CÓDIGOS USANDO DIVISORES DE CERO Y UNIDADES EN ANILLOS DE GRUPO

Autor
OSCAR ANDRÉS SUÁREZ PORRAS

Trabajo de grado como requisito
parcial para optar al título de
Matemático

Director
Alexander Holguín Villa
Doctor en Matemáticas

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Matemáticas
Bucaramanga
2018

Agradecimientos

En primer lugar agradezco a Dios por acompañarme, bendecirme, iluminarme y darme la sabiduría para afrontar todo lo vivido, especialmente este tiempo en la UIS estudiando la carrera de Matemáticas.

Especial y gran agradecimiento a mis padres, Benjamín Suárez Rodríguez y Yaneth Porras Barajas, quienes con gran sacrificio me han dado lo necesario siempre, han formado un excelente hogar y junto a mi hermano Edson Jair Suárez Porras han estado siempre a mi lado aconsejándome, guiándome y brindándome todo su apoyo. Este trabajo es dedicado a ustedes.

A todos los profesores de la escuela de Matemáticas a quienes debo el haberme formado como un excelente profesional, en especial al profesor Alex Holguín, quien fue mi director de esta tesis, por el tiempo que ha dedicado para con su sabiduría ayudarme a comprender mejor los resultados aquí exhibidos. A mis profesores de colegio quienes ayudaron en mi formación y me dieron las bases para poder llegar hasta aquí, en especial a la profesora de algebra del I.T.S. Dámaso Zapata, Elizabeth Prada, gracias por su manera de enseñar que me dio el gusto por la matemática.

A todos mis familiares (abuelitos, tíos, tías, primos y primas) quienes en tiempos difíciles siempre me han ayudado de una u otra manera, lo que me ha dado ánimo para seguir adelante. A Lizeth Soler quien ha estado a mi lado apoyándome y ayudándome durante esta etapa de la carrera y mi vida, a seguir adelante y trazarme nuevas metas para ser una mejor persona.

A mis amigos Carlos Carrillo con quien he compartido desde niño, Catalina Rincón una excelente amiga con quien he compartido mucho desde el colegio, a Yesid Suarez, Tatiana Porras, Karen Lozada, Eliana Pulido y Marcela Peña con quienes comenzamos esta carrera y aunque no todos siguieron aún seguimos compartiendo muchos momentos. Y a todos los demás amigos y compañeros de estudio con quienes he compartido.

Por ultimo a todos los compañeros y entrenadores que he tenido en mi vida deportiva, la cual es otra parte importante en mi vida personal y profesional, y me ha ensañado a dar siempre todo por lo que se quiere y nunca darse por vencido, a la Selección de Futbol Sala UIS, por muchos buenos momentos que he pasado allí, en especial al profesor

Rene Rincón por enseñarme lo que es el futbol sala, al entrenador de porteros Miller Barrera por ayudarme a mejorar mucho en mi posición, y al profesor Javier Isidro Díaz por enseñarme muchas cosas no solo para aplicar al deporte si no a la vida, por ser un amigo más, y por ayudarme, aconsejarme, apoyarme y creer en mí.

Mi más profundo respeto y una completa gratitud para cada uno de ustedes.

Índice general

Resumen

TITULO: CÓDIGOS USANDO DIVISORES DE CERO Y UNIDADES EN ANILLOS DE GRUPO.[1]

AUTOR: Oscar Andrés Suárez Porras.[2]

PALABRAS CLAVE: Anillos de grupos, códigos, submódulos, códigos divisores de cero, códigos derivados de unidad, auto-dual.

DESCRIPCIÓN

Estudiaremos la construcción de códigos a través de codificaciones de anillos de grupo (RG), usando un submódulo W de RG; los cuales consisten principalmente en dos tipos: códigos divisores de cero y derivados de unidad.

En el capítulo 1 serán mostrados algunas definiciones básicas y resultados obtenidos de la teoría de grupos, anillos y álgebras de grupo, necesarios.

En el capítulo 2 mostraremos la estructura de los anillos de grupo, y veremos que un anillo de grupo RG es isomorfo a un determinado anillo de matrices de $n \times n$ sobre R, que notaremos por $\mathcal{M}_{RG}(R)$, así, cada elemento en RG tiene exactamente una matriz asociada llamada RG-matriz, esto nos facilitara la demostración de teoremas, corolarios y lemas aquí mencionados.

Finalmente en los capítulos 3 y 4 mostraremos la forma de los códigos divisores de cero y derivados de unidad. Estableceremos en primer lugar, la dimensión de los códigos divisores de cero y derivados de unidad, que dependerá del submódulo W usado en la codificación, el cual en el caso de los códigos divisores de cero tendrá alguna restricción. Por otra parte, la forma usual del código dual para los códigos ya mencionados. Y por último, las condiciones para que los códigos divisores de cero y derivados de unidad sean auto-duales.

[1] Tesis.

[2] FACULTAD DE CIENCIAS, ESCUELA DE MATEMÁTICAS.
DIRECTOR Dr. Alexander Holguín Villa.

Abstract

TITLE: CODES USING ZERO DIVISORS AND UNITS IN GROUP RINGS.[3]

AUTHOR: Oscar Andrés Suárez Porras.[4]

KEY WORDS: Group rings, codes, submodules, zero-divisor codes, unit-derived codes, self-dual.

DESCRIPTION

We would study the construction of codes through encodings from group rings (RG), using a submodule W of RG; which consists mainly of two types: zero-divisor and unit-derived codes.

In chapter 1 were presented, some basic definitions and results of the theory of groups, rings and group algebras, necessary.

In chapter 2 we would show the structure of the group rings, and we would see that a group ring RG is isomorphic to a certain ring of $n \times n$ matrices on R, that we denote by $\mathcal{M}_{RG}(R)$, thus, each element in RG has a unique associated matrix called RG-matrix, this will facilitate us the proof of theorems, corollaries and lemmas mentioned here.

Finally, in chapters 3 and 4 we will show the form of the zero-divisor codes and unit-derived codes. We would first establish, the dimension of the zero-divisor and unit-derived codes, which would depend on the submodule W used in the encoding, which in the case of the zero-divisor codes will have some restrictions. Otherwise, the usual form of dual code for mentioned codes. And finally, the conditions for the zero-divisor and unit-derived codes are self-dual.

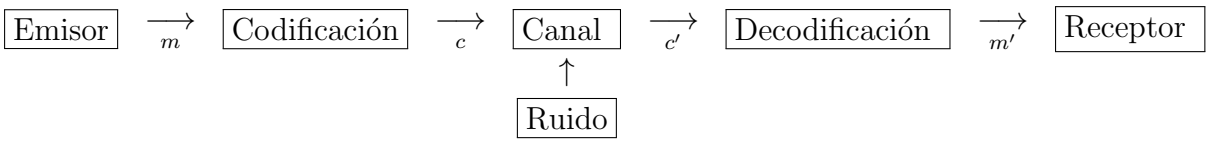
[3]Thesis.

[4]FACULTY OF SCIENCES, SCHOOL OF MATHEMATICS.
DIRECTOR Dr. Alexander Holguín Villa.

Introducción

Una de las áreas de aplicación del álgebra, bastante activa en la actualidad, es la Teoría de Códigos, la cual es una especialidad de la matemática que trata las leyes de la codificación de la información, que se centra principalmente en la construcción de códigos que tengan la capacidad de manejar un alto volumen de información y al tiempo la mayor veracidad posible, esta última parte hace referencia a la capacidad de detectar y corregir errores en un mensaje que ha sido alterado por efectos del ruido.

Veamos brevemente el proceso de un mensaje enviado y recibido. Supongamos que enviamos un mensaje, esto lo hacemos por un *canal de comunicación*, cuyas características dependen de la naturaleza del mensaje a ser enviado (sonido, imagen, datos). En general hay que hacer una *traducción* entre el mensaje original (o *palabra fuente*) m y el tipo de mensaje c que el canal está capacitado para enviar (*palabras código*). Este proceso se llama *codificación*. Cuando se ha codificado el mensaje, éste es llevado a través del canal hasta el punto donde es recibido por el *receptor* en los mismos términos que maneja el canal. Luego de esto, es necesario otro proceso, conocido como *decodificación*, debido a dos razones, la primera, para lograr que el mensaje sea entendido por el receptor en los términos que él es capaz de interpretar, y la segunda, para determinar, y en lo posible corregir, si ha habido algún tipo de error al interior del mensaje, debido al ruido e interferencias que se presentan durante este proceso, esto se ve resumido en el siguiente diagrama:



El presente trabajo está enfocado en códigos desde codificaciones en los anillos de grupo, ello amplía el espacio de códigos posibles y además ofrece un abordaje sencillo e intuitivo, debido principalmente a la fuerte conexión entre anillos de grupo y matrices. Hasta la fecha, el uso de los anillos de grupo para la construcción de códigos ha estado relacionado con los ideales contenidos en ellos. Como los códigos cíclicos son ideales en el anillo de grupo sobre cierto grupo cíclico, esto llevó a considerar la generalización natural de los códigos cíclicos como ideales (ver [10]). De hecho, se ha definido un código de anillo de grupo (ver [5]) como un ideal en un anillo de grupo.

Los códigos desde codificaciones de anillos de grupo presentados aquí y basados en el trabajo "Codes from zero-divisors and units in group rings" son submódulos en el anillo de grupo y sólo en ciertos casos restrictivos son ideales. De hecho, los códigos derivados de unidad nunca son ideales. Los métodos para obtener matrices generadoras y de verificación se aplican en los códigos mencionados. Además, como veremos algunas propiedades del código se pueden expresar más fácilmente en términos de propiedades del anillo de grupo.

Ahora bien, se presentaran técnicas para la construcción de códigos a partir de codificaciones de módulos en anillos de grupo, los cuales consisten principalmente en dos tipos: códigos divisores de cero (zero-divisor codes) y códigos derivados de unidad (unit-derived codes). Se podrán establecer las condiciones generales para que uno de estos códigos sea un ideal, y además, los códigos derivados de unidad que como ya indicamos, a diferencia de los códigos de anillos de grupo, nunca son ideales.

La única restricción para el anillo R en el anillo de grupo RG es que haya un divisor de cero o una unidad dentro de él. Centrándonos en los códigos divisores de cero de anillos de grupo en grupos cíclicos, que son ideales, obtenemos los códigos cíclicos o polinomiales. Como no estamos restringidos a ideales, incluso en el anillo de grupo de un grupo cíclico, los códigos divisores de cero pueden definir códigos distintos de los llamados cíclicos. También se presentaran las condiciones restrictivas en general para que uno de estos códigos sea un ideal en el anillo de grupo.

A partir de un isomorfismo entre el anillo de grupo RG y cierto anillo de matrices, llamadas RG matrices, se probaran algunas propiedades que nos permitirán obtener las matrices generadora y de verificación para los códigos divisores de cero y derivados de unidad.

El trabajo está estructurado de la siguiente manera, en el primer capítulo serán mostrados algunas definiciones básicas y resultados obtenidos de la teoría de grupos, anillos y álgebras de grupo, necesarios.

En el segundo capítulo mostraremos primeramente la estructura de los anillos de grupo, seguido del isomorfismo del anillo de grupo con el anillo de RG-matrices, finalmente veremos la definición de una codificación de anillo de grupo y la forma estándar de los códigos divisores de cero y derivados de unidad que se presentaran en los siguientes capítulos.

En el tercer capítulo mostraremos los códigos divisores de cero, primeramente veremos algunas definiciones importantes y ejemplos básicos, seguidamente se define la independencia lineal, del conjunto $S\mathbf{u}$, con $S \subset G$ y $\mathbf{u}$ el divisor de cero, y de las filas (o columnas) de la RG-matriz U, y la relación entre ambas, luego veremos las condiciones de verificación para los códigos divisores de cero, finalmente se presentara la forma estándar de los códigos dual y auto-dual de un código divisor de cero, y algunos ejemplos.

En el cuarto y último capítulo presentamos los códigos derivados de unidad, primeramente veremos su forma estándar y la equivalencia con un código llamado el código matricial generado, seguidamente se presentaran una forma de las matrices generadora y de verificación para los códigos derivados de unidad, luego se verá mejor la construcción de ellos y se presentaran algunos ejemplos, finalmente se presentara la forma estándar de los códigos dual y auto-dual de un código derivado de unidad.

Capítulo 1

Preliminares

El objetivo principal de este capítulo es presentar algunas definiciones básicas y algunos resultados obtenidos de la teoría de grupos, anillos y álgebras de grupo, necesarios para el desarrollo de esta monografía.

1.1 Teoría de grupos

Definición 1.1. *Una* ***operación binaria****, denotada por* $*$*, sobre un conjunto* G*, es una función que asigna a cada par de elementos de* G *un único elemento de* G*, es decir, si* $a, b \in G$ *entonces* $a * b \in G$*.*

Definición 1.2. *Un* ***Grupo*** *es un conjunto no vacío* G *junto con una operación binaria (denotada por* $*$*) tal que, para todos* $a, b, c, \in G$ *se tienen las siguientes propiedades:*

i) $a * (b * c) = (a * b) * c$ ***(Asociativa)****.*

ii) Existe un elemento que denotaremos por $e \in G$*, tal que* $a * e = e * a = a$ ***(Existencia de neutro)****.*

iii) Para cada elemento $a \in G$ *existe un elemento, que denotaremos por* $a^{-1} \in G$*, tal que* $a * a^{-1} = a^{-1} * a = 1$ ***(Existencia de inverso)****.*

Si además para todos $a, b \in G$ *se satisface la siguiente propiedad*

$$a * b = b * a,$$

el grupo G *es llamado* ***abeliano****.*

Definición 1.3. *Un grupo* G *es llamado* ***cíclico*** *si* $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$*, para algún* $a \in G$*. Por lo tanto, si* $b \in G$*, entonces* $b = a^k$*, para algún* $k \in \mathbb{Z}$*.*

1.2 Teoría de anillos

Definición 1.4. *Un **anillo** es un conjunto R junto con dos operaciones binarias denotadas por $+$ y $*$, llamadas suma y producto respectivamente, tal que para todos $a, b, c \in R$, se cumplen las siguientes propiedades:*

i) $(R, +)$ *es un grupo abeliano.*

ii) $a * (b * c) = (a * b) * c$ *(Asociatividad del producto).*

iii) $a * (b + c) = a * b + a * c$ *y* $(a + b) * c = a * c + a * b$ *(Ditributividad del producto respecto a la suma).*

Si además el producto verifica, $a*b = b*a$, para todos $a, b \in R$ entonces R es llamado anillo **conmutativo**.

En adelante denotamos el producto de a y b, $a * b$, simplemente por ab.

Un anillo R con un elemento $1_R = 1 \neq 0$ tal que $1a = a1 = a$, para todo $a \in R$, es llamado **anillo con identidad**.

Debido al tipo de códigos que son construidos en, [6], se necesitan los siguientes conceptos:

Definición 1.5. *En un anillo R un elemento z diferente de cero es un **divisor de cero** si y sólo si existe $r \in R$ diferente de cero tal que $zr = 0$. Al conjunto de los divisores de cero lo denotaremos por $\mathcal{ZD}(R)$.*

Un anillo R sin divisores de cero es llamado un **dominio**. Si además R tiene $1_R = 1$ y es conmutativo, se le llama **dominio entero**.

Sea R un anillo con identidad 1. Un elemento $u \in R$ es una **unidad** si y sólo si tiene inverso multiplicativo, es decir, si y sólo si existe $v \in R$ tal que $uv = vu = 1$. En este caso, v es único y se denota por u^{-1}.

Al conjunto de las unidades o elementos invertibles de R, se le denota por $\mathcal{U}(R)$, es decir,

$$\mathcal{U}(R) = \{a \in R : \exists a^{-1} \in R, aa^{-1} = a^{-1}a = 1\}.$$

Si $u \in \mathcal{U}(R)$ y si $v \in R$ es tal que $uv = 0$, entonces $v = 0$, es decir, unidades no pueden ser divisores de cero.

Un anillo D con identidad donde todo elemento distinto de cero es invertible y por tanto una unidad, se le llama **anillo con división**. En este último caso, si D conmutativo es llamado **cuerpo**.

Así las cosas si $\mathbb{F}$ es un cuerpo, $\mathcal{U}(\mathbb{F}) = \mathbb{F} \setminus \{0\}$.

Definición 1.6. *Sea R un anillo:*

1. *Un subconjunto $S \subseteq R$ es llamado **subanillo**, si él mismo es un anillo al restringir las operaciones a S. Equivalentemente, $\emptyset \neq S \subseteq R$ es subanillo si y sólo si S es cerrado por diferencia y producto, es decir, si y sólo si, para todos $a, b \in S$*

$$(a - b) \in S \quad y \quad ab \in S.$$

En este caso se denota por $S \leq_{sub} R$, para indicar que S es subanillo de R.

2. *Un subanillo I del anillo R es llamado **ideal** (bilateral) si cumple las siguientes propiedades:*

   i) Si $x, y \in I$, entonces $x - y \in I$.

   ii) Si $x \in I$ y $a \in R$, entonces $ax, xa \in I$.

En el caso que en la condición *ii)* para $x \in I$ y $a \in R$ solo se verifique $ax \in I$ (respectivamente $xa \in I$), I es llamado ideal a izquierda (respectivamente ideal a derecha).

Denotaremos por $I \preceq_l R$, $I \preceq_r R$ o $I \preceq R$, para indicar que I es un ideal a izquierda (a derecha o ideal bilateral) de R.

Ejemplo 1.1.

1. *Dado un elemento a en un anillo R, los conjuntos de múltiplos a izquierda y a derecha de a, denotados respectivamente por*

$$Ra = \{xa : x \in R\} \quad y \quad aR = \{ax : x \in R\},$$

son ideales a izquierda y a derecha de R.

*En el caso de R ser un anillo conmutativo, $aR = Ra$, para todo $a \in R$ y denotamos tal conjunto común por $\langle a \rangle$, el cual es llamado **ideal principal generado** por a.* [1]

2. *Sean R un anillo y $a \in R$. Entonces el conjunto RaR de todas las sumas finitas de la forma $\sum_{i=1}^{n} x_i a y_i$, con $x_i, y_i \in R$ y $n \in \mathbb{Z}^+$, es un ideal.*

De la definición todo ideal $I \preceq R$, es un subanillo de R. Sin embargo, no todo subanillo de R es ideal. Por ejemplo $\mathbb{Z} \leq_{sub} \mathbb{Q}$. Además dados $n \in \mathbb{Z}$, $\frac{a}{b} \in \mathbb{Q}$ con a y b primos relativos y tal que b no es divisor de n, tenemos que $n\frac{a}{b} = \frac{na}{b} \notin \mathbb{Z}$, por lo tanto $\mathbb{Z} \not\preceq \mathbb{Q}$.

[1] Observe que si G es un grupo y $a \in G$, $\langle a \rangle$ es la notación clásica para indicar el subgrupo cíclico generado por a. Sin embargo, el significado pretendido siempre será claro por el contexto.

Definición 1.7. *Un dominio entero R es llamado* ***dominio de ideales principales (DIP)****, si todos sus ideales son principales, es decir, para todo $I \preceq R$, $I = \langle a \rangle$, para algún $a \in R$.*

Dado un ideal $I \preceq R$, el grupo cociente (aditivo) $R/I = \{r + I : r \in R\}$ tiene estructura de anillo, definiendo el producto de manera natural por

$$(s + I)(t + I) = st + I.$$

El anillo R/I es llamado **anillo cociente** de R por I.

A continuación introduciremos el concepto de homomorfismo de anillos, el cual es esencialmente el mismo como en el caso de los grupos, excepto que ahora dos operaciones son involucradas en la definición.

Definición 1.8. *Sean R y S anillos. Una aplicación $\phi : R \to S$ es llamada un* ***homomorfismo de anillos*** *si para todos $a, b \in R$ tenemos:*

$$\phi(a + b) = \phi(a) + \phi(b) \qquad y \qquad \phi(ab) = \phi(a)\phi(b),$$

es decir ϕ preserva las dos operaciones de anillo.

Note que

$$\phi(0) = \phi(0 + 0) = \phi(0) + \phi(0),$$

y así $\phi(0) = 0$. Además,

$$\phi(a) + \phi(-a) = \phi(a - a) = \phi(0) = 0,$$

es decir, $\phi(-a) = -\phi(a)$ (unicidad del inverso aditivo).

Sin embargo en general no es cierto que si R tiene $1_R = 1$ y S tiene $1_S = 1'$, entonces $\phi(1) = 1'$. Por ejemplo, consideremos R y S dados por:

$$R = M_2(\mathbb{Q}) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} : a_{ij} \in \mathbb{Q} \right\} \quad \text{y} \quad S = M_3(\mathbb{Q}) = \left\{ \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} : a_{ij} \in \mathbb{Q} \right\},$$

y definamos $\phi : R \to S$ por

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \overset{\phi}{\mapsto} \begin{bmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Es un ejercicio simple demostrar que ϕ es un homomorfismo de anillos. Además de la definición,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \overset{\phi}{\mapsto} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Existen condiciones bajo las cuales dado un homomorfismo de anillos $\phi : R \to S$, $\phi(1) = 1'$. Por ejemplo, si S es un dominio o si ϕ es sobreyectivo, la identidad es enviada en identidad.

