Universidad Autónoma Metropolitana
Unidad Iztapalapa

División de Ciencias Básicas e Ingeniería

"Dimensión de ideales en álgebras de grupo, y códigos de grupo"

TESIS

QUE PRESENTA:
Elías Javier García Claro
MATRÍCULA 2151801064

PARA OBTENER EL GRADO DE:
Doctor en Ciencias (Matemáticas)

DIRECTOR:
Dr. Horacio Tapia Recillas

JURADOS:
Dr. Horacio Tapia Recillas
Dr. Felipe de Jesús Zaldívar Cruz
Dr. Rogelio Fernández Alonso González
Dr. Juan Jacobo Simón Pinero
Dr. Alberto Gerardo Raggi Cárdenas

Iztapalapa, Ciudad de México, Diciembre de 2020

Resumen

En este trabajo se determinan algunas cotas y relaciones para la dimensión de ideales principales en álgebras de grupo analizando polinomios mínimos de representaciones regulares. Estos resultados son utilizados, primero, en el contexto de álgebras de grupo semisimples, para calcular, para cualquier código abeliano, un elemento con peso de Hamming igual a su dimensión. Luego, para obtener cotas de la distancia mínima de ciertos códigos MDS. Una relación entre una clase de códigos de grupo y códigos MDS es presentada. Se exponen ejemplos ilustrando los resultados principales.

Palabras Clave. álgebras de grupo, ideales principales, idempotentes primitivos, códigos abelianos, códigos de grupo MDS.

Dedicatoria

A la memoria de mi tío Javier, quien fue mi mentor y amigo. Sin su guía y enseñanza, su constante apoyo y motivación, probablemente no habría alcanzando este objetivo.

“ Y sabemos que a los que aman a Dios, todas las cosas les ayudan a bien...”

Romanos 8:28

Agradecimientos

Quiero agradecer a mi familia por su apoyo durante el desarrollo de este doctorado, en particular a mi querida madre Sonia Claro, mis logros también son suyos. A mi prima Paola Barros por ayudarme con la escritura en Inglés del artículo en cual está basada esta tesis, y a mi amigo José Antonio Sosaya por sus valiosos y oportunos comentarios que también me ayudaron a la elaboración de dicho artículo.

Agredezco a mis profesores de Matemáticas, pues todos ellos aportaron en mayor o menor medida a mi formación. En particular quiero agradecer: a mi amigo, el profesor Ismael Gutiérrez, quien me invitó a estudiar Matemáticas y acompañó mi avance durante los primeros años de mi carrera. Al profesor Rafael Ahumada, quien por su exigencia y enseñanza me ayudó a ser más riguroso como matemático durante mis estudios de pregrado. Al profesor Gerardo Raggi que fue quien me introdujo en el Álgebra avanzada y la teoría de representaciones. Todos estos, además de aportar a mi formación, me inspiraron mucho académicamente. Finalmente quiero agradecer al pro-

fesor Horacio Tapia Recillas por su acompañamiento y dirección que permitió el buen desarrollo de este proyecto, y por darme la oportunidad de trabajar como ayudante de investigador CONACYT.

Estoy muy agradecido con el CONACYT (Consejo Nacional de Ciencia y Tecnología), por apoyarme para realizar mis estudios de doctorado con la beca no. 401846 y un posterior financiamiento como ayudante de investigador. Así mismo, agradezco al Departamento de Matemáticas de la Universidad Autónoma Metropolitana, Unidad Iztapalapa, por el apoyo logístico y el apoyo financiero para asistir a eventos, que me ofreció durante mis estudios. Finalmente quiero agradecer a los profesores Roberto Quezada y Patricia Saavedra quienes, como jefes del Departamento de Matemáticas, me dieron la oportunidad de trabajar como ayudante de posgrado cuando terminó mi beca de CONACYT.

Índice general

Introducción

En 1948 Claude Shannon publicó un artículo titulado "A mathematical theory of communication" [41], debido a la importancia y relevancia de este, algunos autores consideran que la Teoría de Códigos tuvo origen con este trabajo. En la práctica, la Teoría de Códigos lineales se ocupa de encontrar soluciones al problema de detectar y corregir errores en el proceso de transmisión de información a través de un medio (canal) de comunicación. En su trabajo, Shannon le asigna a cualquier canal de comunicación dos cantidades llamadas "capacidad del canal" y "razón de tranmisión del canal", luego prueba que si la capacidad es mayor que la razón, existe un sistema de comunicación donde la probabilidad de detectar y corregir errores es tan alta como se desee. En los últimos 70 años la Teoría de Códigos se ha convertido en una disciplina que intersecta a las Matemáticas, la Ingeniería y la Computación con aplicaciones a áreas de la Comunicación tales como la transmisión de información satelital, el grabado de discos compactos, y el almacenamiento de datos, entre otras (cf. [11,29,34,40,46]).

Un código lineal es un espacio vectorial de dimensión finita sobre un campo finito, dotado de una métrica llamada la métrica de Hamming. Para presentar la definición formal, introducimos el siguiente contexto: sea q una potencia de un número primo y $\mathbb{F}_q$ el campo finito con q elementos. Sea $n \in \mathbb{Z}^+$, dados dos vectores en $\mathbb{F}_q^n$ su distancia de Hamming se define como el número de coordenadas en los que estos difieren [27, Sección 1.2]. Un $[n, k, d]$-código lineal C es un subespacio k-dimensional de $\mathbb{F}_q^n$ en el que d es la distancia mínima entre dos elementos distintos del código. El número de errores que se pueden corregir con C es $t = \lfloor (d-1)/2 \rfloor$ [27, Teorema 1.11.4], así que mientras mayor sea la distancia mínima de C, mayor será la capacidad de corregir errores de C. Sin embargo, cuanto mayor sea la distancia mínima, menor será la dimensión del código. Una manera de medir esta relación dimensión-distancia mínima es mediante la cota de Singleton que establece que para cualquier $[n, k, d]$-código lineal, se satisface la siguiente relación $k \leq n - d + 1$ [27, Teorema 2.4.1].

Problemas de interés en la teoría de códigos incluyen: el de construir códigos con buenos parámetros, es decir, tales que su distancia mínima y su dimensión sean lo más grande posibles y el de determinar los parámetros dimensión y distancia mínima de un código dado, o al menos determinar cotas para estos (con métodos que reduzcan la complejidad de los ya conocidos). Para abordar estos problemas se utilizan diversas técnicas de áreas que pasan por la Combinatoria (cf. [8, 43]), Geometría combinatoria y algebraica (cf. [37, 44]), Álgebra conmutativa (cf. [38]), Teoría de representaciones de grupos finitos (cf. [17, 18, 21]) y Teoría de números (cf. [30]), entre otras. Nuestro interés particular se centra en encontrar soluciones al problema de determinar la dimensión de un código. Utilizando teoría de representaciones de grupos finitos obtenemos información de la dimensión de códigos que son ideales de un álgebra de grupo finito, sobre un campo finito.

El álgebra de grupo FG de un grupo finito G sobre un campo F es el conjunto de combinaciones lineales formales de elementos de G con coeficientes en el campo F, es decir, $FG := \left\{\sum_{g\in G} a_g g : a_g \in F\right\}$. Este conjunto es una F-álgebra que tiene a G como base, su suma es la suma usual de vectores y su mutiplicación se obtiene al extender la operación de G (ver Sección 1.2). Si $F = \mathbb{F}_q$, un código de grupo (o G-código) C sobre F es un ideal de FG. Si G es abeliano, entonces se dice que C es un código abeliano. El peso de Hamming $wt(\mathbf{x})$ de un elemento $\mathbf{x} \in FG$ es el número de entradas no-cero en su vector de coordenadas con respecto a la base G. El peso mínimo (o distancia mínima) de un código de grupo es el mínimo de los pesos de Hamming de sus elementos no-cero.

Probablemente el inicio de los códigos de grupo se remonte a [3] y [32], desde entonces se han encontrado estrechas relaciones entre algunos de los códigos lineales más importantes y estos. Por ejemplo, en [5] se muestran algunos códigos de Golay extendidos como ideales de $\mathbb{F}_2 S_4$ y $\mathbb{F}_2 SL(2,3)$, y en [47] muestran que el $[24, 12, 8]$-código de Golay se puede construir a partir de un ideal de $\mathbb{F}_8 G$ para un grupo G de tamaño 24. Los códigos de Reed–Muller pueden ser vistos como ideales de un álgebra de grupo donde G es un grupo p-elemental abeliano [31]. El caso más conocido y estudiado de códigos de grupo es el de los ideales del álgebra de grupo $\mathbb{F}_q C_n$, donde C_n es el grupo cíclico de orden n. Dado que $\mathbb{F}_q C_n$ es un álgebra isomorfa a $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, existe una correspondencia biyectiva entre sus ideales y estos se pueden estudiar utilizando teoría de polinomios (ver Ejemplo 1.2.1). Algunos beneficios obtenidos de dicho isomorfismo son el poder describir la dimensión de estos códigos o el construir códigos con una distancia mínima prefijada como ocurre con los códigos BCH y Reed-Solomon (cf. [33, cap. 7, 8], [27, cap. 4], [27, cap. 5]).

Encontrar métodos para calcular la dimensión de ideales de F-álgebras de dimensión finita es un tema de interés en sí mismo. En el contexto de teoría de códigos, esto es crucial porque la dimensión es un parámetro requerido, además de la distancia mínima (cuyo cálculo es un problema NP-hard, cf. [16, 45]), para determinar qué tan bueno o malo es un código para corrección de errores. Sin embargo, contrario a la distancia mínima, este aspecto es de naturaleza mayormente algebraica y puede ser estudiado utilizando métodos algebraicos. Por otra parte, en álgebras de grupo más generales (que la de un grupo cíclico), este no es un problema sencillo. En la literatura aparecen algunas referencias en las que se exploran este tipo de casos. Por ejemplo, en [21] determinaron relaciones para calcular la dimensión y peso mínimo de códigos abelianos que son minimales (esto es, que sólo se contienen a sí mismos y al ideal 0) en $\mathbb{F}_2(C_{p^n} \times C_p)$ donde p es un primo impar, C_p es el grupo cíclico de orden p, y $n \geq 3$. Luego, en [17], determinaron la dimensión y distancia mínima de ideales bilaterales en el álgebra de grupo semisimple de un grupo diédrico. En [18], abordaron el problema de determinar la dimensión de un código de grupo, que es un ideal principal, estudiando el polinomio característico de la representación regular derecha/izquierda de un generador. Recientemente, en [7] se calcularon cotas para la distancia mínima y dimensión en la clase de códigos BCH-diédricos principales introducidos por los autores, lo cual les permitió dar códigos dihedricos con distancia mínima prescrita.

Los ideales principales en álgebras de grupo están estrechamente relacionados con una clase de códigos llamados checables (cf. [6, 24, 25]) que son aquellos que son anuladores izquierdos/derechos de un elemento. En [6] probaron que un código de grupo es checable si es el dual de un ideal principal y que las álgebras de grupo en las que todo código de grupo es checable están determinadas por la estructura del grupo subyacente. Como consecuencia de esta caracterización se obtiene (altenativamente) un conocido resultado de Passman, el cual establece que si $car(F) = p$, los ideales izquierdos de FG son principales si y solo si G es p-nilpotente con un p-subgrupo de Sylow cíclico.

En este trabajo nos ocupamos de determinar relaciones (como cotas, identidades, y congruencias) para la dimensión de ideales principales en álgebras de grupo estudiando el polinomio mínimo de la representación regular derecha definida por un generador del ideal y usamos estas relaciones para determinar la dimensión de códigos abelianos semisimples. El manuscrito está organizado de la siguiente manera. En el Capítulo 1, son presentados resultados preliminares que serán necesarios a lo largo de este trabajo. En el Capítulo 2, usamos el Teorema de la Descomposición Primaria para obtener relaciones que permitan determinar la dimensión de ciertos ideales principales en álgebras de grupo. Estos resultados son aplicados en las últimos dos capítulos, primero, en el

Capítulo 3 para estudiar la dimensión de códigos abelianos en álgebras de grupo semisimples. Luego, en el Capítulo 4, para calcular cotas en la distancia mínima de algunos códigos de grupo MDS que son ideales principales. Se incluyen ejemplos que ilustran los resultados principales del trabajo. Todos estos resultados aparecen en [22]. En el Capítulo 5 presentamos las principales conclusiones obtenidas durante la elaboración de este trabajo e incluimos algunos problemas de interés que podrían abordarse en investigaciones futuras. El Apéndice **??** incluye los algoritmos de SageMath [42] con con los que elaboramos los ejemplos.

Capítulo 1

Preliminares

En este capítulo se tratan algunos conceptos y resultados que serán necesarios para el desarrollo de este trabajo. Se presentan dos conocidos resultados de descomposición de módulos, se repasan los conceptos de álgebra de grupo y código de grupo, y se muestran resultados elementales de álgebras de grupo semisimples. Se caracterizan los ideales en álgebras de grupo que son principales generados por idempotentes y se da una manera de calcular la dimensión de estos como el rango de una matriz. Todo módulos en este trabajo es un módulo izquierdo, a menos que se especifique lo contrario.

1.1. Algunos resultados de descomposición de módulos

En esta sección recordamos algunos resultados sobre la descomposición de módulos que serán de utilidad más adelante.

Teorema 1.1.1 (Teorema de la descomposición primaria)**.** *[26, Teorema 12, cap. 6] Sea V un F-espacio vectorial de dimensión finita, y T un F-endomorfismo de V. Sea m el polinomio mínimo de T, con*

$$m = p_1^{r_1} \cdots p_t^{r_t}$$

donde los p_i son polinomios mónicos irreducibles distintos sobre F, y los r_i son enteros positivos. Sea W_i el espacio nulo de $p_i(T)^{r_i}$, $i = 1, ..., t$. Entonces

1. *$V = W_1 \oplus \cdots \oplus W_t$.*
2. *W_i es T-invariante para $i = 1, ..., t$.*

3. El polinomio mínimo de $T|_{W_i}$ *es* $p_i^{r_i}$.

Note que V es un $F[x]$-módulo con la multiplicación por escalares dada por $f(x)v := f(T)(v)$ para todo $f \in F[x]$ y $v \in V$, y que un subespacio vectorial W de V es $F[x]$-submódulo si y solo si es T-invariante. Así que el teorema de la descomposición primaria garantiza una descomposición para V como suma directa de un tipo particular de $F[x]$-submódulos.

Sea A un anillo, y M un A-módulo distinto de 0. Sea N un submódulo de M, si existe un submódulo U de M tal que $M = N \oplus U$ se dice que U es **complemento directo** de N. M es llamado **simple** si no tiene submódulos propios distintos de cero; es llamado **semisimple** si M se descompone como suma directa de submódulos simples o, de manera equivalente, si todo submódulo de M tiene complemento directo. Se dice que A es **semisimple**, si todo A-módulo es semisimple

Teorema 1.1.2 (Teorema de Maschke)**.** *[36, Teorema 3.4.7] FG es anillo semisimple si y solo si $|G|$ es invertible en F.*

1.2. Álgebras de grupo y códigos de grupo

En este trabajo G denotará un grupo finito, F un campo (no necesariamente finito), y $R = FG$ el **álgebra de grupo** de G sobre F, esto es, R denotará la colección de las combinaciones lineales formales de la forma

$$x = \sum_{g \in G} a_g g$$

donde $a_g \in F$. R es un F-álgebra con unidad, isomorfa como F-espacio vectorial a $F^{|G|}$. Sus operaciones de anillo estan determinadas por las de G y F de la siguiente manera: si $x = \sum_{g \in G} a_g g$, $y = \sum_{g \in G} c_g g$ son elementos de R, entonces

$$x + y = \sum_{g \in G} (a_g + c_g) g$$

y

$$xy = \sum_{g,h \in G} a_g c_h gh,$$

o de manera equivalente,

$$xy = \sum_{u \in G} w_u u$$

donde $w_u = \sum_{u=gh} a_g c_h$ (similar al producto de polinomios sobre un anillo). La unidad de R denotada por 1 es aquel elemento cuyo coeficiente en el neutro de G es la unidad de F y cero en otro caso.

