Departamento de Matemáticas y Estadística
División de Ciencias Básicas
Universidad del Norte
Tesis de Maestría

Códigos de grupo torcidos

María Camila Sinning López

Dirigido por:
Prof. Dr. Javier de la Cruz Cantillo

2 de diciembre de 2022

Agradecimientos

Doy gracias a Dios porque me ha salvado a través de la muerte y resurrección de su hijo Jesucristo, me guía con su Santo Espíritu y me ha dado la sabiduría para la realización de este trabajo. Agradezco a mis padres porque me han apoyado durante este tiempo y agradezco a los profesores que me acompañaron en este proceso, especialmente al profesor Javier de la Cruz por su orientación para la terminación de esta tesis.

Resumen

En el presente trabajo abordamos el estudio de los códigos de grupo torcidos como una generalización de los códigos de grupo. Concretamente nos centraremos en los resultados probados en [6], en donde se establecen condiciones suficientes y necesarias para que un código lineal dado exista como un código de grupo torcido con relación a cierto grupo G. En particular, demostraremos que ciertos códigos conocidos, tales como el código de Golay ternario extendido $\mathcal{G}_{12}$ y los códigos de Hamming pueden ser vistos como códigos de grupo torcidos.

Índice general

Introducción

La teoría algebraica de códigos es un área de las matemáticas cuyo objetivo central es el estudio de la codificación y la decodificación de la información, usando herramientas del álgebra. Básicamente, en ella se pretende desarrollar modelos matemáticos algebraicos capaces de determinar los mensajes que han sido enviados a través de un canal de comunicación ruidoso, a partir de los mensajes recibidos, los cuales frecuentemente presentan uno o más errores. En particular, es bien conocido que la teoría de códigos lineales, llamada usualmente teoría clásica de códigos, ha sido de los modelos o enfoques algebraicos más estudiados, y que más éxito ha mostrado en el proceso de detección y corrección de errores.

Concretamente, un $[n, k]$ código lineal C no es más que un $\mathbb{F}_q$-subespacio vectorial de dimensión k del espacio ambiente $\mathbb{F}_q^n$, donde $\mathbb{F}_q$ es el cuerpo finito con q elementos. Dados dos vectores en $\mathbb{F}_q^n$, se define la distancia de Hamming entre estos, como el numero de coordenadas en las cuales ellos difieren. Hablamos entonces de un $[n, k, d]$ códigos lineal C, si d corresponde a la menor de todas las distancias entre dos vectores cualesquiera no nulos de C. Este tercer parámetro d es conocido como la distancia mínima del código y es fundamental en el proceso de detección y corrección de errores. Por otra parte, en el espacio ambiente $\mathbb{F}_q^n$ definimos una forma bilineal $\langle \cdot, \cdot \rangle$ no degenerada, dada por el producto interior usual de dos vectores. Entonces el código dual de un código lineal C se define como el conjunto de todos los vectores ortogonales a C, es decir, $C^\perp = \{a \in \mathbb{F}_q^n : \langle c, a \rangle = 0 \text{ para todo } c \in C\}$. En caso de que $C^\perp = C$, decimos que C es autodual. Con base en estos conceptos iniciales y en otras características de los códigos lineales, se describen y se estudian familias de códigos tales como los códigos de Hamming, los códigos

resto cuadráticos, los códigos de Golay, entre otros. Algunos de estos códigos pertenecen a una clase especial de códigos lineales llamados códigos cíclicos, en estos, la translación cíclica de cada vector es nuevamente un vector del código. Es fácil verificar que los códigos cíclicos pueden ser identificados como ideales del álgebra $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, generados por un elemento llamado polinomio generador.

Los códigos cíclicos también pueden ser vistos como ideales del álgebra de grupo $\mathbb{F}_q C_n$, donde C_n es el grupo cíclico de orden n, debido a que $\mathbb{F}_q C_n \cong \mathbb{F}_q[x]/\langle x^n - 1\rangle$ como $\mathbb{F}_q$-álgebras. Recordemos que en general, el álgebra de grupo $\mathbb{F}_q G$, para un grupo finito G, está conformada por las sumas formales $\sum_{g\in G} a_g g$, donde $a_g \in \mathbb{F}_q$ y la multiplicación está dada por $\sum_{g\in G} a_g g \sum_{h\in G} a_h h = \sum_{g,h\in G} a_g b_h gh$. Extendiendo el concepto de código cíclico, definimos los códigos de grupo como ideales del álgebra de grupo $\mathbb{F}_q G$, para algún grupo finito G. Algunos ejemplos de estos códigos son los ya mencionados códigos cíclicos y el código de Golay binario extendido $\mathcal{G}_{24}$, el cual es un ideal para el álgebra de grupo $\mathbb{F}_2\mathrm{Sym}(4)$ [2]. Al ser vistos como ideales de un álgebra, su estructura algebraica se enriquece y su estudio se facilita.