En general, si $\phi : R \to S$ es un homomorfismo de anillos, los conjuntos:

$$Im(\phi) = \{y \in S : \exists x \in R, y = \phi(x)\} \quad \text{y} \quad Ker(\phi) = \{x \in R : \phi(x) = 0\},$$

son subanillo de S e ideal de R respectivamente.

Al igual que en el caso de grupos, se tienen tipos especiales de homomorfismos de anillos.

Definición 1.9. *Un homomorfismo de anillos $\phi : R \to S$ es llamado,*

1. ***Monomorfismo**, si ϕ es inyectivo, es decir, $\phi(x) = \phi(y)$ implica $x = y$, para todos $x, y \in R$. Es fácil demostrar que ϕ es monomorfismo si y sólo si $Ker(\phi) = \{0\}$.*
2. ***Epimorfismo**, si ϕ es sobreyectivo, es decir, $Im(\phi) = S$.*

Finalmente, si ϕ es al mismo tiempo monomorfismo y epimorfismo, ϕ es llamado un **isomorfismo**. En este último caso, decimos que R y S son isomorfos y escribimos $R \cong S$.

En el caso de tener un homomorfismo de un anillo sobre sí mismo, se le denomina **endomorfismo** y si este es isomorfismo, se le llama **automorfismo** de R.

1.3 Módulos y álgebras

Definición 1.10. *Sea R un anillo. Un grupo abeliano (aditivo) M es llamado un **R-módulo** a izquierda (o un **módulo** sobre R) si existe $\mu : R \times M \to M$, $(r, m) \mapsto rm$, tal que para todos $a, b \in R$; $m, m_1, m_2 \in M$, se verifican:*

i) $(a + b)m = am + bm$.

ii) $a(m_1 + m_2) = am_1 + am_2$.

iii) $a(bm) = (ab)m$.

iv) $1m = m$ *(caso* $1 \in R$*).*

Análogamente, se define un módulo a derecha o módulo-R. En adelante a menos que se indique lo contrario usaremos la expresión R-módulo (módulo-R) para referirnos a un R-módulo a izquierda (módulo-R a derecha).

Es claro de la definición, que si R es un cuerpo (denotado por $\mathbb{F}$), entonces el concepto de R-módulo coincide con la noción de R-espacio vectorial.

Definición 1.11. *Sea M un R-módulo. Un subconjunto no vacío $N \subseteq M$ es llamado un R-submódulo de M, si en N se cumplen las siguientes condiciones:*

i) Para todos $x, y \in N$, $x + y \in N$.

ii) Para todo $r \in R$ y todo $x \in N$, $rx \in N$.

En otras palabras, un subconjunto no vacío N de un R-módulo M es un submódulo, si él mismo es un módulo con las operaciones restrictas a él. Si N es un R-submódulo de M, escribimos $N \leq_R M$ o simplemente $N \leq M$ si es claro quién es el anillo R.

Ejemplo 1.2.

1. *Sea $I \preceq_l R$. Dado que el producto de elementos de R por elementos de I es un elemento de I, es decir, $RI \subset I$, entonces todo ideal a izquierda I de R puede verse como un R-módulo. En particular, R mismo es un ideal a izquierda y así, es un R-módulo.*

   Cuando consideremos un anillo dado R como un R-módulo o módulo-R, lo explicitaremos escribiendo ${}_RR$ y R_R respectivamente.

   Note que $\{0\}R = \{0r : r \in R\} = \{0\}$ y dado que $\{0\}$ es un grupo abeliano, entonces $\{0\}$ es un R-módulo.

   A los submódulos $\{0\}$ y R se les llama los submódulos triviales.

2. *Todo grupo abeliano G (aditivo) es un $\mathbb{Z}$-módulo, donde mg, con $g \in G$ y $m \in \mathbb{Z}$ está definido por:*

$$mg = \begin{cases} \underbrace{g + g + ... + g}_{m-veces}, & si \quad m > 0; \\ 0, & si \quad m = 0; \\ |m|\,(-g), & si \quad m < 0. \end{cases}$$

3. *Si I es ideal de R, entonces R/I es un R-módulo donde la acción es dada por:*

$$\begin{aligned} R \times R/I &\to R/I \\ (r, x + I) &\mapsto rx + I. \end{aligned}$$

4. *Si M es un R-módulo y $x \in M$, entonces el conjunto*

$$Rx = \langle x \rangle = \{rx | r \in R\},$$

   es un R-submódulo de M, dado que para todos $r_1, r_2 \in R$ tenemos

$$r_1x - r_2x = (r_1 - r_2)x \in \langle x \rangle, \quad y \quad r_1(r_2x) = (r_1r_2)x \in \langle x \rangle.$$

Definición 1.12. *Sea R un anillo conmutativo. Un R-módulo A es llamado un R-álgebra, si existe una multiplicación definida sobre A, tal que con la suma inicial en A y esta multiplicación, A es un anillo en el cual, para todo $r \in R$ y todos $a, b \in A$, se cumple la siguiente condición:*

$$r(ab) = (ra)b = a(rb). \tag{1.1}$$

Suponga que A visto como anillo tiene unidad 1_A. Entonces, para todo $r \in R$ y todo $a \in A$ (usando la condición (1.1))

$$ra = r(a1_A) = a(r1_A) = ar,$$

es decir,

$$R \cdot 1 \cong R \subseteq \zeta(A),$$

donde $\zeta(A) = \{x \in A : xa = ax, \forall a \in A\}$, denota el centro de A.

1.4 Anillos de grupo

Sean R un anillo con unidad 1_R y G un grupo multiplicativo no necesariamente finito, se denota por RG al conjunto de las sumas formales finitas $\mathbf{a} = \sum_{g \in G} \alpha_g g$, es decir,

$$RG = \left\{ \mathbf{a} = \sum_{g \in G} \alpha_g g : \alpha_g \in R, g \in G \right\},$$

donde $\alpha_g = 0$ casi siempre, esto es, solo un número finito de coeficientes son diferentes de cero en cada una de estas sumas.

Sean $\mathbf{a} = \sum_{g \in G} \alpha_g g$ y $\mathbf{b} = \sum_{h \in G} \beta_h h$ en RG. Se definen las siguientes operaciones :

Adición:

$$\mathbf{a} + \mathbf{b} = \sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g = \sum_{g \in G} (\alpha_g + \beta_g) g.$$

Multiplicación:

$$\mathbf{ab} = \left(\sum_{g \in G} \alpha_g g \right) \left(\sum_{h \in G} \beta_h h \right) = \sum_{g,h \in G} \alpha_g \beta_h gh.$$

Se puede verificar que RG con estas operaciones es un anillo con unidad $1 = \sum_{g \in G} \mu_g g$, donde el coeficiente correspondiente al neutro 1 del grupo es 1_R y, $\mu_g = 0$ para todo elemento $g \neq 1$ en G, llamado el **anillo de grupo** de G sobre R.

Además, para $\lambda \in R$ y $\mathbf{a} \in RG$ tenemos que el producto

$$(\lambda, \mathbf{a}) \mapsto \lambda \cdot \mathbf{a} = \lambda \cdot \left(\sum_{g \in G} \alpha_g g \right) = \sum_{g \in G} (\lambda \alpha_g) g,$$

da a RG estructura de R-módulo. En el caso cuando el anillo R es conmutativo, RG tiene estructura de R-álgebra y más aún, si $\mathbb{F}$ es un cuerpo $\mathbb{F}G$ es un $\mathbb{F}$-espacio vectorial.

Dado un elemento $\mathbf{a} = \sum_{g \in G} \alpha_g g \in RG$, se define el soporte de $\mathbf{a}$, denotado $Supp(\mathbf{a})$, a ser el subconjunto de G de los elementos que efectivamente aparecen en la expresión de $\mathbf{a}$, es decir,

$$Supp(\mathbf{a}) = \{g \in G : \alpha_g \neq 0\}.$$

Así las cosas, dados $\mathbf{a} = \sum_{g \in G} \alpha_g g$ y $\mathbf{b} = \sum_{g \in G} \beta_g g$ en RG se tiene de la definición de *soporte* que $\mathbf{a} = \mathbf{b}$ si y sólo si $\alpha_g = \beta_g$ para todo $g \in G$.

1.5 Códigos

Con el fin de entrar en contexto con los códigos, presentaremos algunas definiciones y resultados generales de la teoría.

Los elementos básicos para construir un código son:

Definición 1.13.

i) Un conjunto finito $\mathbf{A}$*, llamado* ***alfabeto****, donde* $\#(\mathbf{A}) = q$ *denota el número de elementos de* $\mathbf{A}$*, es decir,* $\mathbf{A} = \{a_1, a_2, ..., a_q\}$ *con* $a_i \neq a_j$*, para* $1 \leq i, j \leq q$*,* $i \neq j$*, en este caso llamamos al código q-ario.*

ii) Una n***-cadena*** *o* ***palabra de longitud*** n*,* $c = a_1 a_2 \dots a_n$*, sobre* $\mathbf{A}$*, es una sucesión de n símbolos de* $\mathbf{A}$*. Al conjunto de todas las n-cadenas de* $\mathbf{A}$ *la denotamos por* $\mathbf{A}^n$*. Por practicidad trabajaremos con códigos cuyas palabras tienen igual longitud n, que son llamados códigos de bloque.*

Con estos conceptos en mente, se puede definir un código.

Definición 1.14. *Un código q-ario* $\mathcal{C}$ *de longitud n es cualquier subconjunto de palabras de longitud n, es decir,*

$$\mathcal{C} \subset \underbrace{\mathbf{A} \times \mathbf{A} \times \cdots \times \mathbf{A}}_{n \text{ veces}} = \mathbf{A}^n.$$

Los elementos de $\mathcal{C}$ *se llaman* ***palabras código*** *(****codewords*** *en ingles).*

El número $M = |\mathcal{C}|$ de elementos del código $\mathcal{C}$ es llamado el tamaño del código, el cual también es un dato importante, dado que cuanto mayor sea M, mayor es la cantidad de información que puede ser transmitida. Así, a un código q-ario $\mathcal{C}$, de longitud n que tenga M palabras lo denotaremos por $(n, M)-$código q-ario.

Note que, si $\mathcal{C} \subset \mathbf{A}^n$, entonces todo elemento $c \in \mathcal{C}$ es de la forma $c = (a_1, a_2, \ldots, a_n)$, con $a_i \in \mathbf{A}$, $1 \leq i \leq n$. Sin embargo por practicidad y siempre que sea conveniente escribiremos c como una sucesión de los símbolos a_i's, es decir, $c = a_1 a_2 \ldots a_n$.

Debido a la riqueza de los cuerpos, es usual tomar como alfabeto $\mathbf{A}$ un cuerpo finito de q elementos, es decir, $\mathbf{A} = \mathbb{F}_q$, donde q es una potencia de un primo p. Así, cuando el alfabeto es $\mathbb{F}_2$, $\mathbb{F}_3$ ó $\mathbb{F}_4$, entonces $\mathcal{C}$ es un código *binario*, *ternario* o *cuaternario*, respectivamente.

Ejemplo 1.3.

1. $\mathcal{C}_1 = \{(0,0,0), (0,1,0), (0,0,1), (1,1,1)\}$ *sobre* $\mathbb{F}_2$ *es un* $(3,4)-$*código binario.*
2. $\mathcal{C}_2 = \{(3,0,0,2), (2,1,0,1), (3,0,2,1), (2,1,3,2), (1,2,3,3)\}$ *sobre* $\mathbb{F}_4$ *es un* $(4,5)-$*código cuaternario.*
3. *Dado un alfabeto* $\mathbf{A} = \{a_1, a_2, ..., a_q\}$*, el código:*

$$\mathcal{C}_3 = \{\underbrace{a_1 a_1 \ldots a_1}_{n \text{ veces}}, \underbrace{a_2 a_2 \ldots a_2}_{n \text{ veces}}, \ldots, \underbrace{a_q a_q \ldots a_q}_{n \text{ veces}}\}$$

es llamado ***código de repetición*** *q-ario, de longitud n.*

Las siguientes nociones son intuitivamente sencillas de comprender, y son fundamentales para entender el proceso de decodificación de mensajes.

Definición 1.15. *Sean x e y dos palabras de longitud n sobre el mismo alfabeto $\mathbf{A}$. La* ***distancia de Hamming*** *entre x e y, denotada por $d(x,y)$, se define como el número de componentes en que x e y difieren, es decir si $x = x_1 x_2 ... x_n$ y $y = y_1 y_2 ... y_n$, entonces*

$$d(x,y) = \#\{i : 1 \leq i \leq n, x_i \neq y_i\}.$$

Note que si comparamos la posición i de las palabras x e y:

$$d(x_i, y_i) = \begin{cases} 0, & si \quad x_i = y_i \\ 1, & si \quad x_i \neq y_i \end{cases},$$

entonces

$$d(x,y) = \sum_{i=1}^{n} d(x_i, y_i).$$

La siguiente proposición muestra que la función $d : \mathbf{A}^n \times \mathbf{A}^n \to \{0,1\}$ define una métrica sobre $\mathbf{A}^n$, y así $(\mathbf{A}^n, d)$ es un espacio métrico.

Proposición 1.1. *La función d define una métrica en $\mathbf{A}^n$, es decir, para todos $x, y, z \in \mathbf{A}^n$, las siguientes propiedades son válidas:*

$(P1)$ $d(x, y) \geq 0$.

$(P2)$ $d(x, y) = 0$ *si y sólo si* $x = y$.

$(P3)$ $d(x, y) = d(y, x)$.

$(P4)$ $d(x, y) \leq d(x, z) + d(z, y)$.

Demostración. $(P1), (P2)$ *y* $(P3)$ *son claras por la definición de distancia de Hamming, por tanto, falta solo demostrar* $(P4)$.

Sean

$$W = \{i : x_i = y_i\} \quad y \quad X = \{i : x_i = z_i \wedge z_i = y_i\}.$$

Claramente,

$$X \subseteq W \quad \textit{entonces} \quad W^c \subseteq X^c.$$

De esta manera,

$$d(x, y) = |W^c| \leq |X^c|,$$

donde,

$$\begin{aligned} X^c &= \{i : x_i \neq z_i \vee z_i \neq y_i\} \\ &= \underbrace{\{i : x_i \neq z_i\}}_{Y} \cup \underbrace{\{i : z_i \neq y_i\}}_{Z}, \end{aligned}$$

luego,

$$\begin{aligned} d(x, y) \leq |X^c| &= |Y| + |Z| - |Y \cap Z| \\ &= d(x, z) + d(z, y) - |Y \cap Z| \\ &\leq d(x, z) + d(z, y). \end{aligned}$$

Estrechamente relacionado con la distancia de Hamming, está el concepto de distancia mínima o distancia del código, la cual definimos a continuación.

Definición 1.16. *La* ***distancia mínima*** *de un código $\mathcal{C}$ con al menos dos palabras, denotada por $d(\mathcal{C})$ o $d_{\mathcal{C}}$, se define por:*

$$d(\mathcal{C}) = \textit{mín}\{d(x, y) : x, y \in \mathcal{C}; x \neq y\}.$$

De la definición, tanto la distancia de Hamming como la distancia mínima de un código $\mathcal{C}$, siempre son números enteros.

De esta manera, un código $\mathcal{C}$ de longitud n, tamaño M y distancia mínima d lo denotaremos por $(n, M, d)-$código q-ario.

A partir de la definición de distancia, es posible definir otro importante parámetro en el trabajo de codificación y decodificación de la información, éste es el **peso** y se aplica sobre códigos que tienen como alfabeto un cuerpo finito $\mathbb{F}_q$.

Definición 1.17. *Sea x una palabra en $\mathbb{F}_q^n$, el peso de x, denotado por $wt(x)$, se define como el número de coordenadas no nulas en x, es decir:*

$$wt(x) = d(x; \mathbf{0});$$

donde $\mathbf{0} = \underbrace{00\ldots0}_{n \text{ veces}}$ es la palabra cero del código.

Definición 1.18. *Sea $\mathcal{C}$ un código. El **peso mínimo** (de Hamming) de $\mathcal{C}$, denotado por $wt(\mathcal{C})$ es el mínimo de los pesos de las palabras no nulas de $\mathcal{C}$, es decir:*

$$wt(\mathcal{C}) = mín\{wt(c) : c \in \mathcal{C}; c \neq 0\}.$$

Un $(n, M, d, w)-$código es un código $\mathcal{C} \subset \mathbf{A}^n$, $|\mathcal{C}| = M$, distancia mínima d y peso mínimo w.

Ejemplo 1.4.
Sea $\mathcal{C} = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9\} = \{000000, 011011, 101010, 000111, 100011, 110000, 001001, 010101, 010110\}$ un código sobre $\mathbb{F}_2^6$.

Para $x_2, x_3, x_4, x_8 \in \mathcal{C}$ tenemos que las distancias vienen dadas por:

i) $d(x_2, x_3) = d(011011, 101010) = 3$,
ii) $d(x_2, x_4) = d(011011, 000111) = 3$,
iii) $d(x_2, x_8) = d(011011, 010101) = 3$,
iv) $d(x_3, x_4) = d(101010, 000111) = 4$,
v) $d(x_3, x_8) = d(101010, 010101) = 6$,
vi) $d(x_4, x_8) = d(000111, 010101) = 2$.

La lista completa de distancias viene dada por:

$$\begin{array}{llll}
d(0,x_2)=4, & d(x_2,x_4)=3, & d(x_3,x_7)=3, & d(x_5,x_7)=3,\\
d(0,x_3)=3, & d(x_2,x_5)=3, & d(x_3,x_8)=6, & d(x_5,x_8)=4,\\
d(0,x_4)=3, & d(x_2,x_6)=4, & d(x_3,x_9)=4, & d(x_5,x_9)=4,\\
d(0,x_5)=3, & d(x_2,x_7)=2, & d(x_4,x_5)=2, & d(x_6,x_7)=4,\\
d(0,x_6)=2, & d(x_2,x_8)=3, & d(x_4,x_6)=5, & d(x_6,x_8)=3,\\
d(0,x_7)=2, & d(x_2,x_9)=3, & d(x_4,x_7)=3, & d(x_6,x_9)=3,\\
d(0,x_8)=3, & d(x_3,x_4)=4, & d(x_4,x_8)=2, & d(x_7,x_8)=3,\\
d(0,x_8)=3, & d(x_3,x_5)=2, & d(x_4,x_9)=2, & d(x_7,x_9)=5,\\
d(x_2,x_3)=3, & d(x_3,x_6)=3, & d(x_5,x_6)=3, & d(x_8,x_9)=2.
\end{array}$$

Como se puede ver de lo anterior, el peso de cada palabra en $\mathcal{C}$ es

$$\begin{aligned} wt(x_2) &= 4, \quad & wt(x_3) &= 3, \\ wt(x_4) &= 3, \quad & wt(x_5) &= 3, \\ wt(x_6) &= 2, \quad & wt(x_7) &= 2, \\ wt(x_8) &= 3, \quad & wt(x_9) &= 3, \end{aligned}$$

y por lo tanto, la distancia mínima y el peso mínimo de $\mathcal{C}$ *son*

$$d(\mathcal{C}) = wt(\mathcal{C}) = 2.$$

1.6 Decodificación

A continuación presentaremos en que consiste el principio para hacer una decodificación.

Se llama decodificar al proceso de detectar y corregir los errores en un determinado código. Sea $\mathcal{C} \subset \mathbf{A}^n$ un código q-ario y supongamos que al transmitir la palabra código $c \in \mathcal{C}$, recibimos la palabra $x \notin \mathcal{C}$. ¿Cómo decodificamos x? Existen en la literatura varias estrategias para hacerlo y una de ellas es asignarle a x la palabra código c que sea más cercana. Es decir, si

$$d(x, c) = \min_{y \in \mathcal{C}} \quad d(x, y),$$

donde d es la distancia de Hamming, entonces decodificamos a x por c. A este método se le conoce como **decodificación por distancia mínima** (minimum distance decoding).

Si al transmitir una palabra código se cometen t errores, es decir, si la palabra enviada y la recibida difieren en exactamente t coordenadas, decimos que se cometió un **error de peso** t. Supongamos que $\mathcal{C} \subset \mathbf{A}^n$ es un código q-ario sobre $\mathbf{A}$. Si transmitimos $c \in \mathcal{C}$ y recibimos $x \in \mathbf{A}^n$ con $d(x, c) = t$, entonces existe $e \in \mathbf{A}^n$ tal que

$$x = c + e.$$

A la n palabra $e = x - c$ se le conoce con el nombre de **vector error**. Note que $w(e)$ coincide con el número de errores cometidos en la palabra recibida.