Dado un elemento $x = \sum_{g \in G} a_g g$ se define el soporte de x como el subconjunto de elementos de G que efectivamente aparecen en la expresión de x como combinación lineal de elementos de G, esto es:

$$supp(x) := \{g \in G : \ a_g \neq 0\}$$

En términos del soporte se define el **peso de Hamming** de x como

$$wt(x) := |supp(x)|$$

La función que a cada $x \in R$ le asigna su respectivo peso de Hamming es una norma, y a la función $d : R \times R \to \mathbb{Z}^+$ dada por $(x, y) \mapsto wt(x - y)$ es una distancia llamada la **métrica de Hamming**.

Si $V \subseteq FG$, se define su **peso mínimo** como $wt(V) := mín\{wt(v) : v \in V - \{0\}\}$, y su **distancia mínima** como $d(V) := mín\{d(x, y) : (x, y) \in V \times V \wedge x \neq y\}$. Si V es subgrupo aditivo de FG entonces para $x, y \in V$, $d(x, y) = d(x - y, 0)$, así que

$$\begin{aligned} d(V) &= \text{mín}\{d(x, y) : (x, y) \in V \times V \wedge x \neq y\} \\ &= \{d(x - y, 0) : (x, y) \in V \times V \wedge x - y \neq 0\} \\ &= \{wt(x - y) : (x, y) \in V \times V \wedge x - y \neq 0\} \\ &= \{wt(v) : v \in V \wedge v \neq 0\} \\ &= wt(V) \end{aligned}$$

Si $C \subseteq \mathbb{F}_q G$ se dice que C es un **código de grupo**, si C es un ideal de $\mathbb{F}_q G$, en dicho caso $d(C) = wt(C)$, así que hablar de peso mínimo y distancia mínima para códigos de grupo es exactamente lo mismo. Si C es un código de grupo de $\mathbb{F}_q G$ con G abeliano, se dice que C es un código abeliano.

Ejemplo 1.2.1. *Sea σ el $\mathbb{F}_q$-automorfismo de $\mathbb{F}_q^n$ dado por*

$$\sigma(a_0, a_1, ..., a_{n-1}) := (a_{n-1}, a_0, ..., a_{n-2}),$$

y C_n el grupo cíclico (de orden n) generado por σ. Un código cíclico es un subespacio C de $\mathbb{F}_q^n$ que es invariante bajo σ, esto es, $\sigma(C) = C$ (cf. [27, cap. 4]).

Sea $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. A $\mathbb{F}_q^n$ se le puede dotar de estructura de R_n-módulo como sigue: Si $p(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$ y $v \in \mathbb{F}_q^n$,

$$p(x) \cdot v := \sum_{i=0}^{n-1} c_i \sigma^i(v).$$

Con esta estructura, un código en $\mathbb{F}_q^n$ es σ-invariante si y solo si es un R_n-submódulo.

Si se considera el isomorfismo de F-espacios vectoriales dado por

$$\phi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/\langle x^n - 1\rangle$$
$$(a_0, a_1, ..., a_{n-1}) \longmapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},$$

se tiene que

$$\begin{aligned}\phi(x \cdot (a_0, a_1, ..., a_{n-1})) &= \phi(\sigma(a_0, a_1, ..., a_{n-1})) \\ &= \phi(a_{n-1}, a_0, ..., a_{n-2}) \\ &= a_{n-1} + a_0 x + ... + a_{n-2}x^{n-1} \\ &= x(a_0 + a_1 x + ... + a_{n-1}x^{n-1}) \\ &= x \cdot \phi(a_0, a_1, ..., a_{n-1}).\end{aligned}$$

Por lo que ϕ es un isomorfismo de R_n-módulos, e induce un isomorfismo entre la retícula de submódulos de $\mathbb{F}_q^n$ y la retícula de ideales de R_n. Luego un código $C \leq \mathbb{F}_q^n$ es cíclico si y solo si $\phi(C)$ es un ideal de R_n.

Por otro lado, $\mathbb{F}_q^n$ y R_n son espacios métricos con el peso de Hamming wt (que es una norma) definido como el número de entradas no-cero del vector de coordenadas de un elemento en $\mathbb{F}_q^n$ o R_n con respecto a las base canónica de $\mathbb{F}_q^n$ o la base $\{1, x, ..., x^{n-1}\}$ de R_n, respectivemente. ϕ define un isomorfismo de espacios métricos (con la métrica determinada por la norma wt) pues

$$wt(v) = wt(\phi(v)) \text{ para todo } v \in \mathbb{F}_q$$

Así que en el sentido de la teoría de códigos es lo mismo estudiar códigos cíclicos en $\mathbb{F}_q^n$ que ideales en R_n.

Finalmente, como el álgebra de grupo $\mathbb{F}_q C_n = \{\sum_{i=1}^{n-1} c_i\sigma^i : c_i \in \mathbb{F}_q \text{ para todo } i\}$ *es isomorfa (como álgebra y espácio métrico) a* R_n*, estudiar códigos cíclicos en* $\mathbb{F}_q^n$ *es lo mismo que estudiar ideales de* R_n*. Por lo dicho anteriormente, en adelante nos referiremos a un código cíclico como un ideal de de* R_n *o* $\mathbb{F}_q C_n$*, indistintamente.*

Como R_n *es un anillo cociente, sus ideales están en correspondencia con los ideales de* $\mathbb{F}_q[x]$ *que contienen a* $\langle x^n - 1\rangle$*, en consecuencia, con los divisores de* $x^n - 1$*. De hecho, todo ideal* I *de* R_n *es generado por el polinomio mónico de menor grado que está en* I *(llamado polinomio generador de* I*), el cual es un divisor de* $x^n - 1$ *[27, Corolario 4.2.2]. Esto es muy conveniente para calcular la dimensión de un código cíclico. En efecto, si* $I \leq R_n$ *es un código cíclico con polinomio generador* g *de grado* k*, entonces* $I = R_n g$ *así que*

$$dim(I) = dim(R_n g) = dim(R_n/ann(g)),$$

donde $ann(g)$ *(el anulador de* g*) es generado por el polinomio* $(x^n - 1)/g$*, el cual tiene grado* $n - k$*, i.e.,* $dim(I) = n - k$*.*

1.3. Álgebras de grupo conmutativas semisimples

En esta sección hablaremos de algunas propiedades básicas de las álgebras de grupo conmutativas semisimples. Para un mayor acercamiento a la teoría de anillos y módulos semisimples recomendamos ver [15, Capítulo 3], [12, Capítulo 3].

Se dice que $x, y \in R$ son **ortogonales** si $xy = yx = 0$. Si $e \in R$ es un idempotente (i.e, $e^2 = e$) con la propiedad que $e = f + g$ con $f, g \in R$ idempotentes ortogonales implica $f = 0$ o $g = 0$, se dice que e es un **idempotente primitivo** (cf. [12, pág. 119]).

Sea G un grupo abeliano finito. Si $|G|$ y $car(F)$ son primos relativos, el álgebra de grupo R es semisimple (por Teorema 1.1.2), es decir, existe una colección de R-submódulos (ideales) simples $I_1, ..., I_r$ de R tales que $R = I_1 \oplus \cdots \oplus I_r$. Por lo tanto, $1 = a_1 + \cdots + a_r$ con $a_j \in I_j$ para todo j. Así que, si $x \in R$, entonces $x = x1 = xa_1 + \cdots + xa_r$ con $xa_j \in I_j$, implicando que si $x \in I_j$, $x = xa_j$ y $xa_i = 0$ para $i \neq j$. Luego $I_j = Ra_j$, $a_j^2 = a_j$, y $a_j a_i = 0$ si $i \neq j$ para $1 \leq j \leq r$. Más aún, a_j es un idempotente primitivo, en otro caso, existen idempotentes ortogonales f_j y g_j tales que $a_j = f_j + g_j$, implicando que $I_j = Ra_j = Rf_j \oplus Rg_j$ no es un R-módulo simple. Así que cada I_j es generado por

el idempotente primitivo a_j.

Por otro lado, I_j con la restricción de la multiplicación de R es un anillo con unidad a_j, esto implica que a_j es el único idempotente generador de I_j. Además, por [36, Lema 2.6.2] y [12, Proposición 3.20, parte (iv)], los I_j son únicos, es decir, si existe otra descomposición $R = J_1 \oplus \cdots \oplus J_r$ donde J_k es R-módulo simple para todo k, entonces, con un orden adecuado de los sumandos, $I_k = J_k$ para todo k.

Por lo mencionado anteriormente se tiene el siguiente Teorema.

Teorema 1.3.1. *Si R es semisimple conmutativo, se tienen la siguientes afirmaciones:*

1. *Existe una colección única de (ideales) R-submódulos simples $I_1, ..., I_r$ tales que $R = I_1 \oplus \cdots \oplus I_r$.*

2. *Todo ideal I_j está generado por un único idempotente primitivo e_j, y la colección $\{e_1, ..., e_r\}$ es la colección de todos los idempotentes primitivos de R.*

3. *Si $I \neq 0$ es un ideal de R, entonces existe un único $J \subseteq \{1, ..., r\}$ tal que $I = \oplus_{j \in J} I_j$, e I es principal teniendo como único idempotente generador a $\sum_{j \in J} e_j$.*

Un ideal de R que es simple como R-módulo es también un ideal minimal según el orden dado por contención en la retícula de ideales de R, es por eso que con frecuencia se suele referirse a estos como ideales minimales de R.

Una consecuencia del Teorema 1.3.1 (parte 3) es que los códigos abelianos se escriben de manera única como suma directa de códigos abelianos minimales, y tienen un único idempotente generador.

1.4. Ideales principales en álgebras de grupo

A lo largo de este trabajo, para $b \in R$, r_b (l_b) denotará la **representación regular derecha** (**izquierda**) de b, es decir, el F-endomorfismo de R dado por $r_b(w) = wb$ ($l_b(w) = bw$). Además, $m_b(x)$ y $p_b(x)$ denotarán los polinomios mínimo y característico respectivamente de r_b.

Observe que G es un grupo isomorfo a $\rho(G) := \{r_g : g \in G\}$ con la composición. Así $\varphi : FG \to F\rho(G)$ dado por $\varphi(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g r_g$ es un isomorfismo de F-álgebras. Recordemos que $e \in R$ es llamado idempotente si $e^2 = e$.

Lema 1.4.1. *Sea $b \in R$, y $\kappa(x)$ un polinomio que anula a r_b. Sea $\kappa(x) = f_0(x)f_1(x)$ una descomposición en factores coprimos. Si $u_0(x), u_1(x) \in F[x]$ son tales que $u_0(x)f_0(x) + u_1(x)f_1(x) = 1$, entonces $u_i(b)f_i(b)$ es un idempotente generador de $Rf_i(b)$ para $i = 0, 1$.*

Demostración. Como $f_0(x)$ y $f_1(x)$ son coprimos, existen $u_0(x), u_1(x) \in F[x]$ tales que $1 = u_0(x)f_0(x)+u_1(x)f_1(x)$. Sea $E_i := u_i(r_b)f_i(r_b)$ para $i = 0, 1$. Entonces $id = E_0+E_1$, $E_0 = E_0^2 + E_0E_1$ y $f_0(r_b) = f_0(r_b)E_0 + f_0(r_b)E_1$, pero $E_0E_1 = (u_0(r_b)u_1(r_b))\kappa(r_b) = 0$ y $f_0(r_b)E_1 = u_1(r_b)\kappa(r_b) = 0$, así que E_0 es un idempotente de $F\rho(G)$ y $f_0(r_b) \in F\rho(G)E_0$. Análogamente, E_1 es un idempotente de $F\rho(G)$ and $f_1(r_b) \in F\rho(G)E_1$. Ahora el resultado se sigue del hecho que $\varphi^{-1}(E_i) = u_i(b)f_i(b) \in Rf_i(b)$ para todo i. □

En [18, Corolario 5] se propone calcular idempotentes generadores de ideales que tienen complemento directo, resolviendo un sistema de ecuaciones multivariables cuadráticas y lineales. El Lema 1.4.1 es una alternativa a solucionar ese problema utilizando el Algoritmo Euclideano, pues con dicho algoritmo podemos encontrar los elementos $u_0(x), u_1(x) \in F[x]$ mencionados en este lema.

Recuerde que una de las equivalencias de ser un módulo proyectivo es la siguiente [12, pág. 29]. P es un A-módulo proyectivo si existe un A-módulo P' tal que $A^n \cong P \oplus P'$ para algún $n \in \mathbb{Z}^+$.

Lema 1.4.2. *[13, Lema 2.1] Las siguientes afirmaciones son equivalentes:*

1. *Si $R = R_1 \oplus R_2$ con ideales R_i, entonces existe un idempotente $e \in R$ tal que $R_1 = Re$ y $R_2 = R(1 - e)$.*
2. *Si existe un idempotente $e \in R$, entonces $R = Re \oplus R(1 - e)$.*

Note que el Lema 1.4.2 implica que si un ideal I es generado por un idempotente, entonces es un R-módulo proyectivo, pues existe un ideal I' tal que $I \oplus I' = R$, es decir, un complemento directo de I en R.

Lema 1.4.3. *Sea J un ideal principal no-trivial de R. Las siguientes afirmaciones son equivalentes:*

1. *J tiene un generador b tal que r_b es anulado por un polinomio $\kappa(x) = xh(x)$ con $x \nmid h(x)$.*

2. *J tiene complemento directo.*

3. *J tiene un idempotente generador.*

Demostración. (2) $\Rightarrow$ (3), por Lema 1.4.2 (parte 1).
(3) $\Rightarrow$ (1), pues si $J = Re$ con e idempotente, entonces el polinomio mínimo de r_e es $m_e(x) = x(x-1)$.
(1) $\Rightarrow$ (2). Supongamos que J tiene un generador b tal que es anulado por un polinomio $\kappa(x) = xh(x)$ con $x \nmid h(x)$. Entonces, por Lema 1.4.1, J es generado por un idempotente, así que J tiene complemento directo (por Lema 1.4.2 (parte 2)). □

Ahora veremos cuando las dimensiones del ideal izquierdo y derecho generado por un elemento en R son iguales. Recordemos que el mapeo $\hat{}: R \to R$ dado por $\hat{u} = \sum_{g\in G} a_g g^{-1}$, para $u = \sum_{g\in G} a_g g$, es un anti-isomorfismo de F-álgebras (ver [36, Proposición 3.2.11], [35, pag 5]).

Si M es un R-módulo derecho, el espacio dual de $M^* = Hom_F(M, F)$ se le da estructura de FG-módulo derecho mediante $fg(m) := f(mg^{-1})$ para todo $m \in M$, $f \in M^*$, y $g \in G$.

