u \in C,\ u \neq 0\}.$$

5. Parámetros de un Código y Detección de Errores

Hasta el momento, se tiene que siempre es posible asignar a un código lineal C sobre $\mathbb{A}$ los enteros n, T, $d(C)$ y $\mathrm{k}(C)$ donde n es su longitud, T es su tamaño, $d(C)$ es su distancia mínima y $\mathrm{k}(C)$ es su dimensión. Dichos enteros serán llamados los *parámetros fundamentales* del código lineal C. De esta manera diremos que C es un $(n, \mathrm{k}(C), d(C), T)$*−código lineal* sobre $\mathbb{A}$. Se observa que en el caso clásico, donde $\mathbb{A}$ es un campo, $T = |\mathbb{A}|^{\mathrm{k}(C)}$.

Con los parámetros mencionados anteriormente, podemos con ellos determinar cuándo un código lineal detecta errores.

Sea C un (n, k, d, T)-código lineal sobre $\mathbb{A}$. Cuando se envía una palabra código $x \in C$ y se recibe una palabra diferente, digamos z con $z \in \mathbb{A}^n$, se dice que C puede detectar errores si $z \notin C$. Se dirá que ocurrieron s errores en la transmisión si $\delta(x, z) = s$.

Teorema 1.25. *Sea C un código lineal sobre $\mathbb{A}$ de longitud n y distancia mínima d, se tiene que C puede detectar a lo más $d - 1$ errores.*

Demostración. Supongamos que se envía la palabra código $x \in C$, así el conjunto

$$\{y \in \mathbb{A}^n \mid \delta(x, y) \leq d - 1\},$$

denotado por $B(x, d - 1)$, contiene todas las posibles palabras recibidas en las que ocurren a lo más $d - 1$ errores durante la transmisión. Debido a que la distancia mínima entre cada palabra código es d, se tiene que el conjunto $B(x, d - 1)$ no contiene otras palabras código. De esto, si no ocurren más de $d - 1$ errores, entonces la palabra recibida no es una palabra código. Por lo tanto, C puede detectar a lo más $d - 1$ errores. □

Ejemplo 1.26. El código del Ejemplo 1.24 es un $(3, 2, 2, 4)$-código lineal, que sólo puede detectar a lo más un error. Mientras que el $(1, 2, 1, 6)$-código lineal del Ejemplo 1.12, no detecta errores.

6. Cota de Singleton

En esta sección se dará una generalización de la *cota de Singleton* manejada en los códigos lineales clásicos. La *Cota de Singleton* proporciona una cota superior a la dimensión de un código cuando se han fijado la longitud y la distancia mínima del código.

Proposición 1.27. ***Cota de Singleton.***
Sea C un (n, k, d, T)-código lineal sobre $\mathbb{A}$. Se cumple que

$$k \leq (n - d + 1)\,\mathrm{k}(\mathbb{A}).$$

Demostración. Sea ϕ la proyección de $\mathbb{A}^n$ sobre $\mathbb{A}^{n-d+1}$. Es claro que $\phi(C)$ es un código lineal de $\mathbb{A}^{n-d+1}$. Más aún, $\phi|_C : C \longrightarrow \mathbb{A}^{n-d+1}$ es inyectiva, pues claramente $\ker(\phi|_C) = \{0_C\}$. Por otro lado, se satisface que C y $\phi(C)$ son $\mathbb{A}$-módulos isomorfos. Por lo tanto, $k = \mathrm{k}(\phi(C)) \leq (n-d+1)\,\mathrm{k}(\mathbb{A})$. □

La Cota de Singleton es una generalización de la ya conocida cota de Singleton de los códigos lineales clásicos. En efecto, sea C un (n, k, d, T)-código lineal sobre un campo finito $\mathbb{F}$, se tiene que $k \leq (n - d + 1)\,\mathrm{k}(\mathbb{F})$ pero $\mathrm{k}(\mathbb{F}) = 1$, así $d \leq n - k + 1$, la cual es la cota de Singleton de los códigos lineales clásicos.

Retomando la notación dada para los códigos lineales clásicos, diremos que los códigos lineales cuyos parámetros alcanzan la igualdad en la Cota Singleton se llaman códigos de máxima distancia de separación o *MDS*. Así, un código MDS tiene la mayor dimensión posible que puede tener en términos de su longitud y su distancia mínima.

Ahora, exhibiremos ejemplos de códigos lineales que son códigos MDS, esto permitirá reforzar la utilidad de la Cota de Singleton, más aún, nos sustentará la existencia de códigos MDS.

EJEMPLO 1.28. El $(1, 2, 1, 6)$-código lineal sobre $\mathbb{Z}/6\mathbb{Z}$ del Ejemplo 1.12 es un código MDS.

EJEMPLO 1.29. El $(3, 2, 2, 4)$-código lineal sobre $\mathbb{F}_2$ del Ejemplo 1.24 es un código MDS.

EJEMPLO 1.30. Sea n un entero natural. Consideremos a C igual a $\mathbb{A}(1, \ldots, 1)$, donde $(1, \ldots, 1)$ es un elemento de $\mathbb{A}^n$. C es un $(n, \mathrm{k}(\mathbb{A}), n, |\mathbb{A}|)$-código lineal sobre $\mathbb{A}$ que es un código MDS.

EJEMPLO 1.31. Sean $\mathbb{A}$ un dominio entero finito y n un entero natural. Consideremos a C igual a $\mathbb{A}(1, 2, \ldots, n)$, donde $(1, 2, \ldots, n)$ es un elemento de $\mathbb{A}^n$. C es un $(n, \mathrm{k}(\mathbb{A}), n, |\mathbb{A}|)$-código lineal sobre $\mathbb{A}$ que es un código MDS.

7. Matrices Generadoras y Codificación

En esta sección, el principal objetivo es encontrar una manera eficiente para describir un código lineal exhibiendo todas las palabras código existentes en él, esto es mediante una matriz llamada *matriz generadora*. Más aún, veremos como la matriz permite la *codificación*.

DEFINICIÓN 1.20. Una *matriz generadora* de un código lineal es una matriz cuyos renglones constituyen un conjunto generador del código. Además, a cada renglón de una matriz generadora se le llama *palabra generadora*.

EJEMPLO 1.32. Para el código binario lineal del Ejemplo 1.24 una matriz generadora es

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Hasta el momento hemos asociado una matriz a un código lineal. A continuación estudiaremos como está matriz es usada para trasmitir los mensajes.

Evidenciemos como se va dando la codificación a partir de una matriz generadora.

TEOREMA 1.33. *Sea G una matriz generadora de tamaño $r \times n$, con $r \leq n$, para un código lineal C sobre $\mathbb{A}$ de longitud n. C es el conjunto de todas las palabras uG, con u en $\mathbb{A}^r$.*

Demostración. Si u es un elemento de $\mathbb{A}^r$, entonces uG es una palabra en C, ya que uG es una combinación lineal de los renglones de G. En efecto, si $u = (a_1, \ldots, a_r)$ para algunos $a_1, \ldots, a_r \in \mathbb{A}$ y g_i es el i-ésimo renglón de G para toda $i \in \{1, \ldots, r\}$, entonces $uG = a_1 g_1 + \ldots + a_r g_r$.
Por otro lado, ya que toda palabra v en C es una combinación lineal de las palabras generadoras, entonces $v = uG$ para algún u en $\mathbb{A}^r$. □

Por el Teorema 1.33, un código lineal C sobre $\mathbb{A}$ está determinado por alguna matriz generadora G de tamaño $r \times n$, con $r \leq n$, como

$$C = \{uG \mid u \in \mathbb{A}^r\}.$$

El valor n fija la longitud de las *palabras código* uG en $\mathbb{A}^n$ para algún elemento u de $\mathbb{A}^r$ llamado *palabra información*, así r mide la cantidad de información, sin redundancia, que existe en las palabras código. A este proceso de transformación le llamamos *codificación*.

Otra matriz que permite de manera eficiente describir un código lineal exhibiendo todas las palabras existentes en el, es la matriz de control, definida a continuación.

Definición 1.21. Sea C un código lineal con una matriz generadora G de tamaño $r \times n$ con $r < n$. Sea H una matriz de tamaño $(n - r) \times n$ con entradas en $\mathbb{A}$. H es una *matriz de control* de C si cumple que

$$C = \{v \in \mathbb{A}^n \mid vH^t = 0_{\mathbb{A}^{n-r}}\}.$$

Observación 1.22. A consecuencia de la definición anterior se cumple que $GH^t = 0$.

Ejemplo 1.34. Para el código binario lineal del Ejemplo 1.32 una matriz de control es

$$H = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

La matriz de control permite calcular la distancia mínima del código.

Proposición 1.35. *Sea C un (n, k, d, T)-código lineal no nulo con una matriz de control H de tamaño $(n - r) \times n$. La distancia mínima d de C coincide con el número mínimo de columnas de H que son linealmente dependientes.*

Demostración. Como la distancia mínima es d, entonces existe v en C no nulo con peso igual a d. $v \in C$ si, y sólo si, $vH^t = 0_{A^{n-r}}$. Así, las columnas de H que se corresponden con las d posiciones de v donde no son cero, deben ser linealmente dependientes. Es decir, hay d columnas linealmente dependientes en H. Más aún, no podría haber menos de d columnas dependientes sino se contradice que d es la distancia mínima de C. □

Otra aplicación de la matriz de control es la de determinar el código dual de un código lineal dado, que será visto en la siguiente sección.

8. Código Dual

A partir de un conjunto finito de palabras y con el concepto de ortogonalidad, se construye un código lineal llamado código dual, veamos tal construcción. Para ello definamos el producto escalar y ortogonalidad entre palabras, para después dar de manera natural un código lineal.

Definición 1.23. El *producto escalar* en $\mathbb{A}^n$ es la función

$$\begin{array}{rccc} \cdot : & \mathbb{A}^n \times \mathbb{A}^n & \longrightarrow & \mathbb{A} \\ & (v, w) & \longmapsto & v \cdot w = v_1 w_1 + \ldots + v_n w_n, \end{array}$$

donde $v = (v_1, \ldots, v_n)$ y $w = (w_1, \ldots, w_n)$.

Ahora aplicaremos los conceptos de ortogonalidad de álgebra lineal a los códigos lineales.

Las palabras v y w de longitud n son *ortogonales* si $v \cdot w = 0_{\mathbb{A}}$. Para un conjunto S de palabras de longitud n, diremos que v es *ortogonal al conjunto* S si $v \cdot w = 0_{\mathbb{A}}$ para todo $w \in S$. El conjunto de todas las palabras ortogonales al conjunto S es denotado por $S^{\perp}$ y es llamado el *complemento ortogonal* de S.

Así, para cualquier subconjunto S de $\mathbb{A}^n$, el complemento ortogonal $S^{\perp}$ es un $\mathbb{A}$-submódulo de $\mathbb{A}^n$. Es decir, $S^{\perp}$ es un código lineal. Se induce así la siguiente definición.

Definición 1.24. Sea C un código lineal sobre $\mathbb{A}$. El *código dual* de C es el complemento ortogonal de C, denotado por $C^{\perp}$.

Ejemplo 1.36. El código dual del código lineal del Ejemplo 1.12 es $C^{\perp} = \{6\mathbb{Z}\}$.

Ejemplo 1.37. El código dual del código lineal del Ejemplo 1.13 es $C^{\perp} = \{(0,0,0), (1,1,1)\}$.

La caracterización de los elementos de un código dual se muestra en la siguiente proposición.

Proposición 1.38. *Sea G una matriz generadora de tamaño $r \times n$ de un código lineal C de longitud n, se cumple que*

$$C^{\perp} = \{v \in \mathbb{A}^n \mid vG^t = 0_{\mathbb{A}^r}\}.$$

Demostración. Sea $v \in \mathbb{A}^n$. Hay que tener en cuenta que v es ortogonal a un submódulo si, y sólo si, es ortogonal a los elementos que lo generan, así:

$$\begin{array}{rcl} v \in C^{\perp} & \Leftrightarrow & v \text{ es ortogonal a cada fila de } G \\ & \Leftrightarrow & vG^t = 0_{\mathbb{A}^r}. \end{array}$$

□

A partir de un código dual podemos aportar una matriz de control a nuestro código lineal dado.

Proposición 1.39. *Sea C un código lineal sobre $\mathbb{A}$. Una matriz generadora de $C^\perp$ es una matriz de control para C.*

Demostración. Sea H una matriz generadora de $C^\perp$. Por la Proposición 1.38, se deduce que $H^tG = 0$, donde G es una matriz generadora de C. Así H es una matriz de control de C. □

Como hemos visto, para todo código lineal, su código dual tiene la misma longitud. Esto nos hace preguntarnos sobre la relación entre la dimensión de un código lineal y la dimensión de su código dual. Tal relación se enuncia en la siguiente proposición:

Proposición 1.40. *Sea C un código lineal sobre $\mathbb{A}$ de longitud n. Se satisface que*

$$\mathrm{k}(C^\perp) = \mathrm{k}(\mathbb{A}^n) - \mathrm{k}(C) + \mathrm{k}(C \cap C^\perp),$$

donde $C^\perp$ es el código dual de C.

Demostración. Sea G una matriz generadora de C de tamaño $r \times n$ cuyos renglones son linealmente independientes sobre $\mathbb{A}$. Considérese la aplicación $\mathbb{A}$-lineal

$$\begin{array}{rccc} \phi: & \mathbb{A}^n & \longrightarrow & \mathbb{A}^r \\ & v & \longmapsto & \phi(v) = vG^t. \end{array}$$

Se satisface que $\ker(\phi) = C^\perp$. Así, se construye la siguiente sucesión exacta de $\mathbb{A}$-módulos:

$$0 \longrightarrow C^\perp \longrightarrow \mathbb{A}^n \longrightarrow \mathrm{Im}(\phi) \longrightarrow 0.$$

Debido al Teorema A.19 y a que la dimensión $\mathrm{k}(\mathbb{A})$ de $\mathbb{A}$ es finita, se cumple que

$$\mathrm{k}(\mathrm{Im}(\phi)) = \mathrm{k}(\mathbb{A}^n) - \mathrm{k}(C^\perp).$$

Por otro lado, la aplicación ϕ induce la siguiente aplicación A-lineal ϕ', dada por:

$$\begin{array}{rccc} \phi': & C & \longrightarrow & \mathrm{Im}(\phi) \\ & v & \longmapsto & \phi'(v) = vG^t. \end{array}$$

ϕ es sobreyectiva. En efecto, sea $x \in \mathrm{Im}(\phi')$. Por demostrar que existe un elemento v de C tal que $\phi'(v) = x$. Dado que x es un elemento de $\mathrm{Im}(\phi')$, existe un elemento w en $\mathbb{A}^n$ tal que $x = wG^t$. Basta pues con demostrar que existe $u \in \mathbb{A}^r$ tal que $\phi'(uG) = wG^t$.

Como G tiene rango maximo por renglones, se tiene que GG^t tiene rango maximal, por lo tanto es invertible. Consideremos a u igual a $wG^t(GG^t)^{-1}$. Así,

$$\begin{aligned}\phi'(uG) &= \phi'(wG^t(GG^t)^{-1}G)\\ &= wG^t(GG^t)^{-1}GG^t = wG^t.\end{aligned}$$

Además, se cumple que $\ker(\phi') = C \cap C^\perp$, construyendose así la siguiente sucesión exacta de $\mathbb{A}$-módulos:

$$0 \longrightarrow C \cap C^\perp \longrightarrow C \longrightarrow \mathrm{Im}(\phi) \longrightarrow 0.$$

Por lo tanto, $\mathrm{k}(C) = \mathrm{k}(C \cap C^\perp) + \mathrm{k}(\mathrm{Im}(\phi))$. Al sustituir $\mathrm{k}(\mathrm{Im}(\phi))$ por $\mathrm{k}(\mathbb{A}^n) - \mathrm{k}(C^\perp)$, se concluye que

$$\mathrm{k}(C^\perp) = \mathrm{k}(\mathbb{A}^n) - \mathrm{k}(C) + \mathrm{k}(C \cap C^\perp).$$

□

Ejemplo 1.41. Consideremos C igual a $\mathbb{F}_2(1,0,1)$ donde $(1,0,1) \in \mathbb{F}_2^3$. C es un $(3,1,2,2)$-código lineal sobre $\mathbb{F}_2$. La dimensión del dual de C es $\mathrm{k}(C^\perp) = 2$ pues $C \cap C^\perp = C$. Más aún, $C^\perp = \mathbb{F}_2(1,0,1) + \mathbb{F}_2(1,1,1)$ el cual es un $(3,2,2,4)$-código lineal sobre $\mathbb{F}_2$ donde $(1,1,1)$ es un elemento de $\mathbb{F}_2^3$.

Por consiguiente, se tiene el siguiente resultado:

Corolario 1.42. *Si C es un (n,k)-código lineal sobre $\mathbb{A}$ tal que $C \cap C^\perp = \{0_{\mathbb{A}^n}\}$, entonces*

$$\mathrm{k}(C^\perp) = \mathrm{k}(\mathbb{A}^n) - \mathrm{k}(C).$$

CAPíTULO 2

Códigos de Convolución

En el anterior capítulo se definió a los códigos lineales como submódulos de módulos libres de rango finito sobre un anillo finito. Si dejamos de pedir que el anillo sea finito, pero en cambio, pedimos que el anillo sea un dominio de ideales principales, entonces estaremos proponiendo una generalización (ver Definición 2.1) de los *Códigos de Convolución*, ver (6) y (14).

En este capítulo se propondrá tal generalización, además se tratará de ir conservando en la medida de lo posible, las propiedadades que tienen los códigos de convolución, definidos en (6) y (14, Introducción, párrafo 4, pág. 1881). El interés de esta generalización es porque los códigos de convolución se destacan por su fácil implementación así como su óptima decodificación, ver (16).

Durante el capítulo exhibiremos que dicha propuesta es en efecto una generalización de las definiciones usuales, tal como las plantearon G. D. Forney, Jr. en (6) y los autores J. Rosenthal, J. M. Schumacher y E.V. York en (14). En donde estos últimos, por ejemplo, consideran a los códigos de convolución cómo submódulos de módulos libres de rango finito sobre un anillo de polinomios en una variable con coeficientes en un campo finito.

1. Concepto de los Códigos de Convolución

En esta sección se definen los códigos de convolución, y se dan algunos de sus parámetros fundamentales: *longitud* y *rango*. Así como la relación existente entre estos parámetros.

A lo largo de este capítulo, $\mathcal{A}$ será un dominio de ideales principales.

Definición 2.1. Sean n un entero natural y C un subconjunto de $\mathcal{A}^n$. C es un *código de convolución* sobre $\mathcal{A}$ de *longitud* n si C es un $\mathcal{A}$-submódulo de $\mathcal{A}^n$.

Los códigos de convolución también son conocidos como *códigos convolucionales*.

Ejemplo 2.1. Sea $n \in \mathbb{N}$. $\mathbb{Z}^n$ es un código de convolución sobre $\mathbb{Z}$ de longitud n.

Ejemplo 2.2. Sean $(1,1,0)$ y $(0,1,0)$ elementos de $\mathbb{Z}^3$. Sea C igual a $\mathbb{Z}(1,1,0) + \mathbb{Z}(0,1,0)$. C es un código de convolución sobre $\mathbb{Z}$ de longitud 3, pues es un $\mathbb{Z}$-submódulo de $\mathbb{Z}^3$.

Observación 2.2. Los códigos de convolución pueden ser conjuntos infinitos si el dominio de ideales principales sobre el cual se definen es infinito, por lo tanto no entran en la categoría de códigos expuesta en el primer capítulo.

Aunque no podamos ver a los códigos de convolución como códigos lineales, si podemos definir parámetros tal como lo hacíamos anteriormente en los códigos lineales. Por ejemplo, ya definimos la longitud. Un parámetro que es fundamental para los códigos lineales es la dimensión, que su equivalente en códigos de convolución es llamado *rango*. Sin embargo, esté no coincide con la dimensión, salvo en el caso, de haber construido al código de convolución sobre un campo finito, véase la Proposición 2.6.
A partir de la siguiente proposición veremos que es posible definir el rango.

Proposición 2.3. *Sea r un entero natural. Cualquier $\mathcal{A}$-submódulo M de $\mathcal{A}^r$ es libre de rango finito menor o igual a r.*

Demostración. Se mostrará por inducción sobre r.

Supongamos $r = 1$.

Sea M un $\mathcal{A}$-submódulo de $\mathcal{A}$, así M es un ideal de $\mathcal{A}$. Se tiene que existe $c \in \mathcal{A}$ tal que $M = \mathcal{A}c$, pues $\mathcal{A}$ es un dominio de ideales principales (DIP, en breve). Si $c = 0_{\mathcal{A}}$, entonces $M = \{0_{\mathcal{A}}\}$, por lo tanto $M = \mathcal{A}^0$.
Si $c \neq 0_{\mathcal{A}}$, entonces la siguiente aplicación $\mathcal{A}$-lineal es biyectiva:

$$\begin{array}{rccc} \mu_c : & \mathcal{A} & \longrightarrow & M \\ & \alpha & \longmapsto & \alpha c. \end{array}$$

En efecto, μ_c es sobreyectiva pues $\mathrm{Im}(\mu_c) = \mathcal{A}c$, sólo resta demostrar que μ_c es inyectiva.
Claramente se cumple que $\ker(\mu_c) = \mathrm{Ann}_{\mathcal{A}}(c)$. Dado que $c \neq 0_{\mathcal{A}}$ y $\mathcal{A}$ es un dominio entero, se sigue que $\mathrm{Ann}_{\mathcal{A}}(c) = \{0_{\mathcal{A}}\}$. Por lo tanto, $M \cong \mathcal{A}^1$.
Así, los $\mathcal{A}$-submódulos de $\mathcal{A}$ son libres de rango 0 o 1.