No obstante, existen códigos lineales que no son códigos de grupo. Por ejemplo, los códigos constacíclicos, los cuales son definidos como ideales del anillo cociente de polinomios $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$, donde $\lambda \in \mathbb{F}_q^*$. Estos códigos pueden ser considerados como ideales de un tipo más general de álgebra, conocida como álgebra de grupo torcido. Concretamente, el álgebra de grupo torcido $\mathbb{F}_q^\alpha G$, para un grupo finito G dado, consiste en el espacio vectorial de las sumas formales $\sum_{g\in G} a_g \overline{g}$, donde ahora la multiplicación de anillo se tuerce usando un 2-cociclo de G, esto es, una función $\alpha : G \times G \longrightarrow \mathbb{F}_q^*$ que satisface $\alpha(gh, k)\alpha(g, h) = \alpha(g, hk)\alpha(h, k)$, para todo $g, h, k \in G$. Entonces, la multiplicación en el álgebra $\mathbb{F}_q^\alpha G$ estará dada por $\overline{g}\overline{h} = \alpha(g, h)\overline{gh}$. Es sencillo notar que, para un grupo finito G dado, el álgebra de grupo $\mathbb{F}_q G$ es un caso particular del álgebra de grupo torcido $\mathbb{F}_q^\alpha G$. Específicamente, $\mathbb{F}_q G \cong \mathbb{F}_q^\alpha G$ como $\mathbb{F}_q$-álgebras si el 2-cociclo α de G es tal que $\alpha(g, h) = 1$ para todo $g, h \in G$. Ahora bien, definimos los códigos de grupo torcidos como ideales del álgebra de grupo torcido $\mathbb{F}_q^\alpha G$. Un primer ejemplo de estos códigos son los códigos constacíclicos debido a que $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ es isomorfo como álgebra a $\mathbb{F}_q^{\alpha_\lambda} C_n$, donde C_n es el grupo cíclico de orden n y α_λ es un 2-cociclo adecuado. Otro ejemplo sería el muy conocido código de Golay ternario extendido $\mathcal{G}_{12}$ que, por los resultados mostrados en [16], no es un

código de grupo, para algún grupo G con doce elementos. Sin embargo, como uno de los resultados centrales de este trabajo, estableceremos que $\mathcal{G}_{12}$ puede ser considerado como un ideal del álgebra de grupo torcida $\mathbb{F}_3^{\alpha}\mathrm{Alt}(4)$ para un 2-cociclo de Alt(4) adecuado.

También es natural preguntarnos ¿cuándo un código lineal es un código de grupo? y ¿cuándo es un código de grupo torcido? Dar respuestas a estas preguntas también hace parte de los objetivos de este trabajo. En este orden de ideas, como resultado principal estableceremos condiciones necesarias y suficientes para que un código lineal dado exista como un código de grupo o en general para que sea sea un código de grupo torcido. En particular, aplicando el segundo resultado verificaremos que los conocidos códigos de Hamming pueden ser vistos como códigos de grupo torcidos, para cierto grupo G.

En cuanto a la organización del documento, éste estará dividido en cuatro capítulos. En el Capítulo 1 se presentan los conceptos y resultados básicos sobre G-conjuntos, anillos, espacios vectoriales, álgebras, módulos sobre anillos y el álgebra de grupo, que son fundamentales para el desarrollo de los capítulos posteriores. En el Capítulo 2 se introduce la teoría de códigos lineales, es decir, se define y presentan resultados básicos, tales como la distancia mínima de un código, el código dual y la equivalencia de códigos lineales. Además, se desarrolla la teoría para códigos cíclicos y códigos resto cuadráticos, que permite definir los códigos de Golay y motivan el desarrollo de los siguientes capítulos. En el Capítulo 3 se muestran resultados asociados a los códigos de grupo y su código dual, principalmente se presenta el criterio para determinar cuando un código lineal puede ser visto como un código de grupo. En el Capítulo 4 se establecen resultados análogos a los mostrados en el capítulo anterior, generalizados para los códigos de grupo torcidos. Asimismo, se demuestra que el código de Golay ternario extendido $\mathcal{G}_{12}$ y que los códigos de Hamming pueden ser considerados como códigos de grupo torcidos.