Lema 1.4.4. *[13, Lema 2.3] Si $e \in R$ es idempotente, entonces $\hat{e}R \cong (eR)^*$*

Lema 1.4.5. *Sea $b \in R$. Sean $[r_b]_G$ las matrices asociadas a r_b y l_b en la base G, respectivamente. Entonces,* $\dim(Rb) = \text{rango}([r_b]_G)$*, y si b es idempotente* $\dim(Rb) = \text{rango}([l_b]_G)$.

Demostración. $\dim(Im(r_b)) = \dim(Rb) = \text{rango}([r_b]_G)$. Similarmente, $\dim(Im(l_b)) = \dim(bR) = \text{rango}([l_b]_G)$. Por otro lado, $\widehat{Rb} = \hat{b}R$ porque $\hat{}$ es un anti-automorfismo de F-álgebras. Esto implica que $\text{rango}([r_b]_G) = \dim(Rb) = \dim(\widehat{Rb}) = \dim(\hat{b}R)$. Si b es idempotente, por Lema 1.4.4, $\dim(\hat{b}R) = \dim((bR)^*) = \dim(bR)$ donde $(bR)^*$ denota el módulo dual de bR. □

Si $F = \mathbb{F}_q$, los ideales Rb y $\hat{b}R$ definen códigos de grupo equivalentes (esto es, espacios isométricos) pues $\hat{}$ restringido a G es una permutación.

El Lema 1.4.5 es una versión alternativa de [18, Proposición 1]. Sin embargo, este lema menciona la igualdad de las dimensiones de los ideales izquierdo y derecho generados por un mismo elemento, mientras que la mencionada Proposición no lo hace.

Capítulo 2

Dimensión de ideales en álgebras de grupo

En este capítulo se presentan métodos para la obtención de relaciones (identidades, cotas y congruencias) para determinar la dimensión de ideales principales en álgebras de grupo mediante el estudio de los polinomios mínimo (Teorema 2.1.4) y característico (Teorema 2.2.1) de la representación regular derecha asociada a un generador del ideal.

2.1. Relaciones aritméticas para la dimensión de ideales

Por convención, cuando igualemos un entero con una clase modular, lo que queremos decir es que la reducción de este al respectivo módulo es igual a la clase modular. Esta notación es la misma utilizada en [35, Lema 1.2].

Lema 2.1.1. *Sea $A \in \mathcal{M}_{n\times n}(F)$ una matriz con polinomio mínimo $m_A(x) = x(x-a)^s$ para algún entero $s \geq 1$ y $a \in F - \{0\}$. Entonces se tienen las siguientes afirmaciones:*

1. $\text{traza}(A)a^{-1}$ *es un elemento del subcampo primo de F.*
2. $\text{rango}(A) = \text{traza}(A)a^{-1}$.

Demostración. Por el Teorema 1.1.1, $n = \dim(ker(A)) + \dim(ker(A - aI)^s)$, entonces $\text{rango}(A) = n - \dim(ker(A)) = \dim(ker(A-1)^s)$. Si N es la forma canónica de Jordan de A, entonces $\text{traza}(A) = \text{traza}(N)$ es igual a la suma de a tantas veces como esta aparece en la diagonal principal de N, esto implica que $\text{traza}(A)a^{-1}$ es un

elemento del subcampo primo de F. Por otro lado, el número de entradas no-cero en la diagonal principal de N es igual a $\dim(ker(A-aI)^s)$. Así, si $car(F)=0$, $\text{rango}(A) = \text{traza}(A)a^{-1}$. Si $car(F)=p>0$ y $u=\text{rango}(A)<p$, entonces $\text{rango}(A)=\text{traza}(A)a^{-1}$. Si $u=pc+r$ con $0\leq r<p$, entonces $\text{traza}(A)a^{-1}=\overline{r}$ lo cual es igual a la reducción de u módulo p, terminando la prueba. □

El Lema 2.1.1 (parte 1) tiene relación con [36, Teorema 7.2.1, Teorema 7.2.2]. Cuando se restringen estos resultados a álgebras de grupo de dimensión finita, ambos resultan ser una consecuencia del Lema 2.1.1 (parte 1).

Recordemos que $R=FG$. Si $b\in R$, el coeficiente de b en 1 lo denotaremos por $\lambda_1(b)$, este es llamado la traza de b (ver [36, pág. 221], [35, pág. 31]). Los siguientes resultados serán de utilidad para la demostración del Teorema 2.1.4.

Teorema 2.1.2. *[36, Lema 7.1.1] Sea $b\in R$, entonces*

$$\text{traza}(r_b)=|G|\lambda_1(b)$$

Recordemos que la p-parte del orden de G, denotada por $|G|_p$, es la mayor potencia de p que divide $|G|$.

Teorema 2.1.3. *[28, Corolario 7.16, cap. VII] Sea $car(F)=p>0$ y $|G|_p$ la p-parte de $|G|$. Si P es un R-módulo proyectivo entonces $|G|_p \mid \dim(P)$.*

Teorema 2.1.4. *Sea $b\in R$ tal que $m_b(x)=x^n p_1(x)^{r_1}\cdots p_t(x)^{r_t}$ donde los p_i son factores mónicos irreducibles distintos y $p_i\neq x$ para todo i. Sea $\zeta_n=\dim(ker(r_b^n)/ker(r_b))$. Entonces*

1. $\dim(Rb)=\zeta_n+\sum_{i=1}^{t}\dim(ker(p_i(r_b)^{r_i}))$. *Más aún, Si $p_b(x)=x^u h(x)$ con $x\nmid h(x)$, entonces* $\dim(Rb)=\zeta_n+|G|-u$.

2. *Si $car(F)=p>0$ y $|G|_p$ la p-parte de $|G|$, entonces*

$$\dim(Rb)\geq\begin{cases}(t+1)|G|_p & \text{si } |G|_p\mid\dim(ker(r_b)) \text{ y } n>1\\ t|G|_p & \text{en otro caso}\end{cases}$$

   Más aún, si $n=1$, entonces $|G|_p\mid\dim(Rb)$ y $\dim(Rb)\in[t|G|_p,|G|-|G|_p]$.

3. *Si $m_b(x)=x(x-a)^s$ para algún $s\geq 1$ y $a\in F-\{0\}$, entonces* $\dim(Rb)=|G|\lambda_1(b)a^{-1}$.

Demostración. Sea $U_0 = ker(r_b)$ y $U_1 = ker(r_b^n)$.

1. Sea $W \subset U_1$ tal que $U_1 = U_0 \oplus W$. Entonces, por Teorema 1.1.1 (parte 1), $R = (U_0 \oplus W) \oplus ker(p_1(r_b)^{r_1}) \oplus \cdots \oplus ker(p_t(r_b)^{r_t})$. Así, por el Teorema de la Nulidad-Rango,

$$\begin{aligned}\dim(Rb) &= \dim(Im(r_b)) \\ &= \dim(W) + \sum_{i=1}^{t} \dim(ker(p_i(r_b)^{r_i})) \\ &= \zeta_n + \sum_{i=1}^{t} \dim(ker(p_i(r_b)^{r_i})).\end{aligned}$$

   Sea $p_b(x) = x^u h(x)$ con $x \nmid h(x)$. Sean $U = ker(r_b^{|G|})$, $m_1(x)$ y $m_2(x)$ los polinomios mínimos de $r_b|_{U_1}$ y $r_b|_U$, respectivamente. Por Teorema 1.1.1 (parte 3), $m_1(x) = x^n$. Como $U_1 \subseteq U \subseteq R$ es una cadena de espacios r_b-invariantes, entonces $x^n \mid m_2(x) \mid m_b(x)$. Así, como $m_2(x) \mid x^{|G|}$, $m_2(x) \mid x^n$, implicando que $m_2(x) = x^n$, por lo que $U_1 = U$. Implicando que $\dim(U_1) = \dim(U)$ lo cual es igual a la multiplicidad algebraica u (ver [1, pp 171-172]). Por lo que $\sum_{i=1}^{t} \dim(ker(p_i(r_b)^{r_i})) = |G| - u$.

2. Sea $car(F) = p > 0$ y $|G|_p$ la p-parte de $|G|$. Como r_b es un morfismo de R-módulos, por Teorema 1.1.1 (parte 1), $R = U_1 \oplus ker(p_1(r_b)^{r_1}) \oplus \cdots \oplus ker(p_t(r_b)^{r_t})$ es una descomposición de R como suma de ideales. Así que U_1 y $ker(p_i(r_b)^{r_i})$ son R-módulos proyectivos para todo i, y por Teorema 2.1.3, $|G|_p$ divide a $\dim(U_1)$ y $\dim(ker(p_i(r_b)^{r_i}))$ para todo i. Por lo tanto, $t|G|_p \leq \dim(Rb)$. Además, si $|G|_p \mid \dim(U_0)$, $|G|_p$ es un divisor común de $\dim(U_0)$ y $\dim(U_1)$. Luego, si $n > 1$, $|G|_p \mid \zeta_n \neq 0$, implicando que $(t+1)|G|_p \leq \dim(Rb)$.
   Si $n = 1$, Rb es proyectivo (por Lema 1.4.3), y así $|G|_p$ divide a $\dim(Rb)$. Por lo tanto, como $Rb \neq R$, $\dim(Rb) \in [t|G|_p, |G| - |G|_p]$.

3. Sea $m_b(x) = x(x-a)^s$ para algún $s \geq 1$ y $a \in F - \{0\}$. Entonces, por Lemas 1.4.5 y 2.1.1, $\dim(Rb) = \text{rango}([r_b]_G) = \text{traza}([r_b]_G)a^{-1}$. Finalmente, por Teorema 2.1.2, $\text{traza}([r_b]_G) = |G|\lambda_1(b)$, por lo tanto $\dim(Rb) = |G|\lambda_1(b)a^{-1}$.

□

El siguiente lema es un conocido resultado que está relacionado con el Teorema 2.1.4. Lo enuciaremos para luego detallar dicha relación.

Lema 2.1.5. *[35, Lema 1.2, cap. 2] Sea R semisimple.*

1. *Si $b \in R$ es nilpotente, entonces $\lambda_1(b) = 0$.*
2. *Si $e \in R$ es un idempotente, entonces $\lambda_1(e) = \dim(Re)/|G|$.*

El Teorema 2.1.4 (Parte 3) es una versión más general del Lema 2.1.5 (parte 2), el cual solo es válido con R semisimple y para idempotentes. El beneficio principal de este resultado, cuando lo comparamos con el Lema 2.1.5 (parte 2), es que puede ser aplicado a una mayor cantidad de elementos de R, sin necesidad de ser idempotentes. Sin embargo, por Lema 1.4.3, cualquier elemento que satisface las hipótesis del Teorema 2.1.4 (parte 3), genera un ideal que también tiene un generador idempotente, es decir, ambos resultados sólo son aplicables a ideales principales generados por idempotentes.

Por nuestra convención, si $car(F) = 0$ en el Teorema 2.1.4 (parte 3), obtenemos una formula explícita para la dimensión de Rb. Sin embargo, si $car(F) = p > 0$, solo obtenemos la clase de la dimensión módulo p (la cual es $|G|\lambda_1(b)a^{-1}$). Así tenemos los siguientes dos corolarios.

Corolario 2.1.6. *Sea $b \in R$ y $m_b(x) = x(x-a)^s$ para algún $s \geq 1$ y $a \in F - \{0\}$. Si $car(F) = 0$, entonces $\dim(Rb) = |G|\lambda_1(b)a^{-1}$.*

Corolario 2.1.7. *Sea $b \in R$, $J = Rb$, y $m_b(x) = x(x-a)^s$ para algún $s \geq 1$ y $a \in F - \{0\}$. Sea $car(F) = p > 0$, y r el menor entero positivo en la clase de $|G|\lambda_1(b)a^{-1}$. Entonces se tiene lo siguiente:*

1. *$r \leq \dim(J)$. Más aún, si $\dim(J) \leq p$, entonces $\dim(J) = r$. En particular, si $|G| - 1 \leq p$ y $|G| \neq p$, la dimensión de cualquier ideal no-trivial se puede calcular de esta manera.*
2. *Si $\lambda_1(b) = a = 1$, $|G| \geq p$ y c es el cociente de dividir $|G|$ por p, entonces $\dim(J) = |G| - pt$ para algún $0 \leq t \leq c$.*
3. *$\dim(J)$ es múltiplo de p si y solo si $\lambda_1(b) = 0$ o $p \mid |G|$.*
4. *Si $|G| - 1 > p$, c es el cociente de dividir $|G| - 1$ por p, y $\lambda_1(b) = 0$, entonces $\dim(J) = pt$ para algún $1 \leq t \leq c$.*
5. *Si $\dim(J) = 1$, entonces $\lambda_1(b) = |G|^{-1}a$.*

Demostración. 1. Como $\dim(J)$ está en la clase $|G|\lambda_1(b)a^{-1}$, $r \leq \dim(J)$. Supongamos que $\dim(J) \leq p$, entonces $\dim(J)$ es el mínimo entero positivo en la clase $|G|\lambda_1(b)a^{-1}$, lo cual implica que $\dim(J) = r$. Si $|G| - 1 \leq p$ y $|G| \neq p$, $p \nmid |G|$, así que R es semisimple (por Teorema 1.1.2). Por lo tanto, cualquier ideal no-trivial es principal generado por un idempotente no-trivial y tiene dimensión menor o igual a p.

2. Supongamos que $\lambda_1(b) = a = 1$. Como J es un ideal propio, entonces $\dim(J) = |G| - pt$ para un entero $1 \leq t$, pero el mínimo valor posible que puede tomar $\dim(J)$ es r (por parte 1) y en tal caso t tomaría el valor de c.

3. $\dim(J) = |G|\lambda_1(b)a^{-1} = 0$ si y solo si $|G|$ es múltiplo de p o $\lambda_1(b) = 0$.

4. Ya que $\lambda_1(b) = 0$, $\dim(J)$ es múltiplo de p, pero el mayor múltiplo de p menor o igual a $|G| - 1$ es pc, así que $\dim(J) = pt$ para algún $1 \leq t \leq c$.

5. Si $1 = \dim(J) = |G|\lambda_1(b)a^{-1}$, entonces $\lambda_1(b) = |G|^{-1}a$.

□

Todos los cálculos desarrollados en los ejemplos de este trabajo están hechos en SageMath [42].