A continuación se describen las condiciones para que un código pueda detectar o corregir un determinado número de errores al trabajar con la decodificación por distancia mínima.

Definición 1.19. *(Detectar y Corregir errores)*

1. *Sea* s *un entero positivo. Diremos que un código* $\mathcal{C}$ ***detecta*** s ***errores*** *si cada vez que al enviar una palabra código se comete un error de peso* r, $1 \leq r \leq s$, *la palabra resultante no es una palabra código. Así, un código es* s*-detector si detecta* s *errores pero no detecta* $s + 1$ *errores (es decir, hay al menos un error de peso* $s + 1$ *que el código no detecta).*

2. *Sea t un entero positivo. Diremos que un código $\mathcal{C}$ es* ***corrector de t errores*** *si, al decodificar por distancia mínima, se pueden corregir todos los errores de peso t o menos. Así, un código es t-corrector si corrige t errores pero no corrige $(t+1)$-errores.*

Ejemplo 1.5.

1. *El código binario $\mathcal{C}_1 = \{00, 01, 10, 11\}$ formado por todas las palabras de longitud 2 no detecta ningún error, dado que si un error es cometido en cualquiera de sus palabras código, la palabra resultante es también una palabra código, veamos esto:*

$$\mathcal{C}_1 \ni c_1 = 00 \to \begin{cases} x_1 = 01 \in \mathcal{C}_1 \\ x_2 = 10 \in \mathcal{C}_1 \end{cases}, \quad \mathcal{C}_1 \ni c_2 = 01 \to \begin{cases} x_3 = 11 \in \mathcal{C}_1 \\ x_4 = 00 \in \mathcal{C}_1 \end{cases},$$

$$\mathcal{C}_1 \ni c_3 = 10 \to \begin{cases} x_5 = 11 \in \mathcal{C}_1 \\ x_6 = 00 \in \mathcal{C}_1 \end{cases}, \quad \mathcal{C}_1 \ni c_4 = 11 \to \begin{cases} x_7 = 01 \in \mathcal{C}_1 \\ x_8 = 10 \in \mathcal{C}_1 \end{cases}.$$

2. *Sea $\mathcal{C}_2 = \{000, 011, 101, 110\}$ el código binario obtenido del código $\mathcal{C}_1$ agregando un dígito de verificación, es decir, agregamos un dígito extra a cada palabra código de modo que la suma de los dígitos de cada palabra código sea par. Este es un código 1-detector como vemos a continuación:*

$$\mathcal{C}_2 \ni c_1 = 000 \to \begin{cases} x_1 = 001 \notin \mathcal{C}_2 \\ x_2 = 010 \notin \mathcal{C}_2 \\ x_3 = 100 \notin \mathcal{C}_2 \end{cases}, \quad \mathcal{C}_2 \ni c_2 = 011 \to \begin{cases} x_4 = 010 \notin \mathcal{C}_2 \\ x_5 = 001 \notin \mathcal{C}_2 \\ x_6 = 111 \notin \mathcal{C}_2 \end{cases},$$

$$\mathcal{C}_2 \ni c_3 = 110 \to \begin{cases} x_7 = 111 \notin \mathcal{C}_2 \\ x_8 = 100 \notin \mathcal{C}_2 \\ x_9 = 010 \notin \mathcal{C}_2 \end{cases}, \quad \mathcal{C}_2 \ni c_4 = 110 \to \begin{cases} x_{10} = 111 \notin \mathcal{C}_2 \\ x_{11} = 100 \notin \mathcal{C}_2, \\ x_{12} = 010 \notin \mathcal{C}_2 \end{cases}$$

pero no es 2-detector dado que si cometemos dos errores, por ejemplo, en $c_1 = 000$ obtendríamos $x = 011$, $y = 101$ o $z = 110$ y todas ellas son palabras código. Además, tampoco puede corregir un error, ya que si, por ejemplo, al enviar $c_3 = 101$ recibimos, la palabra $w = 111$, esta podría ser decodificada en las palabras código $c_2 = 011$, $c_3 = 101$ o $c_4 = 110$.

3. *Sea $\mathcal{C}_3 = \{000000, 000111, 111000, 111111\}$ el código binario obtenido nuevamente del código $\mathcal{C}_1$ repitiendo tres veces cada dígito de este último. Este es un código 2-detector y también 1-corrector. Ahora, si mandamos nuestro mensaje y se comete un error, cualquier palabra que nos llegue puede ser corregida. Por ejemplo, para* 000000

$$000000 \xrightarrow[+1\ error]{} \begin{Bmatrix} 100000 \\ 010000 \\ 001000 \\ 000100 \\ 000010 \\ 000001 \end{Bmatrix} \xrightarrow[corregir]{} 000000.$$

Visto desde el código $\mathcal{C}_1$ tenemos el siguiente esquema para la palabra código $c_1 = 00$:

$$00 \xrightarrow[codificamos]{} 000000 \xrightarrow[+1\ error]{} \left\{\begin{matrix}100000\\010000\\001000\\000100\\000010\\000001\end{matrix}\right\} \xrightarrow[corregir]{} 000000 \xrightarrow[decodificamos]{} 00.$$

Aquí, si enviamos 000000 *y recibimos* 000100 *no sólo detectamos el error sino que podemos corregirlo. Intuitivamente,* 000100 *está más cerca de* 000000 *que de* 000111, 111000 *ó* 111111. *Esto mismo lo podemos realizar para cualquier palabra código de $\mathcal{C}_3$.*

Por lo visto en los ejemplos, intuitivamente cuánto más separadas se encuentren las palabras código, más fácil será detectar o corregir errores. Más exactamente se tienen los siguientes resultados.

Teorema 1.1. *Sea $\mathcal{C} \subset \mathbf{A}^n$ un código con distancia mínima $d = d_{\mathcal{C}}$,*

1. *$\mathcal{C}$ es t-detector si y sólo si $d = t + 1$.*
2. *$\mathcal{C}$ es s-corrector si y sólo si $d = 2s + 1$ ó $d = 2s + 2$.*

Corolario 1.1.1. *Si un código $\mathcal{C}$ tiene distancia mínima $d = d_{\mathcal{C}}$, entonces $\mathcal{C}$ es $(d-1)$-detector y $\lfloor (d-1)/2 \rfloor$-corrector.*[2]

1.7 Códigos lineales y cíclicos

Para construir códigos de una manera eficiente introduciremos la definición de código lineal y código cíclico, estos últimos son un caso especial del primero, el trabajo de codificar y decodificar se ve ampliamente facilitado por el hecho de que su estructura se puede describir a partir de una matriz denominada *matriz generadora*, cuyas filas constituyen una base para el código. Por su parte, en el trabajo de decodificación, el determinar si una palabra recibida pertenece o no al código se logra llevar a cabo a partir de otra matriz denominada *matriz de verificación.*

Definición 1.20. *Un código $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ es llamado* ***código lineal*** *si es un subespacio vectorial de $\mathbb{F}_q^n$.*

[2]Sea $x \in \mathbb{R}$. Existe un único entero que representamos por $\lfloor x \rfloor$ que satisface la desigualdad

$$\lfloor x \rfloor \leq x \leq \lfloor x \rfloor + 1.$$

En otras palabras $\lfloor x \rfloor$ es el mayor entero menor o igual que x. Al entero $\lfloor x \rfloor$ lo llamaremos la **parte entera** de x.

Sea $\mathcal{C}$ un código lineal sobre $\mathbb{F}_q$, entonces:

1. El código dual de $\mathcal{C}$, denotado por $\mathcal{C}^\perp$ es el conjunto dado por

$$\mathcal{C}^\perp = \{v \in \mathbb{F}_q^n : v \cdot u = 0, \forall u \in \mathcal{C}\},$$

donde $v \cdot u = v_1u_1 + ... + v_nu_n$, denota el producto interno usual en $\mathbb{F}_q^n$.

2. La dimensión del código $\mathcal{C}$, es la dimensión de $\mathcal{C}$ como espacio vectorial sobre $\mathbb{F}_q$ y se denota con $dim_{\mathbb{F}}(\mathcal{C})$.

Un código lineal de dimensión k sobre $\mathbb{F}_q^n$ se dice que es un $[n, k]$-código lineal, si además tiene distancia mínima d, se denomina como un $[n, k, d]-$código lineal.

Ejemplo 1.6.

Los siguientes conjuntos son ejemplos de subespacios vectoriales sobre $\mathbb{F}_q$ y por lo tanto, de códigos lineales.

1. $\mathcal{C}_1 = \mathbb{F}_q^n$ *y* $\mathcal{C}_2 = \{\boldsymbol{0}\}$*, donde* $\boldsymbol{0}$ *es el vector nulo en* $\mathbb{F}_q^n$.
2. $\mathcal{C}_3 = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\} \subset \mathbb{F}_2^4$ *es un* $[4, 2, 2]$*-código lineal binario.*
3. $\mathcal{C}_4 = \{(0,0,0,0), (1,1,0,0), (2,2,0,0)\} \subset \mathbb{F}_3^4$ *es un* $[4, 1, 2]$*-código lineal ternario.*

Las siguientes propiedades son conocidas, para una prueba de ellas ver [8, pág. 45].

Teorema 1.2. *Sea $\mathcal{C}$ un código lineal de longitud n sobre $\mathbb{F}_q$, entonces:*

1. $|\mathcal{C}| = q^{dim(\mathcal{C})}$ *es decir,* $dim(\mathcal{C}) = log_q|\mathcal{C}|$.
2. $\mathcal{C}^\perp$ *es un código lineal y* $dim(\mathcal{C}) + dim(\mathcal{C}^\perp) = n$.
3. $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Definición 1.21. *Una* ***matriz generadora*** *para un código lineal $\mathcal{C}$ es una matriz L cuyas filas forman una base para $\mathcal{C}$.*

Definición 1.22. *Una* ***matriz de verificación*** *K para un código lineal $\mathcal{C}$ es una matriz generadora para el código dual $\mathcal{C}^\perp$.*

La matriz de verificación K de un código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ permite determinar si una palabra pertenece o no al código, dado que, para $x \in \mathbb{F}_q^n$, $x \in \mathcal{C}$ si y sólo si, $xK^T = 0$.

A continuación presentamos una clase de códigos lineales, los cuales sobresalen debido a su gran estructura matemática que facilita los procesos de codificación y decodificación.

Definición 1.23. *Un código lineal $\mathcal{C} \in \mathbb{F}_q^n$ es llamado **código cíclico**, si es cerrado bajo desplazamientos cíclicos, es decir:*

$$c_0c_1...c_{n-1} \in \mathcal{C} \Rightarrow c_{n-1}c_0...c_{n-2} \in \mathcal{C}.$$

En consecuencia, un código lineal $\mathcal{C}$ es cíclico si es cerrado bajo todos los desplazamientos cíclicos

$$c_0c_1...c_{n-2}c_{n-1} \in \mathcal{C} \mapsto c_k \dots c_{n-1}c_0 \dots c_{k-1} \in \mathcal{C},$$

para todo $k \in \{0, 1, \dots, n-1\}$.

Observación 1.1. *Si $\mathcal{C} \subset \mathbb{F}_q^n$ es un código lineal q-ario, a cada palabra código le podemos asignar un polinomio usando la siguiente función,*

$$\Phi : \mathcal{C} \subset \mathbb{F}_q^n \to \mathbb{F}_q[x]$$

$$c = (c_0, c_1, c_2, ..., c_{n-1}) \mapsto \Phi(c) = \sum_{i=0}^{n-1} c_i x^i.$$

Consideremos $\mathbb{F}_q[x]$ el anillo de polinomios con coeficientes en $\mathbb{F}_q$ y $x^n - 1 \in \mathbb{F}_q[x]$. Sea $R_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$ el anillo cociente usual, es decir el anillo de polinomios de grado menor que n, con la suma y producto de polinomios usual, seguido de reducción modulo $x^n - 1$.

Si $(c_0, c_1, ..., c_{n-1}) \in \mathcal{C}$, entonces

$$x(c_0 + c_1x + ... + c_{n-1}x^{n-1}) = (c_0x + c_1x^2 + ... + c_{n-1}x^n) \ mod(x^n - 1)$$

$$= c_{n-1} + c_0x + ... + c_{n-2}x^{n-1}.$$

La aplicación Φ en realidad es un homomorfismo de anillos que envía palabras del código $\mathcal{C}$ en polinomios en el anillo $\mathbb{F}_q[x]$. Más aún, se puede demostrar que $\mathcal{C}$ es un código cíclico, si y solamente si, $\Phi(\mathcal{C})$ es un ideal del anillo cociente $R_n = \dfrac{\mathbb{F}_q[x]}{\langle x^n - 1 \rangle}$(ver [13, pág.151]). En consecuencia estudiar códigos cíclicos es equivalente a estudiar ideales del anillo R_n, con la particularidad de que R_n es un dominio de ideales principales.

Capítulo 2

Anillos de grupo y matrices

Sean R un anillo con 1_R y G un grupo.

Fijemos la lista finita $\{g_1, g_2, \ldots, g_n\}$ de elementos de G. Dado $\mathbf{a} = \sum_{i=1}^{n} \alpha_{g_i} g_i = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \ldots + \alpha_{g_n} g_n \in RG$, su RG-matriz (que pertenece al anillo de matrices $n \times n$ con entradas en R, $M_n(R)$) es definida por

$$M(RG, \mathbf{a}) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

Podemos ver que las columnas y filas de esta matriz son esencialmente etiquetadas por $g_1, g_2, \ldots, g_n$ y sus inversos respectivamente de la siguiente manera, la primera columna por g_1, la segunda columna por g_2, etc., y análogamente la primera fila por g_1^{-1}, la segunda fila por g_2^{-1}, etc. Además cada fila y cada columna es una permutación, determinada por la multiplicación en el grupo, de la primera fila.

De la definición es posible mostrar que el conjunto de las RG-matrices, que denotaremos por $\mathcal{M}_{RG}(R)$ es un subanillo del anillo de matrices $\mathcal{M}_n(R)$. Además, tenemos el siguiente resultado:

Teorema 2.1. *Dado un grupo G de n elementos, $G = \{g_1, g_2, \ldots, g_n\}$, existe un isomorfismo de anillos*

$$\begin{array}{rccc} \varphi: & RG & \stackrel{\cong}{\to} & \mathcal{M}_{RG}(R) \\ & \mathbf{a} & \mapsto & M(RG, \mathbf{a}) \end{array}$$

entre RG y las RG-matrices sobre R, $\mathcal{M}_{RG}(R)$.

Demostración. *Sean $G = \{g_1, g_2 \ldots, g_n\}$, $\mathbf{a} = \sum_{i=1}^{n} \alpha_{g_i} g_i$, $\mathbf{b} = \sum_{i=1}^{n} \beta_{g_i} g_i \in RG$, luego $\alpha_{g_i}, \beta_{g_i} \in R$ para todo $i = 1, 2, \ldots, n$, y*

$$\begin{array}{rccc} \varphi: & RG & \to & \mathcal{M}_{RG}(R) \\ & \mathbf{a} & \mapsto & M(RG, \mathbf{a}). \end{array}$$

Veamos que φ es un homomorfismo.

$$\varphi(\mathbf{a}) = M(RG, \mathbf{a}) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix},$$

$$\varphi(\mathbf{b}) = M(RG, \mathbf{b}) = \begin{pmatrix} \beta_{g_1^{-1}g_1} & \beta_{g_1^{-1}g_2} & \cdots & \beta_{g_1^{-1}g_n} \\ \beta_{g_2^{-1}g_1} & \beta_{g_2^{-1}g_2} & \cdots & \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{g_n^{-1}g_1} & \beta_{g_n^{-1}g_2} & \cdots & \beta_{g_n^{-1}g_n} \end{pmatrix},$$

Por otra parte $\mathbf{a}+\mathbf{b} = \sum_{i=1}^{n}\alpha_{g_i}g_i + \sum_{i=1}^{n}\beta_{g_i}g_i = \sum_{i=1}^{n}(\alpha_{g_i}+\beta_{g_i})g_i = \sum_{i=1}^{n}((\alpha+\beta)_{g_i})g_i$ *y así*

$$\varphi(\mathbf{a}+\mathbf{b}) = M(RG, \mathbf{a}+\mathbf{b}) = \begin{pmatrix} (\alpha+\beta)_{g_1^{-1}g_1} & (\alpha+\beta)_{g_1^{-1}g_2} & \cdots & (\alpha+\beta)_{g_1^{-1}g_n} \\ (\alpha+\beta)_{g_2^{-1}g_1} & (\alpha+\beta)_{g_2^{-1}g_2} & \cdots & (\alpha+\beta)_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ (\alpha+\beta)_{g_n^{-1}g_1} & (\alpha+\beta)_{g_n^{-1}g_2} & \cdots & (\alpha+\beta)_{g_n^{-1}g_n} \end{pmatrix}.$$

Además,

$$\begin{aligned} \varphi(\mathbf{a}) + \varphi(\mathbf{b}) &= M(RG, \mathbf{a}) + M(RG, \mathbf{b}) \\ &= \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix} + \begin{pmatrix} \beta_{g_1^{-1}g_1} & \beta_{g_1^{-1}g_2} & \cdots & \beta_{g_1^{-1}g_n} \\ \beta_{g_2^{-1}g_1} & \beta_{g_2^{-1}g_2} & \cdots & \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{g_n^{-1}g_1} & \beta_{g_n^{-1}g_2} & \cdots & \beta_{g_n^{-1}g_n} \end{pmatrix} \\ &= \begin{pmatrix} \alpha_{g_1^{-1}g_1} + \beta_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} + \beta_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} + \beta_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} + \beta_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} + \beta_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} + \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} + \beta_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} + \beta_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} + \beta_{g_n^{-1}g_n} \end{pmatrix} \\ &= \begin{pmatrix} (\alpha+\beta)_{g_1^{-1}g_1} & (\alpha+\beta)_{g_1^{-1}g_2} & \cdots & (\alpha+\beta)_{g_1^{-1}g_n} \\ (\alpha+\beta)_{g_2^{-1}g_1} & (\alpha+\beta)_{g_2^{-1}g_2} & \cdots & (\alpha+\beta)_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ (\alpha+\beta)_{g_n^{-1}g_1} & (\alpha+\beta)_{g_n^{-1}g_2} & \cdots & (\alpha+\beta)_{g_n^{-1}g_n} \end{pmatrix} \\ &= M(RG, \mathbf{a}+\mathbf{b}) \end{aligned}$$

Por lo tanto, $\varphi(\mathbf{a}+\mathbf{b}) = \varphi(\mathbf{a}) + \varphi(\mathbf{b})$.

Sea $\mathbf{ab} = \mathbf{c}$ *donde* $\mathbf{c} = \sum_{i=1}^{n}\gamma_{g_k}g_k$, *con* $\gamma_{g_k} = \sum_{g_ig_j=g_k}\alpha_{g_i}\beta_{g_j}$. *Por lo tanto,*

$$\varphi(\mathbf{ab}) = \varphi(\mathbf{c}) = M(RG, \mathbf{c}) = \begin{pmatrix} \gamma_{g_1^{-1}g_1} & \gamma_{g_1^{-1}g_2} & \cdots & \gamma_{g_1^{-1}g_n} \\ \gamma_{g_2^{-1}g_1} & \gamma_{g_2^{-1}g_2} & \cdots & \gamma_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_{g_n^{-1}g_1} & \gamma_{g_n^{-1}g_2} & \cdots & \gamma_{g_n^{-1}g_n} \end{pmatrix}.$$

Por otra parte,

$$\varphi(\mathbf{a})\varphi(\mathbf{b}) = M(RG, \mathbf{a})M(RG, \mathbf{b})$$

$$= \begin{matrix} f_1 \to \\ f_2 \to \\ \vdots \\ f_n \to \end{matrix} \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix} \begin{matrix} c_1 \\ \downarrow \end{matrix} \begin{matrix} c_2 \\ \downarrow \end{matrix} \begin{matrix} \cdots \\ \end{matrix} \begin{matrix} c_n \\ \downarrow \end{matrix} \begin{pmatrix} \beta_{g_1^{-1}g_1} & \beta_{g_1^{-1}g_2} & \cdots & \beta_{g_1^{-1}g_n} \\ \beta_{g_2^{-1}g_1} & \beta_{g_2^{-1}g_2} & \cdots & \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{g_n^{-1}g_1} & \beta_{g_n^{-1}g_2} & \cdots & \beta_{g_n^{-1}g_n} \end{pmatrix}$$

$$= \begin{pmatrix} f_1c_1 & f_1c_2 & \cdots & f_1c_n \\ f_2c_1 & f_2c_2 & \cdots & f_2c_n \\ \vdots & \vdots & \vdots & \vdots \\ f_nc_1 & f_nc_2 & \cdots & f_nc_n \end{pmatrix}.$$

Ahora debemos ver la igualdad de las dos matrices resultantes, para ello veremos que $f_mc_p = \gamma_{g_m^{-1}g_p}$ *para todos* $m, p = 1, 2, \ldots, n$.