Capítulo 1

Preliminares

En el siguiente capítulo presentamos resultados y definiciones relacionados con G-conjuntos, anillos, espacios vectoriales, álgebras y módulos, debido a que son necesarios para el desarrollo de los capítulos posteriores. Estos resultados son conocidos y fueron tomados principalmente de [3] para anillos, álgebras y módulos, y de [8] para espacios vectoriales.

1.1. G-conjuntos

A continuación, definimos las acciones de grupos o G-conjuntos con el objetivo de identificar cuando la acción de un grupo G sobre un conjunto X es regular.

Definición 1.1. Sea X un conjunto y G un grupo. Decimos que G actúa sobre X o que X es un *G-conjunto* si existe una función $\circ : G \times X \longrightarrow X$ tal que

1. $e \circ x = x$ para todo $x \in X$.
2. $gh \circ x = g \circ (h \circ x)$ para todo $g, h \in G$ y $x \in X$.

Ejemplo 1.2.

1. Si $H \leq G$ entonces G es un H-conjunto. En particular, todo grupo G es un G-conjunto.
2. Sea X un grupo de n elementos y $\mathrm{Sym}(n)$ el grupo de todas las permutaciones de n elementos. Entonces X es un $\mathrm{Sym}(n)$-conjunto.

Definición 1.3. Sea X un G-conjunto, definimos el *estabilizador* de x en G, denotado G_x, como $G_x := \{g \in G : g \circ x = x\}$.

Teorema 1.4. *Sea X un G-conjunto. Entonces $G_x \leq G$ para todo $x \in X$.*

Demostración. $G_x \neq \emptyset$ puesto que $e \circ x = x$. Además, para $g, h \in G_x$ se sigue que $gh^{-1} \in G_x$ dado que $gh^{-1} \circ x = gh^{-1} \circ (h \circ x) = ghh^{-1} \circ x = g \circ x = x$. □

Teorema 1.5. *Sea X un G-conjunto, la relación*

$$x_1 \sim x_2 \iff \text{existe } g \in G : g \circ x_1 = x_2$$

es una relación de equivalencia.

Demostración.

1. La relación es reflexiva. $e \circ x_1 = x_1$, es decir, $x_1 \sim x_1$.
2. La relación es simétrica. Si $g \circ x_1 = x_2$, esto es, $x_1 \sim x_2$ entonces $g^{-1} \circ x_2 = g^{-1} \circ (g \circ x_1) = g^{-1}g \circ x_1 = e \circ x_1 = x_1$. Por lo tanto, $x_2 \sim x_1$.
3. la relación es transitiva. Si $x_1 \sim x_2$ y $x_2 \sim x_3$, entonces existen $g, h \in G$ tal que $g \circ x_1 = x_2$ y $h \circ x_2 = x_3$. Luego, $hg \circ x_1 = h \circ (g \circ x_1) = h \circ x_2 = x_3$. En consecuencia, $x_1 \sim x_3$.

□

Definición 1.6. Sea X un G-conjunto y $x \in X$. Definimos la *orbita* de x como su clase de equivalencia bajo la relación anterior, esto es

$$O(x) = \{g \circ x : g \in G\}.$$

Teorema 1.7. *Sea X un G-conjunto. Entonces $|O(x)| = |G : G_x|$ para todo $x \in X$.*

Demostración. Sea $R := \{gG_x : g \in G\}$ el conjunto de las clases laterales de G_x en G y definamos $\phi : O(x) \longrightarrow R$ como $g \circ x \longmapsto gG_x$. Vemos que ϕ está bien definida y es inyectiva puesto que

$$h \circ x = g \circ x \iff g^{-1}h \circ x = x \iff g^{-1}h \in G_x \iff gG_w = hG_x.$$

Además, ϕ es sobreyectiva dado que si $gG_x \in R$, entonces $\phi(g \circ x) = gG_x$. Por lo tanto, existe una biyeccion entre $O(x)$ y R. Luego, $|O(x)| = |R|$. □

Observación 1.8. Por el teorema de Lagrange, $|G| = |G : G_x||G_x|$. Entonces

$$|O(x)| = |G : G_x| = \frac{|G|}{|G_x|}.$$

Definición 1.9. Sea X un G-conjunto no vacío.