Ejemplo 2.1.8. *Sea* $G = \langle x, y \mid x^4 = 1,\ x^2 = y^2 = (xy)^2,\ yxy^{-1} = x^{-1}\rangle = \{1, x, y, x^2, x^3y, xy, x^3, x^2y\}$ *el grupo de los cuaternios y* $R = \mathbb{F}_3G$. *Sea* $b_0 = x + 2y + 2x^2 + 2x^3y + xy + x^2y$ *y* $b_1 = 1 + x + y + x^3y$, *entonces* $m_{b_i}(z) = z(z-1)^2$ *para* $i = 0, 1$. *Así, por Corolario 2.1.7 (parte 4),* $\dim(Rb_0) = 3t$ *donde* $1 \leq t \leq 2$, *es decir,* $\dim(Rb_0)$ *es igual a* 3 *o* 6. *Además, por Corolario 2.1.7 (parte 2),* $\dim(Rb_1) = 8 - 3t$ *donde* $1 \leq t \leq 2$, *es decir,* $\dim(Rb_1)$ *es igual a* 5 *o* 2. *Sea* $b_2 = 2 + 2x + y + x^3y$, *entonces* $m_{b_2}(z) = z(z-2)^2$. *Así, por Teorema 2.1.4 (parte 3),* $\dim(Rb_2) = |G|\lambda_1(b_2)2^{-1} = 2$ *así que* $\dim(Rb_2)$ *es igual a* 2 *o* 5. *De hecho, utilizando Lema 1.4.5, obtenemos que* $\dim(Rb_i)$ *es igual a* $6, 5, 5$ *para* $i = 0, 1, 2$, *respectivamente.*

Ejemplo 2.1.9. *Sea*

$$G = \langle x, y \mid x^2 = y^5 = 1,\ xy = y^{-1}x\rangle = \{1, x, y, xy^4, y^2, xy, xy^3, y^4, y^3, xy^2\}$$

el grupo diédrico de orden 5. *Sea* w *una raíz del polinomio* $p(z) = z^2 + 2z + 2 \in \mathbb{F}_3[z]$ *en algún campo extensión de* $\mathbb{F}_3$. $p(z)$ *es irreducible, así que* $F := \mathbb{F}_3(w) = \mathbb{F}_9$. *Sea* $R = FG$ *y* $b = 2w^2 + (w+2)x + (2w+1)y + wxy^4 + 2y^2 + wxy + 2w^2xy^3 + 2w^2y^4 + wy^3 + (w+2)xy^2 \in R$, *entonces* $m_b(z) = z(z - w^2)^2$. *Luego, por Teorema 2.1.4 (parte 3),*

$$\dim_F(Rb_2) = |G|\lambda_1(b)(w^2)^{-1} = 10(2w^2)(2w^2) = 10(4w^4) = 2.$$

Por lo tanto, $\dim(Rb_2)$ *es igual a* 2, 5 *u* 8. *De hecho, utilizando Lema* 1.4.5, *obtenemos que* $\dim(Rb)$ *es igual a* 8.

Observe que los dos ejemplos anteriores tienen varias cosas en común. Ambos fueron realizados con álgebras de grupo semisimples no-conmutativas finitas. A pesar que los resultados ilustrados en estos ejemplos son válidos para álgebras de grupo sobre campos arbitrarios, trabajamos con álgebras finitas porque estamos interesados en estudiar sus códigos de grupo más adelante. Se eligieron álgebras de grupo semisimples porque, para las no-semisimples, el Teorema 2.1.4 (parte 3) dice que la dimensión del ideal Rb debe ser un múltiplo de la característica del campo; sin embargo, decir eso no es muy relevante, si tenemos en cuenta que (por el Lema 1.4.3) Rb también es generado por un idempotente, así que Rb es proyectivo, implicando (por Teorema 2.1.3) que la dimensión de Rb es igual a un múltiplo de un p-subgrupo de sylow de G, donde p es la característica del campo. Es decir, en el caso no-semisimple, el Teorema 2.1.3 es más fuerte que el Teorema 2.1.4 (parte 3), por lo que no vale mucho la pena usar este último en dicho caso. Se eligieron álgebras de grupo no-conmutativas pues en el caso conmutativo semisimple, si un elemento b tiene polinomio mínimo $m_b(x) = x(x-a)^s$ con $a \neq 0$, entonces $e = a^{-1}b$ es idempotente y $m_b(x) = x(x-a)$ (ver abajo Teorema 2.2.5, parte 1). Así que este caso no es de mucha importancia, por no distar mucho de aquellos en los que se puede aplicar el Lema 2.1.5 (parte 2).

2.2. Dimensión y polinomio característico

En [18, Teorema 6] se presenta una cota inferior para la dimensión de un ideal principal en un álgebra de grupo cuando se conoce la multiplicidad de 0 como raíz del polinomio característico de la representación regular izquierda/derecha asociada a un generador. También se menciona que esta cota resulta ser la dimensión exacta cuando es aplicada al polinomio característico de un idempotente. Nosotros observamos que los únicos elementos para los cuales se tiene dicha igualdad son aquellos cuya representación regular derecha tiene polinomio mínimo con 0 como raíz simple. Así que vamos a reformular dicho resultado.

Teorema 2.2.1. *[18, Teorema 6] Sea* $b \in R$ *tal que* $p_b(x) = x^u h(x)$ *donde* $x \nmid h(x)$, *entonces*

$$|G| - u \leq \dim(Rb) \leq |G| - 1.$$

Más aún, $\dim(Rb) = |G| - u$ *si y solo si* 0 *es una raíz simple de* $m_b(x)$.

Demostración. Por Teorema 2.1.4 (parte 1), $|G| - u \leq \dim(Rb)$. Además, como 0 es un valor propio de r_b, $Rb \subsetneq R$, y así $\dim(Rb) \leq |G| - 1$.
Sea $m_b(x) = x^n w(x)$ con $x \nmid w(x)$. Si $n = 1$, por Teorema 2.1.4 (parte 1), $\dim(Rb) = |G| - u$. Recíprocamente, si $\dim(Rb) = |G| - u$, $\dim(ker(r_b)) = u$. Como $ker(r_b) \subseteq ker(r_b^n) \subseteq ker(r_b^{|G|})$, entonces $ker(r_b) = ker(r_b^n) = ker(r_b^{|G|})$. Así el polinomio mínimo de $r_b|_{ker(r_b)} = r_b|_{ker(r_b^n)}$ es $x = x^n$, y por lo tanto $n = 1$.

□

Corolario 2.2.2. *Sea $b, b' \in R$ tal que $p_b(x) = x^u h(x)$ y $p_{b'}(x) = x^{u'} h'(x)$. Entonces se tiene lo siguiente:*

1. *Si $Rb = Rb'$ y $m_b(x)$ tiene a 0 como raíz simple, entonces $u \leq u'$.*
2. *Si r_b es diagonalizable $\dim(Rb) = |G| - u$. En particular, esto se tiene si b es idempotente.*

Demostración.
1. Por Teorema 2.2.1, $\dim(Rb) = |G| - u$. Así $|G| - u' \leq \dim(Rb')$ $= \dim(Rb) = |G| - u$, por lo que $u \leq u'$.
2. Se sigue del Teorema 2.2.1 y del hecho que r_b es diagonalizable si y solo si todas las raíces de $m_b(x)$ son raíces simples. En particular, si b es idempotente, $m_b(x) = x^2 - x = x(x-1)$, así que r_b es diagonalizable.

□

Ejemplo 2.2.3. *Sea $G = \langle x, y \mid x^3 = y^2 = (xy)^3 = 1\rangle = \{1, x, x^2y, y, x^2yx, x^2, yx, xy, xyx, yxy, yx^2, xyx^2\}$ el grupo alternante de grado 4 y $R = \mathbb{F}_2 G$. Si $b = x + x^2yx$ entonces $m_b(z) = z(z^2 + z + 1)^2$. Así, por Teorema 2.1.4 (parte 2), 4 $\mid \dim(Rb)$ y $4 \leq \dim(Rb) \leq 8$, así que $\dim(Rb)$ es igual a 4 u 8. Alternativamente, podemos usar el Teorema 2.2.1 para calcular $\dim(Rb)$. Como $p_b(z) = z^4(z^2 + z + 1)^4$ y 0 es una raíz simple de $m_b(z)$, entonces $\dim(Rb) = 12 - 4 = 8$. Por otro lado, si $b' = 1 + x + y + x^2yx$, entonces $m_{b'}(z) = z^2(z^2 + z + 1)^2$ y $p_{b'}(z) = z^4(z^2 + z + 1)^4$. Así, por Teorema 2.2.1, $8 = 12 - 4 \lneq \dim(Rb)$. De hecho, utilizando el Lema 1.4.5, obtenemos que $\dim(Rb) =$ rango$([r_b]_G) = 9$. Esto ocurre porque la multiplicidad de z como raíz de $m_{b'}(z)$ no es 1 sino 2.*

Recordemos que F es campo de descomposición para el grupo G (el álgebra FG) si $End_{FG}(V) = F$ para cada FG-módulo simple V. [15, pág. 22].

Proposición 2.2.4. *Sea G abeliano y F campo de descomposición de G. Si FG es semisimple, entonces sus ideales son F-espacios vectoriales de dimensión 1.*

Demostración. Por [15, Corolario 4.4] FG tiene tantos ideales minimales como clases de conjugación, esto es, $|G|$ ideales (pues G es abeliano). Por lo que todos estos deben tener dimensión 1. □

Teorema 2.2.5. *Sea $b \in R = FG$. Si R es un álgebra de grupo conmutativa semisimple, entonces se tienen las siguientes afirmaciones:*

1. *Si $m_b(x) = x(x-a)^s$ con $a \neq 0$, entonces $a = 1$ y $s = 1$ o $a \neq 1$ y $s = 1$, y $a^{-1}b$ es un idempotente.*
2. *Si $p_b = x^u h(x)$ con $x \nmid h(x)$, entonces* $\dim(Rb) = |G| - u$

Demostración. Sea $\mathbf{F}$ una extensión de F que es campo de descomposición para G (esta existe por [15, Proposición 7.13]). Por Teorema 1.3.1 (parte 1) $\mathbf{F}G$ se escribe como suma directa de ideales minimales, y por Proposición 2.2.4, todos estos tienen dimensión 1. Sea $r'_b : \mathbf{F}G \to \mathbf{F}G$ dado por $r'_b(u) = ub$. Como los ideales de $\mathbf{F}G$ tienen dimensión 1, los idempotentes primitivos que generan a estos ideales forman una base de vectores propios de r'_b, por lo que r'_b es diagonalizable. Note que el polinomio mínimo de r'_b es igual al de $r'_b|_R = r_b$, esto es, $m_b(x)$. Por lo tanto, $m_b(x)$ se factoriza en factores lineales distintos en $\mathbf{F}$, es decir, $m_b(x)$ no tiene raíces repetidas.

1. Sea $m_b(x) = x(x-a)^s$ con $a \neq 0$. Si b es idempotente, $m_b(x) = x^2 - x = x(x-1)$, así que $a = 1$ y $s = 1$. Si b no es idempotente, entonces $m_b(x) = x(x-a)^s \neq x(x-1)$ así que $a \neq 1$ o $s \neq 1$ (sin la posibilidad $a = 1$ y $s = 1$), pero $m_b(x)$ no tiene raíces repetidas, así que $s = 1$, por lo que $a \neq 1$. Además, si $u = a^{-1}b$ y $\delta(m_b)$ es el grado de m_b, con la fórmula para calcular el polinomio mínimo de un múltiplo escalar de una matriz, se tiene que

$$\begin{aligned} m_u(x) &= (a^{-1})^{\delta(m_b)} m_b((a^{-1})^{-1}x) = a^{-2} m_b(ax) \\ &= a^{-2}[ax(ax-a)] = a^{-2}[a^2x(x-1)] = x(x-1) \end{aligned}$$

   así que u es idempotente, y $b = au$.

2. Sea $p_b = x^u h(x)$ con $x \nmid h(x)$. Por lo dicho anteriormente $m_b(x)$ no tiene raíces repetidas en $\mathbf{F}$, así que 0 es una raíz simple de $m_b(x)$. Luego, por Teorema 2.2.1, $\dim(Rb) = |G| - u$.

□

Capítulo 3

Dimensión de códigos abelianos

En este capítulo aplicamos algunos resultados del Capítulo 2 al estudio de la dimensión de códigos abelianos en álgebras de grupo semisimples. En particular, se determina una cota inferior y superior para la dimensión basada en cardinalidades de q-órbitas (Teorema 3.1.1). Además se determina la existencia de una transformación lineal (a la que luego llamamos ***el indicador de dimensiones***) con la propiedad que su evaluación en el idempotente generador de un código abeliano tiene peso de Hamming igual a la dimensión del código (Teorema 3.2.5) y se presenta una manera de calcular dicha transformación (Teorema 3.2.2).

3.1. Cotas para la dimensión de códigos abelianos

En lo que resta de este capítulo, $F = \mathbb{F}_q$, $p = car(\mathbb{F}_q)$, G es abeliano de orden primo relativo a q (esto es para poder aplicar el Teorema de Maschke).

El exponente de G es el mínimo común múltiplo de los ordenes de los elementos de G. Sea m el exponente de G, θ una raíz m-ésima primitiva de la unidad en algún campo extensión de F, y $\mathbf{F} := F(\theta)$. Sea $H := Gal(\mathbf{F}/F)$, y α el automorfismo de Frobenius. Entonces H actúa en G como $\alpha \cdot g := g^q$. Las órbitas bajo esta acción son llamadas q-órbitas (o q-subconjuntos [10]; si G es cíclico, clases q-ciclotómicas [27, pág. 122]). Es bien conocido (ver por ejemplo, [19, Teorema 1.3]) que existe una biyección entre los ideales minimales de R y las q-órbitas bajo la cual, el tamaño de una q-órbita es igual a la dimensión del correspondiente ideal. Resumimos esto en el siguiente Teorema.

Teorema 3.1.1. *Sea $\{U_j\}_{j=1}^{w}$ la colección de las q-órbitas de G. Sea $R = \oplus_{j=1}^{r} I_j$ la*

descomposición de R como suma de ideales minimales. Entonces $r = w$ y para una indexación adecuada, $\dim(I_j) = |U_j|$ *para* $j = 1, ..., r$.

Demostración. Se sigue de [19, Theorem 1.3]. □

Corolario 3.1.2. *(cota q-órbitas) Sea $e \in R$ un idempotente primitivo e $I = Re$. Si $Y = \{|U_j| : |U_j| = |G|\lambda_1(e),\ j = 1, ..., r\}$ donde $\lambda_1(e)$ es la traza de e, entonces*

$$\text{mín}(Y) \leq \dim(I) \leq \text{máx}(Y)$$

Demostración. Se sigue del Teorema 3.1.1 y 2.1.4 (parte 3). □

Por Teorema 3.1.1, $1 \leq |Y|$. Si $|Y| = 1$, la cota en el Teorema 3.1.2 nos da la dimensión exacta.

3.2. El indicador de dimensiones

Los siguientes dos teoremas ofrecerán una solución al problema de calcular la dimensión de cualquier código abeliano, para ello, primero introduciremos algo de contexto.

Proposición 3.2.1. *[15, Corolario 24.11] Sea F un campo finito tal que $car(F) \nmid |G|$, m el exponente de G, y θ una raíz m-ésima primitiva de la unidad. Entonces $F(\theta)$ es campo de descomposición para G.*

Sea $G = C_{n_1} \times \cdots \times C_{n_s}$ una descomposición de G como un producto directo de grupos cíclicos con $C_{n_i} = \langle x_i \rangle = \{1, x_i, ..., x_i^{n_i-1}\}$ para todo i. Sea $R_i := \mathbf{F}C_{n_i}$, $l_i : R_i \to R_i$ la transformación $\mathbf{F}$-lineal dada por $l_i(y) = x_i y$, $\{\gamma_{ij_i}\}_{j_i=1}^{n_i}$, y $\{e_{ij_i}\}_{j_i=1}^{n_i}$ el espectro de l_i y la colección de idempotentes primitivos de R_i para todo i, respectivamente. Sea $c_i \equiv |C_{n_i}|^{-1} \bmod p$ para $i = 1, ..., s$.

Teorema 3.2.2. *Asumiendo la notación anterior, se tiene lo siguiente: $[e_{ij_i}]_{C_{n_i}} = c_i(1, \gamma_{ij_i}^{n_i-1}, \gamma_{ij_i}^{n_i-2}, ..., \gamma_{ij_i})$ para $i = 1, ..., s$ y $j_i = 1, ..., n_i$. Además, los vectores de coordenadas de los idempotentes primitivos de $\mathbf{R}$ con respecto a G están dados por $\{[e_{1j_1}]_{C_{n_1}} \otimes \cdots \otimes [e_{sj_s}]_{C_{n_s}} : j_i = 1, ..., n_i\}$, donde $\otimes$ denota el producto de Kronecker.*

Demostración. Sea $\beta = C_{n_1} \otimes \cdots \otimes C_{n_s}$ la base típica del producto tensorial R. Como $\mathbf{F}$ es campo de descomposición para todo C_{n_i}, entonces todo ideal minimal tiene dimensión 1 como $\mathbf{F}$-espacio vectorial (por Proposición 2.2.4). Así, como los ideales de R_i son l_i-invariantes, todo idempotente primitivo en R_i es un vector propio de l_i.