Ahora supongamos que r es un entero mayor o igual que 2. Asumamos por hipótesis de inducción que cualquier $\mathcal{A}$-submódulo de $\mathcal{A}^s$ es libre de rango finito menor o igual que s, para toda $s \in \{1, \ldots, r-1\}$.

Sea $\{e_i \mid i = 1, \ldots, r\}$ la base canónica de $\mathcal{A}^r$. Sea M un $\mathcal{A}$-submódulo de $\mathcal{A}^r$, se cumple que

$$\begin{aligned} M &= M \cap \mathcal{A}^r \\ &= (M \cap \mathcal{A}e_1) \oplus (M \cap (\mathcal{A}e_2 \oplus \ldots \oplus \mathcal{A}e_r)). \end{aligned}$$

Donde $M \cap \mathcal{A}e_1$ es un $\mathcal{A}$-submódulo de $\mathcal{A}e_1$, así $M \cap \mathcal{A}e_1$ es isomorfo a un $\mathcal{A}$-submódulo de $\mathcal{A}$, por hipótesis de inducción se deduce que $M \cap \mathcal{A}e_1$ es libre de rango finito menor o igual que 1. Análogamente $M \cap (\mathcal{A}e_2 \oplus \ldots \oplus \mathcal{A}e_r)$ es un $\mathcal{A}$-submódulo de $\mathcal{A}e_2 \oplus \ldots \oplus \mathcal{A}e_r$, tenemos que $M \cap (\mathcal{A}e_2 \oplus \ldots \oplus \mathcal{A}e_r)$ es isomorfo a un $\mathcal{A}$-submódulo de $\mathcal{A}^{r-1}$, aplicando la hipótesis de inducción se cumple que $M \cap (\mathcal{A}e_2 \oplus \ldots \oplus \mathcal{A}e_r)$ es libre de rango finito menor o igual que $r-1$.
Dado que la suma directa finita de módulos libres de rangos finitos es libre de rango finito, así M es libre de rango finito menor o igual que r. □

Se infiere de la Proposición 2.3, que cada $\mathcal{A}$-submódulo de $\mathcal{A}^n$ está determinado por un entero que pertenece al conjunto $\{0, 1, \ldots, n\}$. Tal valor es único, es por eso que podemos enunciar la siguiente definición.

Definición 2.3. Sea C un código de convolución sobre $\mathcal{A}$ de longitud n. El *rango* de C es el rango de C como $\mathcal{A}$-submódulo de $\mathcal{A}^n$, y se denota por k.

Ejemplo 2.4. El código de convolución de longitud 3 del Ejemplo 2.2 es de rango 2.

Observación 2.4. De la Proposición 2.3 se concluye que siempre el rango de un código de convolución está acotado superiormente por su longitud.

Notación 2.5. Sea C un código de convolución sobre $\mathcal{A}$ de longitud n y rango k. Diremos que C es un (n, k)-código de convolución sobre $\mathcal{A}$.

Ejemplo 2.5. Sea $n \in \mathbb{N}$. $\mathbb{Z}^n$ es un (n, n)-código de convolución sobre $\mathbb{Z}$.

Proposición 2.6. *Sea C un (n, k)-código de convolución sobre un dominio de ideales principales finito $\mathcal{A}$. Se cumple que C es un $(n, \mathrm{k}(C))$-código lineal sobre $\mathcal{A}$. Además, $\mathrm{k}(C)$ es mayor o igual que k.*

Demostración. Como C es isomorfo a $\mathcal{A}^k$, por el Lema A.21 se tiene que $\mathrm{k}(C) = k \cdot \mathrm{k}(\mathcal{A})$ donde $\mathrm{k}(C)$ y $\mathrm{k}(\mathcal{A})$ denotan las dimensiones de C y de $\mathcal{A}$, respectivamente. Por otro lado, siempre se cumple que $\mathrm{k}(\mathcal{A}) \geq 1$, así $\mathrm{k}(C) \geq k$. □

De acuerdo a la notación de la proposición anterior, la dimensión $\mathrm{k}(C)$ de C es mayor o igual que el rango k de C. Estos valores son los mismo cuando la dimensión $\mathrm{k}(A)$ de $\mathcal{A}$ es uno, esto ocurre si, y sólo si, $\mathcal{A}$ es un campo finito (ver el Lema A.22).

2. Representación Matricial

En esta sección veremos que existe una relación biunívoca entre los códigos de convolución y las matrices, tanto es así, que a cada código de convolución le corresponde una *representación*

matricial y a la vez, cada matriz con entradas en el dominio de ideales principales, tal que sus renglones son linealmente independientes determina un código de convolución. Por lo que cada código de convolución tiene asociado una matriz que le determina. Además en la sección se introducirá el concepto de *código dual* de los códigos de convolución, y veremos cómo este está asociado con las *matrices generadoras* y las *matrices de control* del código de convolución.

Sea C un (n,k)-código de convolución sobre $\mathcal{A}$. Se cumple que C es un $\mathcal{A}$-submódulo de $\mathcal{A}^n$, más aún, es isomorfo a $\mathcal{A}^k$ como $\mathcal{A}$-módulo. Por lo que existen un isomorfismo entre $\mathcal{A}^k$ y C, denotado por φ, y un morfismo ι dado por:

$$\begin{array}{rccc} \iota: & C & \longrightarrow & \mathcal{A}^n \\ & v & \mapsto & \iota(v) = v. \end{array}$$

De manera inmediata, se tiene que el morfismo $(\iota \circ \varphi) : \mathcal{A}^k \longrightarrow \mathcal{A}^n$ es inyectivo. Más aún, su imagen es C. Como el morfismo $\iota \circ \varphi$ tiene una representación matricial, digamos G, se sigue que C tiene naturalmente asociada la matriz G. Por otro lado, si existe un morfismo inyectivo Ψ de $\mathcal{A}$-módulos con una representación matricial P, dado por:

$$\begin{array}{rccc} \Psi: & \mathcal{A}^k & \longrightarrow & \mathcal{A}^n \\ & u & \mapsto & \Psi(u) = uP, \end{array}$$

entonces la imagen de Ψ es un (n,k)-código de convolución sobre $\mathcal{A}$. Así, P está asociada de manera clara a un código de convolución de longitud n y rango k. Todo esto da pie a la siguiente definición.

Definición 2.6. Sea C un (n,k)-código de convolución sobre $\mathcal{A}$. Una *matriz generadora* de C es una matriz G de tamaño $k \times n$ con entradas en $\mathcal{A}$ tal que G es una representación matricial de un morfismo inyectivo $\mathcal{G}$ de $\mathcal{A}$-módulos, dado por:

$$\begin{array}{rccc} \mathcal{G}: & \mathcal{A}^k & \longrightarrow & \mathcal{A}^n \\ & u & \mapsto & \mathcal{G}(u) = uG \end{array}$$

donde la imagen $\mathrm{Im}(\mathcal{G})$ de $\mathcal{G}$ es igual a C. Tal morfismo $\mathcal{G}$ es llamado *codificador* asociado a G.

Ejemplo 2.7. Una matriz generadora del código de convolución del Ejemplo 2.1 es

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ejemplo 2.8. Una matriz generadora del código de convolución del Ejemplo 2.2 es

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Una matriz generadora de un código de convolución permite definir de manera explícita a éste.

Proposición 2.9. *Sea C un (n,k)-código de convolución sobre $\mathcal{A}$ con una matriz generadora G. Se cumple que*

$$C = \{uG \mid u \in \mathcal{A}^k\}.$$

Demostración. Sea $\mathcal{G}$ el codificador asociado a G. Se tiene que $\mathrm{Im}(\mathcal{G}) = C$, pero $\mathrm{Im}(\mathcal{G}) = \{uG \mid u \in \mathcal{A}^k\}$, así concluimos con lo deseado. □

Con la notación dada en la Proposición 2.9, el tomar un elemento u de $\mathcal{A}^k$, que llamaremos *palabra información*, y transformarla en uG, un elemento que pertenece a C, llamada *palabra código*, es un proceso llamado *codificación*.

Debido a esto nos gustaría poder determinar cuándo una matriz es una matriz generadora de un código de convolución, más aún, nos gustaría determinarla sin necesidad de usar su codificador asociado y sólamente empleando a la matriz. Por eso enunciamos el siguiente teorema que nos permite caracterizar a las matrices generadoras de un código de convolución.

Teorema 2.10. *Sea C un (n,k)-código de convolución sobre $\mathcal{A}$ y sea G una matriz de tamaño $k \times n$ con entradas en $\mathcal{A}$. Las siguientes afirmaciones son equivalentes:*

1. *G es una matriz generadora de C.*
2. *Los renglones de G son linealmente independientes sobre $\mathcal{A}$ y generan a C como $\mathcal{A}$-módulo.*
3. *G es una matriz invertible por la derecha en $\mathcal{A}$ y $C = \{uG \mid u \in \mathcal{A}^k\}$.*

Demostración.

- Supongamos que G es una matriz generadora de C, por verificar que sus renglones son linealmente independientes sobre $\mathcal{A}$ y que tales generan a C como $\mathcal{A}$-módulo.
  Consideremos a g_i como el i-ésimo renglón de G para toda $i \in \{1, \ldots, k\}$. Sabemos que para todo elemento $u = (u_1, \ldots, u_k)$ de $\mathcal{A}^k$, uG es igual a $u_1g_1 + \ldots + u_kg_k$.
  Más aún, $u_1g_1 + \ldots + u_kg_k = 0_{\mathcal{A}^n}$ si, y sólo si, $uG = 0_{\mathcal{A}^n}$.
  Supongamos que $u_1g_1 + \ldots + u_kg_k = 0_{\mathcal{A}^n}$, para algunos elementos $u_1, \ldots, u_k$ de $\mathcal{A}$. Dado que G es matriz generadora de C, el codificador asociado a G es inyectivo, por lo tanto $u = 0_{\mathcal{A}^k}$.
  Así, $\{g_1, \ldots, g_k\}$ es un conjunto linealmente independiente sobre $\mathcal{A}$. Ahora veamos que tal conjunto genera a C como $\mathcal{A}$-módulo. Obsérvese que

$$\begin{aligned} \mathcal{A}g_1 + \ldots + \mathcal{A}g_k &= \{u_1g_1 + \ldots + u_kg_k \mid (u_1, \ldots, u_k) \in \mathcal{A}^k\} \\ &= \{uG \mid u \in \mathcal{A}^k\}, \end{aligned}$$

y de la Proposición 2.9 se tiene que $C = \mathcal{A}g_1 + \ldots + \mathcal{A}g_k$.

- Demos por hecho la Afirmación 2, por demostrar que se cumple la Afirmación 3.
  Claramente se concluye que $C = \{uG \mid u \in \mathcal{A}^k\}$. Basta mostrar que G es invertible por la derecha en $\mathcal{A}$, es decir, que existe un elemento P de $M_{n\times k}(\mathcal{A})$ tal que $GP = I_k$. Como G tiene rango maximal por renglón, se tiene que GG^t es una matriz cuadrada que tiene rango maximal, por lo tanto es invertible. Se propone a P como $G^t(GG^t)^{-1}$, obteniendo lo deseado.
- De suponer la Afirmación 3 se desea concluir la Afirmación 1.
  Consideremos el codificador $\mathcal{G}$ asociado a G, dado por:

$$\begin{array}{rccc} \mathcal{G}: & \mathcal{A}^k & \longrightarrow & \mathcal{A}^n \\ & u & \mapsto & \mathcal{G}(u) = uG. \end{array}$$

  Por verificar que $\mathcal{G}$ es inyectivo (su núcleo $\ker\mathcal{G}$ es igual a $\{0_{\mathcal{A}^k}\}$) y su imagen $\mathrm{Im}(\mathcal{G})$ es igual a C. En efecto, sea u un elemento de $\mathcal{A}^k$.

$$\begin{array}{rcl} u \in \ker\mathcal{G} & \Leftrightarrow & \mathcal{G}(u) = 0_{\mathcal{A}^n} \\ & \Leftrightarrow & uG = 0_{\mathcal{A}^n}. \end{array}$$

  Por hipótesis existe un elemento P de $M_{n\times k}(\mathcal{A})$ tal que $GP = I_k$. Así,

$$\begin{array}{rcl} uG = 0_{\mathcal{A}^n} & \Rightarrow & uGP = 0_{\mathcal{A}^n}P \\ & \Rightarrow & u = 0_{\mathcal{A}^k}. \end{array}$$

  Implicando que $\ker(\mathcal{G}) \subseteq \{0_{\mathcal{A}^k}\}$. Por otro lado, siempre se cumple que $\{0_{\mathcal{A}^k}\} \subseteq \ker(\mathcal{G})$. Por lo tanto, $\mathcal{G}$ es inyectivo. Además, se tiene que $\mathrm{Im}(\mathcal{G}) = \{uG \mid u \in \mathcal{A}^k\} = C$.

□

Se ha hablado de las matrices generadoras de un código de convolución y como caracterizarlas. Sin embargo, sería agradable poder caracterizar a todas las matrices que nos generan un código de convolución dado. De hecho, se dice que dos matrices generadoras son *equivalentes* si generan el mismo código de convolución.

La siguiente proposición nos enuncia que es posible exhibir todas las matrices equivalentes de un código de convolución, a partir de dar sólo una matriz generadora.

Proposición 2.11. *Sea C un (n,k)-código de convolución sobre $\mathcal{A}$ con una matriz generadora G. El conjunto de matrices generadoras de C es igual al conjunto*

$$\{UG \mid U \in GL_k(\mathcal{A})\}.$$

Demostración. Veamos la doble contención de estos conjuntos. Sea G' una matriz generadora de C, por demostrar que existe un elemento U de $GL_k(\mathcal{A})$ tal que $G' = UG$. Como G' y G son matrices generadoras de C, se sigue que G' y G son representaciones matriciales de morfismos inyectivos $\mathcal{G}'$ y $\mathcal{G}$ de $\mathcal{A}$-módulos, respectivamente. De lo cual se obtiene el siguiente diagrama:

$$\begin{array}{ccc} \mathcal{A}^k & & \\ & \searrow^{\mathcal{G}'} & \\ \mathcal{A}^k & \xrightarrow[\mathcal{G}]{} & \mathcal{A}^n. \end{array}$$

De manera natural estos morfismos inducen isomorfismos $\mathcal{G}'$ y $\mathcal{G}$ de $\mathcal{A}^k$ sobre C. Sea $\mathcal{U} = \mathcal{G}^{-1} \circ \mathcal{G}'$. Debido a esto $\mathcal{U}$ es un isomorfismo de $\mathcal{A}$-módulos, que hace que el siguiente diagrama conmute:

$$\begin{array}{ccc} \mathcal{A}^k & & \\ \downarrow \mathcal{U} & \circlearrowright & \searrow^{\mathcal{G}'} \\ \mathcal{A}^k & \xrightarrow[\mathcal{G}]{} & C \end{array}$$

Además, $\mathcal{U}$ tiene por representación matricial a un elemento U de $M_{k\times k}(\mathcal{A})$. Cómo $\mathcal{U}$ es biyectivo se tiene que $det(U)$ es una unidad de $\mathcal{A}$. Por lo tanto, U es un elemento de $GL_k(\mathcal{A})$. Más aún, como $\mathcal{G}' = \mathcal{G} \circ \mathcal{U}$, se cumple que $G' = UG$.

Alternativamente, sea U un elemento de $GL_k(\mathcal{A})$, por demostrar que UG es una matriz generadora de C, es decir, que el codificador asociado a UG es inyectivo y su imagen es C. Sea $\mathcal{UG}$ tal codificador. Se cumple que $\mathcal{UG} = \mathcal{G} \circ \mathcal{U}$, donde $\mathcal{G}$ y $\mathcal{U}$ son los codificadores asociados a G y a U, respectivamente. Dado que $\mathcal{G}$ y $\mathcal{U}$ son inyectivos, se sigue que $\mathcal{UG}$ es también inyectivo. Sólo resta mostrar que $\text{Im}(\mathcal{UG}) = C$, esto se concluye de que $\text{Im}(\mathcal{UG}) = \text{Im}(\mathcal{G})$. □

Otra matriz que permite describir un código de convolución, exhibiendo todas las palabras existentes en él es la matriz de control, definida a continuación.

Definición 2.7. Sea C un (n, k)-código de convolución sobre $\mathcal{A}$. Sea H una matriz de tamaño $(n-k) \times n$ con entradas en $\mathcal{A}$. H es una *matriz de control* de C si

$$C = \{v \in \mathcal{A}^n \mid vH^t = 0_{\mathcal{A}^{n-k}}\}.$$

Ejemplo 2.12. El (n, n)-código de convolución del Ejemplo 2.1 no tiene matrices de control, puesto que la diferencia que hay entre la longitud y el rango es cero.

Ejemplo 2.13. Una matriz de control del código de convolución del Ejemplo 2.2 es

$$H = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}.$$

Observación 2.8. Con la notación de la definición de matriz de control es inmediato que GH^t es igual a la matriz nula de $M_{k\times(n-k)}(\mathcal{A})$, para toda matriz generadora G de C.

La siguiente proposición es una consecuencia de las propiedades que cumple el rango por renglones de una matriz.

Proposición 2.14. *Sea H una matriz de control de un (n,k)-código de convolución C sobre $\mathcal{A}$, se cumple que los renglones de H son linealmente independientes sobre $\mathcal{A}$.*

Demostración. Sea r_H el rango por renglones de H, siempre se tiene que r_H es igual al rango del $\mathcal{A}$-submódulo de $\mathcal{A}^n$ generado por los renglones de H. Así

$$r_H = n - r(N(H^t))$$

donde $r(N(H^t))$ es el rango del complemento ortogonal del $\mathcal{A}$-submódulo de $\mathcal{A}^n$ generado por los renglones de H^t. Dado que H es una matriz de control de C, se cumple que el complemento ortogonal del $\mathcal{A}$-submódulo de $\mathcal{A}^n$ generado por los renglones de H^t es C, así $r(N(H^t)) = k$. Por lo tanto el rango por renglones de H es $n-k$. Así, los renglones de H son linealmente independientes sobre $\mathcal{A}$. □

Más aún, se verifica la siguiente proposición, su demostración es elemental.

Proposición 2.15. *Sea C un (n,k)-código de convolución sobre $\mathcal{A}$ con una matriz generadora G y una matriz de control H, se satisface que*

$$\{v \in \mathcal{A}^k \mid Gv^t = 0_{\mathbb{A}^k}\} = \{wH \mid w \in \mathcal{A}^{n-k}\}.$$

Así, tanto una matriz generadora como una matriz de control determinan el código dual de un código de convolución, que será definido a continuación.

Definición 2.9. Sea C un (n,k)-código de convolución sobre $\mathcal{A}$ con una matriz generadora G. El *código dual* de C es el conjunto $\{v \in \mathcal{A}^n \mid Gv^t = 0_{\mathcal{A}^k}\}$ y se denota por $C^\perp$.

Ejemplo 2.16. El código dual del código de convolución C del Ejemplo 2.1 es $C^\perp = \{0_{\mathbb{Z}^3}\}$. $C^\perp$ es un $(3,0)$-código de convolución sobre $\mathbb{Z}$.

Ejemplo 2.17. El código dual del código de convolución C del Ejemplo 2.2 es

$$C^\perp = \mathbb{Z}(0,0,1) \cong_{\mathbb{Z}} \mathbb{Z}.$$

$C^\perp$ es un $(3,1)$-código de convolución sobre $\mathbb{Z}$.

Como se ha notado en los ejemplos anteriores, se cumple que el código dual de un código de convolución es también un código de convolución. Lo cual es demostrado a continuación:

PROPOSICIÓN 2.18. *Sea C un (n,k)-código de convolución sobre $\mathcal{A}$ con una matriz de control H. Su código dual $C^{\perp}$ es un $(n, n-k)$-código de convolución sobre $\mathcal{A}$.*

DEMOSTRACIÓN. Debido a la Proposición 2.15, se sigue que los renglones de H genera a $C^{\perp}$ como $\mathcal{A}$-módulo. Más aún, se deduce de la Proposición 2.14, que los renglones de H son una base para $C^{\perp}$. Por lo tanto $C^{\perp}$ es un $(n, n-k)$-código de convolución sobre $\mathcal{A}$ y H es una matriz generadora de $C^{\perp}$. □

Al igual que las matrices generadoras, podemos caracterizar a las matrices de control de un código de convolución, es decir, se puede exhibir todas las matrices de control de un código de convolución a partir de dar sólo una matriz de control, de la siguiente manera:

PROPOSICIÓN 2.19. *Sean C un (n,k)-código de convolución sobre $\mathcal{A}$ y H una matriz de control de C. El conjunto de matrices de control de C es igual a*

$$\{VH \mid V \in GL_{n-k}(\mathcal{A})\}.$$

DEMOSTRACIÓN. Es claro que el conjunto de matrices de control de C es igual al conjunto de matrices generadoras de $C^{\perp}$. Y De la Proposición 2.11, se sigue que el conjunto de matrices generadoras de $C^{\perp}$ es igual a $\{VH \mid V \in GL_{n-k}(\mathcal{A})\}$. □

Bien, hasta el momento hemos conservado en la medida de lo posible, algunas propiedades de las matrices generadoras y de las matrices de control, de los códigos de convolución. Ahora, durante el resto de este texto nos dedicaremos a ver dos casos particulares de estos códigos de convolución. Por ejemplo, uno de ellos lo empezaremos a desarrollar.