Sean $m, p \in \{1, 2, \ldots, n\}$. *Primeramente tenemos,*

$$\gamma_{g_m^{-1}g_p} = \sum_{g_ig_j = g_m^{-1}g_p} \alpha_{g_i}\beta_{g_j},$$

esto por como definimos γ_k *al principio, luego de la multiplicación de matrices tenemos,*

$$f_mc_p = \sum_{h=1}^{n} \alpha_{g_m^{-1}g_h}\beta_{g_h^{-1}g_p}.$$

Multiplicamos los subíndices de α *y* β *de esta última sumatoria, y obtenemos*

$$(g_m^{-1}g_h)(g_h^{-1}g_p) = g_m^{-1}(g_hg_h^{-1})g_p = g_m^{-1}g_p,$$

para todo $h = 1, 2, \ldots, n$, *por lo tanto tenemos,*

$$f_mc_p = \sum_{h=1}^{n} \alpha_{g_m^{-1}g_h}\beta_{g_h^{-1}g_p} = \sum_{g_ig_j = g_m^{-1}g_p} \alpha_{g_i}\beta_{g_j} = \gamma_{g_m^{-1}g_p}.$$

Inyectividad

Sean $\mathbf{a}$ *y* $\mathbf{b} \in RG$ *tales que* $\varphi(\mathbf{a}) = \varphi(\mathbf{b})$. *Entonces* $M(RG, \mathbf{a}) = M(RG, \mathbf{b})$ *y así*

$$\begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix} = \begin{pmatrix} \beta_{g_1^{-1}g_1} & \beta_{g_1^{-1}g_2} & \cdots & \beta_{g_1^{-1}g_n} \\ \beta_{g_2^{-1}g_1} & \beta_{g_2^{-1}g_2} & \cdots & \beta_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \beta_{g_n^{-1}g_1} & \beta_{g_n^{-1}g_2} & \cdots & \beta_{g_n^{-1}g_n} \end{pmatrix},$$

por lo tanto $\alpha_{g_i^{-1}g_j} = \beta_{g_i^{-1}g_j}$, *para todos* $i, j = 1, 2 \ldots, n$.

Ahora existe k *tal que* $g_k = 1_G$ *y* $g_k^{-1} = 1_G$ *entonces*

$$\alpha_{g_i} = \alpha_{1_G g_i} = \alpha_{g_k^{-1}g_i} = \beta_{g_k^{-1}g_i} = \beta_{1_G g_i} = \beta_{g_i},$$

para todo $i = 1, 2, \ldots, n$, *por lo tanto* $\mathbf{a} = \sum_{i=1}^{n} \alpha_{g_i} g_i = \sum_{i=1}^{n} \beta_{g_i} g_i = \mathbf{b}$.

Sobryectividad

Sea $A \in \mathcal{M}_{RG}(R)$, *es decir,* $A = M(RG, \mathbf{a}) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}$ *con* $\mathbf{a} = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$, *es decir, existe* $\mathbf{a} \in RG$ *tal que* $\varphi(\mathbf{a}) = M(RG, \mathbf{a}) = A$.

□

El resultado anterior nos permite intercambiar el anillo RG con el anillo $\mathcal{M}_{RG}(R)$ a conveniencia, obteniendo resultados de uno u otro anillo usando tal isomorfismo.

Para $\mathbf{a} \in RG$, $\varphi(\mathbf{a})$ denota su RG-matriz, la cual denotaremos por su respectiva letra mayúscula, es decir, $\varphi(\mathbf{a}) = A$.

También es posible mostrar que en el álgebra de grupo $\mathbb{F}G$, con $\mathbb{F}$ cuerpo, cada elemento es o un divisor de cero o una unidad, además se establece un método para determinar cada elemento.

Teorema 2.2. *Sea* $\mathbb{F}$ *un cuerpo. Un elemento diferente de cero* $\mathbf{u} \in \mathbb{F}G$ *es un divisor de cero si y sólo si* $det(\varphi(\mathbf{u})) = 0$, *en caso contrario* $\mathbf{u}$ *es una unidad.*

Para su demostración primero tendremos que demostrar los siguientes Teoremas y Corolarios.

Teorema 2.3. *Suponga que* R *tiene identidad. Entonces* $\mathbf{u} \in RG$ *es unidad si y sólo si* $\varphi(\mathbf{u})$ *es una unidad en* $\mathcal{M}_n(R)$.

Demostración. $\Rightarrow$] *Sea* $\mathbf{u} \in RG$ *una unidad, entonces existe* $\mathbf{v} \in RG$ *tal que* $\mathbf{uv} = \mathbf{1_{RG}}$*, esto implica que* $\varphi(\mathbf{uv}) = \varphi(\mathbf{1_{RG}}) = I_n$*, donde* I_n *es la matriz identidad en* $\mathcal{M}_n(R)$*, luego* $\varphi(\mathbf{u})\varphi(\mathbf{v}) = I_n$*, similarmente* $\varphi(\mathbf{v})\varphi(\mathbf{u}) = I_n$*, así* $\varphi(\mathbf{u})$ *es invertible (o unidad) en* $\mathcal{M}_n(R)$*.*

$\Leftarrow$] *Suponga que* $\varphi(\mathbf{u})$ *es unidad en* $\mathcal{M}_n(R)$*, entonces existe* $B \in \mathcal{M}_n(R)$ *tal que* $\varphi(\mathbf{u})B = B\varphi(\mathbf{u}) = I_n$*, ahora sea* $\mathbf{u} = \sum_{i=1}^{n} \alpha_{g_i} g_i = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n$ *entonces*

$$\varphi(\mathbf{u}) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \cdots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \cdots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \cdots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

Ahora bien no sabemos si B *es RG-matriz, entonces sea* $b = (\beta_1, \beta_2, \ldots, \beta_n)$ *la primera fila de* B*. Luego,*

$$\begin{aligned} \beta_1 \alpha_{g_1^{-1}g_1} + \beta_2 \alpha_{g_2^{-1}g_1} + \cdots + \beta_n \alpha_{g_n^{-1}g_1} &= 1, \\ \beta_1 \alpha_{g_1^{-1}g_2} + \beta_2 \alpha_{g_2^{-1}g_2} + \cdots + \beta_n \alpha_{g_n^{-1}g_2} &= 0, \\ &\vdots \\ \beta_1 \alpha_{g_1^{-1}g_n} + \beta_2 \alpha_{g_2^{-1}g_n} + \cdots + \beta_n \alpha_{g_n^{-1}g_n} &= 0. \end{aligned} \tag{2.1}$$

Veamos que $\mathbf{u} = \alpha_{g_1} g_1 + \alpha_{g_2} g_2 + \cdots + \alpha_{g_n} g_n = \alpha_{g_i^{-1}g_1} g_i^{-1} g_1 + \alpha_{g_i^{-1}g_2} g_i^{-1} g_2 + \cdots + \alpha_{g_i^{-1}g_n} g_i^{-1} g_n$ *para todo* $i = 1, 2, \ldots, n$*.*

Sea $\mathbf{b} = \beta_1 g_1 + \beta_2 g_2 + \cdots + \beta_n g_n$*. Luego,*

$$\begin{aligned} (\beta_i g_i)\mathbf{u} &= (\beta_i g_i)(\alpha_{g_1} g_2 + \alpha_{g_1} g_2 + \cdots + \alpha_{g_n} g_n) \\ &= (\beta_i g_i)(\alpha_{g_i^{-1}g_1} g_i^{-1} g_1 + \alpha_{g_i^{-1}g_2} g_i^{-1} g_2 + \cdots + \alpha_{g_i^{-1}g_n} g_i^{-1} g_n) \\ &= \beta_i g_i \alpha_{g_i^{-1}g_1} g_i^{-1} g_1 + \beta_i g_i \alpha_{g_i^{-1}g_2} g_i^{-1} g_2 + \cdots + \beta_i g_i \alpha_{g_i^{-1}g_n} g_i^{-1} g_n \\ &= \beta_i \alpha_{g_i^{-1}g_1} g_1 + \beta_i \alpha_{g_i^{-1}g_2} g_2 + \cdots + \beta_i \alpha_{g_i^{-1}g_n} g_n. \end{aligned}$$

Por tanto,

$$\mathbf{bu} = (\beta_1 g_1 + \beta_2 g_2 + \ldots + \beta_n g_n)(\alpha_1 g_1 + \alpha_2 g_2 + \ldots + \alpha_n g_n)$$

$$
\begin{aligned}
&= \beta_1\alpha_{g_1^{-1}g_1}g_1 + \beta_2\alpha_{g_2^{-1}g_1}g_1 + \cdots + \beta_n\alpha_{g_n^{-1}g_1}g_1 \\
&+ \beta_1\alpha_{g_1^{-1}g_2}g_2 + \beta_2\alpha_{g_2^{-1}g_2}g_2 + \cdots + \beta_n\alpha_{g_n^{-1}g_2}g_2 \\
&+ \quad \cdots \\
&+ \beta_1\alpha_{g_1^{-1}g_n}g_n + \beta_2\alpha_{g_2^{-1}g_n}g_n + \cdots + \beta_n\alpha_{g_n^{-1}g_n}g_n \\
\\
&= g_1(\beta_1\alpha_{g_1^{-1}g_1} + \beta_2\alpha_{g_2^{-1}g_1} + \cdots + \beta_n\alpha_{g_n^{-1}g_1}) \\
&+ g_2(\beta_1\alpha_{g_1^{-1}g_2} + \beta_2\alpha_{g_2^{-1}g_2} + \cdots + \beta_n\alpha_{g_n^{-1}g_2}) \\
&+ \quad \cdots \\
&+ g_n(\beta_1\alpha_{g_1^{-1}g_n} + \beta_2\alpha_{g_2^{-1}g_n} + \cdots + \beta_n\alpha_{g_n^{-1}g_n}) \\
&= g_1 \quad (\textit{usando las ecuaciones 2.1})
\end{aligned}
$$

Entonces $\mathbf{bu} = g_1$*, luego* $g_1^{-1}\mathbf{bu} = g_1^{-1}g_1 = 1$*, por lo tanto* $g_1^{-1}\mathbf{b}$ *es un inverso de* $\mathbf{u}$*, es decir* $\mathbf{u}$ *es unidad en* RG*.*

□

Corolario 2.3.1. *Si la inversa de una RG-matriz existe entonces esta inversa es también una RG-matriz.*

Demostración. *Es inmediato de la demostración del Teorema 2.3 (página 33).*

□

Corolario 2.3.2. *Cuando* R *es conmutativo,* $\mathbf{u}$ *es unidad en* $RG \Leftrightarrow \varphi(\mathbf{u})$ *es unidad en* $\mathcal{M}_n(R) \Leftrightarrow det(\varphi(\mathbf{u}))$ *es unidad en* R*.*

Demostración. *La primera equivalencia es el Teorema 2.3.*

Supongamos que $\varphi(\mathbf{u})$ *unidad en* $\mathcal{M}_n(R)$*, y así, existe* $B \in \mathcal{M}_n(R)$ *tal que* $\varphi(\mathbf{u})B = I_n$*, y así* $det(\varphi(\mathbf{u})B) = det(I_n)$ *luego* $det(\varphi(\mathbf{u}))det(B) = 1_R$ *entonces* $det(\varphi(\mathbf{u}))$ *es unidad en* R*.*

Finalmente si $det(\varphi(\mathbf{u}))$ *unidad en* R*, entonces* $\varphi(\mathbf{u})$ *es invertible en* $\mathcal{M}_n(R)$*, luego existe* $\mathbf{v} \in RG$ *tal que* $\varphi(\mathbf{u})\varphi(\mathbf{v}) = I_n$ *entonces* $\varphi(\mathbf{u})$ *es unidad en* $\mathcal{M}_n(R)$*.*

□

Corolario 2.3.3. $\mathbf{z}$ *es divisor de cero en* $RG \Leftrightarrow \varphi(\mathbf{z})$ *es divisor de cero en* $\mathcal{M}_n(R)$*.*

Demostración. $\Rightarrow$] *Sea* $\mathbf{z}$ *un divisor de cero en* RG*, entonces existe* $\mathbf{v} \neq \mathbf{0} \in RG$ *tal que* $\mathbf{zv} = \mathbf{0}$ *luego* $\varphi(\mathbf{zv}) = \varphi(\mathbf{z})\varphi(\mathbf{v}) = \varphi(\mathbf{0}) = 0$ *es decir* $\varphi(\mathbf{z})$ *es divisor de cero en* $\mathcal{M}_n(R)$*.*

$\Leftarrow$] *Sea* $\varphi(\mathbf{z}) \neq 0$ *divisor de cero en* $\mathcal{M}_n(R)$ *entonces existe* $B \neq 0_{n\times n} \in \mathcal{M}_n(R)$ *tal que* $\varphi(\mathbf{z})B = 0_{n\times n}$*. Sea* $b = (\beta_1, \beta_2, \ldots, \beta_n) \neq 0$ *una columna de* B*, entonces*

$$\begin{aligned}
\beta_1\alpha_{g_1^{-1}g_1} + \beta_2\alpha_{g_2^{-1}g_1} + \cdots + \beta_n\alpha_{g_n^{-1}g_1} &= 0,\\
\beta_1\alpha_{g_1^{-1}g_2} + \beta_2\alpha_{g_2^{-1}g_2} + \cdots + \beta_n\alpha_{g_n^{-1}g_2} &= 0,\\
&\vdots\\
\beta_1\alpha_{g_1^{-1}g_n} + \beta_2\alpha_{g_2^{-1}g_n} + \cdots + \beta_n\alpha_{g_n^{-1}g_n} &= 0.
\end{aligned} \tag{2.2}$$

Definiendo $\mathbf{b} = \beta_1 g_1 + \beta_2 g_2 + \ldots + \beta_n g_n$ *de igual manera que en la demostración del Teorema 2.3 tenemos que* $\mathbf{z} = \alpha_{g_i^{-1}g_1} g_i^{-1} g_1 + \alpha_{g_i^{-1}g_2} g_i^{-1} g_2 + \ldots + \alpha_{g_i^{-1}g_n} g_i^{-1} g_n$ *para todo* $i = 1, 2, \ldots, n$, *y así,*

$$\beta_i g_i \mathbf{z} = \beta_i \alpha_{g_i^{-1}g_1} g_1 + \beta_i \alpha_{g_i^{-1}g_2} g_2 + \ldots + \beta_i \alpha_{g_i^{-1}g_n} g_n$$

para todo $i = 1, 2, \ldots, n$, *por lo tanto,*

$$\begin{aligned}
\mathbf{bz} = {} & \beta_1\alpha_{g_1^{-1}g_1} g_1 + \beta_2\alpha_{g_2^{-1}g_2} g_1 + \ldots + \beta_n\alpha_{g_n^{-1}g_n} g_1\\
& + \beta_1\alpha_{g_1^{-1}g_1} g_2 + \beta_2\alpha_{g_2^{-1}g_2} g_2 + \ldots + \beta_n\alpha_{g_n^{-1}g_n} g_2\\
& + \quad \cdots\\
& + \beta_1\alpha_{g_1^{-1}g_1} g_n + \beta_2\alpha_{g_2^{-1}g_2} g_n + \ldots + \beta_n\alpha_{g_n^{-1}g_n} g_n\\
\\
& = g_1(\beta_1\alpha_{g_1^{-1}g_1} + \beta_2\alpha_{g_2^{-1}g_2} + \ldots + \beta_n\alpha_{g_n^{-1}g_n})\\
& + g_2(\beta_1\alpha_{g_1^{-1}g_1} + \beta_2\alpha_{g_2^{-1}g_2} + \ldots + \beta_n\alpha_{g_n^{-1}g_n})\\
& + \quad \cdots\\
& + g_n(\beta_1\alpha_{g_1^{-1}g_1} + \beta_2\alpha_{g_2^{-1}g_2} + \ldots + \beta_n\alpha_{g_n^{-1}g_n})\\
& = 0 \quad (\textit{usando las ecuaciones 2.2}).
\end{aligned}$$

Luego como $\mathbf{b} \neq \mathbf{0}$ *y* $\mathbf{bz} = \mathbf{0}$ *entonces* $\mathbf{z}$ *es divisor de cero en* RG.

□

Para el caso cuando R es cuerpo tenemos el siguiente corolario.

Corolario 2.3.4. *Cuando* R *es cuerpo,* $\mathbf{z}$ *es un divisor de cero en* $RG \Leftrightarrow \varphi(\mathbf{z})$ *es un divisor de cero en* $\mathcal{M}_n(R) \Leftrightarrow det(\varphi(\mathbf{z})) = 0$.

Demostración (Teorema 2.2). $\mathbf{u} \in \mathbb{F}G$ *es un divisor de cero si y sólo si* $det(\varphi(\mathbf{u})) = 0$ *es el Corolario 2.3.4.*

Supongamos que $det(\varphi(\mathbf{u})) \neq 0 \in \mathbb{F}$. *Entonces* $det(\varphi(\mathbf{u}))$ *es una unidad en* $\mathbb{F}$, *por* $\mathbb{F}$ *ser un cuerpo, luego por el Corolario 2.3.2* $\mathbf{u}$ *es una unidad en* $\mathbb{F}G$ *y recíprocamente.*

□

2.1 Algunos conceptos

Muchos conceptos y propiedades de las matrices resultan tener equivalentes útiles en el contexto de los anillos de grupos. Estos conceptos y propiedades equivalentes son inherentes al anillo de grupo en sí, existiendo independientemente de la lista de grupo escogida lo que es coherente con la equivalencia de matrices.

Comencemos con el 'traspuesto' de un elemento de anillo de grupo

Definición 2.1. *El* ***traspuesto*** *de un elemento* $\mathbf{a} = \sum_{g\in G} \alpha_g g \in RG$ *es* $\mathbf{a}^T = \sum_{g\in G} \alpha_g g^{-1}$, *o equivalentemente,* $\mathbf{a}^T = \sum_{g\in G} \alpha_{g^{-1}} g$.

Esto es consistente con la definición de traspuesta de una matriz. Dado $G = \{g_1, g_2, \ldots, g_n\}$, sea A la RG-matriz de $\mathbf{a}$. La entrada (i, j) de la RG-matriz de $\mathbf{a}^T$ es $\alpha_{(g_i^{-1}g_j)^{-1}} = \alpha_{g_j^{-1}g_i}$, así A^T es la RG-matriz de $\mathbf{a}^T$.

El traspuesto $\mathbf{a}^T$ también ha sido llamado el anti-automorfismo de $\mathbf{a}$,([6] [pág. 62]).

Definición 2.2. $\mathbf{a} \in RG$ *se dice que es* ***simétrico*** *si y sólo si* $\mathbf{a}^T = \mathbf{a}$.

Claramente, la definición es consistente ya que $\mathbf{a}$ es simétrica si y sólo si su RG-matriz A es una matriz simétrica.

Conjuntistamente definimos $W\mathbf{u}$ y $\mathbf{u}W$ con $\mathbf{u} \in RG$ y $W \subset RG$ por:

$$W\mathbf{u} = \{\mathbf{xu} : \mathbf{x} \in W\} \quad \text{y} \quad \mathbf{u}W = \{\mathbf{ux} : \mathbf{x} \in W\}.$$

Para $\underline{x} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in R^n$ asociamos un elemento $\mathbf{x} \in RG$ acorde a la lista $G' = \{g_1, g_2, \ldots, g_n\} \subseteq G$ por medio de la aplicación

$$\begin{array}{rccc} \psi: & R^n & \to & RG' \\ & \underline{x} & \mapsto & \sum_{i=1}^{n} \alpha_i g_i = \mathbf{x}. \end{array}$$

Por ψ^{-1}, entenderemos la aplicación inversa, es decir, $\psi^{-1}(\mathbf{x}) = (\alpha_1, \alpha_2, \ldots, \alpha_n) = \underline{x}$, la cual está bien definida pues es fácil ver que ψ es biyectiva.

2.2 Códigos desde codificaciones de anillos de grupos

Sea RG el anillo de grupo del grupo G sobre R con $G = \{g_1, g_2, \ldots, g_n\}$. Supongamos que W es un submódulo de RG y sea $\mathbf{u} \in RG$.

Definición 2.3. *Sea* $\mathbf{x} \in W$. *Una* ***codificación de anillo de grupo*** *es una aplicación* $\rho : W \to RG$, *tal que* $\rho(\mathbf{x}) = \mathbf{xu}$ *o* $\rho(\mathbf{x}) = \mathbf{ux}$. *En el segundo caso,* ρ *es una* ***codificación de anillo de grupo a izquierda****, y en el primero, una* ***codificación de anillo de grupo a derecha****.*

Un código $\mathcal{C}$ derivado de una codificación de anillo de grupo es entonces la imagen de una codificación de anillo de grupo, es decir, para $\mathbf{u} \in RG$ dado y W un submódulo de RG, $\mathcal{C} = \{\mathbf{ux} : \mathbf{x} \in W\}$ o $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$.