Supongamos que $l_i(e_{ij_i}) = \gamma_{ij_i} e_{ij_i}$ donde $j_i = 1, ..., n_i$ para $i = 1, ..., s$. El polinomio mínimo de l_i es $x^{n_i} - 1$, por lo que l_i tiene tantos valores propios distintos como n_i (pues $(|G|, q) = 1$), implicando que todo espacio propio de l_i tiene dimensión 1 para todo i. Luego, como $1 + \gamma_{ij_i}^{n_i-1} x_i + \gamma_{ij_i}^{n_i-2} x_i^2 + ... + \gamma_{ij_i} x_i^{n_i-1}$ es un vector propio de l_i asociado al valor propio γ_{ij_i} para todo i, e_{ij_i} debe ser un múltiplo de este elemento, por lo tanto $e_{ij_i} = c_i(1+\gamma_{ij_i}^{n_i-1} x_i + \gamma_{ij_i}^{n_i-2} x_i^2 + ... + \gamma_{ij_i} x_i^{n_i-1})$ para todo i (por Corolario 2.1.7, parte 5).

Por otro lado, si $T = R_1 \otimes \cdots \otimes R_s$, los tensores de la forma $e_{1j_1} \otimes \cdots \otimes e_{sj_s}$ son idempotentes primitivos de T pues el conjunto $\{e_{1j_1} \otimes \cdots \otimes e_{sj_s} : j_i = 1, ..., n_i \text{ para } i = 1, ..., s\}$ es un conjunto de idempotentes ortogonales de T con tamaño $|G|$, así que debe ser el conjunto de los idempotentes primitivos de T. Además, por la definición de β, se tiene que $[e_{1j_1} \otimes \cdots \otimes e_{sj_s}]_\beta = [e_{1j_1}]_{C_{n_1}} \otimes \cdots \otimes [e_{sj_s}]_{C_{n_s}}$ para $j_i = 1, ..., n_i$ e $i = 1, ..., s$. Así, como $\chi : \mathbf{R} \to T$ dado por la extensión $\mathbf{F}$-lineal de $\chi(x_1^{\epsilon_1} \cdots x_s^{\epsilon_s}) = x_1^{\epsilon_1} \otimes \cdots \otimes x_s^{\epsilon_s}$ es un isomorfismo de $\mathbf{F}$-álgebras, los vectores de coordenadas de los idempotentes primitivos de $\mathbf{R}$ con respecto a G son los mismos vectores de coordenadas de los idempotentes primitivos de $T = \chi(\mathbf{R})$ con respecto a $\beta = \chi(G)$, terminando la prueba. □

Sea $\mathbf{R} := \mathbf{F}G$ y $\mathbf{R} = \oplus_{j=1}^t \mathbf{R} f_j$ la descomposición de $\mathbf{R}$ en ideales minimales donde f_j es idempotente para todo j. Por [15, Corolario 24.11], $\mathbf{F}$ es campo de descomposición para G, así que $\dim_{\mathbf{F}}(\mathbf{R} f_j) = 1$ para todo j (ver [15, Corolario 4.4]). Esto implica que $\eta := \{f_j\}_{j=1}^t$ es una $\mathbf{F}$-bases para $\mathbf{R}$ y $t = |G|$. Note que H actúa en $\mathbf{R}$ por evaluación en los coeficientes, es decir, $\alpha \odot \sum_{g \in G} \lambda_g g := \sum_{g \in G} \alpha(\lambda_g) g = \sum_{g \in G} \lambda_g^q g$. Además, si $f = \sum_{g \in G} a_g g \in \eta$,

$$\alpha^{-1} \odot f = \alpha^{-1} \odot f^q = \alpha^{-1} \odot (\sum_{g \in G} \alpha(a_g) g^q) = \sum_{g \in G} a_g g^q = \gamma(f) \in \eta,$$

donde γ es el automorfismo de $\mathbf{R}$ que resulta de extender linealmente el automorfismo "elevar a la q" de G. Por lo tanto, H actúa en η. Sea γ_i un valor propio de l_i que es una raíz n_i-primitiva de la unidad (esta existe pues $x^{n_i} - 1$ no tiene raíces repetidas), y $e(\gamma_i) := c_i(1 + \gamma_i^{n_i-1} x_i + \gamma_i^{n_i-2} x_i^2 + ... + \gamma_i x_i^{n_i-1}) \in R_i$ para todo i. Considere la función

$$\begin{array}{rccc} U: & G & \longrightarrow & \eta \\ & \prod_{i=1}^s x_i^{\epsilon_i} & \longmapsto & \prod_{i=1}^s e(\gamma_i^{\epsilon_i}). \end{array}$$

Para cualesquiera dos elementos distintos $g, h \in G$, $U(g)U(h) = 0$, así que U es inyectiva. Implicando que $|Im(U)| = |G| = \eta$, así que U es biyectiva. Más aún,

$$U\left(\alpha \cdot \prod_{i=1}^s x_i^{\epsilon_i}\right) = U\left(\prod_{i=1}^s x_i^{q\epsilon_i}\right) = \prod_{i=1}^s e(\gamma_i^{q\epsilon_i}) = \alpha \cdot U\left(\prod_{i=1}^s x_i^{\epsilon_i}\right),$$

por lo tanto U es un isomorfismo de H-conjuntos. Así, para un orden fijado en G, U induce un orden en η tal que su extensión lineal U es la transformación de cambio de bases que envía a G en η. Sea $A := [U]_G$.

Antes de presentar nuestro siguiente Teorema (3.2.5) enunciaremos un par de resultados necesarios.

Proposición 3.2.3 (descenso de Galois)**.** *[14, Proposición III.6] Los idempotentes primitivos de R son aquellos de la forma $e = \sum_{z\in O} z$ con $O \in \eta/H$*

Lema 3.2.4. *Si $f \in \boldsymbol{R}$, entonces* $\dim_F(Rf) = \dim_{\mathbf{F}}(\mathbf{R}f)$.

Demostración. Se sigue del hecho que $\mathbf{R}f \cong \mathbf{F} \otimes_F Rf$ como $\mathbf{R}$-módulos. □

Teorema 3.2.5. *Se tienen las siguientes afirmaciones:*

1. *Sea $f \in R$ un idempotente primitivo, y D el inverso de U, entonces* $\dim_F(Rf) = wt(D(f))$.

2. *U induce una biyección entre las q-órbitas y los ideales minimales de R, bajo la cual, el tamaño de una q-órbita es igual a la dimensión de su correspondiente ideal.*

Demostración. 1. Sea D el $\mathbf{F}$-automorfismo de $\mathbf{R}$ dado por $D(x) := U^{-1}(x)$, donde U es la transformación de cambio de bases que se presentó anteriormente. Entonces $D|_\eta : \eta \to G$ es un isomorfismo de H-conjuntos. Por el argumento del descenso de Galois (Proposición 3.2.3), existe $O \in \eta/H$ tal que $f = \sum_{z\in O} z$. Por lo que $D(f) = \sum_{z\in O} D(z)$, el cual es una suma de elementos de G pertenecientes a la q-órbita $D(O)$, y así $wt(D(f)) = |O|$.

Por otro lado, $\dim_F(Rf) = \dim_{\mathbf{F}}(\mathbf{R}f)$ (por Lema 3.2.4). Así, como $\mathbf{R}f = \oplus_{z\in O}\mathbf{R}z$ (la suma es directa porque los elementos de O son idempotentes ortogonales dos a dos),

$$\dim_F(Rf) = \dim_{\mathbf{F}}(\mathbf{R}f) = \sum_{z\in O} dim_{\mathbf{F}}(\mathbf{R}z) = \sum_{z\in O} 1 = |O| = wt(D(f))$$

pues $\dim_{\mathbf{F}}(\mathbf{R}z) = 1$ para todo $z \in O$ (por Proposición 2.2.4).

2. Como $U|_G : G \to \eta$ es un isomorfismo de H-conjuntos, U induce una correspondencia biyectiva que preserva cardinalidad $\widehat{U} : G/H \to \eta/H$ dada por $\widehat{U}(S) = U(S)$.

   Sea η' la colección de los idempotentes primitivos de R. Por el argumento de descenso de Galois (Proposición 3.2.3), $v : \eta/H \to \eta'$ dado por $v(O) = \sum_{o \in O} o$ es una función biyectiva. Así que $v \circ \widehat{U} : G/H \to \eta'$ es una biyección entre las q-órbitas y los idempotentes primitivos de R, y como estos idempotentes están en biyección con los ideales minimales que ellos generan, entonces existe una biyección entre q-órbitas y los ideales minimales de R (esto ya lo garantizaba el Teorema 3.1.1, pero ahora conocemos la biyección y no solo de su existencia).

   Ahora, por un argumento similar al presentado al final de la prueba de la parte 1, si $f = v(O)$ con $O \in \eta/H$, entonces $\dim_F(Rf) = |O| = |\widehat{U}^{-1}(O)| = |\widehat{U}^{-1}(v^{-1}(f))|$, es decir, el tamaño de la q-órbita $\widehat{U}^{-1}(v^{-1}(f)) = \widehat{U}^{-1} \circ v^{-1}(f)$ que es la correspondiente al ideal Rf es igual a la dimensión de este.

□

Observe que el Teorema 3.2.5 (parte 2) implica el Teorema 3.1.1. El $\mathbf{F}$-automorfismo D presentado en el Teorema 3.2.5 (parte 1) será llamado ***el indicador de dimensiones de*** R ***asociado a*** $\mathbf{F}$, o simplemente ***el indicador de*** R. Note que como todo código abeliano es suma directa de ideales minimales (por Teorema 1.3.1, parte 3), el indicador de dimensiones de R puede ser utilizado para calcular la dimensión de cualquier código abeliano.

Ahora veremos que el indicador de R está relacionado con la transformada de Fourier discreta. El grupo de caracteres G^* de G es el conjunto de los morfismos de grupo de G a $\mathbf{F} - \{0\}$ con la multiplicación de funciones. Es bien conocido que $G^* \cong G$ (ver, por ejemplo, [9, Sección 1.1]). La transformada de Fourier discreta ϵ (ver [14, Sección II.A], [9, Sección 2]) es el isomorfismo de $\mathbf{F}$-álgebras que va desde $\mathbf{F}G^*$ a su descomposición de Artin-Wederburn $\mathbf{F}^{|G|}$ dado por $\epsilon(f) = (f(g))_{g \in G}$. Sea $\lambda = \epsilon^{-1}$, μ la base canónica de $\mathbf{F}^{|G|}$, y η^* la colección de idempotentes primitivos de $\mathbf{F}G^*$. Note que si $f_1 : \mathbf{F}G \to \mathbf{F}^{|G|}$ y $f_2 : \mathbf{F}G \to \mathbf{F}G^*$ son las transformaciones $\mathbf{F}$-lineales que envían a G en μ y η en η^*, respectivamente, entonces el siguiente diagrama commuta:

$$\begin{array}{ccc} \mathbf{F}G & \xrightarrow{U} & \mathbf{F}G \\ {\scriptstyle f_1}\downarrow & & \downarrow{\scriptstyle f_2} \\ \mathbf{F}^{|G|} & \xrightarrow[\lambda]{} & \mathbf{F}G^* \end{array}$$

Es decir, $\lambda f_1 = f_2 U$, así ${}_{G^*}[\lambda f_1]_G =_{G^*} [f_2 U]_G$, por lo que

$$({}_{G^*}[\lambda]_\mu)({}_\mu[f_1]_G) = ({}_{G^*}[\lambda]_\mu)id =_{G^*} [\lambda]_\mu = ({}_{G^*}[f_2]_G)({}_G[U]_G).$$

Por otro lado, si f_3 es la extensión lineal de un isomorfismo de grupos entre G y G^*, entonces es un isomorfismo de F-álgebras entre $\mathbf{F}G$ y $\mathbf{F}G^*$ que envía a η en η^*, es decir, existe un orden en η en η^* para el cual $f_3 = f_2$. En ese caso ${}_{G^*}[f_2]_G = id$, luego $A =_G [U]_G =_{G^*} [\lambda]_\mu$.

Por el Teorema 3.2.2 podemos calcular el indicador de R como el inverso de la transformación $\mathbf{F}$-lineal de $\mathbf{R}$ cuya matriz en la base G tiene como columnas los vectores de coordenadas de los idempotentes primitivos de $\mathbf{R}$ con respecto a G. Como $A =_{G^*} [\lambda]_\mu$, esto también puede hacerse utilizando Teoría de Caracteres (ver [14, Corolario $II.2$]), pero nosotros estamos motivados principalmente por el hecho que el indicador de R puede obtenerse como una aplicación del Teorema 2.1.4 (parte 3), con un enfoque alternativo al clásico.