Para J. Rosenthal, J. M. Schumacher and E.V. York, la representación matemática de la operación de los códigos de convolución está basada en el uso de polinomios en una variable con coeficientes en un campo finito. Es decir, ellos plantearon que los códigos de convolución viven en los módulos libres de rango finito sobre un anillo de polinomios en una variable con coeficientes en un campo finito, ver (14), es por eso que incorporamos la siguiente sección en la cual introducimos el concepto de polinomios en una variable con coeficientes en un módulo.

3. Polinomios con Coeficientes en un Módulo

En esta sección extenderemos el concepto de polinomios en una variable con coeficientes en un anillo, por el concepto de polinomios en una variable con coeficientes en un módulo. Daremos

una caracterización a estos módulos. Después, tomaremos el caso particular de los polinomios en una variable con coeficientes en un espacio vectorial de dimensión finita y veremos a que módulo es isomorfo.

Sea x una variable sobre un anillo A. Se considera el anillo $A[x]$ de polinomios en la variable x con coeficientes en A como la suma directa de la familia $(Ax^i)_{i\in\mathbb{Z}_+}$ de A-módulos libres de rango 1, es decir,

$$A[x] = \oplus_{i\in Z_+} Ax^i.$$

Definición 2.10. Sean x una variable sobre un anillo A y M un A-módulo. El A-módulo de *polinomios en la variable x con coeficientes en M* es la suma directa de la familia $(Mx^i)_{i\in\mathbb{Z}_+}$ de A-módulos donde $Mx^i = M \otimes_A Ax^i$, para cada $i \in \mathbb{Z}_+$. Tal módulo se denota por $M[x]$.

Con la notación anterior, obsérvese que para toda $i \in I$, un elemento de Mx^i es de esta forma

$$\Sigma_{j=1}^{n}(m_j \otimes\ a_j x^i)$$

donde n es un entero natural, $m_j \in M$ y $a_j \in A$ para toda $j = 1, \ldots, n$. Mediante un cálculo sencillo se puede demostrar que los elementos de Mx^i son de la forma $m \otimes x^i$ con $m \in M$. Se denotará por mx^i a $m \otimes x^i$. Con tal notación podemos decir que $M[x]$ es el conjunto

$$\left\{m_0 + m_1 x + \ldots + m_r x^r \;\middle|\; r \in \mathbb{Z}_+, m_i \in M \text{ para toda } i = 1, \ldots, r\right\}.$$

Además se cumple que $M[x]$ tiene una estructura de módulo sobre el anillo $A[x]$. En efecto, definamos de manera natural la siguiente aplicación:

$$\begin{array}{rccl} * : & A[x] \times M[x] & \longrightarrow & M[x] \\ & (a(x), m(x)) & \mapsto & a(x) * m(x) = \Sigma_{i=0}^{r}\Sigma_{j=0}^{s}\left(a_i m_j x^{i+j}\right). \end{array}$$

donde $a(x) = \Sigma_{i=0}^{r} a_i x^i$ y $m(x) = \Sigma_{j=0}^{s} m_j x^j$. La aplicación * es la operación multiplicación por escalar.

Por otro lado, sabemos que $M \otimes_A A[x]$ tiene una estructura clara de $A[x]$-módulo cuya multiplicación por escalar está dada por:

$$\begin{array}{rccl} \star : & A[x] \times M \otimes_A A[x] & \longrightarrow & M \otimes_A A[x] \\ & (a(x), m \otimes b(x)) & \mapsto & a(x) \star m \otimes b(x) = m \otimes a(x)b(x). \end{array}$$

Proposición 2.20. *Sean x una variable sobre un anillo A y M un A-módulo. Se cumple que $M[x]$ es isomorfo a $M \otimes_A A[x]$ como $A[x]$-módulos y A-módulos.*

Demostración. Por definición $M[x] = \oplus_{i\in I}(M \otimes_A Ax^i)$. Pero dado que el producto tensorial es compatible con la suma directa, véase la Proposición A.15, se tiene que

$$M[x] \cong_A M \otimes_A (\oplus_{i\in I} Ax^i) = M \otimes_A A[x].$$

Aún más, $M[x]$ y $M \otimes_A A[x]$ tienen la misma estructura de $A[x]$-módulo. En efecto, sean $\Sigma_{i=0}^{r} a_i x^i$ un elemento de $A[x]$ y $\Sigma_{j=0}^{s} m_j x^j$ un elemento de $M[x]$.

$$\begin{aligned}
\left(\Sigma_{i=0}^{r} a_i x^i\right) * \left(\Sigma_{j=0}^{s} m_j x^j\right) &= \Sigma_{i=0}^{r}\Sigma_{j=0}^{s}\ a_i m_j x^{i+j} \\
&= \Sigma_{i=0}^{r}\Sigma_{j=0}^{s}\ a_i m_j \otimes x^{i+j} \\
&= \Sigma_{j=0}^{s}\Sigma_{i=0}^{r}\ m_j \otimes a_i x^{i+j} \\
&= \Sigma_{j=0}^{s}\ m_j \otimes \left(\Sigma_{i=0}^{r} a_i x^i\right) x^j \\
&= \Sigma_{j=0}^{s} \left(\Sigma_{i=0}^{r} a_i x^i\right) \star (m_j \otimes x^j) \\
&= \left(\Sigma_{i=0}^{r} a_i x^i\right) \star \left(\Sigma_{j=0}^{s} (m_j \otimes x^j)\right).
\end{aligned}$$

Por lo tanto, $M[x]$ es isomorfo a $M \otimes_A A[x]$ como $A[x]$-módulo. □

Corolario 2.21. *Sean z una variable sobre un campo F y n un entero natural. Se satisface que los $F[z]$-módulos $F^n[z]$ y $F[z]^n$ son isomorfos.*

Demostración. Por la proposición anterior se tiene que

$$F^n[z] \cong_{F[z]} F^n \otimes_F F[z].$$

Pero el producto tensorial es compatible con la suma directa, véase Proposición A.15, por lo tanto

$$F[z]^n \cong_{F[z]} (F \otimes_F F[z])^n .$$

Por otro lado, los $F[z]$-módulos $F[z] \otimes_F F$ y $F[z]$ son isomorfos, pues se deduce de la Proposición A.14. Por lo que tenemos que el $F[z]$-módulo $F^n[z]$ es libre de rango n. □

Como consecuencia del corolario anterior y por abuso de notación, $F^n[z]$ será igual a $F[z]^n$.

4. Códigos de Convolución sobre $\mathbb{F}[z]$

Una clase de dominios de ideales principales está dada por los anillos de polinomios en una variable con coeficientes en un campo, ver Proposición 2.22. Es por esto, que la definición de código de convolución que hemos dado engloba la propuesta de J. Rosenthal, J. M. Schumacher y E.V. York, (14).

Proposición 2.22. *El anillo de polinomios en la variable z con coeficientes en un campo F es un dominio de ideales principales.*

Demostración. Sea I un ideal de $F[z]$. Si $I = \{0_F\}$, entonces $I = F[z]0_F$.
Consideremos $I \neq \{0_F\}$, existe $g \in I$ no nulo de grado mínimo en I. Se afirma que $I = F[z]g$.

Sea $f \in I$, por la división euclidiana, $f = pg + q$ para ciertos $p, q \in F[z]$ con $q = 0_F$ o $\mathrm{gr}(q) < \mathrm{gr}(g)$ cuando $q \neq 0_F$. Supongamos que $q \neq 0_{\mathbb{F}}$, así $\mathrm{gr}(q) < \mathrm{gr}(g)$, por otro lado se tiene que $q = f - pg \in I$, absurdo, pues contradice que g es de grado mínimo en I. Así $q = 0_F$, implicando que $f = pg$, por lo tanto $I \subseteq F[z]g$. □

A continuación veremos algunos ejemplos de códigos de convolución sobre anillos de polinomios en una variable con coeficientes en un campo finito:

Ejemplo 2.23. Sea z una variable sobre el campo $\mathbb{F}_2$ que tiene dos elementos. Consideremos

$$C = \mathbb{F}_2[z](1, z, z^2, z^3) + \mathbb{F}_2[z](0, 1, z, z^2),$$

donde $(1, z, z^2, z^3)$ y $(0, 1, z, z^2)$ son elementos de $\mathbb{F}_2^4[z]$. C es un $(4, 2)$-código de convolución sobre $\mathbb{F}_2[z]$.

Ejemplo 2.24. Sea z una variable sobre el campo $\mathbb{F}_2$ que consta de dos elementos. Consideremos

$$C = \mathbb{F}_2[z](1, z, z^2, z^3) + \mathbb{F}_2[z](0, 1, z, z^2) + \mathbb{F}_2[z](1+z^2, 1+z^3, z+z^4, z^2+z^5) + \mathbb{F}_2[z](1+z, 1+z, z^3+z^4, z^4+z^5),$$

donde $(1, z, z^2, z^3)$, $(0, 1, z, z^2)$, $(1 + z^2, 1 + z^3, z + z^4, z^2 + z^5)$ y $(1 + z, 1 + z, z^3 + z^4, z^4 + z^5)$ son elementos de $\mathbb{F}_2^4[z]$. C' es un $(4, 2)$-código de convolución sobre $\mathbb{F}_2[z]$. Más aún, C' es igual a C donde C es el código de convolución del Ejemplo 2.23.

Ejemplo 2.25. Sea z una variable sobre el campo $\mathbb{F}_3$ que consta de tres elementos. Considere

$$C = \mathbb{F}_3[z](z + 2, z + 1, z),$$

donde $(z + 2, z + 1, z)$ es un elemento de $\mathbb{F}_3^3[z]$. C es un $(3, 1)$-código de convolución sobre $\mathbb{F}_3[z]$.

Ejemplo 2.26. Sea z una variable sobre el campo $\mathbb{F}_3$ cuya cardinalidad es tres. Consideremos

$$C = \mathbb{F}_3[z](z + 2, z + 1, z + 1),$$

donde $(z + 2, z + 1, z + 1)$ es un elemento de $\mathbb{F}_3^3[z]$. C es un $(3, 1)$-código de convolución sobre $\mathbb{F}_3[z]$.

Ejemplo 2.27. Sea z una variable sobre el campo $\mathbb{F}_5$ que consta de cinco elementos. Consideremos

$$C = \mathbb{F}_5[z](2 + z, 2 + 2z) + \mathbb{F}_5[z](2 + 4z, 1 + z) + \mathbb{F}_5[z](0, 2 + 4z + 2z^2),$$

donde $(2 + z, 2 + 2z)$, $(2 + 4z, 1 + z)$ y $(0, 2 + 4z + 2z^2)$ son elementos de $\mathbb{F}_5^2[z]$. C es un $(2, 2)$-código de convolución sobre $\mathbb{F}_5[z]$.

Observación 2.11. A pesar de que el código de convolución del Ejemplo 2.24 es generado por cuatro elementos su rango es 2. Al igual que el código de convolución del Ejemplo 2.27 es generado por tres elementos su rango es 2. En general, el rango de un código de convolución es menor o igual que el número de elementos que lo generan como A-módulo.

Hasta el momento hemos considerado anillos de polinomios en una variable con coeficientes en un campo finito. Si quisiéramos extender a estos anillos de polinomios dotándoles de más variables, entonces nos veríamos tentados por establecer códigos de convolución sobre estos anillos. Sin embargo, esto no es posible puesto que los anillos de polinomios en más de dos variables con coeficientes en un campo, no son dominios de ideales principales, esto es mostrado en la siguiente proposición:

PROPOSICIÓN 2.28. *Sean $z_1, \ldots, z_n$ variables sobre un campo F con n un entero natural. Las siguientes afirmaciones son equivalentes:*

1. *$F[z_1, \ldots, z_n]$ es un dominio de ideales principales.*
2. *n es igual a uno.*

DEMOSTRACIÓN. $\Rightarrow$) Supongamos que $F[z_1, \ldots, z_n]$ es un dominio de ideales principales. Por demostrar que solamente podemos elegir a n igual a 1. Supongamos que $n \geq 2$. Consideremos al ideal $F[z_1, \ldots, z_n]z_1 + F[z_1, \ldots, z_n]z_2$ de $F[z_1, \ldots, z_n]$, por hipótesis $F[z_1, \ldots, z_n]$ es DIP, así existe $q(z_1, \ldots, z_n)$ elemento de $F[z_1, \ldots, z_n]$ tal que

$$F[z_1, \ldots, z_n]z_1 + F[z_1, \ldots, z_n]z_2 = F[z_1, \ldots, z_n]q(z_1, \ldots, z_n).$$

Cómo $z_1 \in F[z_1, \ldots, z_n]q(z_1, \ldots, z_n)$, existe $p(z_1, \ldots, z_n) \in F[z_1, \ldots, z_n]$ tal que

$$z_1 = p(z_1, \ldots, z_n)q(z_1, \ldots, z_n)$$

Al tomar el grado respecto a la variable z_1 y dado que $F[z_1, \ldots, z_n]$ es DIP, se cumple que

$$1 = gr_{z_1}(p(z_1, \ldots, z_n)) + gr_{z_1}(q(z_1, \ldots, z_n)).$$

Con ello, tenemos dos posibilidades:

$$gr_{z_1}(p(z_1, \ldots, z_n)) = 0 \text{ y } gr_{z_1}(q(z_1, \ldots, z_n)) = 1, \text{ o}$$

$$gr_{z_1}(p(z_1, \ldots, z_n)) = 1 \text{ y } gr_{z_1}(q(z_1, \ldots, z_n)) = 0.$$

- Si $gr_{z_1}(q(z_1, \ldots, z_n)) = 1$, entonces $q(z_1, \ldots, z_n) = x_1 r(z_2, \ldots, z_n)$ para algún $r(z_2, \ldots, z_n)$ elemento de $F[z_1, \ldots, z_n]$ tal que $gr_{z_1}(r(z_2, \ldots, z_n)) = 0$.
  Por otro lado, $z_2 \in F[z_1, \ldots, z_n]p[z_1, \ldots, z_n]$, es decir, $z_2 \in F[z_1, \ldots, z_n]r(z_2, \ldots, z_n)z_1$.
  Así z_1 divide a z_2 en $F[z_1, \ldots, z_n]$, absurdo.
- Si $gr_{z_1}(q(z_1, \ldots, z_n)) = 0$, entonces $z_1 \notin F[z_1, \ldots, z_n]q(z_1, \ldots, z_n)$, absurdo.

Por lo tanto n no puede ser mayor o igual que 2.

$\Leftarrow$) Si $n = 1$, entonces $F[z_1]$ es DIP, debido a la Proposición 2.22.

□

Ahora nos concentraremos en estudiar a las matrices generadoras y las matrices de control de los códigos de convolución sobre $\mathbb{F}[z]$ donde z es una variable sobre un campo finito $\mathbb{F}$. Pues a partir de las matrices generadoras se define un nuevo parámetro para los códigos de convolución sobre $\mathbb{F}[z]$ llamado *grado*. Primeros daremos algunos ejemplos de estas matrices.

Ejemplo 2.29. Una matriz generadora del código de convolución del Ejemplo 2.23 es

$$G = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 0 & 1 & z & z^2 \end{pmatrix}.$$

Ejemplo 2.30. Para el $(3, 1)$-código de convolución del Ejemplo 2.25, se tiene que una matriz generadora es

$$G = \begin{pmatrix} z+2 & z+1 & z \end{pmatrix}.$$

Mientras que una matriz de control es

$$H = \begin{pmatrix} z^2+2z+1 & z+1 & 2z^2+z+2 \\ 0 & 2z & z+1 \end{pmatrix}.$$

Con ello, su código dual es

$$C^{\perp} = \mathbb{F}_3[z](z^2+2z+1, z+1, 2z^2+z+2) + \mathbb{F}_3[z](0, 2z, z+1).$$

Ejemplo 2.31. Para el código de convolución del Ejemplo 2.26 una matriz generadora es

$$G = \begin{pmatrix} z+2 & z+1 & z+1 \end{pmatrix}.$$

Por otro lado, una matriz de control es

$$H = \begin{pmatrix} z+1 & 0 & 2z+1 \\ 0 & 1 & 2 \end{pmatrix}.$$

Más aún, su código dual es

$$C^{\perp} = \mathbb{F}_3[z](z+1, 0, 2z+1) + \mathbb{F}_3[z](0, 1, 2).$$

Para el resto de este texto consideraremos a $\mathbb{F}$ un campo finito y z una variable sobre $\mathbb{F}$. Además se considera a $\mathbb{F}[z]$ como el anillo de polinomios en la variable z con coeficientes en $\mathbb{F}$.

Sean G una matriz generadora y H una matriz de control de un (n, k)-código de convolución C sobre $\mathbb{F}[z]$. Por ello se tiene el siguiente morfismo inyectivo de $\mathbb{F}[z]$-módulos

$$\begin{array}{rccc} \mathcal{G}: & \mathbb{F}^k[z] & \longrightarrow & \mathbb{F}^n[z] \\ & u & \longmapsto & \mathcal{G}(u) = uG \end{array}$$

y el morfismo de $\mathbb{F}[z]$-módulos

$$\begin{aligned} \mathcal{H}^t : \quad \mathbb{F}^n[z] &\longrightarrow \mathbb{F}^{n-k}[z] \\ v &\longmapsto \mathcal{H}^t(v) = vH^t. \end{aligned}$$

Tales morfismos cumplen que $\operatorname{Im}\mathcal{G} = \ker\mathcal{H}^t$. Con todo esto, se forma la siguiente sucesión exacta de $\mathbb{F}[z]$-módulos:

$$0 \longrightarrow \mathbb{F}^k[z] \xrightarrow{\mathcal{G}} \mathbb{F}^n[z] \xrightarrow{\mathcal{H}^t} M \longrightarrow 0.$$

Donde M es un $\mathbb{F}[z]$-módulo finitamente generado de rango $n-k$. Tomando entonces duales como $\mathbb{F}[z]$-módulos, resulta otra sucesión exacta

$$0 \longrightarrow \widehat{M} \xrightarrow{\mathcal{H}} \mathbb{F}^n[z] \xrightarrow{\mathcal{G}^t} \widehat{C} \longrightarrow \frac{\widehat{C}}{\operatorname{Im}\mathcal{G}^t} \longrightarrow 0,$$

donde $\widehat{C}/\operatorname{Im}\mathcal{G}^t$ es un $\mathbb{F}[z]$-módulo de torsión, cuyo anulador es

$$\operatorname{Ann}_{\mathbb{F}[z]}\left(\frac{\widehat{C}}{\operatorname{Im}\mathcal{G}^t}\right) = \langle\{k\text{-menores de } G\}\rangle.$$

El morfismo $\mathcal{G}^t$ da luz a la noción de *grado* de un código de convolución sobre $\mathbb{F}[z]$. Tal concepto junto con la longitud y rango del código de convolución nos permiten acotar superiormente la "distancia mínima" existente entre las palabras código. Sin embargo, para definir el grado de un código de convolución hacemos uso de las matrices generadoras *minimales* (ver Definición 3.11), porque tales nos permiten precisar que el concepto de grado de un código de convolución sobre $\mathbb{F}[z]$ este bien definido. Sin embargo por el momento no daremos más detalles de estas matrices, pues lo haremos en el siguiente capítulo. Por ahora sólo enunciaremos el concepto de grado de un código de convolución, dado a continuación:

Definición 2.12. Sea C un (n,k)-código de convolución sobre $\mathbb{F}[z]$ con una matriz generadora minimal G. El *grado* de C es el máximo grado de los k-menores de G. Y se denota por δ.

El grado de un código de convolución es también conocido como *complejidad* o *restricción de longitud total*.

Ejemplo 2.32. El grado del código de convolución del Ejemplo 2.25 es 1, al igual que el grado del código de convolución del Ejemplo 2.26 es 1.

5. Códigos de Convolución de Máxima Distancia de Separación

En esta sección trataremos los códigos de convolución sobre $\mathbb{F}[z]$ de máxima distancia de separación, estos son tales que la "distancia mínima" entre sus palabras código alcanza el mayor de los

valores posibles dados por la longitud, el rango y el grado asociados al código de convolución dado. Tal acotación es llamada la *Cota de Singleton Generalizada*, tal nombre es debido a su semejanza con la cota de Singleton de los códigos lineales clásicos.

Otro parámetro importante para los códigos de convolución sobre $\mathbb{F}[z]$ es la *distancia mínima*, pero tal párametro esta en terminos de la función *peso*, que a continuación daremos.

Definición 2.13. Sea n un entero natural. El *peso* sobre $\mathbb{F}^n[z]$ es la función wt dada por

$$\begin{array}{rccc} \mathrm{wt}: & \mathbb{F}^n[z] & \longrightarrow & \mathbb{Z}_+ \\ & v = \sum_{j=0}^{N} v_j z^j & \longmapsto & \mathrm{wt}(v) = \sum_{j=0}^{N} \mathrm{wt}_{\mathbb{F}^n}(v_j). \end{array}$$

donde $\mathrm{wt}_{\mathbb{F}^n}(v_j)$ denota el usual peso de Hamming de v_j en $\mathbb{F}^n$.

Definición 2.14. Sea C un (n,k)-código de convolución sobre $\mathbb{F}[z]$. La *distancia mínima* de C es $O_{\mathbb{Z}}$ si C es nulo, sino es el entero $min\{\mathrm{wt}(v) \mid v \in C, v \neq 0\}$, donde *wt* es el peso sobre $\mathbb{F}^n[z]$. Y se denota por d.