Dado que el anillo de grupo RG no es necesariamente conmutativo, entonces permitir grupos G no conmutativos posibilita la construcción de códigos no conmutativos. En el caso que $\mathbf{xu} = \mathbf{ux}$ para todo $\mathbf{x} \in W$, $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$ es llamado código conmutativo.

Cuando $\mathbf{u} \in RG$ es un divisor de cero, él genera un **código divisor de cero** y cuando es una unidad, genera un **código derivado de unidad**.

En la práctica, el submódulo W tiene dimensión[1] $r < n$. Este puede tener la base $\{g_1, g_2, \ldots, g_r\}$. Otros submódulos también resultan útiles, como el generado por $\{g_{k_1}, g_{k_2}, \ldots, g_{k_t}\}$ con $1 \leq t < n$ donde $\{k_1, k_2, \ldots, k_t\} \subseteq \{1, 2, \ldots, n\}$.

Para los códigos derivados de unidad existe total libertad en la elección de W (y por tanto de r), es decir, cualquier W submódulo de RG puede ser usado en la codificación. En el caso de los códigos divisores de cero, como mostraremos luego se tienen restricciones sobre el submódulo W, con el objetivo de garantizar la existencia de una aplicación uno a uno desde el código a W.

Cuando RG es finito y tiene una identidad, RG solo contiene divisores de cero y unidades, Teorema 2.2. Esto también pasa cuando R es un cuerpo. Cabe destacar que en otros casos, es posible generar códigos a partir de codificaciones de anillos de grupo que no son ni divisores cero ni derivados de unidad.

---

[1]

Definición 2.4. *Sea* M *un módulo sobre un anillo conmutativo* R *con una base finita. Entonces, el número de elementos en cualquier base de* M *se llama la dimensión de* M.

Teorema 2.4. *Sea* M *un módulo sobre un anillo conmutativo* R. *Supongamos que* M *contiene dos bases finitas* $B_1 = \{v_1, v_2, \ldots, v_m\}$ *y* $B_2 = \{w_1, w_2, \ldots, w_n\}$. *Entonces* $n = m$.

Podemos definir una función $i : G \to RG$ asignando a cada elemento $x \in G$ el elemento $i(x) = \sum_{g \in G} \alpha_g g$, donde $a_x = 1$ y $a_g = 0$ si $g \neq x$.

Por lo tanto, podemos considerar G como un subconjunto de RG. Con esta identificación en mente, podemos decir que G es una base de RG sobre R. Como consecuencia inmediata vemos que, si R es conmutativo, entonces la dimensión de un módulo sobre R está bien definido. Por lo tanto, si G es finito, podemos afirmar que el $rank(RG)$ sobre R es precisamente $|G|$.

Capítulo 3

Códigos desde divisores de cero

Nos centramos ahora en la construcción de códigos a partir de divisores de cero en un anillo de grupo dado RG.

Consideremos G de orden n y dado por $G = \{g_1, g_2, \ldots, g_n\}$. La longitud del código $\mathcal{C}$ será n, es decir, toda palabra código en $\mathcal{C}$ tiene longitud n, y su dimensión dependerá de la elección del submódulo W.

Sean $\mathbf{u} \in RG$ un divisor de cero, es decir, existe $\mathbf{0} \neq \mathbf{v} \in RG$ tal que $\mathbf{uv} = \mathbf{0}$, y W submódulo de RG con base los elementos de grupo $S \subseteq G$.

Como se definió anteriormente en la Sección 2.2, un código divisor de cero resultante es $\mathcal{C} = \{\mathbf{ux} : \mathbf{x} \in W\} = \mathbf{u}W$ o $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\} = W\mathbf{u}$. Así las cosas, el código $\mathcal{C}$ es construido desde un divisor de cero $\mathbf{u}$, un submódulo W y, en el caso de RG no conmutativo, una codificación a izquierda o derecha prefijada. Describiremos el caso de la codificación a derecha, es decir $\mathcal{C} = W\mathbf{u}$. El caso de codificación a izquierda se puede describir de manera similar.

Si $\mathcal{C} = W\mathbf{u}$, decimos que $\mathbf{u}$ es un elemento generador relativo al submódulo W. Naturalmente es posible que $\mathcal{C}$ tenga otro elemento generador y de hecho también puede ser definido en términos de un submódulo diferente W.

Cuando $\mathbf{u}$ es un divisor cero, entonces existe un elemento $\mathbf{v} \neq \mathbf{0}$ con $\mathbf{uv} = \mathbf{0}$ y así, $\mathbf{y} \in \mathcal{C}$ satisface $\mathbf{yv} = \mathbf{0}$. Puede suceder que dicho elemento $\mathbf{v}$ también determine el código.

Definición 3.1. $\mathbf{v} \in RG$ *es llamado un* ***elemento de verificación*** *para un código divisor de cero* $\mathcal{C}$ *si satisface que* $\mathbf{y} \in \mathcal{C}$ *si y sólo si* $\mathbf{yv} = \mathbf{0}$. *El código puede entonces ser escrito* $\mathcal{C} = \{\mathbf{y} \in RG : \mathbf{yv} = \mathbf{0}\}$.

Ejemplo 3.1.

Tomando $R = \mathbb{Z}_2$ *y* $G = C_4 = \langle g : g^4 = 1 \rangle$*, el anillo de grupo será*

$$\mathbb{Z}_2C_4 = \left\{ \sum_{i=0}^{3} \alpha_i g^i : \alpha_i \in \mathbb{Z}_2, g^i \in C_4 \right\}.$$

Sea $\mathbf{u} = 1 + g^2$*, entonces*

$$\mathbf{uu} = \mathbf{u}^2 = (1 + g^2)^2 = 1 + 2g^2 + g^4 = 1 + 1 = \mathbf{0}.$$

Tomando $\mathcal{C} = \mathbb{Z}_2C_4\mathbf{u}$*, entonces veamos que* $\mathbf{u}$ *es elemento de verificación.*

Sea $\mathbf{y} \in \mathbb{Z}_2C_4\mathbf{u}$*, entonces* $\mathbf{y} = \mathbf{xu}$ *para algún* $\mathbf{x} \in \mathbb{Z}_2C_4$*, por lo tanto*

$$\mathbf{yu} = (\mathbf{xu})\mathbf{u} = \mathbf{x}(\mathbf{u}^2) = \mathbf{x0} = \mathbf{0}.$$

Por otro lado, si $\mathbf{yu} = \mathbf{0}$ *con* $\mathbf{0} \neq \mathbf{y} \in \mathbb{Z}_2C_4$*, por lo tanto,* $\mathbf{y} = \sum_{i=0}^{3} \alpha_i g^i = \alpha_0 + \alpha_1 g + \alpha_2 g^2 + \alpha_3 g^3$*, de esta manera tenemos que*

$$\begin{aligned} \mathbf{0} &= \mathbf{yu} \\ &= (\alpha_0 + \alpha_1 g + \alpha_2 g^2 + \alpha_3 g^3)(1 + g^2) \\ &= \alpha_0 + \alpha_1 g + \alpha_2 g^2 + \alpha_3 g^3 + \alpha_0 g^2 + \alpha_1 g^3 + \alpha_2 + \alpha_3 g \\ &= (\alpha_0 + \alpha_2) + (\alpha_1 + \alpha_3)g + (\alpha_0 + \alpha_2)g^2 + (\alpha_1 + \alpha_3)g^3, \end{aligned}$$

por lo tanto $\alpha_0 + \alpha_2 = 0 = \alpha_1 + \alpha_3$*.*

i) Si $\alpha_0 = 0$ *entonces* $\alpha_2 = 0$*, ahora como* $\mathbf{y} \neq \mathbf{0}$*, tenemos que* $\alpha_1 = \alpha_3 = 1$*, así* $\mathbf{y} = g + g^3 = g(1 + g^2) = g\mathbf{u}$*. Para* $\alpha_2 = 0$ *se llega a lo mismo de manera análoga.*

ii) Si $\alpha_1 = 0$ *entonces* $\alpha_3 = 0$*, ahora como* $\mathbf{y} \neq \mathbf{0}$*, tenemos que* $\alpha_0 = \alpha_2 = 1$*, así* $\mathbf{y} = 1 + g^2 = \mathbf{u}$*. Para* $\alpha_3 = 0$ *se llega a lo mismo de manera análoga.*

iii) Si $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 1$ *tenemos que* $\mathbf{y} = 1 + g + g^2 + g^3 = (1 + g^2) + (g + g^3) = (1 + g^2) + g(1 + g^2) = (1 + g^2)(1 + g) = \mathbf{u}(1 + g)$

De esta manera por i), ii) y iii) tenemos que $\mathbf{y} \in \mathbb{Z}_2C_4\mathbf{u}$*.*

Finalmente el código puede ser escrito $\mathcal{C} = \{\mathbf{y} \in \mathbb{Z}_2C_4 : \mathbf{y}(1 + g^2) = \mathbf{0}\}$*.*

Mostraremos más adelante que dado un divisor cero $\mathbf{u}$ y el código $\mathcal{C}$ existe un conjunto $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_t\}$ de elementos en RG tal que $\mathbf{y} \in \mathcal{C}$ si y sólo si $\mathbf{yv}_i = \mathbf{0}$, $1 \leq i \leq t$.

Códigos divisores de cero con un único elemento de verificación son particularmente útiles y existen varios casos.

Hemos definido códigos en RG generados por un divisor cero y relativos a un submódulo W. Note que, además de utilizar un divisor cero como un generador, los códigos también se pueden construir utilizando un divisor cero en su lugar directamente como un elemento de verificación, independientemente de si se tiene o no un único elemento generador.

Definición 3.2. *Suponga que T un submódulo de RG. $T_{\mathbf{v}} = \{\mathbf{x} \in T : \mathbf{xv} = \mathbf{0}\}$ es llamado un código divisor de cero de verificación relativo a T.*

Es de fácil verificación que $T_{\mathbf{v}}$ con la acción $(g_i, \mathbf{x}) \mapsto g_i\mathbf{x}$; $g_i \in G$, $\mathbf{x} \in T_{\mathbf{v}}$, es un submódulo de RG y en el caso donde $T = RG$, $T_{\mathbf{v}}$ es en realidad un ideal izquierdo. Sólo tiene sentido considerar el caso en el que $\mathbf{v}$ es un divisor cero, en cuyo caso $T_{\mathbf{v}} \neq \{0\}$. Supongamos que la RG-matriz resultante V tiene rango $n - r$. Luego $n - r$ de las filas de V son linealmente independientes y las otras son combinaciones lineales de estas. Así, el código puede considerarse un código (n, r) con matriz de verificación de tamaño $(n - r) \times n$. En algunos casos, este código tendrá una única matriz generadora, sin embargo, en cualquier caso, es posible describir un conjunto de elementos generadores.

3.1 Módulos

Restringiremos nuestra atención al caso cuando R es un cuerpo. Algunos de los resultados se mantienen para dominios enteros y anillos en general. Cabe destacar que códigos derivados de unidad no tienen tales restricciones.

Definición 3.3. *Un subconjunto de elementos $T \subset RG$, es llamado **linealmente independiente** si, para $\alpha_{\mathbf{x}} \in R$, $\sum_{\mathbf{x}\in T} \alpha_{\mathbf{x}}\mathbf{x} = 0$, solo cuando $\alpha_{\mathbf{x}} = 0$ para todo $\mathbf{x} \in T$. En caso contrario, T es **linealmente dependiente**.*

Como es usual, definimos el $\mathbf{rank}(T)$ como el número máximo de elementos linealmente independientes de T. Así, $\mathbf{rank}(T) = |T|$ si y sólo si T es un conjunto linealmente independiente.

Note que un código divisor de cero $\mathcal{C} = W\mathbf{u}$, donde W es generado por S, es el submódulo de RG consistente de todos los elementos de la forma $\sum_{g\in S} \alpha_g g\mathbf{u}$. Por tanto la dimensión de este submódulo es $\mathbf{rank}(S\mathbf{u})$.

Si $S\mathbf{u}$ es linealmente dependiente entonces existe un subconjunto $S'\mathbf{u}$ de $S\mathbf{u}$ que es linealmente independiente y genera el mismo módulo que $S\mathbf{u}$. Es en este punto que se requiere que R sea cuerpo. Sea $W' \leq W$ submódulo generado por S', luego el código es $\mathcal{C} = W\mathbf{u} = W'\mathbf{u}$ y $S'\mathbf{u}$ es linealmente independiente.

La dimensión máxima de un código para un divisor cero dado $\mathbf{u}$ es $r = \mathbf{rank}(G\mathbf{u})$. Los códigos divisor cero son así (n, k)-códigos donde $k = \mathbf{rank}(S\mathbf{u})$ y $k \leq r = \mathbf{rank}(G\mathbf{u})$. Como se ha señalado, para $\mathbf{u}$ y W dados, siempre es posible encontrar un submódulo W'

de W (que puede ser el mismo W) tal que W' es generado por S' con $S'\mathbf{u}$ linealmente independiente y $W\mathbf{u} = W'\mathbf{u}$. Una manera de encontrar S' dentro de S es la siguiente, usar la RG-matriz U asociada a $\mathbf{u}$ y obtener una base apropiada para la matriz que consiste de las filas relevantes de U correspondientes a los elementos de $S\mathbf{u}$.

Un (n, t) código divisor cero puede ser encontrado obteniendo t filas linealmente independientes filas $i_1, i_2, \ldots, i_t$ de U. Luego, $S = \{g_{i_1}, g_{i_2}, \ldots, g_{i_t}\}$ es tal que $S\mathbf{u}$ es linealmente independiente y genera un (n, t)-código. El caso $t = \mathbf{rank}(U)$ es el código $RG\mathbf{u}$ y puede ser obtenido al considerar cualquier $t = \mathbf{rank}(U)$ filas linealmente independientes de U. Los códigos con $t < \mathbf{rank}(S\mathbf{u})$ son conocidos con el nombre de códigos 'acortados'. Sus matrices generadora y de verificación se obtienen fácilmente mediante los métodos descritos a continuación.

Sea $S\mathbf{u}$ linealmente independiente, y supongamos que $W \leq RG$ contiene algún $\mathbf{v} \neq \mathbf{0}$ divisor de cero de $\mathbf{u}$. Así $\mathbf{v} = \sum_{g \in S} \alpha_g g$, luego

$$\begin{aligned} \mathbf{vu} &= \left(\sum_{g \in S} \alpha_g g \right) \mathbf{u} \\ &= \sum_{g \in S} \alpha_g g\mathbf{u} \\ &= \mathbf{0}. \end{aligned}$$

Dado que $S\mathbf{u}$ es linealmente independiente, $\alpha_g = 0$ para todo $g \in S$ y así, $\mathbf{v} = \mathbf{0}$. Se sigue que W no contiene divisores de cero de $\mathbf{u}$. La afirmación recíproca es probada de manera similar.

Ejemplo 3.2.

1) Sea RG el anillo de grupo donde R es cuerpo y $G = C_n = \langle g : g^n = 1 \rangle$ el grupo cíclico de orden n. Supongamos que $\mathbf{u} \in RG$ es un divisor de cero. Sea $r \in \mathbb{N}$ el primer valor tal que el conjunto $\{\mathbf{u}, g\mathbf{u}, g^2\mathbf{u}, \ldots, g^r\mathbf{u}\}$ es linealmente dependiente. Luego r es igual al $\mathbf{rank}(U)$ y el conjunto $S = \{1, g, g^2, \ldots, g^{r-1}\}$, genera W.

En efecto, de la dependencia lineal, se tiene que existen escalares $\alpha_i \in R$, $0 \leq i \leq r$, no todos ceros tales que,

$$\alpha_0\mathbf{u} + \alpha_1 g\mathbf{u} + \alpha_2 g^2\mathbf{u} + \cdots + \alpha_{r-1} g^{r-1}\mathbf{u} + \alpha_r g^r\mathbf{u} = \mathbf{0}.$$

Suponiendo sin pérdida de generalidad que $\alpha_r \neq 0$, se sigue que existen escalares $\beta_i \in R$, $0 \leq i \leq r-1$, con

$$g^r\mathbf{u} = \beta_0\mathbf{u} + \beta_1 g\mathbf{u} + \beta_2 g^2\mathbf{u} + \cdots + \beta_{r-1}g^{r-1}\mathbf{u}.$$

Multiplicando la anterior expresión por g^l, se tiene que

$$g^{r+l}\mathbf{u} = \beta_0\mathbf{u}g^l + \beta_1 gl + 1\mathbf{u} + \beta_2 g^{l+2}\mathbf{u} + \cdots + \beta_{r-1}g^{r-1+l}\mathbf{u}.$$

Así, teniendo presente que $g^n = 1$, dado $\mathbf{x} = \sum_{i=1}^{n-1}\beta_{g_i}g_i \in RG$, se sigue que $\mathbf{xu}$ puede ser escrito en la forma $\sum_{i=1}^{r-1}\beta_{g_i}g_i\mathbf{u}$, es decir, $\mathbf{xu}$ se escribe como combinación lineal de los elementos del conjunto $\{\mathbf{u}, g\mathbf{u}, g^2\mathbf{u}, \ldots, g^{r-1}\mathbf{u}\}$ y la afirmación se sigue.

2) Consideremos el anillo de grupo RD_{2n}, donde R es cuerpo y $D_{2n} = \langle a, b : a^2 = 1 = b^n, a^{-1}ba = b^{-1}\rangle$ el grupo dihedral de orden n. Sea $\mathbf{u} \in RG$ y $S' = \{1, b, b^2, \ldots, b^{k-1}\} \subseteq \{1, b, b^2, \ldots, b^{n-1}\}$ tal que $\left(S' \cup \{b^k\}\right)\mathbf{u}$ es linealmente dependiente. Ahora bien, sea $S = S' \cup \{a, ab, \ldots, ab^l\}$ el primer conjunto tal que $S\mathbf{u}$ es linealmente dependiente. Entonces el $rank(U) = |S|$.

Como en el ejemplo anterior, de la dependencia lineal existen escalares $\alpha_i \in R$, $0 \leq i \leq k-1$, tales que

$$b^k\mathbf{u} = \left(\alpha_0 + \alpha_1 b + \cdots + \alpha_{k-1}b^{k-1}\right)\mathbf{u}.$$

Al multiplicar a la izquierda en ambos lados, se sigue que para cada $k \leq m < n$, $b^m\mathbf{u}$ puede ser escrito en términos de las potencias anteriores a k de b (veces $\mathbf{u}$) y así, en términos de S'. Además, para algunos $\beta_i \in R$, $0 \leq i \leq l-1$,

$$ab^l\mathbf{u} = \left(\alpha_0 + \alpha_1 b + \cdots + \alpha_{k-1}b^{k-1} + \beta_0 + \beta_1 ab + \cdots + \beta_{l-1}ab^{l-1}\right)\mathbf{u}.$$

Multiplicando por izquierda por b^{m-l} a ambos lados se tiene que

$$\begin{aligned} ab^m\mathbf{u} = \big(&\alpha_0 b^{m-l} + \alpha_1 b^{m-l+1} + \cdots + \alpha_{k-1}b^{m-l+k-1} \\ &+\beta_0 b^{m-l} + \beta_1 ab^{m-l+1} + \cdots + \beta_{l-1}ab^{m-1}\big)\mathbf{u}. \end{aligned}$$

Por lo tanto, para cada $l \leq m < n$, $ab^m\mathbf{u}$ puede ser escrito como combinación lineal de los términos $b^i\mathbf{u}$, los cuales, como se mostró arriba, pueden ser escritos en las primeras k potencias de b y en términos de los l elementos anteriores de la forma ab^i.

3.2 Independencia lineal

La relación entre filas linealmente independientes (dependientes) de la RG-matriz U y la independencia (dependencia) lineal del conjunto $S\mathbf{u}$ será evidenciada.

Suponga que $S = \{g_{i_1}, g_{i_2}, \ldots, g_{i_r}\} \subset G = \{g_1, g_2, \ldots, g_n\}$ y que U es obtenida de esta enumeración de G. Específicamente, se demuestra que las filas $\{\underline{u}_{i_1}, \underline{u}_{i_2}, \ldots, \underline{u}_{i_r}\}$ de U son linealmente independientes si y sólo si $S\mathbf{u}$ es linealmente independiente.