Ejemplo 3.2.6. *Sea $F = \mathbb{F}_3$ y $G = C_2 \times C_4$ donde $C_2 = \{1, x_1\}$ y $C_4 = \{1, x_2, x_2^2, x_2^3\}$ son los grupos cíclicos de orden 2 y 4, respectivamente. Sea γ una raíz en alguna extensión de F del polinomio $z^2 - z - 1$. Como γ^2 es una raíz 4-ésima primitiva de la unidad, $\mathbf{F} := F(\gamma) = F(\gamma^2)$ es un campo de descomposición para G. Sea l_i como en el Teorema 3.2.2, y $\sigma(l_i)$ el espectro de l_i para $i = 1, 2$. Entonces $\sigma(l_1) = \{1, 2\}$ y $\sigma(l_2) = \{1, \gamma^2, \gamma^4 = 2, \gamma^6\}$. Así, por Teorema 3.2.2, los vectores de coordenadas de los idempotentes primitivos de $R_1 = \mathbf{F}C_2$ y $R_2 = \mathbf{F}C_4$ son $\{(2,2),(2,1)\}$ y $\{(1,1,1,1),(1,2,1,2),(1,\gamma^6,2,\gamma^2),(1,\gamma^2,2,\gamma^6)\}$, respectivamente. Note que $2\gamma^6 = \gamma^2$. Luego, por Teorema 3.2.2,*

$$\begin{array}{lcl}
(2,2) \otimes (1,1,1,1) & = & (2,2,2,2,2,2,2,2) \\
(2,2) \otimes (1,\gamma^6,2,\gamma^2) & = & (2,\gamma^2,1,\gamma^6,2,\gamma^2,1,\gamma^6) \\
(2,2) \otimes (1,2,1,2) & = & (2,1,2,1,2,1,2,1) \\
(2,2) \otimes (1,\gamma^2,2,\gamma^6) & = & (2,\gamma^6,1,\gamma^2,2,\gamma^6,1,\gamma^2) \\
(2,1) \otimes (1,1,1,1) & = & (2,2,2,2,1,1,1,1) \\
(2,1) \otimes (1,\gamma^6,2,\gamma^2) & = & (2,\gamma^2,1,\gamma^6,1,\gamma^6,2,\gamma^2) \\
(2,1) \otimes (1,2,1,2) & = & (2,1,2,1,1,2,1,2) \\
(2,1) \otimes (1,\gamma^2,2,\gamma^6) & = & (2,\gamma^6,1,\gamma^2,1,\gamma^2,2,\gamma^6)
\end{array}$$

son los vectores de coordenadas de los idempotentes primitivos de $\mathbf{R} = \mathbf{F}G$ *con respecto a* $G = \{1, x_2, x_2^2, x_2^3, x_1, x_1x_2, x_1x_2^2, x_1x_2^3\}$ *(ordenado lexicográficamente con* $x_2 < x_1$*). Por otro lado, como* 2 *y* γ^2 *son una raíz* 2*-primitiva y* 4*-primitiva de la unidad, respectivamente, se puede definir un isomorfismo de* H*-conjuntos entre* G *y* η *en términos de* 2 *y* γ^2 *como*

$$\begin{aligned} U: \ G &\longrightarrow \quad \eta \\ x_1^{\epsilon_1}x_2^{\epsilon_2} &\longmapsto e(2^{\epsilon_1})e(\gamma^{2\epsilon_2}), \end{aligned}$$

donde $e(2^{\epsilon_1}) = 2(1 + 2^{\epsilon_1}x_1)$ *y* $e(\gamma^{2\epsilon_2}) = 1 + \gamma^{6\epsilon_2}x_2 + 2^{\epsilon_2}x_2^2 + \gamma^{2\epsilon_2}x_2^3$*, y su extensión lineal* U *es la matriz de cambio de bases que envía a* G *en* η*. Por lo que la matriz del indicador* D *en la base* G *es* $A^{-1} = [U]_G^{-1}$*, la cual esta dada por*

$$A^{-1} = \begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & \gamma^2 & 1 & \gamma^6 & 2 & \gamma^2 & 1 & \gamma^6 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ 2 & \gamma^6 & 1 & \gamma^2 & 2 & \gamma^6 & 1 & \gamma^2 \\ 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\ 2 & \gamma^2 & 1 & \gamma^6 & 1 & \gamma^6 & 2 & \gamma^2 \\ 2 & 1 & 2 & 1 & 1 & 2 & 1 & 2 \\ 2 & \gamma^6 & 1 & \gamma^2 & 1 & \gamma^2 & 2 & \gamma^6 \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \gamma^2 & 2 & \gamma^6 & 1 & \gamma^2 & 2 & \gamma^6 \\ 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 1 & \gamma^6 & 2 & \gamma^2 & 1 & \gamma^6 & 2 & \gamma^2 \\ 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 1 & \gamma^2 & 2 & \gamma^6 & 2 & \gamma^6 & 1 & \gamma^2 \\ 1 & 2 & 1 & 2 & 2 & 1 & 2 & 1 \\ 1 & \gamma^6 & 2 & \gamma^2 & 2 & \gamma^2 & 1 & \gamma^6 \end{pmatrix}.$$

Ahora daremos una tabla donde se presentan los elementos de G*, sus imagenes bajo* U *y los vectores de coordenadas de estas. Además identificaremos con distintos colores las* 3*-órbitas de* G *y las órbitas de los idempotentes primitivos de* $\boldsymbol{F}G$ *bajo la acción (por evaluación en coeficientes) del grupo de Galois.*

Por el argumento del descenso de Galois podemos concluir que los idempotentes primitivos de FG *son los idempotentes que aparecen en los reglones impares del Cuadro*

g	$U(g)$	$[U(g)]_G$
1	$2+2x_2+2x_2^2+2x_2^3+2x_1+2x_1x_2+2x_1x_2^2+2x_1x_2^3$	$(2,2,2,2,2,2,2,2)$
x_2	$2+\gamma^2x_2+x_2^2+\gamma^6x_2^3+2x_1+\gamma^2x_1x_2+x_1x_2^2+\gamma^6x_1x_2^3$	$(2,\gamma^2,1,\gamma^6,2,\gamma^2,1,\gamma^6)$
x_2^2	$2+x_2+2x_2^2+x_2^3+2x_1+x_1x_2+2x_1x_2^2+x_1x_2^3$	$(2,1,2,1,2,1,2,1)$
x_2^3	$2+\gamma^6x_2+x_2^2+\gamma^2x_2^3+2x_1+\gamma^6x_1x_2+x_1x_2^2+\gamma^2x_1x_2^3$	$(2,\gamma^6,1,\gamma^2,2,\gamma^6,1,\gamma^2)$
x_1	$2+2x_2+2x_2^2+2x_2^3+x_1+x_1x_2+x_1x_2^2+x_1x_2^3$	$(2,2,2,2,1,1,1,1)$
x_1x_2	$2+\gamma^2x_2+x_2^2+\gamma^6x_2^3+x_1+\gamma^6x_1x_2+2x_1x_2^2+\gamma^2x_1x_2^3$	$(2,\gamma^2,1,\gamma^6,1,\gamma^6,2,\gamma^2)$
$x_1x_2^2$	$2+x_2+2x_2^2+x_2^3+x_1+2x_1x_2+x_1x_2^2+2x_1x_2^3$	$(2,1,2,1,1,2,1,2)$
$x_1x_2^3$	$2+\gamma^6x_2+x_2^2+\gamma^2x_2^3+x_1+\gamma^2x_1x_2+2x_1x_2^2+\gamma^6x_1x_2^3$	$(2,\gamma^6,1,\gamma^2,1,\gamma^2,2,\gamma^6)$

Cuadro 3.1: Imagen de U e identificación en colores de órbitas bajo las acciones de H en G y η.

3.1, $1+2x_2^2+x_1+2x_1x_2^2$ *(la suma de los idempotentes de los reglones 2 y 4 del Cuadro* *3.1*), *y* $1+2x_2^2+2x_1+x_1x_2^2$ *(la suma de los idempotentes de los reglones 6 y 8 del Cuadro* *3.1*), *pues* $\gamma^2+\gamma^6=0$.

Como $D|_\eta:\eta\to G$ *es un isomorfismo de* H*-conjuntos, la imagen de cualquier idempotente de* R *bajo* D *es una suma de elementos de* G *pertenecientes a una unión de* q*-órbitas. Sea* $v_1=20002111$, $v_2=01111101$, $v_3=11212101$, $v_4=21111111$, *y* $v_5=00200202$. *Un cálculo directo muestra que el elemento* $f_i\in R$ *tal que* $[f_i]_G=v_i$ *es idempotente para todo* i. *Aplicando el Lema* *1.4.5* *para calcular* $\dim_F(Rf_i)$, *obtenemos que este coincide con* $wt(D(f_i))$ *para todo* i, *como lo garantiza el Teorema* *3.2.5*. *De hecho, las funciones* **`rank(_)`** *y* **`codes.LinearCode(_).minimum_distance()`** *de SageMath* *[42]* *aplicadas a la matriz* $[r_{f_i}]_G$ *dan la dimensión y distancia mínima del código de grupo* Rf_i. *Lo anterior se resume en el Cuadro* *3.2*:

i	$v_i=[f_i]_G$	$[D(f_i)]_G=[D]_Gv_i$	$wt(D(f_i))$	Parámetros de Rf_i
1	20002111	10000111	4	$[8,4,4]$
2	01111101	00100101	3	$[8,3,4]$
3	11212101	01111010	5	$[8,5,2]$
4	21111111	01111111	7	$[8,7,2]$
5	00200202	01111101	6	$[8,6,2]$

Cuadro 3.2: Ilustración del Teorema 3.2.5 (parte 1).

Note que en la tercera columna del Cuadro *3.2*, *para cada vector de coordenadas, aparecerá 1 de un color determinado si y solo si el idempotente primitivo de* FG *co-*

rrespondiente a dicho color aparece en la descomposición de f_i como suma de idempotentes primitivos para todo i. Por ejemplo, para f_1 aparece un uno en la posición primera, sexta y octava, y séptima, entonces f_1 se escribe como la suma de los idempotentes azul, naranja y negro de FG. Esto se puede comprobar observando que $20002111 = 22222222 + 10202010 + 21211212$.

De acuerdo a la tabla [23], los códigos Rf_i resultaron ser óptimos para todo i, es decir, con la distancia mínima más grande posible para un código con longitud 8 y dimensión correspondiente.

Ejemplo 3.2.7. *Sea $F = \mathbb{F}_3$ y $G = \langle x_1\rangle \times \langle x_2\rangle \times \langle x_3\rangle$ donde $\langle x_i\rangle = \{1, x_i\}$ para todo i. Note que $exp(G) = 2$ es una raíz 2-primitiva de la unidad. Luego, por Teorema 3.2.1, F es un campo de descomposición para G. Sea l_i como en el Teorema 3.2.2, y $\sigma(l_i)$ el espectro de l_i para $i = 1, 2, 3$. Entonces $\sigma(l_i) = \{1, 2\}$ para todo i. Así, por Teorema 3.2.2, los vectores de coordenadas de los idempotentes primitivos de $R_i = \mathbf{F}C_2$ son $\{(2, 2), (2, 1)\}$ para todo i.*

Sea β como en el Teorema 3.2.2, es decir, $\beta = \{1 \otimes 1 \otimes 1, 1 \otimes 1 \otimes x_3, 1 \otimes x_2 \otimes 1, 1 \otimes x_2 \otimes x_3, x_1 \otimes 1 \otimes 1, x_1 \otimes 1 \otimes x_3, x_1 \otimes x_2 \otimes 1, x_1 \otimes x_2 \otimes x_3\}$ (orden lexicográfico con $x_3 < x_2 < x_1$), entonces

$$\begin{array}{rcl}
(2,2)\otimes(2,2)\otimes(2,2) & = & (2,2)\otimes(1,1,1,1) = (2,2,2,2,2,2,2,2)\\
(2,2)\otimes(2,2)\otimes(2,1) & = & (2,2)\otimes(1,2,1,2) = (2,1,2,1,2,1,2,1)\\
(2,2)\otimes(2,1)\otimes(2,2) & = & (2,2)\otimes(1,1,2,2) = (2,2,1,1,2,2,1,1)\\
(2,2)\otimes(2,1)\otimes(2,1) & = & (2,2)\otimes(1,2,2,1) = (2,1,1,2,2,1,1,2)\\
(2,1)\otimes(2,2)\otimes(2,2) & = & (2,1)\otimes(1,1,1,1) = (2,2,2,2,1,1,1,1)\\
(2,1)\otimes(2,2)\otimes(2,1) & = & (2,1)\otimes(1,2,1,2) = (2,1,2,1,1,2,1,2)\\
(2,1)\otimes(2,1)\otimes(2,2) & = & (2,1)\otimes(1,1,2,2) = (2,2,1,1,1,1,2,2)\\
(2,1)\otimes(2,1)\otimes(2,1) & = & (2,1)\otimes(1,2,2,1) = (2,1,1,2,1,2,2,1)
\end{array}$$

son los vectores de coordenadas de los idempotentes primitivos de $R_1 \otimes R_2 \otimes R_3$ con respecto a β. Si suponemos que G tiene el orden determinado por β, es decir, $G = \{1, x_3, x_2, x_2x_3, x_1, x_1x_3, x_1x_2, x_1x_2x_3\}$, y χ es como en el Teorema 3.2.2, entonces ${}_\beta[\chi]_G = Id$. Por lo tanto, estos también son los vectores de coordenadas de los idempotentes primitivos de $\mathbf{R}$ con respecto G. Por otro lado, como 2 es una raíz 2-primitiva de la unidad, se puede definir un isomorfismo de H-conjuntos entre G y η en términos de 2 como

$$\begin{array}{rccc}
U: & G & \longrightarrow & \eta\\
 & x_1^{l_1}x_2^{l_2}x_3^{l_3} & \longmapsto & e(2^{l_1})e(2^{l_2})e(2^{l_3}),
\end{array}$$

donde $e(2^{l_i}) = 2(1 + 2^{l_i}x_i)$ *para todo* i*, y su extensión lineal* U *es la matriz de cambio de bases que envía a* G *en* η*. Por lo que la matriz del indicador* D *en la base* G *es* $A^{-1} = [U]_G^{-1}$*, la cual esta dada por*

$$A^{-1} = \begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 2 & 1 & 2 & 1 & 2 & 1 & 2 & 1 \\ 2 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\ 2 & 1 & 1 & 2 & 2 & 1 & 1 & 2 \\ 2 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 1 & 1 & 2 & 1 & 2 \\ 2 & 2 & 1 & 1 & 1 & 1 & 2 & 2 \\ 2 & 1 & 1 & 2 & 1 & 2 & 2 & 1 \end{pmatrix}^{-1}$$

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

Como $D|_\eta : \eta \to G$ *es un isomorfismo de* H*-conjuntos, la imagen de cualquier idempotente de* R *bajo* D *es una suma de elementos de* G *pertenecientes a una unión de* q*-órbitas. Sea* $v_1 = 11000011$*,* $v_2 = 12112210$*,* $v_3 = 12222022$*,* $v_4 = 20100000$*, y* $v_5 = 01012222$*. Un cálculo directo muestra que el elemento* $f_i \in R$ *tal que* $[f_i]_G = v_i$ *es idempotente para todo* i*. Aplicando el Lema 1.4.5 para calcular* $\dim_F(Rf_i)$*, obtenemos que este coincide con* $wt(D(f_i))$ *para todo* i*, como lo garantiza el Teorema 3.2.5. De hecho, las funciones* `rank(_)` *y* `codes.LinearCode(_).minimum_distance()` *de SageMath [42] aplicadas a la matriz* $[r_{f_i}]_G$ *dan la dimensión y distancia mínima del código de grupo* Rf_i*. Lo anterior se resume en el Cuadro 3.3:*

De acuerdo a la tabla [23], los códigos Rf_i *resultaron ser óptimos para* $i = 2, 3, 5$*, es decir, con la distancia mínima más grande posible para un código con longitud* 8 *y dimensión* $5, 5, 3$*, respectivamente.*

i	$v_i = [f_i]_G$	$[D(f_i)]_G = [D]_G v_i$	$wt(D(f_i))$	Parámetros de Rf_i
1	11000011	10000010	2	$[8, 2, 4]$
2	12112210	10110110	5	$[8, 5, 2]$
3	12222022	11011010	5	$[8, 5, 2]$
4	20100000	00110011	4	$[8, 4, 2]$
5	01012222	11000100	3	$[8, 3, 4]$

Cuadro 3.3: Ilustración del Teorema 3.2.5 (parte 1).

Capítulo 4

Códigos de grupo MDS

En este capítulo se estudian distintas relaciones de la teoría desarrollada en el Capítulo 2 con los códigos de grupo MDS. En particular, se describen los parámetros de códigos de grupo MDS que son ideales principales, mediante el análisis de los polinomios minimales y característicos de la representación regular derecha asociada a un generador (Teorema 4.1.2 partes $1, 2$). Se presenta el concepto de ***código de grupo de dimensión fácilmente calculable*** y distintas relaciones que este tiene con los códigos MDS (Teorema 4.1.2 parte 3, y Teorema 4.2.5).

Asumiremos que $F = \mathbb{F}_q$ y $car(F) = p > 0$ a menos que se indique lo contrario. La cota de Singleton establece que si existe un $[n, k, d]$-código lineal sobre F, entonces $k \leq n - d + 1$ [27, Teorema 2.4.1]. Un código para el cual se obtiene la igualdad en esta cota es llamado un código de distancia máxima separable (maximum distance separable) o MDS (por sus siglas en Inglés). Estos códigos son optimales en el sentido que estos alcanzan la mayor distancia mínima posible para una longitud y dimensión fija, así que estos son de gran interés para la corrección de errores.