Ejemplo 2.33. La distancia mínima del código de convolución del Ejemplo 2.23 es 3.

Ejemplo 2.34. La distancia mínima del código de convolución del Ejemplo 2.25 es 5.

Ejemplo 2.35. La distancia mínima del código de convolución del Ejemplo 2.26 es 6.

Hasta el momento hemos dado cuatro parámetros fundamentales de los códigos de convolución sobre $\mathbb{F}[z]$. Sea C un código de convolución sobre $\mathbb{F}[z]$ de longitud n, rango k, grado δ y distancia mínima d, diremos que C es un (n,k,δ,d)-código de convolución sobre $\mathbb{F}[z]$. Estos parámetros no son aleatorios, existe una relación entre ellos dada en el siguiente teorema, la demostración de este se encuentra en (15, Teorema 2.2).

Teorema 2.36. ***Cota de Singleton Generalizada.***
Sea C un (n,k,δ,d)-código de convolución sobre $\mathbb{F}[z]$ no nulo. Se cumple que

$$d \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1.$$

Los códigos de convolución cuyos parámetros alcanzan la igualdad en la Cota Singleton Generalizada se llaman códigos de convolución de *Máxima Distancia de Separación* o MDS. Llamados así, ya que la distancia mínima de estos códigos de convolución tienen el mayor valor posible que pueden tener en términos de su longitud, rango y grado dados.

Ejemplo 2.37. Del Ejemplo 2.23, C es un $(4,2,2,3)$-código de convolución sobre $\mathbb{F}_2[z]$ que no es de MDS.

EJEMPLO 2.38. Del Ejemplo 2.25, C es un $(3, 1, 1, 5)$-código de convolución sobre $\mathbb{F}_3[z]$ que no es de MDS.

EJEMPLO 2.39. Del Ejemplo 2.26, C es un $(3, 1, 1, 6)$-código de convolución de MDS sobre $\mathbb{F}_3[z]$.

EJEMPLO 2.40. Considere la siguiente matriz con entradas en $\mathbb{F}_5[z]$:

$$G = \begin{pmatrix} 1 & 1 & 1 \\ z+1 & z+2 & 2z+3 \end{pmatrix}.$$

Es un $(3, 2, 1, 3)$-código de convolución de MDS sobre $\mathbb{F}_5[z]$ el $\mathbb{F}_5[z]$-módulo generado por los renglones de G.

CAPíTULO 3

Índices de Forney de los Códigos de Convolución

Mediante el uso de los *índices de Forney* es más sencillo estimar el grado de un código de convolución, más aún, con ellos se determina la *memoria* del código de convolución. Además, estos índices son usados para la demostración de la cota de Singleton Generalizada. Es por ello que en este capítulo mostraremos interés en estos índices, para lo cual se enunciará un concepto más general de los códigos de convolución sobre $\mathbb{F}[z]$ y se dará, no solamente, los conceptos y las propiedades necesarias para la definición de estos, sino también, la relación de estos índices con el grado del código de convolución.

1. Grado Interno y Grado Externo

Un código de convolución sobre $\mathbb{F}[z]$ tiene asociado una infinidad de matrices generadoras, así que estamos interesados en buscar aquellas matrices que cumplan ser las más óptimas en términos del *grado interno* y *del grado externo*.

Definición 3.1. Sea G una matriz generadora de un (n,k)-código de convolución sobre $\mathbb{F}[z]$. El *grado interno* de G es el entero $max\{\text{gr}(\gamma) \mid \gamma \text{ es un } k\text{-menor de } G\}$, y es denotado por $\text{gr}_{in}(G)$.

Ejemplo 3.1. Sea G la matriz dada en el Ejemplo 2.29. Es decir,

$$G = \begin{pmatrix} 1 & z & z^2 & z^3 \\ 0 & 1 & z & z^2 \end{pmatrix}.$$

Se tiene que $\text{gr}_{in}(G) = 2$.

Ahora, se introducirá la noción de *grado externo* para el cual se dará el concepto de *grado de un vector*:

Definición 3.2. Sean n un entero natural y $v = (v_1, \ldots, v_n)$ un elemento de $\mathbb{F}^n[z]$. El *grado* de v es el entero $max\{\text{gr}(v_i) \mid i = 1, \ldots, n\}$, y es denotado como $\text{gr}(v)$.

Notación 3.3. Por convención, el grado del elemento nulo de $\mathbb{F}[z]$ es cero.

Ejemplo 3.2. El grado del elemento $(0, 1, z, z^2)$ de $\mathbb{F}^4[z]$ es 2.

Con tal concepto es posible dar la siguiente definición:

Definición 3.4. Sea G una matriz generadora de un (n,k)-código de convolución sobre $\mathbb{F}[z]$ y sea $\{g_1,\ldots,g_k\}$ el conjunto de los renglones de G. El *grado externo* de G es el entero $\Sigma_{i=1}^{k}\,\mathrm{gr}(g_i)$, y es denotado por $\mathrm{gr}_{ex}(G)$.

Ejemplo 3.3. El grado externo de la matriz G del Ejemplo 3.1 es 5. Obsérvese que el grado externo de G es estrictamente mayor que su grado interno.

El grado interno y el grado externo de una matriz generadora de un código de convolución sobre $\mathbb{F}[z]$ tienen una relación comparativa dada en el siguiente lema:

Lema 3.4. *Sea $G=(g_{ij})$ una matriz generadora de un (n,k)-código de convolución sobre $\mathbb{F}[z]$. Se cumple que*

$$\mathrm{gr}_{in}(G)\leq \mathrm{gr}_{ex}(G). \tag{3.1}$$

Demostración. Sea g_i el i-ésimo renglón de G para toda $i\in\{1,\ldots,k\}$ y sea Γ el conjunto de los k-menores de G.
Probar la desigualdad 3.1 es equivalente a demostrar que $\mathrm{gr}(\gamma)$ es menor o igual que $\mathrm{gr}_{ex}(G)$, para cada γ en Γ. En efecto, sea $\gamma\in\Gamma$. Así, γ es el determinante de una k-submatriz de G, digamos que es N donde

$$N=\begin{pmatrix} g_{1n_1} & \cdots & g_{1n_k}\\ \vdots & \ddots & \vdots\\ g_{kn_1} & \cdots & g_{kn_k}\end{pmatrix},$$

con $\{n_1,\ldots,n_k\}\subseteq\{1,\ldots,n\}$ tal que $n_1<\ldots<n_k$.

Obsérvese que debido a las propiedades de los determinantes de matrices, cada uno de los $k!$ términos de γ son multiplicación de k entradas de N, donde cada una de estas entradas elimina la oportunidad de que las otras entradas pertenezcan al renglón y a la columna donde se encuentra dicha entrada.
Sea $s\in\{1,\ldots,k!\}$, denotemos por γ_s al s término de γ. Así, para cada γ_s, con $s\in\{1,\ldots,k!\}$, existen dos únicas permutaciones α y β de k elementos tales que

$$\gamma_s=\lambda_s g_{\alpha(1)n_{\beta(1)}}\cdots g_{\alpha(k)n_{\beta(k)}},$$

donde $\lambda_s\in\{1_{\mathbb{F}},-1_{\mathbb{F}}\}$. Al estimar el grado de γ_s, tenemos que

$$\begin{aligned}\mathrm{gr}(\gamma_s) &= \mathrm{gr}(g_{\alpha(1)n_{\beta(1)}})+\ldots+\mathrm{gr}(g_{\alpha(k)n_{\beta(k)}})\\ &\leq \mathrm{gr}(g_{\alpha(1)})+\ldots+\mathrm{gr}(g_{\alpha(k)})=\mathrm{gr}_{ex}(G).\end{aligned}$$

Por lo tanto, el grado de cada uno de los $k!$ términos de γ esta acotado superiormente por el grado externo de G. Con ello se sigue la última desigualdad de las siguientes desigualdades:

$$\text{gr}(\gamma) \quad \leq \quad max\{\text{gr}(\gamma_s) \mid s = 1, \ldots, k!\} \leq \text{gr}_{ex}(G).$$

Se concluye que $\text{gr}(\gamma) \leq \text{gr}_{ex}(G)$ para todo γ elemento de Γ. □

A continuación daremos una condición suficiente para aseverar la igualdad en la Ecuación 3.1.

Lema 3.5. *El grado interno y el grado externo de cada matriz generadora de un* $(n, 1)$*-código de convolución sobre* $\mathbb{F}[z]$ *son iguales.*

Demostración. Sea G una matriz generadora de un $(n, 1)$-código de convolución sobre $\mathbb{F}[z]$. Por lo que G es igual a $(g_{11} \ \ldots \ g_{1n})$ para ciertos elementos $g_{11}, \ldots, g_{1n}$ de $\mathbb{F}[z]$. Se tiene que

$$\text{gr}_{in}(G) = max\{\text{gr}(g_{1j}) \mid j = 1, \ldots, n\} = \text{gr}_{ex}(G).$$

□

Ejemplo 3.6. Consideremos a G como $(z \ z^2 + 1 \ z^3)$, la cual es una matriz generadora de un $(3, 1)$-código de convolución sobre $\mathbb{F}[z]$. Se cumple que $\text{gr}_{in}(G) = 3 = \text{gr}_{ex}(G)$.

Ahora, será necesario dar unas notaciones para la enunciación del Teorema 3.7.

$\mathcal{U}(\mathbb{F}[z])$ denota el conjunto de las unidades de $\mathbb{F}[z]$, y $\text{div}(\Gamma)$ denota al conjunto de los divisores comunes de los elementos de Γ donde Γ es un subconjunto de $\mathbb{F}[z]$. Más aún, puntualicemos que a las matrices cuadradas con entradas en $\mathbb{F}[z]$ que son invertibles en $\mathbb{F}[z]$ se les dice *unimodulares*.

Teorema 3.7. *Sean* G *una matriz generadora de un* (n, k)*-código de convolución sobre* $\mathbb{F}[z]$ *y* Γ *el conjunto de los* k*-menores de* G*. Las siguientes afirmaciones son equivalentes:*

1. $\langle \Gamma \rangle = \mathbb{F}[z]$.
2. $\text{div}(\Gamma) = \mathcal{U}(\mathbb{F}[z])$.
3. *Para todo elemento* G' *de* $M_{k\times n}(\mathbb{F}[z])$ *y para todo elemento* U *de* $M_{k\times k}(\mathbb{F}[z])$ *tales que* $G = UG'$*, se cumple que* U *es unimodular.*

Demostración.

- Veamos que se obtiene la afirmación 2 a partir de la afirmación 1. Siempre se cumple que $\mathcal{U}(\mathbb{F}[z]) \subseteq \text{div}(\Gamma)$, por lo que sólo falta mostrar que $\text{div}(\Gamma) \subseteq \mathcal{U}(\mathbb{F}[z])$. En efecto, sea $d \in \text{div}(\Gamma)$. Se deduce que $\langle \Gamma \rangle \subseteq \mathbb{F}[z]d$, debido a la hipótesis se tiene que $\mathbb{F}[z] = \mathbb{F}[z]d$. Por lo tanto, $d \in \mathcal{U}(\mathbb{F}[z])$.

- Consideremos que se tiene la afirmación 2, por verificar que se cumple la afirmación 3. Sean G' un elemento de $M_{k\times n}(\mathbb{F}[z])$ y U un elemento de $M_{k\times k}(\mathbb{F}[z])$ tales que $G = UG'$. Observemos que los k-menores de G son los k-menores de G' multiplicados con $\det(u)$, es decir, que para todo γ elemento de Γ,

$$\gamma = det(U)\beta,$$

donde β es un k-menor de G'. Así, $det(U) \in \text{div}(\Gamma)$, aplicando la hipótesis se concluye que $\det(U) \in \mathcal{U}(\mathbb{F}[z])$, es decir, que U es unimodular.

- Para deducir la aseveración 1, demos por hecho la afirmación 3. Del Teorema C.1, se tiene que existen elementos P en $GL_k(\mathbb{F}[z])$ y Q en $GL_n(\mathbb{F}[z])$, tales que

$$PGQ = \begin{pmatrix} \lambda_1 & \dots & 0 & \\ \vdots & \ddots & \vdots & 0_{k\times(n-k)} \\ 0 & \dots & \lambda_k & \end{pmatrix} \tag{3.2}$$

donde $\lambda_1, \dots, \lambda_k$ son elementos no nulos de $\mathbb{F}[z]$. Como P y Q son matrices invertibles se puede reexpresar a la Ecuación 3.2 de la siguiente manera

$$G = P^{-1}\begin{pmatrix} \lambda_1 & \dots & 0 & \\ \vdots & \ddots & \vdots & 0_{k\times(n-k)} \\ 0 & \dots & \lambda_k & \end{pmatrix} Q^{-1}.$$

Equivalentemente tenemos que

$$G = P^{-1}\begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_k \end{pmatrix}\begin{pmatrix} 1 & \dots & 0 & \\ \vdots & \ddots & \vdots & 0_{k\times(n-k)} \\ 0 & \dots & 1 & \end{pmatrix} Q^{-1}.$$

Debido a la hipótesis se tiene que la siguiente matriz es unimodular:

$$P^{-1}\begin{pmatrix} \lambda_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda_k \end{pmatrix},$$

es decir, $det(P)^{-1}\lambda_1 \cdots \lambda_k \in \mathcal{U}(\mathbb{F}[z])$. Más aún, $\lambda_1 \cdots \lambda_k \in \mathcal{U}(\mathbb{F}[z])$.
Alternativamente, se deduce de la Ecuación 3.2 y de que $\mathbb{F}[z]$ es un dominio de ideales principales, que $\langle\Gamma\rangle = \mathbb{F}[z]e$ donde $e = \alpha\lambda_1 \cdots \lambda_k$ con $\alpha \in \mathcal{U}(\mathbb{F}[z])$. Con ello $e \in \mathcal{U}(\mathbb{F}[z])$. Así $\langle\Gamma\rangle = \mathbb{F}[z]$.

□

Si conocemos el grado interno de una matriz generadora de un código de convolución, podremos determinar el grado interno de una familia de matrices generadoras. Veamos cómo es esto.

LEMA 3.8. *Sea G una matriz generadora de un (n,k)-código de convolución sobre $\mathbb{F}[z]$ y sea U un elemento de $M_{k\times k}(\mathbb{F}[z]) \cap GL_k(\mathbb{F}(z))$. Se satisface que*

$$\mathrm{gr}_{in}(UG) = \mathrm{gr}(det(U)) + \mathrm{gr}_{in}(G).$$

En particular, si U es unimodular, entonces $\mathrm{gr}_{in}(UG) = \mathrm{gr}_{in}(G)$.

DEMOSTRACIÓN. Observemos primeramente que una k-submatriz de UG es UP donde P es una k-submatriz de G. Consecuentemente, un k-menor de UG es $det(U)\gamma$, donde γ es un k-menor de G. Dado que $\mathbb{F}[z]$ es dominio entero, se tiene que para todo k-menor de G, digamos γ, se cumple que

$$\mathrm{gr}(det(U)\gamma) = \mathrm{gr}(det(U)) + \mathrm{gr}(\gamma).$$

Y de esto se deduce la igualdad que se desea. □

2. Matrices Básicas, Reducidas y Minimales

Como hemos mencionado, ya enunciamos a los códigos de convolución desde el punto de vista en que J. Rosenthal, J. M. Schumacher and E.V. York (14) lo plantearon. Pero los códigos de convolución sobre $\mathbb{F}[z]$ se pueden definir a partir de conceptos más generales que estos, considerando a los códigos de convolución sobre el campo infinito de funciones racionales $\mathbb{F}(z)$ en la variable z (ver la Definición 3.5), tal como lo desarrollaron: G.D. Forney Jr. (6), R. McEliece (11) y J.A. Domínguez, et al. (3), por mencionar algunos.

Recordemos el concepto de los códigos de convolución sobre $\mathbb{F}(z)$, según G.D. Forney Jr. (6), por ejemplo. Obsérvemos que dicho concepto es un caso particular de nuestra definición de códigos de convolución sobre dominios de ideales principales (ver la Definición 2.1), pues $\mathbb{F}(z)$ es un dominio de ideales principales:

DEFINICIÓN 3.5. Un (n,k)-*código de convolución sobre* $\mathbb{F}(z)$ es un $\mathbb{F}(z)$-subespacio vectorial de $\mathbb{F}(z)^n$ de dimensión k.

Dado que el concepto de matriz generadora está presente en estos códigos. Podemos realizar una clasificación de estas matrices cuando todas sus entradas son polinomios.

DEFINICIÓN 3.6. Sea G una matriz generadora de un (n,k)-código de convolución sobre $\mathbb{F}(z)$. G es una *matriz generadora polinomial* si sus entradas son elementos de $\mathbb{F}[z]$.

Sabíamos con anterioridad que las matrices generadoras de los códigos de convolución sobre $\mathbb{F}[z]$ tenían asociados dos parámetros: grado interno y grado externo. Estos se definían en términos de los grados de los polinomios. Por lo que preservaremos estos parámetros solamente para las matrices generadoras polinomiales y seguiremos utilizando la misma notación. Más aún, se conservan las propiedades de los Lemas 3.4 y 3.8, de la siguiente manera:

Teorema 3.9. *Sea G una matriz generadora polinomial de un (n,k)-código de convolución sobre $\mathbb{F}(z)$. Se cumple que*

1. $\mathrm{gr}_{in}(G) \leq \mathrm{gr}_{ex}(G)$.
2. *Para todo elemento U de $GL_k(\mathbb{F}(z))$ tal que UG pertenece a $M_{k\times n}(\mathbb{F}[z])$, se tiene que*

$$\mathrm{gr}_{in}(UG) = \mathrm{gr}(det(U)) + \mathrm{gr}_{in}(G).$$

En particular, si U es unimodular, entonces $\mathrm{gr}_{in}(UG) = \mathrm{gr}_{in}(G)$.

Demostración. Es análoga a la realizada tanto en el Lema 3.4 como en el Lema 3.8. □

Ahora bien, el grado interno y el grado externo de las matrices generadoras polinomiales dan pie a la etiquetación de tales matrices en: *básicas*, *reducidas* y *minimales*. Veamos cómo se definen y de que manera podemos caracterizarlas.

La siguiente definición nos permite dar una familia de matrices que son óptimas en término del grado interno, veamos cómo es esto.

Definición 3.7. Sea G una matriz generadora polinomial de un (n,k)-código de convolución sobre $\mathbb{F}(z)$. G es *básica* si

$$\mathrm{gr}_{in}(G) = min\{\mathrm{gr}_{in}(UG) \mid U \in GL_k(F(z)), UG \in M_{k\times n}(\mathbb{F}[z])\}.$$

Ejemplo 3.10. Consideremos a G como $(z\ z^2+1\ z^3)$, la cual es una matriz generadora de un $(3,1)$-código de convolución sobre $\mathbb{F}(z)$. G es básica. En efecto, sea U un elemento de $GL_1(\mathbb{F}(z))$ tal que $UG \in M_{1\times 3}(\mathbb{F}[z])$, así $U \in \mathbb{F}[z] - \{0_{\mathbb{F}}\}$. Se satisface que

$$\begin{aligned}\mathrm{gr}_{in}(UG) &= max\{\mathrm{gr}(Uz),\ \mathrm{gr}(U(z^2+1)),\ \mathrm{gr}(Uz^3)\}\\ &= max\{\mathrm{gr}(U)+1,\ \mathrm{gr}(U)+2,\ \mathrm{gr}(U)+3\}\\ &= \mathrm{gr}(U)+3.\end{aligned}$$

Así, $min\{\mathrm{gr}_{in}(UG) \mid U \in \mathbb{F}[z] - \{0_{\mathbb{F}}\}\} = 3$. Por otro lado, se cumple que $\mathrm{gr}_{in}(G) = 3$. Por lo tanto, G es básica.

Ejemplo 3.11. Consideremos la siguiente matriz la cual es una matriz generadora polinomial de un $(2,2)$-código de convolución sobre $\mathbb{F}[z]$:

$$G = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}.$$

G es básica. En efecto, sea U un elemento de $GL_2(\mathbb{F}(z))$ tal que $UG \in M_{2\times 2}(\mathbb{F}[z])$, se tiene así que $U \in M_{2\times 2}(\mathbb{F}[z])$ con $det(U) \neq 0_{\mathbb{F}}$. Se satisface que $\mathrm{gr}_{in}(UG) = gr(det(U))$, pero U es una matriz polinomial así $gr(det(U)) \geq 0_{\mathbb{Z}} = \mathrm{gr}_{in}(G)$. Así

$$min\{\mathrm{gr}_{in}(UG) \mid U \in GL_2(\mathbb{F}(z)), UG \in M_{2\times 2}(\mathbb{F}[z])\} = \mathrm{gr}_{in}(G).$$

El determinar si una matriz generadora de un código de convolución es básica, tiene un elevado costo computacional, así que se desea dar una caracterización que reduzca tal costo. Esta caracterización siempre es posible.