1. La acción de G en X es *transitiva* si para todo $x_1, x_2 \in X$ existe un $g \in G$ tal que $g \circ x_1 = x_2$. Es decir, X es la única orbita de G.

2. La acción de G en X es *libre* si dados $g_1, g_2 \in G$ y la existencia de $x \in X$ tal que $g_1 \circ x = g_2 \circ x$, entonces $g_1 = g_2$. De forma equivalente, la acción es libre si dado $g \in G$ y la existencia de $x \in X$ tal que $g \circ x = x$, entonces $g = e$.

3. La acción de G en X es *regular* si es transitiva y libre. Es decir, para $x_1, x_2 \in X$ existe un único $g \in G$ tal que $g \circ x_1 = x_2$.

Lema 1.10. *Sea X un G-conjunto. Las siguientes afirmaciones son equivalentes*

1. *G actúa regularmente sobre X.*

2. *La acción de G en X es transitiva y $|X| = |G|$.*

3. *La acción de G en X es libre y $|X| = |G|$.*

Demostración. (1) $\Rightarrow$ (2). Por definición una acción es regular si es transitiva. Luego, por el Teorema 1.7, $|X| = |O(x)| = |G|/|G_x|$ para todo $x \in X$. Como la acción es libre, se sigue que $G_x = \{e\}$ para todo $x \in X$. Por lo tanto, $|X| = |G|/1 = |G|$.
(2) $\Rightarrow$ (3). Si la acción es transitiva, entonces $|X| = |G|/|G_x|$. Como $|X| = |G|$ se tiene que $|G_x| = 1$, es decir, si $g \circ x = x \Rightarrow g = e$. Por lo tanto, la acción es libre.
(2) $\Rightarrow$ (1). Si la acción es libre, entonces $|G_x| = 1$. Luego, $|O(x)| = |G|/1 = |G| = |X|$, es decir, la acción es transitiva y por ende, es regular. □

1.2. Anillos

En esta sección, presentaremos algunos de los resultados básicos de la teoría de anillos. Concretamente describiremos conceptos y resultados sobre

anillos, subanillos, ideales, cuerpos, anillo cociente, homomorfismos y característica de un anillo.

Definición 1.11. Un *anillo* es un conjunto no vacío R con dos operaciones binarias $(+)$ y $(\cdot)$ llamadas adición y multiplicación respectivamente, tales que

1. $(R, +)$ es un grupo abeliano.
2. $(R, \cdot)$ es asociativa.
3. $a(b + c) = ab + ac$ y $(b + c)a = ba + ca$, para todo $a, b, c \in R$.

Denotamos el anillo R como $(R, +, \cdot)$. Si $ab = ba$ para todo $a, b \in R$, decimos que R es un *anillo conmutativo* y si existe $1 \in R$ tal que $a \cdot 1 = 1 \cdot a = a$, decimos que R es un *anillo con identidad*.

Observación 1.12. Supondremos que todos anillos son anillos con identidad, que tienen más de dos elementos, y que $1 \neq 0$.

Ejemplo 1.13.
1. Los conjuntos $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son anillos conmutativos con unidad.
2. Sea $M_n(R)$ el conjunto formado por las matrices de tamaño $n \times n$ con entradas en el anillo R. El conjunto $M_n(R)$ es un anillo no conmutativo bajo la suma y multiplicación de matrices usual.

Definición 1.14. Sea R un anillo.

1. Un elemento $a \in R$ es *invertible* si existe $b \in R$ tal que $ab = ba = 1$. En este caso escribimos $b = a^{-1}$.
2. Un elemento $a \in R$ es un *divisor de cero izquierdo (derecho)* si existe $0 \neq b \in R$ tal que $ab = 0$ $(ba = 0)$. Además, a es un *divisor de cero* si existe $0 \neq b \in R$ tal que $ab = ba = 0$.
3. Un anillo conmutativo que no tiene divisores de cero se R denomina *dominio entero*.
4. Un anillo en el cual todo elemento no nulo es invertible se denomina un *anillo con división*.
5. Un anillo con división conmutativo se denomina *campo* o *cuerpo*.

Observación 1.15. Todo cuerpo es un dominio entero, sin embargo el reciproco no es siempre cierto. Por ejemplo, $\mathbb{Z}$ es un dominio entero con elementos invertibles $\{1, -1\}$.