R tiene una forma bilineal simétrica, no degenerada, y G-invariante dada por

$$\langle g, h\rangle = \delta_{gh},\ para\, todo\, g, h \in G$$

Donde G-invariante significa que $\langle gx, gy\rangle = \langle x, y\rangle$ para todo $x, y \in R$ y $g \in G$.

Respecto a esta forma bilineal se define el ortogonal (dual) $C^{\perp}$ de un código de grupo $C \leq R$ como

$$C^{\perp} = \{x \in R : \langle x, c\rangle = 0\, para\, todo\, c \in C\}$$

Como $\langle \bullet, \bullet \rangle$ es G-invariante, $C^{\perp}$ también es un ideal de R.

Una transformación monomial M de R es una transformación lineal $M : R \to R$ tal que

$$M(\sum_{g \in G} \lambda_g g) = \sum_{g \in G} m_g \lambda_{\sigma(g)} g$$

donde $m_g \in F - \{0\}$ para todo $g \in G$ y $\sigma \in S_G$.

Dos códigos de grupo $C, C' \leq R$ se dice que son monomialmente equivalentes si existe una transformación monomial M de R tal que $M(C) = C'$.

Dos códigos de grupo monomialmente equivalentes tienen la misma distancia mínima y las mismas distribuciones de pesos.

C es un código de grupo MDS si C es un ideal de FG tal que sus parámetros satisfacen la igualdad en la cota de Singleton. Si C es un código de grupo MDS de R, se dirá que es trivial si $C = R$ o C es monomialmente equivalente a $R(\sum_{g \in G} g)$ (el código repetición) o a su dual (el ideal de aumentación) (ver definición para códigos lineales [27, pp 71-72]).

4.1. Cota de Singleton y Códigos ECD

Observe que el Corolario 2.1.7 (parte 1) presenta una manera sencilla de calcular la dimensión de ciertos códigos de grupo, esto nos lleva a introducir nuestra próxima definición. Sea J un ideal de R, si J es principal generado por un idempotente, y $\dim_{\mathbb{F}_q}(J) \leq p$, entonces se dirá que J es un ***código de grupo de dimensión fácilmente calculable*** (easily computable dimension group code), abreviado ECD (por sus siglas en Inglés). Si cualquier ideal distinto de 0 y R es un código de grupo ECD, entonces se dirá que R es un ***álgebra de grupo de dimensión fácilmente calculable*** abreviado ECD. A continuación usaremos el Teorema de Maschke para clasificar las álgebras de grupo ECD.

Teorema 4.1.1. *R es ECD si y solo si $|G| \leq p + 1$ y $|G| \neq p$.*

Demostración. Supongamos que R es ECD. Sea C un ideal no-trivial de R, entonces $C = Re$ para algún idempotente $e \in R$ y $\dim(C) \leq p$. Como C es generado por un

idempotente, C tiene un complemento directo. Por lo tanto R es semisimple (pues todo ideal tiene complemento directo, ver [15, Lema 2.3]), y por Teorema 1.1.2 $p \nmid |G|$, luego $p \neq |G|$. Por otro lado, si $e_G := \frac{1}{|G|}\sum_{g\in G} g$, $\dim(R(1-e_G)) = |G| - 1 \leq p$, implicando que $|G| \leq p+1$.

Supongamos que $|G| \leq p+1$ y $|G| \neq p$. Entonces $p \nmid |G|$, y por Teorema 1.1.2 R es semisimple, así que todo ideal de R es generado por un idempotente (por Teorema 1.3.1, parte 3). Además la desigualdad $|G| \leq p+1$, implica que la dimensión de todo ideal propio de R es menor o igual a p.

□

El siguiente resultado es una consecuencia directa de la cota de Singleton, Teorema 2.1.4 y Corolario 2.1.7 (parte 1).

Corolario 4.1.2. *Sea $b \in R$ tal que $m_b(x) = x^n p_1(x)^{r_1} \cdots p_t(x)^{r_t}$ donde los p_i son factores mónicos irreducibles distintos con $p_i \neq x$ para todo i. Sea $p_b(x) = x^u h(x)$ donde $x \nmid h(x)$. Sea d la distancia mínima de Rb. Entonces se tienen las siguientes afirmaciones:*

1. *Si $\zeta_n = \dim(ker(r_b^n)/ker(r_b))$, entonces $d \leq u - \zeta_n + 1$. Además, Rb es un código MDS si y solo si es un $[|G|, |G|-u+\zeta_n, u-\zeta_n+1]$-código. En particular, si $n = 1$, $d \leq u+1$; Rb es código de grupo MDS si solo si es un $[|G|, |G|-u, u+1]$-código.*

2. $$d \leq \begin{cases} |G| - (t+1)|G|_p + 1 & si\ |G|_p \mid \dim(ker(r_b))\ and\ n > 1 \\ |G| - t|G|_p + 1 & en\ otro\ caso \end{cases}$$

   Además, si $n = 1$ y Rb es un código de grupo MDS, entonces $d \equiv 1 \pmod{|G|_p}$ y $|G|_p + 1 \leq d \leq |G| - t|G|_p + 1$.

3. *Si $m_b(x) = x(x-a)^s$ para algún entero $s \geq 1$ y $a \in F - \{0\}$, r es el menor entero positivo en la clase $|G|\lambda_1(b)a^{-1}$; y Rb es un código de grupo ECD, entonces $d \leq |G| - r + 1$. Además, Rb es un código de grupo MDS y ECD si solo si es un $[|G|, r, |G| - r + 1]$-code.*

Ejemplo 4.1.3. *Sea G un grupo de orden mp^l con $l \geq 1$, $m \neq 1$, y $p \nmid m$. Sea $b \in R$, $m_b(x) = x^n p_1(x)^{r_1} \cdots p_t(x)^{r_t}$ donde los p_i son factores mónicos irreducibles con $p_i \neq x$ para todo i. Entonces, por Teorema 2.1.3, p^l divide a $\dim(ker(r_b^n))$ y $\dim(ker(p_i(r_b)^{r_i}))$*

para $i = 1, ..., t$, por lo que $1 \leq t < m$. Así, si $m = 2$, entonces $m_b(x)$ solamente tiene dos factores irreducibles. Por lo tanto, si $n = 1$ y Rb es un código de grupo MDS, entonces Rb es proyectivo (por Lema 1.4.3) y su distancia mínima d debe ser $p^l + 1$ (por Corolario 4.1.2, parte 2).

Sea $G = \langle a, b \mid a^3 = b^2 = 1, bab^{-1} = a^2 \rangle = \{1, b, a, a^2, ba^2, ba\}$ el grupo simétrico de grado 3, y $R = \mathbb{F}_9 G$. Si α es un elemento de $\mathbb{F}_9$ con polinomio mínimo $z^2 + z + 1$, entonces $b = (2\alpha + 2) + (\alpha + 1)b + \alpha a + (2\alpha + 1)a^2 + (\alpha + 1)ba^2 + ba$ es tal que $m_b(x) = x(x+2\alpha)^2$. En este caso, Rb es un $[6, 3, 4]$-código MDS, y así $d = 3+1$ como se estableció en el Corolario 4.1.2 (parte 2). Por otro lado, $b' = (\alpha+1)+\alpha b+2a+2a^2+2ba$ es tal que $m_{b'}(x) = x^2(x + \alpha + 2)^2$. En este caso, Rb' es un $[6, 4, 3]$-código MDS, y así $d = 3 \lneq 3 + 1$, esto ocurre porque la multiplicidad de 0 como raíz de $m_{b'}(x)$ no es 1 sino 2.

4.2. Relación de existencia entre códigos MDS y ECD

Ahora estudiaremos una relación entre los códigos de grupo MDS y ECD. Para ese propósito recordamos la Conjetura-MDS.

Conjetura-MDS [27, pág. 265]: Si existe un código (lineal) MDS con parámetros $[n, k]$ sobre $\mathbb{F}_q$, entonces

$$n \leq \begin{cases} q + 2 & \text{si } q \text{ par, y } k = 3 \text{ o } k = q - 1 \\ q + 1 & \text{en otro caso} \end{cases}$$

Lema 4.2.1. *[27, Teorema 2.4.4] Si C es un código MDS binario, entonces C es trivial.*

Lema 4.2.2. *[39, Teorema 1] Si C es un código cíclico de longitud p sobre $\mathbb{F}_p$, entonces C es equivalente a un código MDS*

Lema 4.2.3. *Sea p un número primo. Si la Conjetura-MDS es verdadera, entonces los únicos códigos de grupo MDS no-triviales en el álgebra de grupo no-semisimple $\mathbb{F}_p G$ existen cuando $G = C_p$ y p es impar; y son equivalentes a códigos MDS.*

Demostración. Si $\mathbb{F}_p G$ no es semisimple, por Teorema 1.1.2, $p \mid |G|$. Supongamos que la Conjectura-MDS es cierta y que existe un código de grupo MDS C en $\mathbb{F}_p G$. Entonces

si $p = 2$, cualquier código de grupo MDS en $\mathbb{F}_2 G$ es trivial (por Lema 4.2.1), así que C es trivial. Si p es un primo impar, $|G| \leq p+1$ (por la Conjetura-MDS), así que $p \mid |G|$ y $|G| \leq p+1$. Como la igualdad $|G| = p+1$ no es posible, $p \mid |G|$ y $|G| < p+1$, así $G = C_p$. Implicando que C es un código de grupo en $\mathbb{F}_p C_p$, es decir, C es un código cíclico de longitud p sobre $\mathbb{F}_p$. Por lo tanto, C es equivalente un código cíclico MDS (por Lema 4.2.2). □

Teorema 4.2.4. *[2, Corolario 9.1] Un código MDS de dimensión k sobre $\mathbb{F}_q$ tiene longitud a lo mas*

$$q + k + 1 - min(k, p) \text{ donde } k \leq q.$$

Teorema 4.2.5. *Se tienen las siguientes afirmaciones:*

1. *Si existe un código de grupo MDS y ECD en R, entonces $|G| \leq q+1$*
2. *Sea p un primo impar. Supongamos que la Conjetura-MDS es cierta y que $G \neq C_p$. Si existe un código de grupo MDS no-trivial en $\mathbb{F}_p G$, entonces $\mathbb{F}_p G$ es un álgebra de grupo ECD.*

Demostración. 1. Se sigue del Teorema 4.2.4.

2. Si existe un código de grupo MDS no-trivial en $\mathbb{F}_p G$, por Lema 4.2.3, $\mathbb{F}_p G$ es semisimple o $G = C_p$ con p impar. Así $\mathbb{F}_p G$ es semisimple, y por la Conjectura-MDS, $|G| - 1 \leq p$, implicando que R es un álgebra de grupo ECD.

□

Capítulo 5

Conclusiones y perspectivas

En este último capítulo se presentarán las principales conclusiones obtenidas a lo largo de este trabajo, y se plantearán prespectivas que se podrían abordar en investigaciones futuras.

5.1. Conclusiones

Las principales conclusiones que se han obtenido en el desarrollo de este proyecto son las siguientes:

- Se proponen distintas técnicas para describir la dimensión de ideales principales en álgebras de grupo (Teoremas 2.1.4 y 3.1.2, Corolarios 2.1.6 y 2.1.7), obteniendo en algunos casos fórmulas explícitas (Teorema 2.1.4, parte 1, y Teoremas 2.2.1 y 2.2.5, parte 2). Algunos de estos resultados generalizan o complementan otros ya conocidos en la literatura.
- Se introduce el indicador de dimensiones de un álgebra de grupo conmutativa semisimple finita, el cual permite calcular la dimensión de cualquier código abeliano de manera sencilla (Teoremas 3.2.5), y se presenta un método para calcularlo.
- Via la Conjectura-MDS se obtiene una relación entre los códigos de dimensión fácilmente calculable y los códigos MDS, de manera que la existencia de los primeros implica la de los segundos (Teorema 4.2.5). Una consecuencia directa del Teorema 4.2.5 es que todo código de grupo MDS no-cíclico en $\mathbb{F}_p G$ es un código de dimensión fácilmente calculable.
- Se han dado ejemplos que ilustran los principales resultados.

5.2. Perspectivas

En esta sección se presentarán los problemas abiertos relacionados con los resultados presentados en esta tesis. Algunos de estos se encuentran relacionados con el problema de describir la dimensión de ideales en álgebras de grupo sobre un campo arbitrario, y otros son referentes a la dimensión de códigos de grupo.

- Los Teoremas 2.1.4 y 2.2.1 han mostrado ser útiles para describir la dimensión de ideales principales en álgebras de grupo. Sin embargo, su alcance es limitado si se quieren aplicar a ideales principales generados por elementos nilpotentes, ya sea porque sus consecuencias se vuelven triviales, o porque no pueden aplicarse. Así que un problema abierto sería el de encontrar alternativas teóricas que describan con éxito la dimensión de ideales principales generados por nilpotentes en término de relaciones como identidades, cotas y congruencias.

- El Teorema 3.1.2 presenta una cota inferior y superior para la dimensión de un código abeliano en un álgebra de grupo semisimple. Un problema abierto sería el de determinar bajo qué condiciones podemos obtener la igualdad de la dimensión del código con estas cotas.

- Sea F un campo arbitrario y G un grupo finito. En [19] se presenta el concepto de F-clase ciclotómica, que es una generalización del concepto de q-órbita. Luego se prueba que existe una correpondencia biunívoca entre los ideales minimales del centro de $FG/J(FG)$ (donde $J(FG)$ denota el radical de Jacobson de FG) y las F-clases ciclotómicas de G, y que cada ideal tiene dimensión igual al tamaño de su F-clase ciclotómica correspondiente [19, Teorema 1.3]. Este resultado es una generalización del Teorema 3.1.1. Como este último es una consecuencia del Teorema 3.2.5 (parte 2), es natural preguntarse si se pueden generalizar las ideas que se usaron para construir el isomorfismo U que aparece en este, de manera que se encuentre explícitamente una biyección como la mencionada en [19, Teorema 1.3]. Esto permitiría determinar la dimensión de los ideales del centro de $FG/J(FG)$, tal cual como lo hicimos para los ideales de un álgebra de grupo conmutativa semisimple sobre un campo finito.

- El Teorema 4.2.5 nos garantiza, bajo ciertas condiciones, la existencia de un código de grupo MDS en $\mathbb{F}_pG$ implica que $\mathbb{F}_pG$ es un álgebra de grupo de dimensión fácilmente calculable. Un problema abierto es el de determinar si el hecho de que $\mathbb{F}_pG$ sea ECD implica la existencia de un código de grupo MDS en $\mathbb{F}_pG$, y si no es así, evaluar si es posible encontrar condiciones bajo las cuales esto sea cierto.

Apéndice A
Ejemplos en SageMath

En este apéndice presentamos funciones que fueron útiles para el desarrollo de los Ejemplos de esta tesis (2.1.8, 2.1.9, 2.2.3, 4.1.3, 3.2.6 y 3.2.7). Para estos ejemplos, se crearon funciones personalizadas en Python y luego se cargaron en SageMath. Antes de ejecutar funciones personalizadas creadas con algoritmos propios, se debe tener un archivo `"nombre.py"` (que es el tipo de extensión de archivos Python) que contenga dichas funciones en una carpeta interna de SageMath y luego cargarlo dentro de una página de trabajo de SageMath escribiendo `load("nombre.py")` y presionando `Shift+Enter`. De esta manera todas las funciones personalizadas se cargarán como si fueran funciones propias de SageMath.