Teorema 3.12. *Sea G una matriz generadora polinomial de un (n,k)-código de convolución sobre $\mathbb{F}(z)$. Las siguientes afirmaciones son equivalentes:*

1. *G es básica.*
2. *Los factores invariantes de G son unidades.*
3. *Los cerrados de Zariski asociados a los ideales generados por los factores invariantes de G son vacíos.*
4. *El cerrado de Zariski asociado al ideal generado por el máximo común divisor de los k-menores de G es vacío.*
5. *El máximo común divisor de los k-menores de G es una unidad.*
6. *Para toda α en la cerradura algebraica de $\mathbb{F}$, $G(\alpha)$ tiene rango k, donde $G(\alpha)$ es la especialización de G en α.*
7. *G es invertible por la derecha en $\mathbb{F}[z]$.*
8. *Para todo elemento v de $\mathbb{F}(z)^k$, si vG es un elemento de $\mathbb{F}^n[z]$, entonces v pertenece a $\mathbb{F}^k[z]$.*
9. *G es una submatriz de una matriz unimodular.*

Demostración. 1)→ 2). Debido al Teorema C.1, existen elementos P en $GL_k(\mathbb{F}[z])$ y Q en $GL_n(\mathbb{F}[z])$, tales que

$$PGQ = \begin{pmatrix} \alpha_1 & \dots & 0 & \\ \vdots & \ddots & \vdots & 0_{k\times(n-k)} \\ 0 & \dots & \alpha_k & \end{pmatrix} \tag{3.3}$$

donde $\alpha_1, \ldots, \alpha_k$ son los factores invariantes de G en $\mathbb{F}[z]$. Si denotamos por Δ_i al máximo común divisor de los i-menores no nulos de G, con $i \in \{1, \ldots, q\}$, se cumple que

$$\begin{aligned} \alpha_1 &= \Delta_1 \\ \alpha_i &= \frac{\Delta_i}{\Delta_{i-1}}, \quad i = 2, \ldots, k. \end{aligned}$$

Ahora, consideremos la siguiente matriz:

$$\Gamma_k = \begin{pmatrix} \alpha_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & \alpha_k \end{pmatrix}.$$

Así, $\Gamma_k^{-1}P$ es un elemento de $GL_k(\mathbb{F}(z))$, pues $det(\Gamma_k^{-1}P) = det(P)/\Delta_k \neq 0$. Más aún, $\Gamma_k^{-1}PG$ es una matriz generadora polinomial por lo que podemos estimar su grado interno.

$$\begin{aligned} gr_{in}(\Gamma_k^{-1}PG) &= gr(det(\Gamma_k^{-1}P)) + gr_{in}(G) \\ &= gr(det(P)/\Delta_k) + gr_{in}(G). \end{aligned}$$

Si $\Delta_k \notin \mathcal{U}(\mathbb{F}(z))$, entonces $gr(det(P)/\Delta_k) < 0$, implicando que $gr_{in}(\Gamma_k^{-1}PG) < gr_{in}(G)$, absurdo, pues G es básica. Así que $\Delta_k \in \mathcal{U}(\mathbb{F}(z))$, es decir, $\alpha_1 \cdots \alpha_k \in \mathcal{U}(\mathbb{F}(z))$. Por lo tanto $\alpha_i \in \mathcal{U}(\mathbb{F}(z))$ para toda $i \in \{1, \ldots, k\}$.

2)→ 3). De acuerdo a las definiciones dadas en la demostración anterior, podemos suponer que $\lambda_1, \ldots, \lambda_k$ son unidades de $\mathbb{F}[z]$. Así, para cada $i \in \{1, \ldots, k\}$, se tiene que $\mathbb{F}[z]\lambda_i = \mathbb{F}[z]$. Por el Lema B.3, el cerrado de Zariski $V(\mathbb{F}[z]\lambda_i)$ es vacío.

3)→ 4). Siguiendo la notación planteada en las anteriores demostraciones, Δ_k es el máximo común divisor de los k-menores de G y $\alpha_1, \ldots, \alpha_k$ son los factores invariantes de G en $\mathbb{F}[z]$. Se cumple que

$$\Delta_k = \alpha_1 \cdots \alpha_k.$$

Así, $V(\mathbb{F}[z]\Delta_k) = V(\mathbb{F}[z]\alpha_1 \cdots \alpha_k)$. Sin embargo, $V(\mathbb{F}[z]\alpha_1 \cdots \alpha_k) = V(\mathbb{F}[z]\alpha_1 \cdots \mathbb{F}[z]\alpha_k)$. Debido al Lema B.2, se sigue que $V(\mathbb{F}[z]\alpha_1 \cdots \mathbb{F}[z]\alpha_k) = V(\mathbb{F}[z]\alpha_1) \cup \cdots \cup V(\mathbb{F}[z]\alpha_k)$, por hipótesis estos cerrados son vacíos, por lo tanto $V(\mathbb{F}[z]\Delta_k) = \emptyset$.

4)→ 5). De acuerdo a la notación anterior, Δ_k es el máximo común divisor de los k-menores de G. Supongamos que $V(\mathbb{F}[z]\Delta_k)$ es vacío. Por el Lema B.3, se sigue que $\mathbb{F}[z]\Delta_k = \mathbb{F}[z]$, así Δ_k es una unidad de $\mathbb{F}[z]$.

5)→ 7). Supongamos que el máximo común divisor de los k-menores de G es una unidad. Denotemos a los k-menores de G por γ_j para $j \in \{1, \ldots, \binom{n}{k}\}$. Por la regla de Crammer, para cada $j \in \{1, \ldots, \binom{n}{k}\}$, hay una pseudo-inversa para G con factor γ_j, es decir, existe $H_j \in M_{n\times k}(\mathbb{F}[z])$ tal que

$$GH_j = \gamma_j I_k.$$

Debido a que el máximo común divisor de los γ_j's es una unidad, existe una combinación lineal polinomial de los γ_j's que es igual a $1_{\mathbb{F}}$. digamos que es

$$\Sigma_{j=1}^{\binom{n}{k}} \lambda_j \gamma_j = 1_{\mathbb{F}},$$

donde $\lambda_j \in \mathbb{F}[z]$ para toda $j \in \{1, \ldots, \binom{n}{k}\}$. De esto se sigue que

$$H = \Sigma_{j=1}^{\binom{n}{k}} \lambda_j H_j$$

es una matriz inversa polinomial derecha de G.

7)→ 8). Supongamos que G tiene una matriz inversa polinomial derecha H. Sea v un elemento de $\mathbb{F}(z)^k$. Si $vG \in \mathbb{F}^n[z]$, entonces $vGH \in \mathbb{F}^k[z]$, es decir, $v \in \mathbb{F}^k[z]$.

8)→ 1). Para verificar que G es básica, basta con mostrar que para todo elemento U de $GL_k(\mathbb{F}(z))$ tal que UG pertenece a $M_{k\times n}(\mathbb{F}[z])$, se cumple que

$$gr_{in}(UG) \geq gr_{in}(G).$$

Sea U un elemento de $GL_k(\mathbb{F}(z))$ tal que $UG \in M_{k\times n}(\mathbb{F}[z])$. Debido a la hipótesis se sigue que U es elemento de $M_{k\times n}(\mathbb{F}[z])$ y con ello que $gr(det(U)) \geq 0$. Por otro lado, del Teorema 3.9(2), se tiene que

$$gr_{in}(UG) = gr(det(U)) + gr_{in}(G).$$

Implicando con esto que $gr_{in}(UG) \geq gr_{in}(G)$.

5)→ 6). Sea α un elemento en la cerradura algebraica de $\mathbb{F}$ y sea $p(z)$ el polinomio minimal de α. Dado que el máximo común divisor de los k-menores de G es una unidad, se sigue que debe existir al menos un k-menor de G que no es divisible por $p(z)$, lo cual significa que el correspondiente k-menor de $G(\alpha)$ es invertible, es decir, $G(\alpha)$ tiene rango k.

6)→ 5). Supongamos que el máximo común divisor de los k-menores de G no es una unidad, lo cual significa que es divisible por algún polinomio irreducible $p(z)$. Si α es una raíz de $p(z)$ en alguna extensión de $\mathbb{F}$, entonces todo k-menor de $G(\alpha)$ es cero, así $G(\alpha)$ tiene rango menor que k.

2)→ 9). Supóngase que los factores invariantes de G son unidades. Así, la descomposición de G en la Ecuación 3.3, se puede escribir cómo:

$$G = A \begin{pmatrix} I_k & 0_{k\times(n-k)} \end{pmatrix} B$$

donde $A = P^{-1}\Gamma_k$ y $B = Q^{-1}$. Más aún, si descomponemos a B cómo:

$$B = \begin{pmatrix} B_U \\ B_L \end{pmatrix}$$

donde $B_U \in M_{k\times n}(\mathbb{F}[z])$ y $B_L \in M_{(n-k)\times n}(\mathbb{F}[z])$, entonces $G = AB_U$. Sin embargo, como la siguiente matriz fue obtenida a partir de la matriz unimodular B por medio de operaciones elementales de los primeros k renglones, se tiene es unimodular:

$$\begin{pmatrix} AB_U \\ B_L \end{pmatrix}.$$

9)→ 2). Si $B = \begin{pmatrix} G \\ H \end{pmatrix}$ es unimodular para algún H elemento de $M_{(n-k)\times n}(\mathbb{F}[z])$, entonces la siguiente ecuación muestra que los factores invariantes de G son unidades:

$$G = I_k \begin{pmatrix} \Gamma_k & 0_{k\times(n-k)} \end{pmatrix} B.$$

□

Ejemplo 3.13. Consideremos la siguiente matriz:

$$G = \begin{pmatrix} 1 & z & z^2 & z^4 \\ 0 & 1 & z & z^2 \end{pmatrix}.$$

G es una matriz generadora polinomial de un $(4, 2)$-código de convolución sobre $\mathbb{F}(z)$. Se afirma que G es básica pues el máximo común divisor de los 2-menores de G es 1.

Ejemplo 3.14. Consideremos la siguiente matriz:

$$G' = \begin{pmatrix} z & z^2 & z^3 & z^4 \end{pmatrix}.$$

G' es una matriz generadora polinomial de un $(4, 2)$-código de convolución sobre $\mathbb{F}(z)$ que no es básica, pues el máximo común divisor de los 2-menores de G' es z.

Ejemplo 3.15. La siguiente matriz es una matriz polinomial generadora de un $(4, 2)$-código de convolución sobre $\mathbb{F}(z)$:

$$G' = \begin{pmatrix} z & z^2 & z^3 & z^5 \\ 0 & z & z^2 & z^3 \end{pmatrix}.$$

G' no es básica pues el máximo común divisor de los 2-menores de G' es z^2.

La siguiente proposición nos permite encontrar una familia de matrices básicas a partir de dar una matriz básica, sólo con el concepto de matriz unimodular.

Proposición 3.16. *Sean G una matriz generadora básica de un (n, k)-código de convolución sobre $\mathbb{F}(z)$ y U un elemento de $GL_k(\mathbb{F}[z])$. Se tiene que UG es básica.*

Demostración. Se satisface que UG es una matriz generadora del mismo código de convolución que genera G. Además, se sabe que para todo elemento U' de $GL_k(\mathbb{F}(z))$ tal que $U'UG$ pertenece a $M_{k\times k}(\mathbb{F}[z])$, se tiene que $U'U$ es también un elemento de $GL_k(\mathbb{F}(z))$ tal que $U'UG$ esta en $M_{k\times n}(\mathbb{F}[z])$. Con ello se cumple que

$$min\{\mathrm{gr}_{in}(U'UG) \mid U' \in GL_k(\mathbb{F}(z)), U'UG \in M_{k\times n}(\mathbb{F}[z])\} \geq \mathrm{gr}_{in}(G).$$

Para verificar que UG es básica, basta con mostrar que $\mathrm{gr}_{in}(UG) = \mathrm{gr}_{in}(G)$, sin embargo esto se deduce del Teorema 3.9(2). □

Si pretendiéramos aplicar el concepto de matriz básica a las matrices generadoras de códigos de convolución sobre $\mathbb{F}[z]$ como lo hicimos en la Definición 3.7, entonces nuestra acción no tendría relevancia. Pues, diríamos que una matriz generadora G de un código de convolución sobre $\mathbb{F}[z]$ es básica si el grado interno $gr_{in}(G)$ de G es el mínimo de todos los grados mínimos de las matrices equivalentes a G. Sin embargo, siempre se cumple que $gr_{in}(UG) = gr_{in}(G)$ para toda matriz unimodular U, ver el Lema 3.8. Así que G siempre es básica.

O también, diríamos que una matriz generadora G de un código de convolución sobre $\mathbb{F}[z]$ es básica si es invertible en $\mathbb{F}[z]$ por la derecha, este hecho siempre ocurre pues G es matriz generadora, ver Teorema 2.10(3).

Es por eso que no tiene sentido extender el concepto de matriz básica a las matrices generadoras de códigos de convolución sobre $\mathbb{F}[z]$.

Ahora daremos una clase de matrices generadoras de códigos de convolución sobre $\mathbb{F}(z)$, llamadas matrices reducidas y mostraremos una caracterización de ellas.

Definición 3.8. Sea G una matriz generadora polinomial de un (n,k)-código de convolución sobre $\mathbb{F}(z)$. G es *reducida* si

$$\mathrm{gr}_{ex}(G) = min\{\mathrm{gr}_{ex}(UG) \mid U \in GL_k(F[z])\}.$$

Al igual que se ha observado en matrices básicas, el verificar si una matriz es reducida es costoso hablando computacionalmente, es por eso que se da el siguiente teorema que caracteriza tales matrices.

Teorema 3.17. *Sea $G = (g_{ij})$ una matriz generadora polinomial de un (n,k)-código de convolución sobre $\mathbb{F}(z)$. Denotemos los k renglones de G por $g_1, \ldots, g_k$ y sean $e_1, \ldots, e_k$ sus respectivos grados. Las siguientes afirmaciones son equivalentes:*

1. *G es reducida.*

2. *$\bar{G}$ tiene rango k, donde $\bar{G} = (\bar{g}_{ij})$ y $\bar{g}_{ij}$ es el coeficiente de z^{e_i} en g_{ij}, para toda $i \in \{1, \ldots, k\}$ y toda $j \in \{1, \ldots, n\}$.*
3. *$gr_{ex}(G) = gr_{in}(G)$.*
4. *Para todo elemento $v = (v_1, \ldots, v_k)$ de $\mathbb{F}^k[z]$, se cumple que*

$$gr(vG) = max\{gr(v_i) + e_i \mid i = 1, \ldots, k\}.$$

Demostración. 1)→ 2). Sin pérdida de generalidad, consideremos que G tiene ordenados sus renglones de manera que $e_1 \leq \ldots \leq e_k$. Supongamos que $\bar{G}$ tiene rango menor que k, así pues existe $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{F}^k$ tal que $\alpha\bar{G} = 0_{\mathbb{F}^n}$. Y de esto, se tiene que el coeficiente de z^{e_k} es cero en

$$g'_k = \alpha_1 z^{e_k - e_1} g_1 + \ldots + \alpha_k z^{e_k - e_k} g_k.$$

Si reemplazamos a g_k por g'_k en G, entonces se tiene que G ha reducido su grado externo. Así, G no es reducida.

2)→ 3). Denotemos las k-submatrices de $\bar{G}$ por $\bar{G}_s$, para $s = 1, \ldots, \binom{n}{k}$. Dado que $\bar{G}$ tiene rango k existe algún $s_0 \in \{1, \ldots, \binom{n}{k}\}$, tal que $det(\bar{G}_{s_0}) \neq 0_{\mathbb{F}}$. Más aún, el coeficiente de $z^{e_1+\ldots+e_k}$ en $det(G_{s_0})$ es $det(\bar{G}_{s_0})$. Por lo tanto $gr_{in}(G) \geq gr_{ex}(G)$. Y del Teorema 3.9(1), la otra desigualdad siempre se cumple para toda matriz polinomial .

3)→ 1). Para verificar que G es reducida, basta con mostrar que para toda matriz unimodular U de tamaño k se cumple que $gr_{ex}(UG) \geq gr_{ex}(G)$.
Sea $U \in GL_k(\mathbb{F}[z])$. Se tiene por el Teorema 3.9(1) que $gr_{ex}(UG) \geq gr_{in}(UG)$. Sin embargo, del Teorema 3.9(2) se cumple que $gr_{in}(UG) \geq gr_{in}(G)$. Además, la hipótesis es que $gr_{in}(G) = gr_{ex}(G)$. Así, combinando estas desigualdades se satisface lo deseado.

2)↔ 4). Sea $v = (v_1, \ldots, v_k)$ un elemento de $\mathbb{F}^k[z]$. Se sigue que $vG = v_1 g_1 + \ldots + v_k g_k$.
Si denotamos el grado de v_i por d_i, para toda $i = 1, \ldots, k$, entonces el $gr(vG)$ es a lo más

$$d = max\{d_i + e_i \mid i = 1, \ldots, k\}.$$

d es llamado la *predicción* de vG. Para probar la predicción, notemos que el vector de los coeficientes de z^d en vG es $(\alpha_1, \ldots, \alpha_k)\bar{G}$, donde α_i es el coeficiente de z^{d-e_i} en v_i, para toda $i = 1, \ldots, k$.
Así $gr(vG) = d$ si, y sólo si, existe $i_0 \in \{1, \ldots, k\}$ tal que $\alpha_{i_0} \neq 0_{\mathbb{F}}$, esto es equivalente a que $(\alpha_1, \ldots, \alpha_k)\bar{G} \neq 0_{\mathbb{F}^n}$, implicando que $\bar{G}$ tiene rango k.
Por otro lado, si $\bar{G}$ tiene rango k, entonces para toda α en $\mathbb{F}^k$ se tiene que $\alpha\bar{G} \neq 0_{\mathbb{F}^n}$. Por lo tanto, para todo $v \in \mathbb{F}^k[z]$, se cumple que $gr(vG) = max\{d_i + e_i \mid i = 1, \ldots, k\}$.

□

Ejemplo 3.18. Como se ha mencionado, la matriz del Ejemplo 3.11 cumple que su grado interno es igual a su grado externo. Por lo tanto, tal matriz es reducida.

Ejemplo 3.19. El grado interno de la matriz del Ejemplo 3.13 es 6, mientras que su grado externo es 5. Por lo tanto esta matriz no es reducida.

Ejemplo 3.20. Por el Lema 3.5 se tiene que la matriz del Ejemplo 3.14 es reducida.

Ejemplo 3.21. La matriz del Ejemplo 3.15 no es reducida pues su grado interno es 7 y su grado externo es 6.

Podemos extender el concepto de matriz reducida en las matrices generadoras de los códigos de convolución sobre $\mathbb{F}[z]$. Diremos así, que una matriz generadora de un código de convolución sobre $\mathbb{F}[z]$ es reducida si tiene el minimo grado externo sobre todas las matrices equivalentes a ella. Así, las afirmaciones del anterior teorema son aplicables a tales matrices.

Por otro lado, deseamos precisar si la matriz que estamos empleando para generar un código de convolución sobre $\mathbb{F}(z)$ es de grado externo mínimo sobre todas las posibles matrices que nos generen dicho código de convolución. Tal condición la cumplen las matrices minimales. Demos el concepto de matriz minimal

Definición 3.9. Sea G una matriz generadora polinomial de un (n,k)-código de convolución sobre $\mathbb{F}(z)$. G es *minimal* si

$$\mathrm{gr}_{ex}(G) = min\{\mathrm{gr}_{ex}(UG) \mid U \in GL_k(\mathbb{F}(z)), UG \in M_{k\times n}(\mathbb{F}[z])\}.$$

El encontrar todas las matrices que nos generen un código de convolución se convierte en una laboriosa tarea. Por lo que, la siguiente proposición nos facilita el trabajo al verificar si una matriz es minimal.

Proposición 3.22. *Sea G una matriz generadora polinomial de un (n,k)-código de convolución sobre $\mathbb{F}(z)$. Se satisface que G es minimal si, y sólo si, es básica y reducida.*

Demostración. Primero veamos que es suficiente que G sea minimal, para que sea básica y reducida.
Para verificar que G sea básica es equivalente a mostrar que, para todo elemento U en $GL_k(\mathbb{F}(z))$ tal que $UG \in M_{k\times n}(\mathbb{F}[z])$, se cumple que $gr_{in}(UG)$ es mayor o igual que $gr_{in}(G)$, esto se deduce del Teorema 3.9(2).
Y para mostrar que G es reducida es equivalente a verificar que, para todo elemento U en $GL_k(\mathbb{F}[z])$, se tiene que $gr_{ex}(UG)$ es mayor o igual que $gr_{ex}(G)$. En efecto, sea U un elemento de $GL_k(\mathbb{F}[z])$. Así, UG es un elemento de $M_{k\times n}(\mathbb{F}[z])$, y dado que G es minimal, se concluye que $gr_{ex}(UG) \geq gr_{ex}(G)$.

Resta verificar que para que G sea minimal es necesario que sea básica y reducida. En efecto, sea U un elemento de $GL_k(\mathbb{F}(z))$ tal que UG pertenece a $M_{k\times n}(\mathbb{F}[z])$, por mostrar que $gr_{ex}(UG)$ es mayor o igual que $gr_{ex}(G)$.
Observe que del Lema 3.4 se tiene que $gr_{ex}(UG) \geq gr_{in}(UG)$. Dado que G es básica, se deduce que $gr_{ex}(UG) \geq gr_{in}(G)$. Más aún, como G es reducida se concluye que $gr_{ex}(UG) \geq gr_{ex}(G)$. □

Ejemplo 3.23. La matriz del Ejemplo 3.11 es minimal, pues es básica y reducida.

Ejemplo 3.24. La matriz del Ejemplo 3.13 no es minimal, pues aunque es básica, no es reducida.

Ejemplo 3.25. La matriz del Ejemplo 3.14 no es minimal, pues no es básica aunque si reducida.

Ejemplo 3.26. La matriz del Ejemplo 3.15 no es minimal, dado que no es básica ni reducida.