Teorema 3.1. *Suponga* $\mathbf{rank}(U) = t$. *Sea* $S \subset G$ *un conjunto de elementos de grupo tal que* $\mid S \mid = t + 1$. *Entonces,* $S\mathbf{u}$ *es linealmente dependiente.*

Demostración. *Sean* $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_n$ *las filas de* U *en ese orden.*

Suponga que $S\mathbf{u} = \{g_{j_1}\mathbf{u}, g_{j_2}\mathbf{u}, \ldots, g_{j_{t+1}}\mathbf{u}\}$. *De la definición, cualquier* $t + 1$ *filas de* U *son dependientes, así existen,* $\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_{t+1}} \in R$ *no todos ceros tales que* $\sum_{k=1}^{t+1} \alpha_{j_k} \underline{u}_{j_k} = 0_{1\times n}$. *Sea* A *la* RG*-matriz que tiene en la primera fila* α_{j_k} *en la posición* j_k*-ésima para* $1 \leq k \leq t + 1$ *y ceros en las demás posiciones.*

Así A *es la* RG*-matriz asociada al elemento de anillo de grupo* $\mathbf{a} = \alpha_{j_1} g_{j_1} + \alpha_{j_2} g_{j_2} + \ldots + \alpha_{j_{t+1}} g_{j_{t+1}}$. *Además,* AU *es una* RG*-matriz cuya primera fila consiste de ceros y, por tanto,* $AU = 0_{n\times n}$. *Del isomorfismo,* $\mathbf{au} = \mathbf{0}$ *y por tanto,* $\{g_{j_1}\mathbf{u}, g_{j_2}\mathbf{u}, \ldots, g_{j_{t+1}}\mathbf{u}\}$ *es linealmente dependiente como se deseaba.*

□

Luego, del último Teorema, se deduce que podemos tomar a S con r elementos donde $r \leq \mathbf{rank}(U)$. Si $r > \mathbf{rank}(U)$, $S\mathbf{u}$ es generado por r elementos $S'\mathbf{u}$ (donde $S' \subset S$) y el código es dado por $\mathcal{C} = W'\mathbf{u}$ donde W' es el módulo generado por S'.

De manera alternativa, y asumiendo que $\mathbf{rank}(U) \geq r$, podemos escoger o encontrar r filas linealmente independientes $\underline{u}_{i_1}, \underline{u}_{i_2}, \ldots, \underline{u}_{i_r}$ de U y luego construir S teniendo los u_{i_j} como referencia. Sea $S = \{g_{i_1}, g_{i_2}, \ldots, g_{i_r}\}$. Luego $S\mathbf{u}$ es linealmente independiente.

Defina G_j como la RG-matriz correspondiente al elemento de grupo $g_j \in G$. Esto es consistente con la notación para la RG-matriz correspondiente a g_j. Entonces G_j es la matriz cuya primera fila tiene un 1 en la j-ésima posición y cero en las restantes. De esto sigue que G_jU es la RG-matriz con la primera fila $\underline{u}_j$.

Lema 3.1. *Suponga que* $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_s$ *son las primeras filas (o primeras columnas) de las* RG*-matrices* $U_1, U_2, \ldots, U_s$ *respectivamente. Entonces* $\alpha_1\underline{u}_1 + \alpha_1\underline{u}_2 + \ldots + \alpha_s\underline{u}_s = 0_{1\times n}$ *si y sólo si* $\alpha_1 U_1 + \alpha_1 U_2 + \ldots + \alpha_s U_s = 0_{n\times n}$.

Demostración. *Suponga* $\alpha_1\underline{u}_1 + \alpha_2\underline{u}_2 + \ldots + \alpha_s\underline{u}_s = 0_{1\times n}$. *Sea* $U = \alpha_1 U_1 + \alpha_2 U_2 + \ldots + \alpha_s U_s$. *Entonces* U *es una* RG*-matriz donde la primera fila consisten de ceros y*

así $U = 0_{n\times n}$.

De otro lado, es claro que si $\alpha_1 U_1 + \alpha_2 U_2 + \ldots + \alpha_s U_s = 0_{n\times n}$ *entonces* $\alpha_1 \underline{u}_1 + \alpha_2 \underline{u}_2 + \ldots + \alpha_s \underline{u}_s = 0_{1\times n}$.

□

Como una consecuencia directa del resultado anterior tenemos.

Lema 3.2. *El conjunto* $S\mathbf{u} = \{g_{i_1}\mathbf{u}, g_{i_2}\mathbf{u}, \ldots, g_{i_r}\mathbf{u}\}$ *es linealmente independiente si y sólo si* $\{\underline{u}_{i_1}, \underline{u}_{i_2}, \ldots, \underline{u}_{i_r}\}$ *es linealmente independiente.*

Demostración. *Sea* $S\mathbf{u} = \{g_{i_1}\mathbf{u}, g_{i_2}\mathbf{u}, \ldots, g_{i_r}\mathbf{u}\}$ *linealmente independiente, entonces el conjunto* $\{G_{i_1}U, G_{i_2}U, \ldots, G_{i_r}U\}$ *de las RG-matrices correspondientes respectivamente a los* $g_{i_j}\mathbf{u}$ *es linealmente independiente, y por lo tanto el conjunto* $\{U_{i_1}, U_{i_2}, \ldots, U_{i_r}\}$ *de las primeras filas correspondientes respectivamente a las RG-matrices* $G_{i_j}U$ *es linealmente independiente.*

La afirmación reciproca se demuestra de manera análoga.

□

Ahora bien, si el $\mathbf{rank}(U) = r$ y, $\{\underline{u}_{i_1}, \underline{u}_{i_2}, \ldots, \underline{u}_{i_r}\}$ es linealmente independiente, sigue del Lema 3.2, que $S\mathbf{u}$ es linealmente independiente. Además en esta situación se tiene que $\mathcal{C} = RG\mathbf{u}$, el ideal a derecha generado por $\mathbf{u}$.

3.3 Elementos de verificación

A lo largo de esta sección, consideramos (n, r)-códigos donde n y r son la longitud y dimensión de $\mathcal{C}$ respectivamente, además $r = \mathbf{rank}(U)$. La subsección 3.3.2 describe cómo obtener condiciones de verificación para los (n, k)-códigos donde $k < \mathbf{rank}(U)$.

Claramente, $\mathbf{cv} = \mathbf{0}$ para cualquier palabra código $\mathbf{c}$. La situación más conveniente es cuando el código $\mathcal{C}$ tiene un único elemento de verificación, es decir, que $\mathbf{y} \in \mathcal{C}$ es una palabra código si y sólo si $\mathbf{yv} = \mathbf{0}$.

3.3.1 Elementos de verificación

Definición 3.4. *Un divisor de cero* $\mathbf{u}$ *con el* $\mathbf{rank}(U) = r$*, es llamado* ***divisor de cero principal*** *si y sólo si existe* $\mathbf{v}$ *en RG tal que* $\mathbf{uv} = \mathbf{0}$ *y* $\mathbf{rank}(V) = n - r$.

Esta es la situación, por ejemplo, cuando RG es un dominio de ideales principales, que es el caso cuando G es un grupo cíclico como vimos en el Ejemplo 3.2.

Lo anterior también es posible en otros casos donde para un divisor cero dado $\mathbf{u}$ existe un $\mathbf{v}$ con $\mathbf{uv} = \mathbf{0}$ y $\mathbf{rank}(U) + \mathbf{rank}(V) = n$; por ejemplo si $\mathbf{u}^2 = \mathbf{0}$ o $\mathbf{uu}^T = \mathbf{0}$

y $\mathbf{rank}(U) = n/2$ entonces $\mathbf{rank}(U^T) = n/2$.

Supongamos que $\mathbf{uv} = \mathbf{0}$ y $\mathbf{rank}(V) = n - r$. Entonces $\mathbf{y}$ es una palabra código si y sólo si $\mathbf{yv} = \mathbf{0}$ si y sólo si $YV = 0_{n\times n}$. Esto no es inmediatamente obvio y depende del hecho de que U y V son RG-matrices; la prueba, en etapas, se muestra a continuación.

Lema 3.3. *Sea $\underline{y}$ la primera fila de una RG-matriz Y. Suponga V una RG-matriz. Entonces $YV = 0_{n\times n}$ si y sólo si $\underline{y}V = 0_{1\times n}$.*

Demostración. *Si $YV = 0_{n\times n}$ entonces claramente $\underline{y}V = 0_{1\times n}$.*

De otro lado, si $\underline{y}V = 0_{1\times n}$, entonces YV es una RG-matriz con la primera fila consistente de ceros, $YV = 0_{n\times n}$.

□

Teorema 3.2. *Sea $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$ donde W es generado por S tal que $S\mathbf{u}$ es linealmente independiente y $|S| = \mathbf{rank}(U) = r$. Supongamos además que $\mathbf{uv} = \mathbf{0}$ en el anillo de grupo RG de modo que $\mathbf{rank}(V) = n - r$, es decir, $\mathbf{u} \in RG$ es un divisor de cero principal. Entonces $\mathbf{y}$ es una palabra código si y sólo si $\mathbf{yv} = \mathbf{0}$.*

Demostración. $\Rightarrow$] *Si $\mathbf{y}$ es una palabra código entonces $\mathbf{y} = \mathbf{xu}$ para algún $\mathbf{x} \in W$ y así $\mathbf{yv} = \mathbf{xuv} = \mathbf{x0} = \mathbf{0}$.*

$\Leftarrow$] *Ahora bien, si $\mathbf{yv} = \mathbf{0}$, entonces dado que $\mathbf{uv} = \mathbf{0}$ en RG, se tiene $UV = 0_{n\times n}$ donde $\mathbf{rank}(U) = r$ y $\mathbf{rank}(V) = n - r$. Por definición el espacio nulo de V dado por $\eta(V) = \{\underline{x} : \underline{x}V = 0_{1\times n}\}$, es el conjunto de todos los vectores (fila) que anulan a V. Como el $\mathbf{rank}(V) = n - r$, del Teorema de la Dimensión, el rango de $\eta(V)$ es r. Dado que U tiene rango r, las filas de U generan el espacio nulo de V, $\eta(V)$.*

Una vez que $YV = 0_{n\times n}$, de la definición, las filas de Y pertenecen a $\eta(V)$ y por tanto, las filas de Y son combinaciones lineales de las filas de U. En particular, la primera fila de Y viene dada por $\underline{y} = \underline{q}U$ donde $\underline{q}$ es un vector $1 \times n$. Sea Q la RG-matriz cuya primera fila es $\underline{q}$; como sabemos las RG-matrices quedan totalmente definidas por su primera fila y así, QU es una RG matriz cuya primera fila es $\underline{y}$, la primera fila de Y. Por lo tanto, $Y = QU$. De esto, se sigue que $\mathbf{y} = \mathbf{qu}$ (donde $\mathbf{q}$ es el elemento de anillo de grupo correspondiente a la RG matriz Q).

Necesitamos mostrar que $\mathbf{qu} \in \mathcal{C}$. Sea $\mathbf{q} = \sum_{i=1}^{n} \alpha_i g_i$ y supongamos que g_j tiene coeficiente no nulo en dicha suma con $g_j \notin S$. Entonces $\{g_{i_1}\mathbf{u}, g_{i_2}\mathbf{u}, \ldots, g_{i_r}\mathbf{u}, g_j\mathbf{u}\}$ es linealmente dependiente por Teorema 3.1, donde los primeros r elementos son linealmente independientes. Así las cosas, existen escalares no todos ceros tales que $g_j\mathbf{u} = \sum_{k=1}^{r} \beta_k g_{i_k}\mathbf{u}$, es decir, $g_j\mathbf{u}$ es una combinación lineal de elementos de $S\mathbf{u}$ y por tanto $\mathbf{q} \in W$ y $\mathbf{y} \in \mathcal{C}$.

□

Corolario 3.2.1. *El código* $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$ *tiene un único elemento de verificación si y sólo si* $\mathbf{u}$ *es un divisor de cero principal.*

Demostración. $\Rightarrow$] *Sea* $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$ *un código generado por el divisor de cero* $\mathbf{u}$ *y el submódulo* W *de* RG *con un único elemento de verificación* $\mathbf{v} \in RG$*. Supongamos que el* $\mathbf{rank}(U) = r$ *y* $\mathbf{uv} = \mathbf{0}$*, luego* $UV = 0_{n\times n}$*. Por lo tanto* $V^T U^T = 0_{n\times n}$ *y* $\mathbf{rank}(U^T) = r$ *y de esta manera* $\mathbf{rank}(\eta(U^T)) = n-r$*, por el teorema de la dimensión.*

De la definición de rango basta considerar el caso $\mathbf{rank}(V^T) = m \geq n - r$*, es decir,* V^T *tiene* m *filas linealmente independientes,* $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_m$*.*

Si $m > n-r$*, de la igualdad* $V^T U^T = 0_{n\times n}$*, las filas de* V^T *pertenecen al espacio nulo* $\eta(U^T)$*, es decir,* $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_m \in \eta(U^T)$*, lo cual contradice que* $\mathbf{rank}(\eta(U^T)) = n - r$*.*

$\Leftarrow$] *Sea* $\mathbf{u}$ *un divisor de cero principal en* RG*, es decir, existe* $\mathbf{v} \in RG$ *tal que* $\mathbf{uv} = \mathbf{0}$ *y* $\mathbf{rank}(V) = n - r$*, luego por Teorema 4.2* $\mathbf{y}$ *es una palabra código si y sólo si* $\mathbf{yv} = \mathbf{0}$*, es decir,* $\mathbf{v}$ *es un elemento de verificación.*

Supongamos ahora que $\mathbf{v}$ *no es el único, es decir, existe* $\mathbf{z} \in RG$ *otro elemento de verificación para* $\mathcal{C}$*, luego* $\mathbf{y} \in \mathcal{C}$ *si y sólo si* $\mathbf{yz} = \mathbf{0}$*, es decir* $\mathbf{xuz} = \mathbf{0}$ *para todo* $\mathbf{x} \in W$*, por lo tanto* $\mathbf{uz} = \mathbf{0}$*.*

Por hipótesis tenemos que $\mathbf{uv} = \mathbf{0}$*, de ahí que* $UV = 0_{n\times n}$*, por lo tanto* $V^T U^T = 0_{n\times n}$*, es decir, las filas de* V^T *pertenecen a* $\eta(U^T)$*, y también tenemos que* $\mathbf{rank}(V) = n - r$*, luego* $\mathbf{rank}(V^T) = n - r$*, además como* $\mathbf{rank}(U) = r$ *entonces* $\mathbf{rank}(U^T) = r$*, por lo tanto* $\mathbf{rank}(\eta(U^T)) = n - r$*, y así las filas de* V^T *generan* $\eta(U^T)$*.*

Ahora como $\mathbf{uz} = \mathbf{0}$*, entonces* $UZ = 0_{n\times n}$*, por lo tanto* $Z^T U^T = 0_{n\times n}$*, así las filas de* Z^T *pertenecen a* $\eta(U^T)$*, entonces las filas de* Z^T *son combinaciones lineales de las filas de* V^T*, por lo tanto las filas de* Z *son combinaciones lineales de las filas de* Z*, entonces* $\mathbf{w}$ *es un múltiplo escalar de* $\mathbf{v}$*.*

□

3.3.2 Condiciones generales de verificación

En esta sección el espacio nulo de U será $\eta(U) = \{\underline{x} : U\underline{x} = 0_{n\times 1}\}$ donde $\underline{x}$ es un vector $n \times 1$. Dado que U tiene rango r, del Teorema de la Dimensión, el rango de $\eta(U)$ es $n - r$. Sea $\{\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_{n-r}\}$ una base para $\eta(U)$; donde los $\underline{v}_i$ son vectores columna $n \times 1$. Sea V_i la RG-matriz con primera columna $\underline{v}_i$. Claramente $UV_i = 0_{n\times n}$ para $1 \leq i \leq n - r$ dado que UV_i es la RG-matriz con la primera fila consistente de ceros, y así debe ser la matriz $0_{n\times n}$. Así las cosas, $\mathbf{uv}_i = \mathbf{0}$ donde $\mathbf{v}_i$ es el elemento de anillo de grupo correspondiente a la RG-matriz V_i.

Note que el espacio nulo de U se obtiene fácil y rápidamente usando operaciones lineales sobre las filas de U. La base para el espacio nulo puede leerse de la forma escalonada reducida de U, que también da al generador en su forma estándar. La forma escalonada reducida también permite producir una matriz de verificación para la correspondiente codificación $R^r \to R^n$.

Así, si $\mathbf{y}$ es una palabra código, entonces $\mathbf{y}\mathbf{v}_i = \mathbf{0}$ para $1 \leq i \leq n-r$. Siguiendo una demostración similar a la del Teorema 4.2 obtenemos el siguiente resultado.

Teorema 3.3. *Suponga* $\mathbf{u}$ *es un divisor de cero,* $\mathbf{rank}(U) = r$ *y* W *es generado por* S *con* r *elementos tal que* $S\mathbf{u}$ *es linealmente independiente. Sea* $\mathbf{v}_i$ *definido como arriba. Entonces* $\mathbf{y} \in \mathcal{C}$ *si y sólo si* $\mathbf{y}\mathbf{v}_i = \mathbf{0}$ *para todo* $1 \leq i \leq n-r$. *Más aún* $\mathbf{y}$ *es una palabra código si y sólo si* $YV_i = 0_{n\times n}$.

No son necesarios todos los $\mathbf{v}_i$, solo los suficientes para que las correspondientes matrices V_i contengan una base para el espacio nulo. En muchos casos, se puede encontrar un V_i particular de rango $n-r$.

3.4 Códigos dual y auto-dual

Por definición, el dual de un código $\mathcal{C}$, denotado por $\mathcal{C}^\perp$, considerado como vectores sobre R^n es su complemento ortogonal, es decir $\mathcal{C}^\perp = \{v \in R^n : v \cdot u = 0, \forall u \in \mathcal{C}\}$.

Sean $\mathbf{x} = \sum_{g\in G} \alpha_g g$, $\mathbf{y} = \sum_{h\in G} \beta_h h \in RG$. El producto interno o punto de $\mathbf{x}$ e $\mathbf{y}$ es dado por la expresión

$$\mathbf{x} \cdot \mathbf{y} = \sum_{g,h\in G} \alpha_g \beta_h.$$

Así, el dual de un código a partir de una codificación de anillo de grupo viene dada por

$$\mathcal{C}^\perp = \{\mathbf{y} \in RG : \mathbf{y} \cdot (\mathbf{x}\mathbf{u}) = \mathbf{0}, \forall \mathbf{x} \in W\}.$$

En el caso de un código divisor de cero tenemos.

Teorema 3.4. *Sean* $\mathbf{u}, \mathbf{v} \in RG$, *con* U *y* V *sus* RG*-matrices y tales que* $\mathbf{uv} = \mathbf{0}$, $\mathbf{rank}(U) = r$ *y* $\mathbf{rank}(V) = n-r$. *Sea* W *un submódulo de* RG *con base* $S \subset G$ *de dimensión* r *tal que* $S\mathbf{u}$ *es linealmente independiente y denótese por* $W^\perp$ *el submódulo de* RG *con base* $G \setminus S$. *Entonces el código* $\mathcal{C} = \{\mathbf{x}\mathbf{u} : \mathbf{x} \in W\}$ *tiene código dual* $\mathcal{C}^\perp = \{\mathbf{x}\mathbf{v}^T : \mathbf{x} \in W^\perp\} = \{\mathbf{y} \in RG : \mathbf{y}\mathbf{u}^T = \mathbf{0}\}$.

Demostración. *Note que* $\mathbf{v}^T$ *es un divisor de cero, que* $\mathbf{rank}(V^T) = n-r$ *y que* $W^\perp$ *no contiene un divisor de cero de* $\mathbf{v}^T$, *ver Sección 3.1. Así, hay una aplicación* $1-1$ *entre los conjuntos* $W^\perp$ *y* $\{\mathbf{x}\mathbf{v}^T : \mathbf{x} \in W^\perp\}$.

Resta mostrar que este último es el dual de $\mathcal{C}$.

Sea $\mathbf{z} \in RG$ *no nulo.*

Afirmación: $\mathbf{xu} \cdot \mathbf{z} = \mathbf{0}$, *para todo* $\mathbf{x} \in W$ *si y sólo si* $\mathbf{z} = \mathbf{yv}^T$ *para algún* $\mathbf{y} \in W^{\perp}$.

Suponga $\mathbf{z} = \mathbf{yv}^T$ *y sean* $\mathbf{x}, \mathbf{y} \in RG$.

Recuerde que $\underline{x} = \psi^{-1}(\mathbf{x}), \underline{y} = \psi^{-1}(\mathbf{y})$ *son los vectores en* R^n *correspondientes a* $\mathbf{x}$ *e* $\mathbf{y}$. *Así*

$$\mathbf{xu} \cdot \mathbf{z} = \mathbf{xu} \cdot \mathbf{yv}^T = \underline{x}U(\underline{y}V^T)^T = \underline{x}(UV)\underline{y}^T = \mathbf{0}.$$

Recíprocamente, suponga que $\mathbf{xu} \cdot \mathbf{z} = \mathbf{0}$, *para todo* $\mathbf{x} \in W$. *Sin pérdida de generalidad, supongamos* $\mathbf{1} \in W$.