5.3. Funciones Python usadas en los Ejemplos 2.1.8, 2.1.9, 2.2.3, y 4.1.3.

En esta sección presentamos las funciones Python utilizadas para elaborar los ejemplos 2.1.8, 2.1.9, 2.2.3, y 4.1.3. Dichas funciones se hicieron con el propósito de obtener para cualquier $b \in R$ la matriz de $[r_b]_G$, donde el grupo G es un grupo de permutaciones que viene con un orden (como base del álgebra de grupo) fijado por SageMath.

Dada un tupla `(g, F, G)` donde g es un elemento de G, la función `grrep(g,F,G)` retorna la matriz $[r_g]_G$. El orden de la base ordenada G viene fijado por SageMath ya que G se construye como un grupo de permutaciones de SageMath.

```
def grrep(g,F,G):
    A = GroupAlgebra(G, F)
```

```
    u=list(A.basis())
    l1=[]
    for i in u:
        l2=[]
        for j in u:
            if i*g==j:
                l2.append(1)
            else:
                l2.append(0)
        l1.append(l2)
    return Matrix(F,l1).transpose()
```

Dada una tupla `(F,G)`, la función `grbasisrep(F,G)` retorna la colección $\{[r_g]_G : g \in G\}$.

```
def grbasisrep(F,G):
    c=[]
    A = GroupAlgebra(G, F)
    u=list(A.basis())
    for i in u:
        c.append(rrep(i,F,G))
    return c
```

Dada un tupla `(v, F, G)` donde $v \in F^{|G|}$, es decir, v es el vector de coordenadas de un elemento $v' \in FG$ con respecto a G, la función `grtraduction(v, F, G)` retorna la matriz $[r_{v'}]_G$.

```
def grtraduction(v, F, G):
    w=vector(F,v)
    c=matrix.zero(F, w.length())
    u=rbasisrep(F,G)
    for j in range(w.length()):
        c=c+w[j]*u[j]

    return c
```

`grtraduction(v, F, G)` fue utilizada en la elaboración de los Ejemplos 2.1.8, 2.1.9, 2.2.3, y 4.1.3, para el cálculo de $m_b(x)$ y el cálculo de $dim(Rb)$ como el rango de $[r_b]_G$.

5.4. Funciones Python usadas en los Ejemplos 3.2.6 y 3.2.7.

En esta sección presentamos las funciones Python utilizadas para elaborar los ejemplos 3.2.6 y 3.2.7. Dichas funciones solo pueden ser aplicadas para grupos abelianos y se se hicieron con el propósito de obtener, para cualquier $b \in R$, la matriz de $[r_b]_G$, donde el grupo G es un grupo abeliano con un orden (como base del álgebra de grupo) prefijado por nosotros. En estas podemos determinar el orden del grupo G, lo cual no se podía hacer con las funciones Python presentadas en la sección anterior. El poder controlar el orden de G es indispensable para poder aplicar el Teorema 3.2.2, pues si G tiene el orden de β inducido por χ, entonces ${}_\beta[\chi]_G = Id$, implicando que los vectores de coordenadas de los idempotentes primitivos de T con respecto a β sean los mismos que los de los idempotentes primitivos de FG con respecto a G.

Sea G es abeliano y $G = C_{n_1} \times ... \times C_{n_s}$ una descomposición en grupos cílicos, donde $C_{n_i} = \langle x_i \rangle$ para todo i. Es un ejercicio sencillo ver que

$$\begin{array}{rccc} \phi: & FG & \longrightarrow & \dfrac{F[x_1,...,x_r]}{\langle x_1^{n_1}-1,...,x_r^{n_r}-1\rangle} \\ & \prod_{i=1}^r g_i^{e_i} & \longmapsto & \prod_{i=1}^r x_i^{e_i}, \end{array}$$

es un isomorfismo de F-algebras. Usando este hecho definiremos funciones Python en el anillo cociente. Por ejemplo, para crear $\mathbf{F}_3(C_2 \times C_2 \times C_2)$, se ejecutó el siguiente código en una hoja de trabajo de SageMath.

```
F=GF(3); P.<r,s,t> = PolynomialRing(F, 3);
 R.<x,y,z> = QuotientRing(P, P.ideal([r^2 - 1, s^2 - 1, t^2 -1]))
```

de esta manera los monomios del anillo cociente R se interpretan como elementos de G. Luego para organizar estos elementos (con orden monomial con $y < x$) se uso el siguiente algoritmo

```
b=[]
for i in range(2):
    for j in range(2):
        for k in range(2):
            b.append(x^i*y^j*z^k)
print(b)
```

Dada una tupla `(g,M,F)` donde g es un elemento de G, M es una lista ordenada de monomios (con un orden fijado, por ejemplo, un orden lexicográfico) cuyos elementos son los elementos de $\phi(G)$, la función `arrep(g,M,F)` retorna la matriz $[r_g]_M$.

```
def arrep(g,M,F):
    l1=[]
    for i in M:
        l2=[]
        for j in M:
            if i*g==j:
                l2.append(1)
            else:
                l2.append(0)
        l1.append(l2)
    return Matrix(F,l1).transpose()
```

Dada una tupla `(M, F)`, la función `arbasisrep(M,F)` retorna la colección $\{[r_g]_M : g \in M\}$.

```
def arbasisrep(M, F):
    c=[]
    for i in M:
        c.append(grrep(i,M,F))
    return c
```

Dada un tupla `(v, M, F)` donde $v \in F^{|G|}$, es decir, v es el vector de coordenadas de un elemento $v' \in FG$ con respecto a la base ordenada M (que es G como conjunto), la función `artraduction(v, M, F)` retorna la matriz $[r_{v'}]_M$.

```
def artraduction(v, M, F):
    w=vector(F,v)
    c=matrix.zero(F, w.length())
    u=grbasisrep(M, F)
    for j in range(w.length()):
        c=c+w[j]*u[j]
    return c
```

`artraduction(v, M, F)` fue utilizada en la elaboración de los Ejemplos 3.2.6 y 3.2.7 para el cálculo de la matriz $[r_{f_i}]_G$ a la que luego se le aplicaron las funciones **`rank(_)`** y **`codes.LinearCode(_).minimum_distance()`** de SageMath.

Bibliografía

[1] S. Axler: *Linear Algebra Done Right*. Springer-Verlag New York Berlin Heidelberg, 1997.

[2] S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis. J. Eur. Math. Soc., **14** (2012), 733–748.

[3] S. D. Berman, On the theory of group codes. Kibernetika, **3**(1) (1967), 31-39.

[4] S. D. Berman, Semisimple cyclic and abelian codes. Kibernetika, **3**(3) (1967), 21-30.

[5] F. Bernherdt, P. Landrock, O. Manz, The Extended Golay Codes Considered as Ideal. Journal of Combinatorial Theory, Series A **55** (1990), 235-246.

[6] M. Borello, J. de la Cruz and W. Willems, On checkable codes in group algebras. arXiv: 1901.10979, 2019.

[7] M. Borello, A. Jamous, Dihedral codes with prescribed minimum distance. arXiv:2003.11125, 2020.

[8] I.F. Blake, R.C. Mullin: *An Introduction to Algebraic and Combinatorial Coding Theory*. Academic Press, 1976.

[9] P. Camion, Abelian codes Univ. of Wisconsin, MRC Tech. Sum., Madison, Wisconsin, USA, Rep. 1059 (1970).

[10] Chabanne H., Gröbner Bases and Abelian Codes. In: Camion P., Charpin P., Harari S. (eds) Eurocode '92. International Centre for Mechanical Sciences (Courses and Lectures), **339** (1993). Springer, Vienna. https://doi.org/10.1007/978-3-7091-2786-5_21.

[11] D. J. Costello, J. Hagenauer, H. Imai, S. B. Wicker, Applications of Error Control Coding. IEEE Transactions on Information Theory, **44** (1998), 2531-2560.

[12] C. W. Curtis, I. Reiner: *Methods of representation theory with applications to finite groups and orders*. vol. 1. John Wiley and Sons, 1981.

[13] J. De la Cruz, W. Willems, On group codes with complementary duals. Des. Codes Cryptogr., **86** (2018), 2065–2073.

[14] C. Ding, D. R. Kohel, S. Ling, Split group codes. IEEE Transactions on Information Theory, **46**(2) (2000), 485-495.

[15] L. Dornhoff: *Group Representation Theory*, Part *A*. M. Dekker, New York, 1971.

[16] I. Dumer, D. Micciancio, M. Sudan, Hardness of Approximating the Minimum Distance of a Linear Code. IEEE Transactions on Information Theory, **49**(1) (2003), 22-37.

[17] F. S. Dutra, R. Ferraz, C. Polcino, Semisimple group codes and dihedral codes, Algebra and Discrete Mathematics, **3** (2009), 28-48.

[18] M. Elia, E. Gorla, Computing the dimension of ideals in group algebras, with an application to coding theory, JP Journal of Algebra, Number Theory and Applications, **45**(1) (2020), 13-28. https://www.doi.org/10.17654/NT045010013.

[19] R. Ferraz, Simple components of the center of $FG/J(FG)$, Communications in Algebra, **36** (2008), 3191-3199.

[20] R. Ferraz, Simple components and central units in group algebras, Journal of Algebra, **279** (2004), 191-203.

[21] R. Ferraz, M. Guerreiro, and C. Polcino, G-equivalence in group algebras and minimal abelian codes, IEEE Transactions on Information Theory, **60** (2013), 252-26.

[22] E. J. García-Claro, H. Tapia-Recillas, On the dimension of ideals in group algebras, and group codes. Published Online in Journal of Algebra and Its Applications on 7 November 2020.

[23] M. Grassl, Bounds on the minimum distance of linear codes. Online http://www.codetables.de.

[24] S. Jitman, S. Ling, H. Liu and X. Xie, Checkable codes from group rings. arXiv: 1012.5498v1, 2010.

[25] S. Jitman, S. Ling, H. Liu and X. Xie, Abelian codes in principal ideal group algebras, IEEE Transactions on Information Theory, **59** (2013), 3046-3058.

[26] K. Hoffman, R. Kunze: *Linear algebra* (second edition). Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1971.

[27] W. C. Huffman, V. Pless: *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2003.

[28] B. Huppert, N. Blackburn: *Finite Groups II*. Springer, Berlin, 1982.

[29] J. D. Key, *Some error-correcting codes and their applications*. D. R. Shier and K. T. Wallenius, Chapman & Hall/ CRC press, Boca Raton, FL., 1999.

[30] W. Kositwattanarerk, S. S. Ong, F. Oggier. Construction A of Lattices Over Number Fields and Block Fading (Wiretap) Coding. IEEE Transactions on Information Theory, **61**(5) (2015), 2273-2282.

[31] P. Landrock, O. Manz, Classical codes as ideals in group algebras. Des., Codes and Cryptogr., **2** (1992), 273–285.

[32] F.J. MacWilliams, Binary Codes Which Are Ideals in the Group Algebra of an Abelian Group. Bell System Technical Journal, **49** (1970), 987-1011.

[33] F. J. MacWilliams and N. J. A. Sloane: *The Theory of Error-Correcting Codes*. NorthHolland, 1977.

[34] N. M. Nikityuk, The method of symdrome decoding and its applications for data compresion and processing in high energy physics experiments. LNCS, **357** (1988), 324-335.

[35] D. S. Passman: *The algebraic structure of group rings*. John Wiley and Sons, 1997.

[36] C. Polcino and S. K. Sehgal: *An Introduction to Group Rings*. Kluwer academic publishers, 2002.

[37] C. Rentería, Códigos Geométricos y Códigos Asociados a Gráficas. Tesis Doctoral. UAM-I, 1994.

[38] C. Rentería, and H. Tapia-Recillas. H. Reed-Muller Codes: An Ideal Theory Approach. Communications in Algebra 25 (1997) 401-413.

[39] R. M. Roth, G. Seroussi, On Cyclic MDS Codes of Length q Over $GF(q)$, IEEE Transactions on Information Theory, **39**(2) (1986), 284-285.

[40] K. A. Schouhamer, P. H. Siegel, J. K. Wolf, Codes for Digital Recorders. IEEE Transactions on Information Theory, **44** (1998), 2260-2299.

[41] C. Shannon, A mathematical theory of communication, Bell System Tech. J., **27** (1948), 379–423 and 623–656.

[42] W. A. Stein et al. Sage Mathematics Software (Version 7.0), The Sage Development Team, 2016, http://www.sagemath.org.

[43] V.D. Tonchev, Combinatorial Configurations: Designs, Codes, Graphs. Pitman Monographs and Surveys in Pure and Applied Mathematics 40. Longman Scientific & Technical, 1988.

[44] J.H. van Lint and G. van der Geer: *Introduction to Coding Theory and Algebraic Geometry*. Birkhauser, DMV Seminar Band 12, 1988.

[45] A. Vardy, The Intractability of Computing the Minimum Distance of a Code. IEEE Transactions on Information Theory, **43**(6) (1997), 1757-1766.

[46] S.B. Wicker, Deep Space Applications. Chapter 25 of: *Handbook of Coding Theory*. Edited by V. S. Pless and W. C. Huffman. Elsevier Science, 1998.

[47] J. Wolfmann, A new construction of the binary Golay code (24,12,8) using a group algebra over a finite field. Discrete Mathematics, **31** (1980), 337-338.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE DISERTACIÓN PÚBLICA

No. 00073
Matrícula: 2151801064

Dimensión de ideales en álgebras de grupo, y códigos de grupo

Con base en la Legislación de la Universidad Autónoma Metropolitana, en la Ciudad de México se presentaron a las 10:00 horas del día 17 del mes de diciembre del año 2020 POR VÍA REMOTA ELECTRÓNICA, los suscritos miembros del jurado designado por la Comisión del Posgrado:

DR. HORACIO TAPIA RECILLAS
DR. ROGELIO FERNANDEZ ALONSO GONZALEZ
DR. JUAN JACOBO SIMON PINERO
DR. ALBERTO GERARDO RAGGI CARDENAS
DR. FELIPE DE JESUS ZALDIVAR CRUZ

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron a la presentación de la Disertación Pública cuya denominación aparece al margen, para la obtención del grado de:

DOCTOR EN CIENCIAS (MATEMATICAS)

DE: ELIAS JAVIER GARCIA CLARO

y de acuerdo con el artículo 78 fracción IV del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

APROBAR

Acto continuo, el presidente del jurado comunicó al interesado el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

UNIVERSIDAD AUTONOMA METROPOLITANA
Casa abierta al tiempo
DIRECCION DE SISTEMAS ESCOLARES

Elías García Claro

ELIAS JAVIER GARCIA CLARO
ALUMNO

REVISÓ

MTRA. ROSALIA SERRANO DE LA PAZ
DIRECTORA DE SISTEMAS ESCOLARES

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JESUS ALBERTO OCHOA TAPIA

PRESIDENTE

T. Recillas H.

DR. HORACIO TAPIA RECILLAS

VOCAL

R. Fernández A.

DR. ROGELIO FERNANDEZ ALONSO GONZALEZ

VOCAL

DR. JUAN JACOBO SIMON PINERO

VOCAL

DR. ALBERTO GERARDO RAGGI CARDENAS

SECRETARIO

DR. FELIPE DE JESUS ZALDIVAR CRUZ

El presente documento cuenta con la firma –autógrafa, escaneada o digital, según corresponda- del funcionario universitario competente, que certifica que las firmas que aparecen en esta acta – Temporal, digital o dictamen- son auténticas y las mismas que usan los c.c. profesores mencionados en ella