Observación 3.10. Si definimos a las matrices minimales de los códigos de convolución sobre $\mathbb{F}[z]$ de manera análoga en cómo lo hemos hecho en la Definición 3.9, entonces es lo mismo etiquetar como matriz minimal que como matriz reducida a las matrices generadoras de códigos de convolución sobre $\mathbb{F}[z]$. Por lo que solo nos quedaremos con la etiqueta de matriz minimal cuando hablemos de las matrices generadoras de códigos de convolución sobre $\mathbb{F}[z]$.

Definición 3.11. Sea G una matriz generadora de un (n,k)-código de convolución sobre $\mathbb{F}[z]$. G es *minimal* si $\mathrm{gr}_{ex}(G) = min\{\mathrm{gr}_{ex}(UG) \mid U \in GL_k(\mathbb{F}[z])\}$.

Sin embargo, como lo vimos anteriormente si una matriz generadora de un código de convolución sobre $\mathbb{F}[z]$ es minimal, es lo mismos que decir que es reducida. Tenemos así el siguiente resultado:

Proposición 3.27. *Sea G una matriz generadora de un (n,k)-código de convolución sobre $\mathbb{F}[z]$. Se satisface que G es minimal si, y sólo si, $gr_{in}(G) = gr_{ex}(G)$.*

Ejemplo 3.28. La matriz del ejemplo 3.1, no es minimal.

Ejemplo 3.29. La matriz del ejemplo 3.6, es minimal.

En general, un código de convolución sobre $F(z)$ puede tener diferentes matrices minimales, sin embargo, todas estas matrices comparten algunas características, por ejemplo, algunas de ellas se enuncian en los siguientes teoremas, cuyas demostraciones se encuentran en (11, Corolario 3.9, Teorema 3.10):

Teorema 3.30. *Sean G y G' matrices generadoras polinomiales de un (n,k)-código de convolución sobre $\mathbb{F}(z)$ donde G es minimal. Sean los conjuntos $\{e_1,\ldots,e_k\}$ y $\{f_1,\ldots,f_k\}$ consistentes de los grados por renglón de estas matrices, respectivamente, tales que $e_1 \leq \ldots \leq e_k$ y $f_1 \leq \ldots \leq f_k$. Se cumple que $e_i \leq f_i$ para toda $i = 1,\ldots,k$.*

Teorema 3.31. *El conjunto de grados de los renglones de las matrices minimales es el mismo para cualquier* (n, k)*-código de convolución sobre* $\mathbb{F}(z)$.

Debido a este último teorema, es que podemos decir que el conjunto de los grados de los renglones de una matriz minimal es invariante para un (n, k)-código de convolución sobre $\mathbb{F}(z)$. Es por eso que damos la siguiente definición:

Definición 3.12. Sean C un (n, k)-código de convolución sobre $\mathbb{F}(z)$ con G una matriz generadora minimal. Los *índices de Forney* de C forman el conjunto $\{e_1, \ldots, e_k\}$ donde e_i es el grado del i-ésimo renglón de G, para $i = 1, \ldots, k$, tal que $e_1 \leq \ldots \leq e_k$. La *memoria* de C es e_k.

Ejemplo 3.32. El índice de Forney del $(3, 1)$-código de convolución sobre $\mathbb{F}(z)$ del Ejemplo 3.11 es 3. Y tal código de convolución tiene memoria 3.

Al igual, que los códigos sobre $\mathbb{F}(z)$, se cumple en los códigos sobre $\mathbb{F}[z]$ que las matrices minimales tienen el mínimo grado para sus renglones respecto a otras matrices generadoras y que el conjunto de grados de los renglones de las matrices minimales es el mismo para cualquier (n, k)-código de convolución sobre $\mathbb{F}(z)$. Es por ello que es posible dar la siguiente definición:

Definición 3.13. Sean C un (n, k)-código de convolución sobre $\mathbb{F}[z]$ con G una matriz generadora minimal. Los *índices de Forney* de C forman el conjunto $\{e_1, \ldots, e_k\}$ donde e_i es el grado del i-ésimo renglón de G, para $i = 1, \ldots, k$, tal que $e_1 \leq \ldots \leq e_k$. La *memoria* de C es e_k.

Y como es claro, se cumple que el grado de un código de convolución es la suma de sus índices de Forney. Por lo que se ha dado una manera más sencilla de estimar este parámetro. Por otro lado, la memoria índica el número de palabras información necesarias para dar una palabra del código de convolución.

Líneas Abiertas de Investigación

Todavía queda mucho por hacer en códigos lineales y códigos de convolución, esta tesis ha aportado algunas ideas y contribuciones. Otros aspectos esperan ser resueltos, es por ello que este apartado se enumera algunas ideas que considero pueden servir de punto inicial de partida para su planteamiento.

Con esta tesis aporte el concepto de códigos lineales que extiende a los códigos lineales clásicos. Al considerar los códigos lineales como submódulos de módulos libres de rango finito sobre anillos finitos, además de considerar la dimensión de tales códigos como la longitud del código visto como módulo sobre el anillo finito. Es por ello que una primera línea de investigación, es extender lo más posible estás definiciones y que sigan siendo compatibles con la teoría existente.

Además, proporcione una generalización a la ya conocida cota de Singleton, dándola en términos de longitud de módulos. Sin embargo, uno pensaría que es posible tomar como línea de investigación el mejorar esta cota, pero di ejemplos de códigos lineales que satisfacían la igualdad en tal cota. Por lo que sería más prudente proponer una distancia que generalice la distancia de Hamming que se enunció, intentando con esto, proponer nuevas relaciones entre los parámetros de los códigos lineales.

Respecto a los códigos de convolución, también plante una generalización de estos, con respecto a los ya anteriormente establecidos. Al hacer este planteamiento, sólo extendí los parámetros de longitud y rango de así como la matriz generadora de estos, falta aún extender los demás parámetros, por ejemplo, el grado.

Apéndices

APÉNDICE A

Teoría de Módulos en Breve

En este apéndice se darán las definiciones de producto directo de módulos así como la suma directa de módulos para con ello dar el concepto de módulos libres y su rango, también se demostrarán las propiedades de producto tensorial que se utilizaron en algunas demostraciones del capítulo 2. Además en este apéndice se concretará el concepto de longitud de un módulo sobre un anillo y se aducirán algunas propiedades que se cumplen en módulos de longitud finita. Para más detalles, ver (1; 10).

Durante el apéndice, A es un anillo.

1. Producto Directo y Suma Directa de Módulos

En esta sección veremos que a partir de una familia de módulos sobre el mismo anillo se construye un nuevo módulo sobre el anillo dado, esta construcción está basada en el concepto del producto cartesiano de conjuntos. Además exhibiremos un submódulo particular del producto directo de módulos llamado suma directa de dichos módulos. Aún más se demostrarán las propiedades universales tanto del producto directo como de la suma directa.

Definición A.1. Sea $(M_i)_{i\in I}$ una familia de A-módulos con I un conjunto no vacío. El *producto directo* o simplemente *producto* de los M_i's es el conjunto

$$\left\{(m_i)_{i\in I}\middle|\ m_i \in M_i,\ \text{para toda } i \in I\right\},$$

que denotaremos por $\prod_{i\in I} M_i$.

De una manera natural se tiene que $(\prod_{i\in I} M_i, +, \bullet)$ es un módulo sobre A con la adición $+$ y la multiplicación $\bullet$ definidas por:

$$\begin{array}{rccc} + : & \prod_{i\in I} M_i \times \prod_{i\in I} M_i & \longrightarrow & \prod_{i\in I} M_i \\ & \left((m_i)_{i\in I}, (m_i')_{i\in I}\right) & \mapsto & (m_i)_{i\in I} + (m_i')_{i\in I} = (m_i + m_i')_{i\in I}. \end{array}$$

$$\begin{array}{rccc} \bullet : & A \times \prod_{i\in I} M_i & \longrightarrow & \prod_{i\in I} M_i \\ & (a, (m_i)_{i\in I}) & \mapsto & a \bullet (m_i)_{i\in I} = (a \cdot m_i)_{i\in I}. \end{array}$$

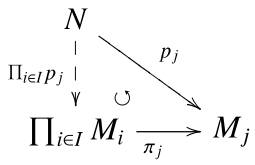
Por ejemplo verifiquemos que la multiplicación $\bullet$ está bien definida.
Sean $(a,(m_i)_{i\in I})$ y $(a',(m'_i)_{i\in I})$ elementos de $(A\times\prod_{i\in I}M_i)$ tales que $(a,(m_i)_{i\in I})=(a',(m'_i)_{i\in I})$. Así $a=a'$ y $m_i=m'_i$ para toda $i\in I$. Por lo que para toda $i\in I$ se cumple que $a\cdot m_i=a'\cdot m'_i$. Por lo tanto, $(a\cdot m_i)_{i\in I}=(a\cdot m'_i)_{i\in I}$.

Proposición A.1. *Sea $(M_i)_{i\in I}$ una familia de A-módulos con I un conjunto no vacío. Para cada $j\in I$, la aplicación*

$$\begin{array}{rccc}\pi_j: & \prod_{i\in I}M_i & \longrightarrow & M_j\\ & (m_i)_{i\in I} & \mapsto & \pi_j((m_i)_{i\in I})=m_j\end{array}$$

es un morfismo sobreyectivo de A-módulos. A π_j se le llama la proyección *del producto $\prod_{i\in I}M_i$ a la componente M_j, y a $(\pi_j)_{j\in I}$ se le llama* familia de proyecciones *de $\prod_{i\in I}M_i$*

Teorema A.2. ***Propiedad Universal del Producto Directo de Módulos.***
Sea $\prod_{i\in I}M_i$ el producto de la familia $(M_i)_{i\in I}$ de A-módulos con I un conjunto no vacío y sea la familia de proyecciones $(\pi_j)_{j\in I}$ de $\prod_{i\in I}M_i$.
Si N es un A-módulo con una familia de morfismos de A-módulos $(p_j)_{j\in I}$ donde $p_j: N\to M_j$ para toda $j\in I$, entonces existe un único morfismo de A-módulos $\Pi_{i\in I}p_i: N\to\prod_{i\in I}M_i$ tal que $\pi_j\circ\Pi_{i\in I}p_i=p_j$ para toda $j\in I$, es decir, para toda $j\in I$, el siguiente diagrama es conmutativo:



Demostración. Consideremos la siguiente función

$$\begin{array}{rccc}\Pi_{i\in I}p_i: & N & \longrightarrow & \prod_{i\in I}M_i\\ & n & \mapsto & \prod_{i\in I}p_i\,(n)=(p_i(n))_{i\in I}.\end{array}$$

Es inmediato que $\Pi_{i\in I}p_i$ es un morfismo de A-módulos. Más aún, para toda $j\in I$ se sigue que $\pi_j\circ\Pi_{i\in I}p_i=p_j$. En efecto, sea $n\in N$.

$$\begin{aligned}\pi_j\circ\Pi_{i\in I}p_i(n) &= \pi_j(\Pi_{i\in I}p_i(n))\\ &= \pi_j((p_i(n))_{i\in I})\\ &= p_j(n).\end{aligned}$$

Lo que queda por verificar es que $\Pi_{i\in I}p_i$ es única. Esto es, para todo $g\in\mathrm{Hom}_A(N,\prod_{i\in I}M_i)$ tal que $\pi_j\circ g=p_j$ para toda $j\in I$, se tiene que $g=\prod_{i\in I}p_i$. Consideremos un tal g, se sigue que para todo

$n \in N$:

$$\begin{aligned} g(n) &= (\pi_j(g(n)))_{j\in I} \\ &= (\pi_j \circ g(n))_{j\in I} \\ &= (\pi_j \circ \Pi_{i\in I} p_i(n))_{j\in I} \\ &= (\pi_j(\Pi_{i\in I} p_i(n)))_{j\in I} \\ &= \Pi_{i\in I} p_i(n). \end{aligned}$$

Así $g(n) = \prod_{i\in I} p_i(n)$ para todo $n \in N$. Por lo tanto, $g = \prod_{i\in I} p_i$. □

Una caracterización de la propiedad universal del producto de módulos es la siguiente:

Proposición A.3. *Sean $(M_i)_{i\in I}$ una familia de A-módulos con I un conjunto no vacío y N un A-módulo. Los A-módulos $\mathrm{Hom}_A(N, \prod_{i\in I} M_i)$ y $\prod_{i\in I} \mathrm{Hom}_A(N, M_i)$ son isomorfos.*

Demostración. Sea la familia de proyecciones $(\pi_j)_{j\in I}$ de $\prod_{i\in I} M_i$.
Considere la asignación Ψ dada por:

$$\begin{array}{rccc} \Psi: & \mathrm{Hom}_A(N, \prod_{i\in I} M_i) & \longrightarrow & \prod_{i\in I} \mathrm{Hom}_A(N, M_i) \\ & \varphi & \mapsto & \Psi(\varphi) = (\pi_i \circ \varphi)_{i\in I} \end{array}$$

Por demostrar que Ψ está bien definida. Sean φ y ϕ elementos de $\mathrm{Hom}_A(N, \prod_{i\in I} M_i)$ tales que $\varphi = \phi$, por demostrar que $\Psi(\varphi) = \Psi(\phi)$, es decir, que para toda $i \in I$ se tiene que $\pi_i \circ \varphi = \pi_i \circ \phi$. En efecto, sean $i \in I$ y $n \in N$, así

$$\begin{aligned} (\pi_i \circ \varphi)(n) &= \pi_i(\varphi(n)) \\ &= \pi_i(\phi(n)) \\ &= (\pi_i \circ \phi)(n). \end{aligned}$$

Se sigue que Ψ es A-lineal pues la operación composición lo es. Además Ψ es inyectiva, pues $\ker(\Psi) = \{0_{\mathrm{Hom}_A(N, \prod_{i\in I} M_i)}\}$. En efecto, sea $\varphi \in \mathrm{Hom}_A(N, \prod_{i\in I} M_i)$.

$$\begin{aligned} \varphi \in \ker(\Psi) &\Leftrightarrow \Psi(\varphi) = 0_{\prod_{i\in I} \mathrm{Hom}_A(N, M_i)} \\ &\Leftrightarrow (\pi_i \circ \varphi)_{i\in I} = (0_{\mathrm{Hom}_A(N, M_i)})_{i\in I} \\ &\Leftrightarrow \pi_i \circ \varphi = 0_{\mathrm{Hom}_A(N, M_i)}, \text{ para toda } i \in I \\ &\Leftrightarrow (\pi_i \circ \varphi)(n) = 0_{M_i}, \text{ para toda } n \in N \text{ y para toda } i \in I \\ &\Leftrightarrow \pi_i(\varphi(n)) = 0_{M_i}, \text{ para toda } i \in I \text{ y para toda } n \in N \\ &\Leftrightarrow \varphi(n) = 0_{\prod_{i\in I} M_i}, \text{ para toda } n \in N \\ &\Leftrightarrow \varphi = 0_{\mathrm{Hom}_A(N, \prod_{i\in I} M_i)}. \end{aligned}$$

Por otro lado, Ψ es sobreyectiva por la propiedad universal del producto. En efecto, sea $(f_i)_{i\in I}$ un elemento de $\prod_{i\in I}\mathrm{Hom}_A(N, M_i)$, existe $\prod_{i\in I} f_i$ un elemento de $\mathrm{Hom}_A(N, \prod_{i\in I} M_i)$ tal que $\pi_i \circ \prod_{i\in I} f_i = f_i$ para toda $i \in I$. Por lo tanto, $\Psi(\prod_{i\in I} f_i) = (\pi_i \circ \prod_{i\in I} f_i)_{i\in I} = (f_i)_{i\in I}$. □

Un submódulo particular del producto directo de módulos es la suma directa, veamos cómo se define.

Definición A.2. Sea $(M_i)_{i\in I}$ una familia de A-módulos con I un conjunto no vacío. La *suma directa* de los M_i's es el siguiente subconjunto del producto $\prod_{i\in I} M_i$:

$$\left\{(m_i)_{i\in I} \in \prod_{i\in I} M_i \,\middle|\, m_i = 0_{M_i}, \text{ para toda } i \in I - J \text{ donde } J \subseteq I \text{ finito}\right\},$$

que denotaremos por $\bigoplus_{i\in I} M_i$.

Se tiene que $\bigoplus_{i\in I} M_i$ es un A-submódulo de $(\prod_{i\in I} M_i, +, \bullet)$.

Proposición A.4. *Sea $(M_i)_{i\in I}$ una familia de A-módulos con I un conjunto no vacío. Para cada $j \in I$, la aplicación*

$$\begin{array}{rccl} \iota_j : & M_j & \longrightarrow & \oplus_{i\in I} M_i \\ & m & \mapsto & \iota_j(m) = (m_i)_{i\in I} \text{ donde } m_i = \begin{cases} m & \text{si } i = j, \\ 0_{M_i} & \text{si } i \in I - \{j\}. \end{cases} \end{array}$$

es un morfismo inyectivo de A-módulos. A ι_j se le llama la inclusión *de la componente M_j en la suma directa $\oplus_{i\in I} M_i$, y a $(\iota_j)_{j\in I}$ se le llama* familia de inclusiones *en $\oplus_{i\in I} M_i$.*

Teorema A.5. ***Propiedad Universal de la Suma Directa de Módulos.***
Sea $\oplus_{i\in I} M_i$ la suma directa de la familia $(M_i)_{i\in I}$ de A-módulos donde I es un conjunto no vacío con la familia de inclusiones $(\iota_j)_{j\in I}$ en $\oplus_{i\in I} M_i$.
Sea N un A-módulo con una familia de morfismos de A-módulos $(f_j)_{j\in I}$ donde $f_j : M_j \to N$ para toda $j \in I$, entonces existe un único morfismo de A-módulos $\oplus_{i\in I} f_i : \oplus_{i\in I} M_i \to N$ tal que $(\oplus_{i\in I} f_i) \circ \iota_j = f_j$ para toda $j \in I$, es decir, para toda $j \in I$ se tiene que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} M_j & & \\ {\scriptstyle \iota_j}\downarrow & \circlearrowleft & \searrow^{f_j} \\ \oplus_{i\in I} M_i & \xrightarrow[\oplus_{i\in I} f_i]{} & N \end{array}$$

Demostración. Con la notación del teorema, consideremos la siguiente asignación:

$$\begin{array}{rccl} \oplus_{i\in I} f_i : & \oplus_{i\in I} M_i & \longrightarrow & N \\ & (m_i)_{i\in I} & \mapsto & \oplus_{i\in I} f_i\,((m_i)_{i\in I}) = \Sigma_{i\in I} f_i(m_i). \end{array}$$

Es inmediato que $\oplus_{i\in I}$ es un morfismo de A-módulos. Más aún para toda $j \in I$ se cumple que $(\oplus_{i\in I} f_i) \circ \iota_j = f_j$. En efecto, Sea $m \in M_j$, se cumple que

$$((\oplus_{i\in I} f_i) \circ \iota_j)(m) = \oplus_{i\in I} f_i\ (\iota_j(m))$$

sin embargo $\iota_j(m) = (m_i)_{i\in I}$ donde $m_j = m$ y $m_i = 0_{M_i}$, para toda $i \in I - \{j\}$. Así $\oplus_{i\in I} f_i\ ((m_i)_{i\in I}) = f_j(m)$. Por lo tanto, $((\oplus_{i\in I} f_i) \circ \iota_j)(m) = f_j(m)$.
Falta verificar que $\oplus_{i\in I} f_i$ es única, es decir, que para toda $g \in \mathrm{Hom}_{\mathrm{A}}(\oplus_{i\in I} M_i, N)$ tal que $g \circ \iota_j = f_j$ para toda $j \in I$, se cumple que $\oplus_{i\in I} f_i = g$. En efecto, sea g con tales características y sea $(m_i)_{i\in I} \in \oplus_{i\in I} M_i$,

$$\begin{aligned}
g((m_i)_{i\in I}) &= g(\Sigma_{i\in I}\iota_i(m_i)) \\
&= \Sigma_{i\in I} g(\iota_i(m_i)) \\
&= \Sigma_{i\in I}(g \circ \iota_i)(m_i) \\
&= \Sigma_{i\in I} f_i(m_i) \\
&= \Sigma_{i\in I}(\oplus_{i\in I} f_i \circ \iota_i)(m_i) \\
&= \Sigma_{i\in I}(\oplus_{i\in I} f_i(\iota_i(m_i)) \\
&= (\oplus_{i\in I} f_i)(\Sigma_{i\in I}\iota_i(m_i)) \\
&= (\oplus_{i\in I} f_i)((m_i)_{i\in I}).
\end{aligned}$$

□

La propiedad universal de la suma de módulos tiene una caracterización dada en la siguiente proposición:

Proposición A.6. *Sean $(M_i)_{i\in I}$ una familia de A-módulos con I un conjunto no vacío y N un A-módulo. Los A-módulos* $\mathrm{Hom}_{\mathrm{A}}(\oplus_{i\in I} M_i, N)$ *y* $\prod_{i\in I} \mathrm{Hom}_{\mathrm{A}}(M_i, N)$ *son isomorfos.*

Demostración. Sea la familia de inclusiones $(\iota_j)_{j\in I}$ en $\oplus_{i\in I} M_i$.
Considere la asignación Φ dada por:

$$\begin{array}{rccc}
\Phi: & \mathrm{Hom}_{\mathrm{A}}(\oplus_{i\in I} M_i, N) & \longrightarrow & \prod_{i\in I} \mathrm{Hom}_{\mathrm{A}}(M_i, N) \\
& \varphi & \mapsto & \Phi(\varphi) = (\varphi \circ \iota_i)_{i\in I}
\end{array}$$

Por demostrar que Φ está bien definida. Sean φ y ϕ elementos de $\mathrm{Hom}_{\mathrm{A}}(\oplus_{i\in I} M_i, N)$ tales que $\varphi = \phi$, por demostrar que $\Phi(\varphi) = \Phi(\phi)$, es decir, que para toda $i \in I$ se tiene que $\varphi \circ \iota_i = \phi \circ \iota_i$. En efecto,

sean $i \in I$ y $x \in \oplus_{i\in I} M_i$, así

$$\begin{aligned}(\varphi \circ \iota_i)(x) &= \varphi(\iota_i(x)) \\ &= \phi(\iota_i(x)) \\ &= (\phi \circ \iota_i)(x).\end{aligned}$$

Aún más Φ es A-lineal pues la operación composición lo es. También Φ es inyectiva, dado que $\ker(\Phi) = \{0_{\mathrm{Hom}_A(\oplus_{i\in I} M_i, N)}\}$. En efecto, sea $\varphi \in \mathrm{Hom}_A(\oplus_{i\in I} M_i, N)$.

$$\begin{aligned}\varphi \in \ker(\Phi) &\Leftrightarrow \Phi(\varphi) = 0_{\prod_{i\in I} \mathrm{Hom}_A(M_i,N)} \\ &\Leftrightarrow (\varphi \circ \iota_i)_{i\in I} = (0_{\mathrm{Hom}_A(M_i,N)})_{i\in I} \\ &\Leftrightarrow \varphi \circ \iota_i = 0_{\mathrm{Hom}_A(M_i,N)}, \text{ para toda } i \in I \\ &\Leftrightarrow (\varphi \circ \iota_i)(m_i) = 0_{M_i}, \text{ para toda } m_i \in M_i \text{ y para toda } i \in I \\ &\Leftrightarrow \varphi(\iota_i(m_i)) = 0_{M_i}, \text{ para toda } m_i \in M_i \text{ y para toda } i \in I \\ &\Leftrightarrow \varphi((m_i)_{i\in I}) = 0_{M_i}, \text{ para toda } (m_i)_{i\in I} \in \oplus_{i\in I} M_i \\ &\Leftrightarrow \varphi = 0_{\mathrm{Hom}_A(\oplus_{i\in I} M_i, N)}.\end{aligned}$$

Por otro lado, Φ es sobreyectiva por la propiedad universal del producto. En efecto, sea $(f_i)_{i\in I}$ un elemento de $\prod_{i\in I} \mathrm{Hom}_A(M_i, N)$, existe $\oplus_{i\in I} f_i$ un elemento de $\mathrm{Hom}_A(\oplus_{i\in I} M_i, N)$ tal que $(\oplus_{i\in I} f_i) \circ \iota_i = f_i$ para toda $i \in I$. Por lo tanto, $\Psi(\oplus_{i\in I} f_i) = ((\prod_{i\in I} f_i) \circ \iota_i)_{i\in I} = (f_i)_{i\in I}$. □

Observación A.3. Con la notación anterior, claramente se concluye que si I es un conjunto finito, entonces $\prod_{i\in I} M_i = \bigoplus_{i\in I} M_i$, para toda familia de A-módulos $(M_i)_{i\in I}$ indexada por I.