Entonces $\mathbf{u} \cdot \mathbf{z} = \mathbf{0}$ *implica* $\mathbf{zu}^T = \mathbf{0}$ *y como* $\mathbf{u}^T$ *es el elemento de verificación para el código generado por,* $\mathbf{v}^T$, $\mathbf{z} = \mathbf{yv}^T$ *para algún* $\mathbf{y} \in W^{\perp}$.

□

Como una consecuencia tenemos en el caso de códigos auto-duales que:

Corolario 3.4.1. $\mathcal{C}^{\perp} = \mathcal{C}$ *si y sólo si* $\mathbf{uu}^T = \mathbf{0}$ *y* $\mathbf{rank}(U) = n/2$.

Demostración. $\Rightarrow$] *Supongamos* $\mathcal{C}^{\perp} = \mathcal{C}$, *y sea* $\mathbf{y} \in \mathcal{C}$, *es decir,* $\mathbf{y} = \mathbf{xu}$ *para* $\mathbf{x} \in W$. *De la hipótesis,* $\mathbf{y} \cdot (\mathbf{xu}) = \mathbf{0}$, *para todo* $\mathbf{x} \in W$, *así*

$$\mathbf{y} \cdot (\mathbf{xu}) = \mathbf{0},$$

$$(\mathbf{xu}) \cdot (\mathbf{xu}) = \mathbf{0},$$

$$\mathbf{xu}(\mathbf{xu})^T = \mathbf{0},$$

$$\mathbf{xuu}^T\mathbf{x}^T = \mathbf{0},$$

para todo $\mathbf{x} \in W$. *Por lo tanto* $\mathbf{uu}^T = \mathbf{0}$.

De la definición de rango basta considerar el caso $\mathbf{rank}(U) = r \geq n/2$, *es decir, U tiene r filas linealmente independientes,* $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_r$, *además* $\mathbf{rank}(U^T) = r$ *y por lo tanto* $\mathbf{rank}(\eta(U^T)) = n - r$, *por el teorema de la dimensión.*

Si $r > n/2$ *entonces* $-r < -n/2$, *y así* $n - r < n - n/2 = n/2$. *De la igualdad* $\mathbf{uu}^T = \mathbf{0}$ *tenemos que* $UU^T = 0_{n \times n}$, *y por lo tanto* $\underline{u}_1, \underline{u}_2, \ldots, \underline{u}_r \in \eta(U^T)$, *lo cual contradice que* $\mathbf{rank}(\eta(U^T)) = n - r < n/2$.

$\Leftarrow$] *Sea* $\mathbf{uu}^T = \mathbf{0}$ *tal que* $\mathbf{rank}(U) = \mathbf{rank}(U^T) = n/2$. *Se sigue que* $\mathbf{u}$ *es un divisor de cero principal, y así del Corolario 3.2.1* $\mathbf{u}^T$ *es el único elemento de verificación, por lo tanto de la Definición 3.1* $\mathcal{C} = \{\mathbf{y} \in RG : \mathbf{yu}^T = \mathbf{0}\}$.

Finalmente del Teorema 3.4 tenemos que $\mathcal{C}^{\perp} = \{\mathbf{y} \in RG : \mathbf{y}\mathbf{u}^T = \mathbf{0}\}$, *así,* $\mathcal{C} = \mathcal{C}^{\perp}$.

□

De los resultados anteriores, un código divisor de cero auto-dual es un código obtenido del divisor de cero $\mathbf{u}$ con $\mathbf{u}\mathbf{u}^T = \mathbf{0}$ y $\mathbf{rank}(U) = n/2$. Diremos que un código obtenido de $\mathbf{u}$ es de auto-verificación si $\mathbf{u}^2 = \mathbf{0}$, en cuyo caso es equivalentemente auto-dual, dado que el código y su dual son equivalentes.

Ejemplo 3.3.

Teniendo presente los resultados anteriores, podemos obtener códigos auto-duales en RG de la siguiente manera. Suponga que $|G| = n = 2m$ *y* $G = \{g_1, g_2, \ldots, g_n\}$. *Si* $\mathbf{u} \in RG$ *satisface*

i) $\mathbf{u}^2 = \mathbf{0}$,
ii) $\mathbf{u} = \mathbf{u}^T$, *luego* $\mathbf{u}\mathbf{u}^T = \mathbf{0}$,
iii) $rank(U) = m$.

Entonces $\mathbf{u}$ *genera un código auto-dual. Veamos dos ejemplos específicos.*

1) Sea $G = C_2 \times C_4$ *donde* $C_4 = \langle a : a^4 = 1\rangle$ *y* $C_2 = \langle h : h^2 = 1\rangle$. *Consideremos el anillo de grupo* $\mathbb{Z}_2G$ *donde un elemento genérico es*

$$1 + a + a^2 + a^3 + h + ha + ha^2 + ha^3.$$

Sea $\mathbf{u} = 1 + h(a + a^2 + a^3)$ *elemento en este anillo. Entonces,*

$$\mathbf{u}^2 = 1 + h^2(a^2 + a^4 + a^6) = 1 + a^2 + 1 + a^2 = 0,$$
$$\mathbf{u}^T = 1^{-1} + (ha)^{-1} + (ha^2)^{-1} + (ha^3)^{-1} = 1 + ha^3 + ha^2 + ha = \mathbf{u}$$

Así, $rank(U) \leq 4$ *y la RG-matrix de* $\mathbf{u}$ *está dada por* $U = \begin{pmatrix} I & B \\ B & I \end{pmatrix}$ *de lo cual se sigue que* $rank(U) = 4$.

Algunos cálculos en $\mathbb{Z}_2G$ *nos llevan a que los elementos en* $\mathbb{Z}_2G\mathbf{u}$ *son:*

$$\{0, 1 + a + a^2 + ha^3, 1 + a + a^3 + ha^2, 1 + a + h + ha, 1 + a^2 + a^3 + ha,$$
$$1 + a^2 + h + ha^2, 1 + a^3 + h + ha^3, 1 + ha + ha^2 + ha^3, a + a^2 + a^3 + h,$$
$$a + a^2 + ha + ha^2, a + a^3 + ha + ha^3, a + h + ha^2 + ha^3, a^2 + a^3 + ha^2 + ha^3,$$
$$a^2 + h + ha + ha^3, a^3 + h + ha + ha^2, 1 + a + a^2 + a^3 + h + ha + ha^2 + ha^3\}$$

Para el cálculo de la distancia $d(\mathcal{C})$, *haremos uso de la Tabla 3.1 donde* $\mathbf{a}_i$ *en la vertical representa alguno de los elementos en* $\mathcal{C} = \mathbb{Z}_2G\mathbf{u}$.

Como se puede ver en la Tabla 3.1 $d(\mathbf{a}_i, \mathbf{a}_j) \geq 4$, $i \neq j$. *Luego* $d(\mathcal{C}) = 4$ *y así tenemos un* $(8, 4, 4)$ *código que debe coincidir con el código auto-dual extendido de Hamming.*

	1	a	a^2	a^3	h	ha	ha^2	ha^3
$\mathbf{a}_0$	0	0	0	0	0	0	0	0
$\mathbf{a}_1$	1	1	1	0	0	0	0	1
$\mathbf{a}_2$	1	1	0	1	0	0	1	0
$\mathbf{a}_3$	1	1	0	0	1	1	0	0
$\mathbf{a}_4$	1	0	1	1	0	1	0	0
$\mathbf{a}_5$	1	0	1	0	1	0	1	0
$\mathbf{a}_6$	1	0	0	1	1	0	0	1
$\mathbf{a}_7$	1	0	0	0	0	1	1	1
$\mathbf{a}_8$	0	1	1	1	1	0	0	0
$\mathbf{a}_9$	0	1	1	0	0	1	1	0
$\mathbf{a}_{10}$	0	1	0	1	0	1	0	1
$\mathbf{a}_{11}$	0	1	0	0	1	0	1	1
$\mathbf{a}_{12}$	0	0	1	1	0	0	1	1
$\mathbf{a}_{13}$	0	0	1	0	1	1	0	1
$\mathbf{a}_{14}$	0	0	0	1	1	1	1	0
$\mathbf{a}_{15}$	1	1	1	1	1	1	1	1

Tabla 3.1: Elementos en $\mathbb{Z}_2 G\mathbf{u}$

2) ***El código binario extendido de Golay***. *Consideremos el anillo de grupo* $\mathbb{Z}_2 D_{24}$ *con* $D_{24} = \langle a, b : a^2 = 1 = b^{12}, ab = b^{-1}a \rangle$ *el grupo dihedral de orden* 24. *El código se puede construir utilizando cualquiera de los dos siguientes divisores de cero:*

$$\mathbf{u} = 1 + a(b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9), \ y$$
$$\mathbf{v} = 1 + a(b^3 + b^5 + b^6 + b^7 + b^8 + b^{10} + b^{11}).$$

Usaremos el primer divisor cero. Todos los resultados y propiedades dados a continuación son válidos para el segundo.

Como se menciona en [9], "Los divisores de cero anteriores fueron descubiertos por búsqueda computacional usando GAP [4]." Los autores escribieron un programa para buscar todos los anillos de grupo sobre $\mathbb{Z}_2$ *con grupos de orden veinticuatro. La búsqueda fue orientada a divisores de cero de rango doce y que genere un código con distancia mínima ocho. Treinta y seis mil ochocientos sesenta y cuatro de tales divisores de cero se encontraron en el anillo de grupo dihedral.*

De estos, veinticuatro tienen la forma $1 + a\mathbf{x}$, *donde* $\mathbf{x}$ *es una suma de potencias del elemento de grupo* b, *similares a* $\mathbf{u}$ *y* $\mathbf{v}$ *anteriores. Para el caso de* $\mathbf{u}$ *y* $\mathbf{v}$ *tenemos*

$$\mathbf{u} = 1 + a\mathbf{d} \quad y \quad \mathbf{v} = 1 + a\mathbf{f}.$$

Curiosamente, los otros veintidós tienen la forma $1 + a(b^i)\mathbf{d}$ *y* $1 + a(b^i)\mathbf{f}$ *para* $1 \leq i \leq 11$. *Como es claro* $\mathbf{d}$ *y* $\mathbf{f}$ *son elementos del anillo de grupo, y así usando la definición de trasposición dada en la Sección 2.1,*

$$\mathbf{d}^T = (b^{-1}+b^{-2}+b^{-4}+b^{-5}+b^{-6}+b^{-7}+b^{-9}) = b^3+b^5+b^6+b^7+b^8+b^{10}+b^{11} = \mathbf{f}.$$

Como veremos a continuación el cálculo de la distancia mínima del código asociado con el elemento $\mathbf{u}$ *es bastante sencillo.*

Para tal efecto usaremos la lista $D_{24} = \{1, b, b^2, \ldots, b^{11}, a, ab, ab^2, \ldots, ab^{11}\}$. *De esta lista, las RG matrices de todos los elementos son de la forma:*

$$\begin{bmatrix} X & Y \\ Y & X \end{bmatrix},$$

donde X *e* Y *son respectivamente matriz circulante y circulante inversa. La submatriz* X *contiene los coeficientes de los elementos de grupo de la forma* b^i *para* $0 \leq i \leq 11$. *Del mismo modo, en* Y *aparecen los coeficientes de* ab^i.

En el caso de $\mathbf{u} = 1 + a(b + b^2 + b^4 + b^5 + b^6 + b^7 + b^9)$, *su RG-matriz* U *viene dada por:*

$$U = \begin{bmatrix} I & A \\ A & I \end{bmatrix},$$

donde $I = I_{12}$ *es la matriz identidad de orden* 12 *y la matriz* A *de orden* 12×12 *viene dada por:*

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Para la auto-dualidad de $\mathbf{u}$, *veamos que* $\mathbf{u}$ *genera un código auto-dual, usando las condiciones anteriormente mencionadas,*

$$\mathbf{u} = \mathbf{u}^T, \mathbf{u}^2 = \mathbf{0} \quad y \quad rank(U) = |D_{24}|/2.$$

Ahora calculemos $\mathbf{u}^T$ *y comparémoslo con* $\mathbf{u}$*. En efecto, cada elemento de la forma* ab^i *en* D_{24} *es su propio inverso, dado que*

$$\begin{aligned} ab^iab^i &= b^{-1}ab^{i-1}ab^i \\ &= b^{-2}ab^{i-2}ab^i \\ &\vdots \\ &= b^{-i}aab^i = 1. \end{aligned}$$

Así las cosas,

$$\mathbf{u}^T = (1)^{-1}+(ab)^{-1}+(ab^2)^{-1}+(ab^4)^{-1}+(ab^5)^{-1}+(ab^6)^{-1}+(ab^7)^{-1}+(ab^9)^{-1} = \mathbf{u},$$

de donde sigue directamente que $U = U^T$*.*

Ahora bien,

$$\mathbf{u}^2 = (1+ad)^2 = 1^2 + 2ad + (ad)^2 = 1 + adad = 1 + a^2d^Td = 1 + d^Td,$$

donde $d = b+b^2+b^4+b^5+b^6+b^7+b^9$*. La condición* $1+d^Td = 0$ *que necesitamos, se cumple si y sólo si* $d^Td = (b^{11}+b^{10}+b^8+b^7+b^6+b^5+b^2)(b+b^2+b^4+b^5+b^6+b^7+b^9) = 1$*, lo cual es cierto. Así las cosas,* $\mathbf{u}^2 = \mathbf{0}$*.*

Veamos que la dimensión del código es doce. La dimensión del código generado por $\mathbf{u}$ *es el rango de su RG-matriz* U*. Como vimos* $\mathbf{u}^2 = 0$*, lo que implica que* $U^2 = 0_{24\times 24}$*, la matriz nula de veinticuatro por veinticuatro. Esto implica que el rango de* $\eta(U)$ *es mayor o igual que el rango de* U*. Por lo tanto, el rango de* U *es a lo más doce. Dado que* U *tiene la matriz identidad de orden* 12 *en su parte superior izquierda, su rango es al menos doce. Así las cosas* $rank(U) = 12$*.*

Por tanto el código generado por $\mathbf{u}$ *es auto-dual de dimensión* 12*. Nos falta por determinar su distancia mínima.*

La forma estándar de la matriz generadora de un código sobre un anillo de grupo es la RG-matriz en forma escalonada reducida. Como vimos la RG-matriz U *es de rango* 12 *y sus primeras doce filas consisten de la matriz de identidad de orden* 12 *y la matriz* A *descrita arriba. Por tanto, la matriz* $G = [I|A]$ *es la matriz generadora de nuestro código. Nuestra construcción ha creado* G *en forma estándar. Como vemos, la primera fila de* G *es de peso ocho, y por construcción las restantes filas son simplemente una permutación de esta primera fila. Así, todas las filas de*

G son de peso ocho.

Ahora, dado que el código generado por $\mathbf{u}$ *es auto-dual este es auto-ortogonal. Es bien sabido que cualquier código auto-ortogonal generado por una matriz cuyas filas son todas de pesos divisibles por cuatro solo contiene palabras código de peso congruente a cero módulo cuatro (ver [11]). Por tanto, cada palabra código en el código generado por* $\mathbf{u}$ *tiene peso congruente a cero módulo cuatro.*

Es claro que cualquier combinación de n filas de la matriz identidad tiene exactamente peso n. La matriz G contiene la matriz identidad I y, por tal motivo, cualquier combinación de n filas de G tiene un peso al menos n. Así, cada combinación de cinco filas o más de G tiene un peso mayor a cuatro.

Además, como ya vimos cada fila de G tiene un peso de ocho. Por lo tanto, solo necesitamos mostrar que ninguna combinación de dos a cuatro filas de G tiene un peso de cuatro.

Así, $G = [I|A]$ *y cada suma de n filas de I tiene peso n. Usando estos hechos podemos reducir nuestro argumento para probar que ninguna combinación de dos a cuatro filas de G tiene peso cuatro.*

Ninguna suma de ninguna cantidad (aparte de cero) de filas de A suman cero ya que es de rango completo. Esto se deduce del hecho de que $U^2 = 0$*. Usando multiplicación por bloques tenemos:*

$$\begin{aligned} U^2 &= \begin{bmatrix} I & A \\ A & I \end{bmatrix} \begin{bmatrix} I & A \\ A & I \end{bmatrix} \\ &= \begin{bmatrix} I + A^2 & A + A \\ A + A & I + A^2 \end{bmatrix} = 0_{24\times 24} \\ &\Rightarrow I + A^2 = 0_{12\times 12} \\ &\Rightarrow A^2 = I \end{aligned}$$

Por lo tanto, A es su propia inversa y, en particular, es de rango completo doce.

Esto concluye la prueba de que G genera un código con distancia mínima de ocho. Por lo tanto, de la unicidad, este es el código binario extendido de Golay [14].

Como vemos, el código binario extendido de Golay puede ser construido a partir de un divisor de cero en un anillo de grupo, así, es posible usarlo en el marco ofrecido por anillos de grupo.

Capítulo 4

Códigos de unidades

En este capítulo, se construyen códigos a partir de unidades en anillos de grupo. Sea $\mathbf{u}$ una unidad en RG, donde $G = \{g_1, g_2, \ldots, g_n\}$. Sea W un submódulo de RG generado (como un R-módulo) por r elementos de grupo $S = \{g_{k_1}, g_{k_2}, \ldots, g_{k_r}\}$ con $r < n$.

Como se definió en la Sección 2.2, el código derivado de unidad $\mathcal{C} = \{\mathbf{ux} : \mathbf{x} \in W\}$ o $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$, se construye así a partir de una unidad $\mathbf{u}$, un submódulo W, y, cuando RG es no conmutativo se elige una codificación a izquierda o derecha. En lo que sigue trabajaremos con codificación a derecha ($\mathbf{x} \mapsto \mathbf{xu}$). El caso de codificación a izquierda ($\mathbf{x} \mapsto \mathbf{ux}$) es análogo.

Ahora $\mathbf{c}$ es una palabra código (es decir, $\mathbf{c}$ pertenece a $\mathcal{C}$) si y sólo si $\mathbf{cu}^{-1} \in W$, es decir, si y sólo si los coeficientes de elementos en $G \setminus S$ en la representación de $\mathbf{cu}^{-1}$ son cero. Como lo vemos multiplicar una palabra código por el inverso de la unidad permite recuperar la entrada original.

Un código derivado de unidad también puede ser considerado como una aplicación de R^r en R^n. Primero, el vector $\underline{x} = (\alpha_1, \alpha_2, \ldots, \alpha_r) \in R^r$ es enviado vía $\lambda_W(\underline{x}) = \sum_{i=1}^{r} \alpha_i g_{k_i}$ a un elemento $\mathbf{x} \in W$. Así se obtiene una palabra código $\mathbf{xu} \in \mathcal{C}$ que puede ser escrita por $\mathbf{xu} = \sum_{i=1}^{n} \beta_i g_i$. Esto da una codificación $\mathbf{x} \mapsto (\beta_1, \beta_2, \ldots, \beta_n)$ la cual es la aplicación de $R^r \to R^n$ deseada.

También asociamos a cada código derivado de unidad un código equivalente $\mathcal{D}$ llamado **código matricial generado**. Este es un código de R^r en R^n que tiene una matriz generadora $r \times n$ extraída de la RG-matriz U y una matriz de verificación que se extrae de U^{-1}. Si A es tal matriz generadora, entonces $\mathcal{D} = \{\underline{x}A : \underline{x} \in R^r\}$. La distinción entre los códigos $\mathcal{C}$ y $\mathcal{D}$ es de conveniencia. Como son equivalentes, cualquier implementación práctica funciona en la producción de $\mathcal{D}$ o $\mathcal{C}$ directamente, dependiendo de lo que se desee.

4.1 Matrices generadora y de verificación

Examinemos ahora las matrices generadora y de verificación que resultan de un código derivado de una unidad. Supongamos $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$ en el anillo de grupo y sean U y U^{-1} las correspondientes RG-matrices de orden n.

Primero, considere W el submódulo generado por $\{g_1, g_2, \ldots, g_r\}$ con $r < n$ (es decir, tiene como base los primeros r elementos en la lista elegida de G). El caso en que W tiene una base general de elementos de grupo puede ser tratado de una manera similar. De la definición de W un elemento $x \in W$ tiene la forma

$$\mathbf{x} = \sum_{i=1}^{r} \alpha_i g_i.$$

Dividiendo las matrices U y U^{-1} en matrices por bloque en la forma

$$U = \begin{pmatrix} A \\ B \end{pmatrix} \quad \text{y} \quad U^{-1} = \begin{pmatrix} C & D \end{pmatrix},$$

donde los órdenes de A y B son respectivamente $r \times n$ y $(n-r) \times n$ y, los de C y D son $n \times r$ y $n \times (n-r)$.