2. Módulos Libres

En esta sección definiremos los módulos libres y sus rangos. Además demostraremos que cuando el rango es finito este es único.

Los módulos libres salvo isomorfismo es una clase particular de la suma directa de módulos. En efecto, si $(M_i)_{i\in I}$ es una familia de A-módulos con I un conjunto no vacío, tal que $M_i = A$ para toda $i \in I$, entonces en este caso especial la suma directa se denota por $A^{(I)}$. Más aún, si I es un conjunto finito de cardinal n con $n \in \mathbb{Z}_+$, entonces $A^{(I)}$ se denota como A^n. Por convención A^0 es el módulo cero. Esto da pie al concepto de módulos libres:

Definición A.4. Sea M un A-módulo. M es *libre* si es isomorfo a $A^{(I)}$ donde I es un conjunto. Además, a la cardinalidad del conjunto I se le conoce como *rango* del módulo libre. Si la cardinalidad de I es finita se dice que el módulo libre es de *rango finito*.

Una característica suave de los módulos libres es el hecho de que dos módulos libres de rango finito son isomorfos si, y sólo si, tienen el mismo rango. Esto lo demostraremos a continuación.

PROPOSICIÓN A.7. *Sean M y N módulos libres sobre A de rango finito m y n respectivamente. Se cumple que M y N son isomorfos si, y sólo si, los enteros n y m son iguales.*

DEMOSTRACIÓN. Basta con mostrar que $A^m \cong_A A^n$ si, y sólo si, $m = n$.
La condición de necesidad claramente se cumple. Basta verificar la condición de suficiencia de la afirmación.
Sea $\mathfrak{m} \in \mathrm{Max}(A)$. Al tensorizar con el campo $A/\mathfrak{m}$ se preserva el isomorfismo, es decir

$$A^m \otimes_A \frac{A}{\mathfrak{m}} \cong A^n \otimes_A \frac{A}{\mathfrak{m}}$$

Dado que la suma directa es compatible con el producto tensorial, se tiene que

$$\left(A \otimes_A \frac{A}{\mathfrak{m}}\right)^m \cong \left(A \otimes_A \frac{A}{\mathfrak{m}}\right)^n$$

El producto tensorial de cualquier A-módulo con el anillo A como A-módulos es isomorfo al módulo. Por lo que tenemos que

$$\left(\frac{A}{\mathfrak{m}}\right)^m \cong \left(\frac{A}{\mathfrak{m}}\right)^n$$

La dimensión de espacios vectoriales es única, por lo tanto, $m = n$. □

De esta proposición se concluye que el rango esta unívocamente determinado en los módulos de rango finito.

3. Producto Tensorial en Breve

En el capítulo 2, se ha mencionado el producto tensorial y se ha utilizado en algunas de sus propiedades, en esta sección se darán las demostraciones de tales propiedades usadas. Para ello se seguirá lo desarrollado por Atiyah en (1).

DEFINICIÓN A.5. Sean M y N A-módulos. El *producto tensorial* de M con N sobre A es el A-módulo cociente

$$\frac{A^{(M\times N)}}{\langle \Gamma \rangle},$$

donde

$$\Gamma = \left\{ \begin{array}{l} (m+m',n)-(m,n)-(m',n) \\ (m,n+n')-(m,n)-(m,n') \\ (\lambda m,n)-\lambda(m,n) \\ (m,\lambda n)-\lambda(m,n) \end{array} \right| \; m,m' \in M,\ n,n' \in N,\ \lambda \in A \Bigg\}.$$

Tal A-módulo se denota como $M \otimes_A N$.

El producto tensorial de módulos permite reducir el estudio de las aplicaciones bilineales a sólo el estudio de aplicaciones lineales. Demos entonces la definición de aplicación bilineal.

Definición A.6. Sean P, Q y R A-módulos. Una aplicación $\chi : P \times Q \to R$ es *A-bilineal* si para toda $(p, q) \in P \times Q$ las siguientes aplicaciones son A-lineales

$$\begin{array}{rccl} \chi_p : & Q & \to & R \\ & s & \mapsto & \chi_p(s) = \chi(p, s), \end{array}$$

y

$$\begin{array}{rccl} \chi_q : & P & \to & R \\ & s & \mapsto & \chi_q(s) = \chi(s, q). \end{array}$$

El A-módulo de las aplicaciones A-bilineales de $P \times Q$ en R se denota por $\mathrm{Bil_A}(P \times Q, R)$.

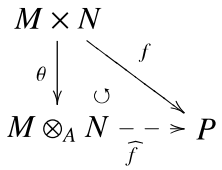
Proposición A.8. *Para todo A-módulos M y N existe una aplicación A-bilineal, dado por*

$$\begin{array}{rccl} \theta : & M \times N & \longrightarrow & M \otimes_A N \\ & (m, n) & \mapsto & \theta(m, n) = m \otimes n. \end{array}$$

Tal θ es llamada aplicación A-bilineal canónica *de $M \times N$ en $M \otimes_A N$.*

El siguiente teorema es la Proposición 2.12 de (1).

Teorema A.9. ***Propiedad Universal del Producto Tensorial.***
Sean M y N módulos sobre A. Considere el par $(M \times_A N, \theta)$ donde θ es la aplicación A-bilineal canónica de $M \times N$ en $M \otimes_A N$.
Para cada par (P, f) donde P es un A-módulo y $f \in \mathrm{Bil_A}(M \times N, P)$, existe una aplicación A-lineal única $\widehat{f} : M \otimes_A N \to P$ tal que $f = \widehat{f} \circ \theta$, es decir, el siguiente diagrama es conmutativo:



Además $(M \times_A N, \theta)$ es el único par salvo isomorfismo que satisface esta propiedad.

La siguiente proposición se da como consecuencia de la propiedad universal del producto tensorial.

Proposición A.10. *Sean M, N y P módulos sobre A. Se cumple que los A-módulos $\mathrm{Hom_A}(M \otimes_A N, P)$ y $\mathrm{Bil_A}(M \times N, P)$ son isomorfos.*

Demostración. Consideremos la siguiente asignación:

$$\begin{array}{rcl} \Phi: \mathrm{Hom_A}(M\otimes_A N,P) & \longrightarrow & \mathrm{Bil_A}(M\times N,P) \\ \varphi: M\otimes_A N \to P & & \Phi(\varphi): M\times N \to P \\ m\otimes n \mapsto \varphi(m\otimes n) & \mapsto & (m,n) \mapsto \Phi(\varphi)(m,n)=\varphi(m\otimes n) \end{array}$$

Es fácil demostrar que Φ está bien definida, por ejemplo el hecho de demostrar que $\Phi(\varphi)$ es A-bilineal para toda $\varphi\in \mathrm{Hom_A}(M\otimes_A N,P)$. En efecto, sea $\varphi\in \mathrm{Hom_A}(M\otimes_A N,P)$.
Sean $m\in M$ y $n\in N$, las siguientes aplicaciones son A-lineales pues φ lo es:

$$\begin{array}{rccl} \Phi(\varphi)_m: & N & \to & P \\ & n & \mapsto & \Phi(\varphi)_m(n)=\Phi(\varphi)(m,n)=\varphi(m\otimes n), \end{array}$$

y

$$\begin{array}{rccl} \Phi(\varphi)_n: & M & \to & P \\ & m & \mapsto & \Phi(\varphi)_n(m)=\Phi(\varphi)(m,n)=\varphi(m\otimes n). \end{array}$$

Es inmediato que Φ es A-lineal. Basta mostrar que Φ es biyectivo.
Primero mostraremos que Φ es inyectivo, esto se sigue de que $\ker(\Phi)=0_{\mathrm{Hom_A}(M\otimes_A N,P)}$. En efecto, sea $\varphi\in \mathrm{Hom_A}(M\otimes_A N,P)$).

$$\varphi\in\ker(\Phi)\Leftrightarrow \Phi(\varphi)=0_{\mathrm{Bil_A}(M\times N,P)}$$

Se tiene así que para todo $m\otimes n\in M\otimes_A N$, $\varphi(m\otimes n)=0_P$. Por lo tanto, $\varphi=0_{\mathrm{Hom_A}(M,\mathrm{Hom_A}(N,P)}$.
Por otro lado Φ es sobreyectivo por la propiedad universal del producto tensorial □

No tan sólo $\mathrm{Bil_A}(M\times N,P)$ es isomorfo a $\mathrm{Hom_A}(M\otimes_A N,P)$ para todo A-módulos M, N y P, sino también $\mathrm{Bil_A}(M\times N,P)$ es isomorfo a $\mathrm{Hom_A}(M,\mathrm{Hom_A}(N,P))$, esto se demuestra en la siguiente proposición.

Proposición A.11. *Sean M, N y P módulos sobre A. Se cumple que los A-módulos $\mathrm{Hom_A}(M,\mathrm{Hom_A}(N,P))$ y $\mathrm{Bil_A}(M\times N,P)$ son isomorfos.*

Demostración. Consideremos la siguiente asignación:

$$\begin{array}{rcl} \Phi: \mathrm{Hom_A}(M,\mathrm{Hom_A}(N,P)) & \longrightarrow & \mathrm{Bil_A}(M\times N,P) \\ \varphi: M\to \mathrm{Hom_A}(N,P) & & \\ \quad m\mapsto \varphi(m): N\to P & & \Phi(\varphi): M\times N\to P \\ \quad\quad n\mapsto \varphi(m)(n) & \mapsto & (m,n)\mapsto \Phi(\varphi)(m,n)=\varphi(m)(n) \end{array}$$

Con sencillas operaciones es fácil demostrar que Φ está bien definida, por ejemplo el hecho de demostrar que $\Phi(\varphi)$ es A-bilineal para toda $\varphi\in \mathrm{Hom_A}(M,\mathrm{Hom_A}(N,P))$. En efecto, sea

$\varphi \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$. Sea $m \in M$, la aplicación siguiente es A-lineal pues $\varphi(m)$ lo es:

$$\begin{array}{rccl} \Phi(\varphi)_m : & N & \to & P \\ & n & \mapsto & \Phi(\varphi)_m(n) = \Phi(\varphi)(m,n) = \varphi(m)(n). \end{array}$$

Sea $n \in N$, la aplicación siguiente es A-lineal pues φ lo es:

$$\begin{array}{rccl} \Phi(\varphi)_n : & M & \to & P \\ & m & \mapsto & \Phi(\varphi)_n(m) = \Phi(\varphi)(m,n) = \varphi(m)(n). \end{array}$$

Es inmediato que Φ es A-lineal. Basta mostrar que Φ es biyectivo.
Primero mostraremos que Φ es inyectivo, esto se sigue de que $\ker(\Phi) = 0_{\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))}$. En efecto, sea $\varphi \in \mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$.

$$\varphi \in \ker(\Phi) \Leftrightarrow \Phi(\varphi) = 0_{\mathrm{Bil}_A(M\times N,P)}$$

Se tiene así que para todo $(m,n) \in M \times N$, $\varphi(m)(n) = 0_P$. En particular, para toda $m \in M$, se tiene que $\varphi(m) = 0_{\mathrm{Hom}_A(N,P)}$. Es así que $\varphi = 0_{\mathrm{Hom}_A(M,\mathrm{Hom}_A(N,P))}$.
Sólo falta demostrar que Φ es sobreyectivo. Esto es que para toda ψ en $\mathrm{Bil}_A(M \times N, P)$, existe un elemento φ de $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$ tal que $\Phi(\varphi) = \psi$, veamos que se cumpla. Sea ψ un elemento de $\mathrm{Bil}_A(M \times N, P)$, considere la siguiente asignación

$$\begin{array}{rccl} \varphi : & M & \to & \mathrm{Hom}_A(N,P) \\ & m & \mapsto & \varphi(m) : \begin{array}{ccl} N & \to & P \\ n & \mapsto & \varphi(m)(n) = \psi(m,n). \end{array} \end{array}$$

Se tiene que φ es A-lineal debido a que ψ es A-bilineal y aún más se tiene que $\Phi(\varphi) = \psi$. □

A consecuencia de las Proposiciones A.10 y A.11, se tiene la siguiente proposición.

Proposición A.12. *Sean M, N y P módulos sobre A. Se cumple que los A-módulos* $\mathrm{Hom}_A(M \otimes_A N, P)$ *y* $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N,P))$ *son isomorfos.*

El siguiente Lema es la técnica a utilizar en la demostraciones de las siguiente proposiciones.

Lema A.13. *Sean M, N módulos sobre A. Se cumple que M es isomorfo a N si, y sólo si, los A-módulos* $\mathrm{Hom}_A(M,P)$ *y* $\mathrm{Hom}_A(N,P)$ *son isomorfos para todo A-módulo P.*

Cuando se realiza el producto tensorial de un A-módulo N con el anillo A no es simplemente más que el módulo N.

Proposición A.14. *Sea N un A-módulo. Se tiene que $A \otimes_A N$ es isomorfo a N.*

Demostración. Considerando al módulo M como A en la Proposición A.12, se tiene que para todo A-módulo P, $\mathrm{Hom}_A(A \otimes_A N, P) \cong_A \mathrm{Hom}_A(A, \mathrm{Hom}_A(N, P))$. Más aún, $\mathrm{Hom}_A(A, \mathrm{Hom}_A(N, P))$ es isomorfo a $\mathrm{Hom}_A(N, P)$. Por lo tanto, $\mathrm{Hom}_A(A \otimes_A N, P) \cong_A \mathrm{Hom}_A(N, P)$ para todo A-módulo P, por el Lema A.13 se tiene que $A \otimes_A N$ es isomorfo a N. □

Otra propiedad del producto tensorial es que es compatible con la suma directa. Esto es lo que demuestra la siguiente proposición:

Proposición A.15. *Sean $\{N_i\}_{i\in I}$ una familia de A-módulos con I un conjunto no vacío y M un A-módulo. Los A-módulos $M \otimes_A (\oplus_{i\in I} N_i)$ y $\oplus_{i\in I}(M \otimes_A N_i)$ son isomorfos.*

Demostración. Debido al Lema A.13, basta mostrar que para todo A-módulo P, los A-módulos $\mathrm{Hom}_A(M \otimes_A (\oplus_{i\in I} N_i), P)$ y $\mathrm{Hom}_A(\oplus_{i\in I}(M \otimes_A N_i), P)$ son isomorfos. En efecto, sea P un A-módulo.

$$\begin{aligned}
\mathrm{Hom}_A(M \otimes_A (\oplus_{i\in I} N_i), P) &\cong_A \mathrm{Hom}_A(M, \mathrm{Hom}_A(\oplus_{i\in I} N_i, P)) \\
&\cong_A \mathrm{Hom}_A(M, \Pi_{i\in I} \mathrm{Hom}_A(N_i, P)) \\
&\cong_A \Pi_{i\in I} \mathrm{Hom}_A(M, \mathrm{Hom}_A(N_i, P)) \\
&\cong_A \Pi_{i\in I} \mathrm{Hom}_A(M \otimes_A N_i, P) \\
&\cong_A \mathrm{Hom}_A(\oplus_{i\in I}(M \otimes_A N_i), P).
\end{aligned}$$

Por el Lema A.13 se tiene que $M \otimes_A (\oplus_{i\in I} N_i)$ y $\oplus_{i\in I}(M \otimes_A N_i)$ son isomorfos como A-módulos. □

4. Longitud de un Módulo

En álgebra conmutativa, la longitud de un módulo sobre un anillo es una medida del "tamaño"del módulo sobre el anillo. La longitud de un módulo sobre un anillo es una generalización del concepto de dimensión para espacios vectoriales.

Definición A.7. Sea M un A-módulo. Una *cadena de submódulos* de M es una sucesión finita $(M_i)_{i\in\{0,\ldots,n\}}$ de A-submódulos de M tal que

$$\{0_M\} = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$$

con n un entero no negativo.

Recordemos que un A-módulo M no nulo es simple cuando sus únicos submódulos son los triviales, es decir, $\{0_M\}$ y M. Con esto podemos dar la siguiente definición.

Definición A.8. Sea M un A-módulo. Una *serie de composición* de M es una cadena de submódulos de M que es maximal. Esto es, una cadena de submódulos $(M_i)_{i\in\{0,\ldots,n\}}$ de M, con $n \in \mathbb{Z}_+$, tal que

M_i/M_{i-1} es un A-módulo simple para todo $i \in \{1, \ldots, n\}$. Diremos que la *longitud* de esta serie de composición es n.

Como los A-submódulos de M_i/M_{i-1} se corresponden biyectivamente con los A-submódulos de M_i que contienen a M_{i-1}, el que M_i/M_{i-1} sea simple equivale a que no existe un A-módulo N tal que

$$M_{i-1} \subsetneqq N \subsetneqq M_i.$$

Por lo tanto, que una cadena de submódulos sea una serie de composición equivale a decir que no podemos añadirle más "eslabones". Es por esto que es posible dar la definición de longitud de un módulo.

Definición A.9. Sea M un A-módulo. M tiene *longitud infinita sobre A* si no existe una serie de composición de M. En caso contrario, M tiene *longitud finita sobre A* y la *longitud de M sobre A* es el mínimo de las longitudes de las series de composición de M. Denotamos por $\ell_A(M)$ la longitud de M sobre A.

Observación A.10. Para todo A-módulo M. $\ell_A(M) \in \mathbb{Z}_+ \cup \{\infty\}$.

Es natural preguntarse cómo se comporta la longitud de un submódulo con respecto a la longitud del módulo al que pertenece. La siguiente proposición nos da la respuesta.

Proposición A.16. *Sean M un A-módulo y N un A-submódulo de M. Se satisface que $\ell_A(N) \leq \ell_A(M)$. Más aún, $\ell_A(N) = \ell_A(M)$ si, y sólo si, $N = M$.*

Demostración. Si M es de longitud infinita sobre A, entonces se sigue el resultado. Por lo que podemos suponer que $\ell_A(M) = n$ para algún $n \in \mathbb{Z}_+$. Si $n = 0$, entonces se cumple lo deseado. Consideremos $n > 0$. Sea $(M_i)_{i\in\{0,\ldots,n\}}$ una serie de composición de M, así

$$\{0_M\} = M_0 \subsetneqq M_1 \subsetneqq \ldots \subsetneqq M_n = M.$$

Podemos considerar la siguiente sucesión $(N_i)_{i\in\{0,\ldots,n\}}$ de A-submódulos de N, donde $N_i = N \cap M_i$ para toda $i \in \{0, \ldots, n\}$, cumpliéndose que

$$\{0_M\} = N_0 \subsetneqq N_1 \subsetneqq \ldots \subsetneqq N_n = N.$$

Dado que N_i es un A-submódulo de M_i para toda $i \in \{0, \ldots, n\}$, se tiene que para toda $i \in \{1, \ldots, n\}$

$$\frac{N_i}{N_{i-1}} \text{ es } A\text{-submódulo de } \frac{M_i}{M_{i-1}}.$$

Sea $i \in \{1, \ldots, n\}$. Como M_i/M_{i-1} es simple, se sigue que

$$N_i = N_{i-1} \qquad \text{ó} \qquad \frac{N_i}{N_{i-1}} \cong \frac{M_i}{M_{i-1}}.$$

Así N_i/N_{i-1} es un A-módulo simple siempre que $N_i \neq N_{i-1}$ con $i \in \{1, \ldots, n\}$. Por lo tanto, se induce una serie de composición para N de longitud menor o igual que n. Así, $\ell_A(N) \leq \ell_A(M)$.

Si $\ell_A(N) = \ell_A(M)$, entonces $N_i/N_{i-1} \cong M_i/M_{i-1}$ para toda $i \in \{1, \ldots, n\}$. Con ello $N_i = M_i$ para toda $i \in \{1, \ldots, n\}$. En particular, $N = M$. □

Si recordamos hemos definido a la longitud de un módulo en términos de las longitudes de sus series de composición, la siguiente proposición nos permite redefinir la longitud de un módulo cuando esta es finita, pues todas las series de composición tendrán la misma longitud.

Proposición A.17. *Sea M un A-módulo de longitud finita. Toda serie de composición de M tiene la misma longitud.*

Demostración. Suponga que M tiene al menos una serie de composición, así M es de longitud finita, por lo que existe $r \in \mathbb{Z}_+$ talque $\ell_A(M) = r$, además existe una serie de composición $(M_i)_{i\in\{0,\ldots,r\}}$ de M. Por la Proposición A.16, se tiene que

$$0 = \ell_A(M_0) < \ell_A(M_1) < \ldots < \ell_A(M_r) = \ell_A(M).$$

Lo que implica que $r \leq \ell_A(M)$, por otro lado $\ell_A(M) \leq r$. Por tanto $r = \ell_A(M)$. □

Ahora bien, sabiendo la relación dada por el Teorema de la correspondencia de Módulos Cociente, desearíamos saber si existe relación entre la longitud de un módulo cociente con respecto a la longitud del módulo que aparece en el numerador de tal cociente. Es por eso que enunciamos y demostramos la siguiente proposición.

Proposición A.18. *Sean M un A-módulo y N un A-submódulo de M. $\ell_A(M/N) \leq \ell_A(M)$.*

Demostración. Si M es de longitud infinita sobre A, se satisface lo deseado. Así, podemos suponer que $\ell_A(M) = n$ para algún $n \in \mathbb{Z}_+$.
Si N es el módulo nulo, entonces se tiene la igualdad. Por lo que, consideraremos que $N \neq \{0_M\}$. Con ello se tiene que $M \neq \{0_M\}$. Así $n > 0$.
Sea $(M_i)_{i\in\{0,\ldots,n\}}$ una serie de composición de M. Sea $k \in \{1, \ldots, n\}$ tal que $M_{k-1} \subsetneq N \subseteq M_k$. Por tanto $N = M_k$, pues M_k/M_{k-1} es A-módulo simple. Se construye así una sucesión $(M'_j)_{j\in\{0,\ldots,n-k\}}$ de A-submódulos de M que contienen a N tal que

$$N = M'_0 \subsetneq M'_1 \subsetneq \ldots \subsetneq M'_{n-k} = M$$

donde $M'_j = M_{k+j}$ para toda $j \in \{0, \ldots, n-k\}$. Más aún, M'_j/M'_{j-1} es simple para $j = 1, \ldots, n-k$. Por el Teorema de la Correspondencia de Módulos Cociente, se sigue que $(M'_j/N)_{j\in\{0\ldots,n-k\}}$ es una

serie de composición para M/N, así

$$N = \frac{M'_0}{N} \subsetneqq \frac{M'_2}{N} \subsetneqq \ldots \subsetneqq \frac{M'_{n-k}}{N} = \frac{M}{N}.$$

Por lo que tenemos que $\ell_A(M/N) \leq (n-k) < \ell_A(M)$. □

Hasta el momento hemos mostrado que la longitud se comporta de manera noble, acaso será posible que la longitud sea compatible con las sucesiones exactas. Tal respuesta la da la proposición siguiente:

Teorema A.19. *Sea* $0 \longrightarrow N \xrightarrow{\alpha} M \xrightarrow{\beta} L \longrightarrow 0$ *una sucesión exacta de A-módulos. M es de longitud finita sobre A si, y sólo si, N y L son de longitud finita sobre A. Cumpliéndose en este caso la relación* $\ell_A(M) = \ell_A(L) + \ell_A(N)$.

Demostración.

⇐) Supongamos que N y L son de longitud finita sobre A. Por demostrar que M es de longitud finita sobre A. Digamos que la longitud de N sobre A es r mientras que la longitud de L sobre A es t. Así existen series de composición $(N_i)_{i=\{0,\ldots,r\}}$ de N y $(L_j)_{j=\{0,\ldots,t\}}$ de L. Por lo tanto

$$\{0_N\} = N_0 \subsetneqq N_1 \subsetneqq \ldots \subsetneqq N_r = N$$

y

$$\{0_L\} = L_0 \subsetneqq L_1 \subsetneqq \ldots \subsetneqq L_t = L.$$

Con ello, se tiene que

$$\{0_M\} = \alpha(N_0) \subsetneqq \alpha(N_1) \subsetneqq \ldots \subsetneqq \alpha(N_r) \subsetneqq \beta^{-1}(L_1) \subsetneqq \ldots \subsetneqq \beta^{-1}(L_t) = M$$

implica una serie de composición de M, puesto que $\beta^{-1}(L_1)/\alpha(N_r) \cong \beta^{-1}(L_1)/\ker\beta$ es simple. Luego $\ell_A(M) = r + t = \ell_A(N) + \ell_A(L)$.

⇒) Supongamos que M es de longitud finita sobre A. Por demostrar que N y L son de longitud finita sobre A. Como α es inyectiva, se cumple que $N \cong \alpha(N) \subseteq M$, así por la Proposición A.16 se tiene que $\ell_A(N) \leq \ell_A(M)$. Por lo tanto N es de longitud finita sobre A. Por otro lado $L \cong M/\ker\beta$ así $\ell_A(L) = \ell_A(M/\ker\beta)$, y por $\ell_A(M/\ker\beta) \leq \ell_A(M)$ por la Proposición A.18. Así L es de longitud finita sobre A.

□

Corolario A.20. *Sea N un A-submódulo de un A-módulo M tal que M es de longitud finita.*

$$\ell_A(M) = \ell_A(N) + \ell_A\left(\frac{M}{N}\right).$$

Demostración. Aplicando el Teorema A.19 a la sucesión exacta natural de A-módulos

$$0 \longrightarrow N \longrightarrow M \longrightarrow \frac{M}{N} \longrightarrow 0$$

se tiene que $\ell_A(M) = \ell_A(N) + \ell_A(M/N)$ □

Ahora nos es posible determinar la longitud de módulos libres, veamos cómo.

Lema A.21. *Sea $n \in \mathbb{N}$. Si $\ell_A(A)$ es finita, entonces $\ell_A(A^n) = n\ell_A(A)$.*

Demostración. La demostración se seguirá por principio de inducción sobre n.

- Sea $n = 1$. Claramente se cumple que $\ell_A(A^1) = 1\ell_A(A)$.
- Tómese por hipótesis de inducción cuando $n = s$ para $s \in \mathbb{N}$. La afirmación $\ell_A(A^s) = s\ell_A(A)$ se cumple. Verificar para $s + 1$
- Sea $n = s + 1$. Por demostrar que $\ell_A(A^{s+1}) = (s + 1)\ell_A(A)$. Se tiene la siguiente sucesión exacta natural

  $$0 \longrightarrow A \longrightarrow A^{s+1} \longrightarrow A^s \longrightarrow 0$$

  y por el Teorema A.19 se tiene que $\ell_A(A^{s+1}) = \ell_A(A) + \ell_A(A^s)$. Por la hipótesis de inducción se sigue que $\ell_A(A^{s+1}) = \ell_A(A) + s\ell_A(A) = (s + 1)\ell_A(A)$.

□

La siguiente proposición permite caracterizar a los campos en terminos de su longitud sobre ellos mismos.

Lema A.22. *Sea A un anillo. Las siguientes afirmaciones son equivalentes:*

1. *A es un campo.*
2. *La longitud de A sobre A es uno.*

Demostración. Primero mostremos que es suficiente que A sea un campo para que $\ell_A(A)$ sea igual a uno.
En efecto, si A es un campo, entonces $\{0_A\}$ es un ideal maximal de A, implicando con ello que solamente se puede construir una serie de composición de A de longitud uno.
Ahora, verifiquemos que para que A sea campo es necesario que $\ell_A(A) = 1$.
Supongamos que $\ell_A(A) = 1$. Por lo tanto, A tiene una serie de composición de longitud uno, tal serie debe tener la siguiente forma $\{0_A\} \subsetneq A$, donde $A/\{0_A\}$ es un A-módulo simple. Consecuentemente, $\{0_A\}$ es un ideal maximal de A. Por lo tanto, A es un campo. □

APÉNDICE B

Espacio de Zariski de un Anillo en Breve

En el Teorema 3.12 se emplearon algunos conceptos de geometría algebraica, tales conceptos serán detallados en este apéndice. Para más detalles se pueden consultar (7; 13).

A cada ideal I de un anillo A le asociaremos un conjunto $\mathrm{V}(I)$, obteniendo así una familia de conjuntos que cumplirá las condiciones requeridas para una topología sobre el espectro de A, que sabemos es el conjunto de todos los ideales primos de A y que denotamos por $\mathrm{Spec}(A)$. Por lo tanto, $\mathrm{Spec}(A)$ será un espacio topológico.

Definición B.1. Sea I un ideal de un anillo A. El conjunto de ideales primos de A que contienen a I será denotado por $\mathrm{V}(I)$.

Con las notaciones dadas en la definición anterior, enunciaremos algunas propiedades que satisfacen los elementos de la familia $\{\mathrm{V}(I) \mid I \text{ es un ideal de } A\}$.

Lema B.1. *Sea A un anillo. Se cumple lo siguiente:*

1. $\emptyset = \mathrm{V}(A)$.
2. $\mathrm{Spec}(A) = \mathrm{V}(\{0_A\})$.
3. *Para todo conjunto Λ no vacío que parametriza a una familia $(I_\lambda)_{\lambda\in\Lambda}$ de ideales de A.*

$$\bigcap_{\lambda\in\Lambda} \mathrm{V}(I_\lambda) = \mathrm{V}\left(\sum_{\lambda\in\Lambda} I_\lambda\right).$$

4. *Sean I y J ideales de A. Se tiene que*

$$\mathrm{V}(IJ) = \mathrm{V}(I) \cup \mathrm{V}(J) = \mathrm{V}(I \cap J).$$

Demostración. 1) Supongamos que $\mathrm{V}(A)$ es distinto del vacío. Así, existe un ideal primo p de A que contiene a A, por lo tanto $p = A$, absurdo.

2) Como todo ideal primo contiene al ideal cero, se sigue que $\mathrm{V}(\{0_A\}) = \mathrm{Spec}(A)$.

3) Basta mostrar que para todo elemento p de $\mathrm{Spec}(A)$, se cumple que

$$p \in \mathrm{V}\left(\sum_{\lambda\in\Lambda} I_\lambda\right) \Leftrightarrow p \in \bigcap_{\lambda\in\Lambda} \mathrm{V}(I_\lambda).$$

En efecto, sea $p \in \operatorname{Spec}(A)$.

$$\begin{aligned} p \in \mathrm{V}\left(\sum_{\lambda\in\Lambda} I_\lambda\right) &\Leftrightarrow \sum_{\lambda\in\Lambda} I_\lambda \subseteq p \\ &\Leftrightarrow I_\lambda \subseteq p, \text{ para toda } \lambda \in \Lambda \\ &\Leftrightarrow p \in \mathrm{V}(I_\lambda), \text{ para toda } \lambda \in \Lambda \\ &\Leftrightarrow p \in \bigcap_{\lambda\in\Lambda} \mathrm{V}(I_\lambda). \end{aligned}$$

4) Demostraremos las contenciones siguientes:

$$\mathrm{V}(I \cap J) \subseteq \mathrm{V}(IJ) \subseteq \mathrm{V}(I) \cup \mathrm{V}(J) \subseteq \mathrm{V}(I \cap J).$$

Sea p un elemento de $\operatorname{Spec}(A)$.

$$\begin{aligned} p \in \mathrm{V}(I \cap J) &\Leftrightarrow I \cap J \subseteq p \\ &\Rightarrow IJ \subseteq p \\ &\Rightarrow p \in \mathrm{V}(IJ). \end{aligned}$$

Así, $\mathrm{V}(I \cap J) \subseteq \mathrm{V}(IJ)$. Por otro lado,

$$\begin{aligned} p \in \mathrm{V}(IJ) &\Leftrightarrow IJ \subseteq p \\ &\Rightarrow I \subseteq p \text{ o } J \subseteq p \\ &\Rightarrow p \in \mathrm{V}(I) \text{ o } p \in \mathrm{V}(J) \\ &\Rightarrow p \in \mathrm{V}(I) \cup \mathrm{V}(J). \end{aligned}$$

Por lo tanto, $\mathrm{V}(IJ) \subseteq \mathrm{V}(I) \cup \mathrm{V}(J)$. Más aún,

$$\begin{aligned} p \in \mathrm{V}(I) \cup \mathrm{V}(J) &\Leftrightarrow p \in \mathrm{V}(I) \text{ o } p \in \mathrm{V}(J) \\ &\Leftrightarrow I \subseteq q \text{ o } J \subseteq q \\ &\Rightarrow I \cap J \subseteq p \\ &\Rightarrow p \in \mathrm{V}(I \cap J). \end{aligned}$$

Por lo que, $\mathrm{V}(I) \cup \mathrm{V}(J) \subseteq \mathrm{V}(I \cap J)$.

□

Como consecuencia del Lema B.1, $\{\operatorname{Spec}(A) \setminus \mathrm{V}(I) \mid I \text{ es un ideal de } A\}$ es una topología de $\operatorname{Spec}(A)$, tal topología es llamada la *topología de Zariski* de A. Además, para cada ideal I de A, diremos que $V(I)$ es el *cerrado de Zariski* asociado a I.

Los siguientes lemas son propiedades que satisfacen los cerrados de Zariski de $\operatorname{Spec}(A)$:

LEMA B.2. *Sean $k \in \mathbb{N}$ e $I_1, \ldots, I_k$ ideales de un anillo A. Se cumple que*

$$\mathrm{V}(I_1 \cdots I_k) = \mathrm{V}(I_1) \cup \ldots \cup \mathrm{V}(I_k).$$

DEMOSTRACIÓN. La demostración se seguirá por principio de inducción sobre k.

- Si $k = 1$, entonces el resultado es claro.
- Supongamos por hipótesis de inducción que para cada s en $\{1, \ldots, k-1\}$, se tiene que

  $$\mathrm{V}(I_1 \cdots I_s) = \mathrm{V}(I_1) \cup \ldots \cup \mathrm{V}(I_s).$$

  Por el Lema B.1(4), se cumple que

  $$\mathrm{V}(I_1 \cdots I_s I_{s+1}) = \mathrm{V}(I_1 \ldots I_s) \cup \mathrm{V}(I_{s+1})$$

  Y aplicando la hipótesis de inducción, se sigue que

  $$\mathrm{V}(I_1 \cdots I_s I_{s+1}) = \mathrm{V}(I_1) \cup \ldots \cup \mathrm{V}(I_s) \cup \mathrm{V}(I_{s+1}).$$

□

LEMA B.3. *Sea I un ideal de un anillo A. $\mathrm{V}(I)$ es vacío si, y solo si, I es igual a A.*

DEMOSTRACIÓN. La condición de suficiencia claramente se cumple debido al Lema B.1(1). Resta mostrar que si $\mathrm{V}(I) = \emptyset$, entonces $I = A$.
Supongamos que $I \neq A$. Existe un ideal maximal de A que contiene a I. Debido a que todo ideal maximal es un ideal primo, tenemos que existe un ideal primo de A que contiene a I, así $\mathrm{V}(I) \neq \emptyset$, absurdo. □

APÉNDICE C

Forma Normal Canónica de Smith de una Matriz en Breve

En los Teoremas 3.7 y 3.12 se hace uso de los factores invariantes de las matrices con coeficientes en un dominio de ideales principales, es por ello que damos una aclaración sobre tales factores que se obtienen del siguiente teorema cuya demostración se encuentra en (9, Teorema 3.8, pág. 181).

TEOREMA C.1. *Sea G una matriz de tamaño $k \times n$ con coeficientes en un dominio de ideales principales $\mathcal{A}$. Existen unas matrices $P \in GL_k(\mathcal{A})$ y $Q \in GL_n(\mathcal{A})$ tales que*

$$PGQ = \begin{pmatrix} \lambda_1 & \dots & 0 & \\ \vdots & \ddots & \vdots & 0_{q\times(n-q)} \\ 0 & \dots & \lambda_q & \\ 0_{(k-q)\times q} & & & 0_{(k-q)\times(n-q)} \end{pmatrix},$$

donde q es el rango de G y $\lambda_1, \dots, \lambda_k$ son elementos de $\mathcal{A}$.
Se llama forma normal canónica de Smith *de G a la matriz PGQ. Y a los elementos $\lambda_1, \dots, \lambda_q$ de su diagonal se les llama* factores invariantes *de G.*
Más aún, los factores invariantes están dados por:

$$\begin{aligned} \lambda_1 &= \Delta_1, \ y \\ \lambda_i &= \frac{\Delta_i}{\Delta_{i-1}}, \ para\ cada \quad i = 2, \dots, q. \end{aligned}$$

donde Δ_i es el máximo común divisor de los i-menores de G, para toda $i \in \{1, \dots, q\}$.

Bibliografía

[1] M. F. Atiyah, I. G. MacDonald. *Introduction to Commutative Algebra*.
Addison-Wesley Publishing Company, (1969).

[2] B. L. De La Rosa Navarro. *Sobre los parámetros de los códigos y los anillos de Cox de superficies racionales*.
Tesis de Maestría (13 de Agosto de 2009). Posgrado Conjunto en Ciencias Matemáticas UNAM-UMSNH. Asesor: M. Lahyane. Coasesor: I. Moreno Mejía.

[3] J. A. Domínguez Pérez, [et al.]. *Algebraic geometry constructions of convolutional codes*.
En Martínez-Moro, E., Munera, C. y Ruano, D. (Eds.), *Advances in algebraic geometry codes* (May 16, 2008) pp. 365-391. New Jersey. World Scientific.

[4] J. A. Domínguez Pérez, J. M. Muñoz Porras. *Códigos convolucionales y geometría algebraica*. Conferències FME, Volum V. Curs Riemann (2007-2008).
Facultat de Matemàtiques i Estadística. Universitat Politècnica de Catalunya, (2008). pp. 199-209.

[5] P. Elias. *Coding for noisy channels*.
I.R.E. Nat. Conv. Record 3, (1955), pp.34-35.

[6] G. D. Forney, Jr. *Convolutional codes I: algebraic structure*.
IEEE Trans. Inform. Theory, vol IT-16 (November, 1970), pp. 720-738.

[7] J. B. Frías Medina. *Sobre el carácter algebraico de los morfismos de esquemas afines*.
Tesis de Licenciatura (09 de Septiembre de 2010). Universidad de Colima. Asesor: M. Lahyane.

[8] D. G. Hoffman...[et al.]. *Coding Theory: the essentials*.
Marcel Dekker, INC. (1992).

[9] N. Jacobson. *Basic Algebra I (Second Edition).*
W. H. Freeman and Company, New York, (1985).

[10] H. Matsumura. *Commutative Algebra (Second Edition).*
The Benjamin/Cummings Publishing Company Inc., (1980).

[11] R. J. McEliece. *The algebraic theory of convolutional codes.*
In V. Pless and W. Huffman, editors. Handbook of Coding Theory, Vol. 1, (1998). pp. 1065-1138. Elsevier, Amsterdam.

[12] R. J. McEliece, Richard P. Stanley. *The general theory of convolutional codes.*
Jet Propulsion Laboratory TDA Progres Report, vol. 42-113 (May 15, 1993), pp. 89-98.

[13] D. Robles López. *Sobre la dimensión de fibras de morfismos entre espacios de Zariski.*
Tesis de Maestría. Instituto de Matemáticas de la Universidad Nacional Autónoma de México. Estado en progreso. Asesor: M. Lahyane.

[14] J. Rosenthal, J. M. Schumacher y E.V. York. *On behaviors and convolutional codes.*
IEEE Trans. Inform. Theory. 42(6):1881-1891, (1996).

[15] J. Rosenthal, R. Smarandache. *Maximun distance separable convolutional codes.*
Appl. algebra Engrg. Comm. Comput., 10(1):15-32, (1999).

[16] A.J. Viterbi. *Error bounds for convolutional codes and an asymptotically optimum decoding algorithm.*
IEEE Trans. Inform. Theory, vol IT-13 (April, 1967), pp. 260-269.

[17] J. Walker. *Algebraic geometric codes over rings.*
Journal of pure and applied algebra, vol. 144-1, (1999), pp. 91-110.

Índice alfabético