Ahora, como $UU^{-1} = I$ entonces $AD = 0$. Es fácil ver que A es una matriz generadora para el código matricial generado. A continuación mostramos que D^T es una matriz de verificación:

Teorema 4.1. *Sean $\underline{y} \in R^n$ y $\mathcal{D} = \{\underline{x}A : \underline{x} \in R^r\}$. Entonces $\underline{y} \in \mathcal{D}$ si y sólo si $\underline{y}D = 0$.*

Demostración. *Si $\underline{y} = \underline{x}A$ para un cierto $\underline{x} \in R^r$, entonces claramente, $\underline{y}D = \underline{x}(AD) = 0$.*

De otro lado, si $\underline{y}D = 0$,

$$\underline{y} = \underline{y}U^{-1}U = \underline{y}\begin{pmatrix} C & D \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \underline{y}C & \underline{y}D \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \underline{y}C & 0 \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \underline{y}CA.$$

Ahora $\underline{y}C$ pertenece a R^r, y por tanto $\underline{y} = \underline{y}U^{-1}U = \underline{x}A$ para algún $\underline{x} \in R^r$ como se requería.

□

Del último resultado $\underline{y} \in \mathcal{D}$ si y sólo si $\underline{y}D = 0$, lo que equivale a decir que $D^T\underline{y}^T = 0$ y por lo tanto, $\underline{y} \in \mathcal{D}$ si y sólo si $\underline{y}D = 0$ si y sólo si $D^T\underline{y}^T = 0$. Note que la matriz generadora A de orden $r \times n$ y la matriz de verificación D^T de orden $(n-r) \times n$ producidas desde la unidad $\mathbf{u}$ y el submódulo W tienen rango completo permitido, r y $n-r$ respectivamente.

Dado que una unidad $\mathbf{u}$ en un anillo de grupo se asocia a una matriz no singular U, podemos construir códigos desde unidades. Es claro que cualquier matriz no singular produce un código usando los argumentos arriba mencionados, solo que en este caso no es posible explotar la estructura algebraica del anillo de grupo.

Cuando W es generado por una base general, $S = \{g_{k_1}, g_{k_2}, \ldots, g_{k_r}\}$, las matrices generadora y de verificación son obtenidas borrando y adicionando ciertas filas y columnas de U y U^{-1}. Una matriz generadora resulta de la matriz $r \times n$ que consiste en las filas $k_1, k_2, \ldots, k_r$ de U. Además, sea D la matriz $(n-r) \times n$ obtenida borrando las columnas $k_1, k_2, \ldots, k_r$ de U^{-1} y así, D^T es una matriz de verificación.

4.2 Construcción de códigos derivados de unidad

Las matrices generadora y de verificación para el código matricial generado $\mathcal{D}$ son inmediatas de la construcción. Sin embargo, trabajar con el código derivado de unidad $\mathcal{C}$ directamente puede ser ventajoso. Por ejemplo, usar las condiciones de verificación del anillo de grupo directamente puede ser el mejor método para decodificar.

En resumen, el código derivado de unidad de longitud n y dimensión r puede construirse de manera relativamente sencilla como sigue. Elija un grupo G de orden n y un anillo R sobre el cual se definirá el código. Normalmente, R es un cuerpo pero esto no es un requisito; códigos sobre el anillo de los enteros, anillos de matrices u otros anillos son también útiles.

Tomando una unidad $\mathbf{u}$ y su inverso $\mathbf{u}^{-1}$ en el anillo de grupo RG. Como se ha demostrado anteriormente, en el Capítulo 2, si R es un cuerpo o RG es de orden finito, cada elemento en RG es un divisor cero o una unidad. Los anillos de grupo RG son ricos en unidades.

En general, cualquier conjunto de r elementos del grupo asocia un submódulo W, el cual generara un código; en particular, los primeros r elementos $\{g_1, g_2, \ldots, g_r\}$ de acuerdo con una lista de G sirven para tal efecto.

Puede resultar ventajoso escoger otra (apropiada) base , con el propósito de incrementar la distancia mínima del código u optimizar algún otro de sus parámetros. Esta libertad en la escogencia de la base conduce al concepto de **base óptima** para una unidad dada $\mathbf{u} \in RG$ y dimensión r, llamada la mejor base:

$$\arg\max_{S \subset G, |S|=r} \min_{\mathbf{x} \in W(S)} wt(\mathbf{xu}), \qquad (*)$$

donde $W(S)$ denota el submódulo generado por S, $wt(\mathbf{xu})$ el número de coeficientes distintos de cero de $\mathbf{xu}$ y la función arg max, está definida de la siguiente manera:

$\arg\max_{x\in A} f(x) =: \left\{x \in A : f(x) = \max_{y\in A} f(y)\right\}$, es decir, el conjunto de elementos de A que son máximos globales en A. Por lo tanto para nuestro caso $(*)$ nos da el $S \subset G$, con $|S| = r$, tal que $\min_{\mathbf{x}\in W(S)} wt(\mathbf{xu})$ sea máximo, es decir, el peso minimo de $\mathcal{C}$ sea máximo.

Esta flexibilidad en la elección de r y W son las principales ventajas de un código derivado de una unidad sobre un código divisor de cero.

Ejemplo 4.1.

En el anillo de grupo $\mathbb{Z}_2G$, si $\mathbf{v}^2 = 0$, entonces $(1+\mathbf{v})^2 = 1$. Consideremos el anillo de grupo $\mathbb{Z}_2C_{2n}$ con $C_{2n} = \langle g : g^{2n} = 1\rangle$, sea $\mathbf{v}_i = g^i + g^{n-i} + g^{n+i} + g^{2n-i} \in \mathbb{Z}_2C_{2n}$.

Entonces,

$$\begin{aligned}\mathbf{v}_i^2 &= (g^i)^2 + (g^{n-i})^2 + (g^{n+i})^2 + (g^{2n-i})^2\\ &= g^{2i} + g^{2n-2i} + g^{2n+2i} + g^{4n-2i}\\ &= g^{2i} + g^{2n}g^{-2i} + g^{2n}g^{2i} + g^{4n}g^{-2i}\\ &= g^{2i} + g^{-2i} + g^{2i} + g^{-2i} = \mathbf{0},\end{aligned}$$

y

$$\mathbf{v}_i^T = (g^i)^{-1} + (g^{n-i})^{-1} + (g^{n+i})^{-1} + (g^{2n-i})^{-1} = g^{2n-i} + g^{n+i} + g^{n-i} + g^i = \mathbf{v}_i.$$

Por lo tanto todos los $\mathbf{v}$, que son combinaciones de los $\mathbf{v}_i$'s, satisfacen que $\mathbf{v}^2 = \mathbf{v}\mathbf{v}^T = \mathbf{0}$. Finalmente, $\mathbf{u} = \mathbf{1} + \mathbf{v}$ satisface que $\mathbf{u}^2 = \mathbf{u}\mathbf{u}^T = \mathbf{1}$ y da una serie de unidades ortogonales. Como ya vimos, no hay problemas de rango ya que estos son códigos derivados de unidades.

Un ejemplo específico de lo anterior es el siguiente: tomando $n = 7$ tenemos el anillo de grupo $\mathbb{Z}_2C_{14}$ con $C_{14} = \langle g : g^{14} = 1\rangle$, si tomamos $i = 2$, entonces $\mathbf{v}_2 = g^2 + g^5 + g^9 + g^{12}$ y por lo tanto

$$\mathbf{u} = 1 + \mathbf{v}_2 = 1 + g^2 + g^5 + g^9 + g^{12},$$

satisface que $\mathbf{u}^2 = \mathbf{u}\mathbf{u}^T = \mathbf{1}$. Ahora bien, tomando el submódulo W dado por

$$W = \left\{\sum_{i=0}^{13}\alpha_i g^i : \alpha_i \in \mathbb{Z}_2, \sum_{i=0}^{13}\alpha_i = 0\right\},$$

algunos cálculos de multiplicar elementos de W por $\mathbf{u}$ son:

$$\begin{aligned}(1+g^7)\mathbf{u} &= \mathbf{u} + g^7\mathbf{u}\\ &= 1 + g^2 + g^5 + g^9 + g^{12} + g^7 + g^9 + g^{12} + g^{16} + g^{19}\\ &= 1 + g^2 + g^5 + g^9 + g^{12} + g^7 + g^9 + g^{12} + g^2 + g^5\\ &= 1 + g^7,\end{aligned}$$

$$\begin{aligned}(g^2+g^5+g^9+g^{12})\mathbf{u} &= g^2\mathbf{u}+g^5\mathbf{u}+g^9\mathbf{u}+g^{12}\mathbf{u}\\ &= g^2+g^4+g^7+g^{11}+g^{14}+g^5+g^7+g^{10}+g^{14}+g^{17}+\\ &\quad g^9+g^{11}+g^{14}+g^{18}+g^{21}+g^{12}+g^{14}+g^{17}+g^{21}+g^{24}\\ &= g^2+g^4+g^7+g^{11}+1+g^5+g^7+g^{10}+1+g^3+\\ &\quad g^9+g^{11}+1+g^4+g^7+g^{12}+1+g^3+g^7+g^{10}\\ &= g^2+g^5+g^9+g^{12},\end{aligned}$$

$$\begin{aligned}(g^3+g^4+g^6+g^8+g^{10}+g^{11})\mathbf{u} &= g^3\mathbf{u}+g^4\mathbf{u}+g^6\mathbf{u}+g^8\mathbf{u}+g^{10}\mathbf{u}+g^{11}\mathbf{u}\\ &= g^3+g^5+g^8+g^{12}+g^{15}+g^4+g^6+g^9+\\ &\quad g^{13}+g^{16}+g^6+g^8+g^{11}+g^{15}+g^{18}+g^8\\ &\quad +g^{10}+g^{13}+g^{17}+g^{20}+g^{10}+g^{12}+g^{15}+g^{19}\\ &\quad +g^{22}+g^{11}+g^{13}+g^{16}+g^{20}+g^{23}\\ &= g^3+g^5+g^8+g^{12}+g+g^4+g^6+g^9\\ &\quad +g^{13}+g^2+g^6+g^8+g^{11}+g+g^4+g^8\\ &\quad +g^{10}+g^{13}+g^3+g^6+g^{10}+g^{12}+g+g^5\\ &\quad +g^8+g^{11}+g^{13}+g^2+g^6+g^9\\ &= g+g^{13}.\end{aligned}$$

De manera análoga para los demás elementos de W, se obtiene que $W\mathbf{u}=W$, y por lo tanto el código $\mathcal{C}$ es

$$\mathcal{C}=\left\{\sum_{i=0}^{13}\alpha_i g^i : \alpha_i\in\mathbb{Z}_2, \sum_{i=0}^{13}\alpha_i=0\right\}.$$

De esto último se puede ver que la distancia del código es $d(\mathcal{C})=2$. Así las cosas $\mathcal{C}$ es un $(14,7,2)$ código derivado de unidad.

4.3 Obtención de unidades

Los anillos de grupo son una fuente rica de unidades. Existen unidades y son conocidas en RG, donde R puede ser cualquier anillo y no solo un cuerpo, y, a partir de ellas, se pueden construir códigos de diferentes tipos. Una vez que se conoce una unidad, aún se tiene opción para el submódulo y dimensión del código y por tanto códigos de diferentes dimensiones pueden ser obtenidos desde de una unidad dada.

Para describir completamente un código derivado de unidad en términos de condiciones del generador y las condiciones de verificación, son necesarios una unidad y su inverso. El inverso puede ser conocido desde el álgebra; fórmulas explícitas generales para ciertas unidades y sus inversas, en anillos de grupo son conocidas, consultar [13,

Cap. 8] y las referencias allí mencionadas. En el caso de anillos de grupo sobre grupos cíclicos, vale la pena señalar que el algoritmo euclidiano, el cual es extremadamente rápido, puede usarse para obtener un inverso, dado que $RG \cong \frac{R[x]}{< x^n - 1 >}$. Una variación del algoritmo euclidiano también puede usarse para encontrar inversos en RG cuando G es un grupo dihedral.

La combinación de unidades en un anillo de grupo es también una unidad. Esto puede explotarse para producir nuevas unidades, que no son de la misma forma que las originales y de las cuales se pueden derivar nuevos códigos.

4.4 Códigos dual y auto-dual

Recordemos de la Sección 3.4 que el dual de un código de una codificación de anillo de grupo es $\mathcal{C}^{\perp} = \{\mathbf{y} \in RG : (\mathbf{xu}) \cdot \mathbf{y} = \mathbf{0}, \forall \mathbf{x} \in W\}$, y de la Sección 2.1 el concepto de transposición de un elemento de anillo de grupo. A continuación veamos la obtención del código dual de un código derivado de la unidad $\mathbf{u}$, a partir de $(\mathbf{u}^{-1})^T$.

Teorema 4.2. *Sean W un submódulo con base de elementos de grupo $S \subset G$ y $W^{\perp}$ el submódulo con base $G \setminus S$. Sea $\mathbf{u} \in RG$ una unidad tal que $\mathbf{u}\mathbf{u}^{-1} = \mathbf{1}$. Entonces el código dual de $\mathcal{C} = \{\mathbf{xu} : \mathbf{x} \in W\}$ es $\mathcal{C}^{\perp} = \left\{\mathbf{x}\,(\mathbf{u}^{-1})^T : \mathbf{x} \in W^{\perp}\right\}$.*

Demostración. *Sea $\mathbf{z} \neq \mathbf{0}$ un elemento en RG. Es necesario demostrar que $(\mathbf{xu}) \cdot \mathbf{z} = \mathbf{0}$ para todo $\mathbf{x} \in W$ si y sólo si $\mathbf{z}\mathbf{u}^T \in W^{\perp}$. Lo que es lo mismo $\mathbf{z} \in \mathcal{C}^{\perp}$ si y sólo si $\mathbf{z}\mathbf{u}^T \in W^{\perp}$.*

Si $\mathbf{z}\mathbf{u}^T \in W^{\perp}$, entonces, para todo $\mathbf{x} \in W$,

$$\mathbf{0} = \mathbf{x} \cdot (\mathbf{z}\mathbf{u}^T) = \mathbf{x}(\mathbf{z}\mathbf{u}^T)^T = \mathbf{x}(\mathbf{u}\mathbf{z}^T) = (\mathbf{xu})\mathbf{z}^T = (\mathbf{xu}) \cdot \mathbf{z}.$$

Recíprocamente, si $(\mathbf{xu}) \cdot \mathbf{z} = \mathbf{0}$ para todo $\mathbf{x} \in W$ entonces,

$$(\mathbf{xu}) \cdot \mathbf{z} = (\mathbf{xu})\mathbf{z}^T = \mathbf{x}(\mathbf{u}\mathbf{z}^T) = \mathbf{x}(\mathbf{z}\mathbf{u}^T)^T = \mathbf{x} \cdot (\mathbf{z}\mathbf{u}^T) = \mathbf{0},$$

para todo $\mathbf{x} \in W$, por lo tanto $\mathbf{z}\mathbf{u}^T \in W^{\perp}$.

Veamos ahora que $\{\mathbf{y} \in RG : (\mathbf{xu}) \cdot \mathbf{y} = \mathbf{0}, \forall \mathbf{x} \in W\} = \left\{\mathbf{z}\,(\mathbf{u}^{-1})^T : \mathbf{z} \in W^{\perp}\right\}$.

Sea $\mathbf{y} \in RG$ tal que $(\mathbf{xu}) \cdot \mathbf{y} = \mathbf{0}$ para todo $\mathbf{x} \in W$ así de lo anterior, $\mathbf{y}\mathbf{u}^T \in W^{\perp}$. Luego $\mathbf{y}\mathbf{u}^T = \mathbf{z} \in W^{\perp}$, y por tanto $\mathbf{y} = \mathbf{z}\,(\mathbf{u}^{-1})^T$.

Por otro lado, para $\mathbf{z}\,(\mathbf{u}^{-1})^T$ con $\mathbf{z} \in W^{\perp}$, se tiene,

$$\begin{aligned}\mathbf{xu}\cdot\mathbf{z}\left(\mathbf{u}^{-1}\right)^T &= \mathbf{xu}\left(\mathbf{z}\left(\mathbf{u}^{-1}\right)^T\right)^T \\ &= \mathbf{xu}\left(\mathbf{u}^{-1}\mathbf{z}^T\right) \\ &= \mathbf{x}\left(\mathbf{u}\mathbf{u}^{-1}\right)\mathbf{z}^T \\ &= \mathbf{x}\mathbf{z}^T \\ &= \mathbf{x}\cdot\mathbf{z} = \mathbf{0}, \qquad (\mathbf{x}\in W, \mathbf{z}\in W^{\perp})\end{aligned}$$

□

La estricta equivalencia de un código derivado de unidad y su dual, y de lo cual $\mathcal{C} = \mathcal{C}^{\perp}$, requiere que para todo $\mathbf{x} \in W$, $\mathbf{xuu}^T \in W^{\perp}$, lo que impone una restricción poco práctica. Sin embargo, es natural decir que un código derivado de unidad es **auto-dual** si $\mathcal{C}$ y $\mathcal{C}^{\perp}$ son códigos equivalentes, o equivalentemente, que los códigos $\mathcal{D}$ y $\mathcal{D}^{\perp}$, matriciales generados, resultantes son iguales.

Definición 4.1. *Una unidad* $\mathbf{u} \in RG$ *es* ***ortogonal*** *si y sólo si* $\mathbf{uu}^T = 1$. *Es fácil ver que la RG-matriz de una unidad ortogonal* $\mathbf{u}$ *es una matriz ortogonal.*

Como sabemos un código lineal $\mathcal{C}$ es auto-dual si $\mathcal{C} = \mathcal{C}^{\perp}$, [8, pág. 45], por tanto usando el Teorema 4.2, con $\mathbf{u}$ unidad ortogonal y un submódulo de dimensión $n/2$ obtenemos un código derivado de unidad auto-dual.

Capítulo 5

Conclusiones

- Mostramos como el isomorfismo entre RG y $\mathcal{M}_{RG}(R)$ (las RG-matrices $n \times n$ sobre R), lo cual nos facilitó la demostración de Teoremas, Corolarios y Lemas importantes posteriores a dicho resultado.

- La definición de codificación de anillo de grupo a través de un submódulo W en RG nos permitió ver la forma estándar de los códigos que analizamos, códigos divisores de cero y derivados de unidad.

- Para los códigos divisores de cero pudimos establecer que la dimensión del código dependerá del rango del conjunto $S\mathbf{u}$, con $S \subset G$, que genera el submodulo W, y el rango de la RG-matriz U.

  Además en la sección 3.4 se pudo determinar la forma para el dual de un código divisor de cero y también, las condiciones para que dicho código sea auto-dual.

- Para los códigos derivados de unidad, motramos la equivalencia entre el código $\mathcal{C}$ y un código $\mathcal{D} \in R^r$, llamado código matricial generado, lo cual facilita encontrar las matrices generadora y de verificación.

  En la sección 4.4 pudimos ver la forma usual del código dual de un código derivado de unidad, y también la condición para que el código derivado de unidad sea auto-dual.

Bibliografía

[1] Barajas Ávila G. L.(2016). *Teoría de códigos y álgebras de grupo* (tesis de pregrado). Universidad Industrial de Santander, Bucaramanga, Colombia.

[2] Díaz Portillo J. O.(2016). *Introducción a la teoría de códigos cíclicos* (tesis de pregrado). Universidad de Nariño,San Juan de Pasto, Colombia.

[3] Gallian J. A.(2012). *Contemporary Abstract Algebra,* 8^{th} *edition.* Minnesota, Estados Unidos: CENGAGE Learning.

[4] *GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra, version 4.4.9*, http://www.gap-system.org.

[5] Hughes G.(2000). *Constacyclic codes, cocycles and a* $u + v$*-*$u - v$ *construction*, IEEE Trans. Inform. Theory, Vol. **46**: 674-680.

[6] Hurley P. & Hurley T.(2009). *Codes from zero-divisors and units in group rings.* Int. J. Information and Coding Theory, Vol. **1**, No. **1**: 57-87.

[7] Jiménez B. L. R., Gordillo Ardila J. E. & Rubiano Ortegón G. N.(2004). *Teoría de números [para principiantes],*2^A *edición.* Bogota, Colombia: Pro-Offset.

[8] Ling S. & Xing C.(2004). *Coding Theory A First Course.* New York, Estados Unidos.

[9] MacLoughlin Ian & Hurley T.(2008). *A Group Ring Construction of the Extended Binary Golay Code*, IEEE Transactions on Information Theory, Volume: 54.

[10] MacWilliams F.J.(1969). *Codes and ideals in group algebras*, Combinatorial Mathematics and its Applications. 312-328.

[11] Podestá R. A.(2006). *Introducción a la teoría de códigos autocorrectores.* Córdoba, Argentina.

[12] Polcino Milies C.(2010). *Introdução à Teoria Algébrica de Códigos.* São Paulo, Brasil.

[13] Polcino Milies C. & Sehgal S. K.(2002). *A Course in Group Rings*. Dordrecht, Netherlands: Kluwer Academic Publishers.

[14] Snover S. L.(1973) *The uniqueness of the Nordstrom-Robinson and the Golay binary codes*. Michigan Estados Unidos.