Lema 1.16. *Un dominio entero finito es un cuerpo.*

Demostración. Sea D un anillo con n elementos y sea $0 \neq a \in D$. Como D es un dominio entero,

$$ax_1 = ax_2 \Rightarrow ax_1 - ax_2 = 0 \Rightarrow a(x_1 - x_2) = 0 \Rightarrow x_1 = x_2$$

para todo $x_1, x_2 \in D$. Si definimos $aD^\times := \{ax \mid 0 \neq x \in D\}$, entonces $|aD^\times| = n - 1 = |D^\times|$. En consecuencia, existe un x en D tal que $ax = 1$ puesto que $1 \in D$. Es decir, a es invertible. □

Definición 1.17. Sea R un anillo. $\emptyset \neq S \subseteq R$ es un *subanillo* de R si S es una anillo bajo las operaciones de R.

Lema 1.18. *Sea R un anillo y $\emptyset \neq S \subseteq R$. Entonces S es un subanillo si y solo si*

1. *$x - y \in S$ para todo $x, y \in S$.*
2. *$xy \in S$ para todo $x, y \in S$.*
3. *$1_R \in S$.*

Demostración. Del ítem $x - y \in S$ para todo $x, y \in S$ se concluye que S es un grupo abeliano. Las propiedades asociativa y distributiva se siguen de que $S \subseteq R$. De la propiedad $xy \in S$ se tiene la cerradura de la operación y de $1_R \in S$ se tiene que S es un anillo con identidad. □

Ejemplo 1.19. El conjunto de matrices diagonales de tamaño $n \times n$ con entradas en el anillo R es un subanillo de $M_n(R)$.

Definición 1.20. Sea R un anillo. $\emptyset \neq I \subseteq R$ es un *ideal derecho* de R si y solo si

1. $(I, +)$ es un subgrupo de R.
2. $xa \in I$ para todo $x \in I$ y $a \in R$.

De forma similar se define el *ideal izquierdo*. Si I es un ideal izquierdo y derecho entonces I es un *ideal bilateral* de R.

Lema 1.21. *Sea R un anillo y $\emptyset \neq I \subseteq R$. Entonces I es un ideal derecho si y solo si*

1. *$x + y \in I$ para todo $x, y \in I$.*
2. *$xa \in I$ para todo $a \in R$ y $x \in I$.*

Demostración. Solo debemos demostrar que I es un subgrupo de R. Si $y \in I$, entonces $-y = y \cdot (-1) \in I$. Luego, $x + (-y) \in I$ para todo $x, y \in R$. □

Definición 1.22. Sea $S \subseteq R$ donde R es un anillo. El *ideal derecho generado* por S, denotado $\langle S \rangle_d$, se define como la intersección de los ideales derechos de R que contienen a S. Es decir, $\langle S \rangle_d$ es el mínimo ideal derecho que contiene a S. Similarmente se define el ideal izquierdo y el ideal bilateral generado por S, denotados $\langle S \rangle_i$ y $\langle S \rangle$, respectivamente.

Lema 1.23. *Sea R un anillo y $S \subseteq R$. Entonces*

$$\langle S \rangle_d := \left\{ \sum_{i=1}^{m} s_i a_i : s_i \in S, a_i \in R, m \in \mathbb{N} \right\}.$$

Demostración. Sea $I := \{\sum_{i=1}^{m} s_i a_i : s_i \in S, a_i \in R, m \in \mathbb{N}\}$. Es sencillo verificar que I es un ideal que contiene a S, entonces $\langle S \rangle_d \subseteq I$. Por otro lado, para cualquier ideal J de R que contenga a S se tiene que $I \subseteq J$. Luego $I \subseteq \langle S \rangle_d$. Por lo tanto, $I = \langle S \rangle_d$. □

Definición 1.24.

1. Si $\{0\}$ y R son los únicos ideales del anillo R, decimos que R es un *anillo simple*.
2. En el caso que $I = \langle x \rangle_d = xR$, decimos que I es un ideal principal derecho. Similarmente, definimos un ideal principal izquierdo. El anillo R es denominado *anillo de ideales principales* si todos sus ideales derechos o izquierdos son ideales principales derechos o izquierdos, respectivamente.
3. Sean I y J ideales derechos del anillo R. Definimos el ideal derecho $I + J$ como $I + J = \{x + y : x \in I, y \in J\}$.

Teorema 1.25. *1. Todo anillo con división es simple.*

2. *Todo campo es simple.*

3. *Todo anillo simple conmutativo es un cuerpo.*

Demostración. 1. Sea R un anillo con división y I un ideal derecho de R. Si $0 \neq x \in I$, entonces $1 = xx^{-1} \in I$. Por lo tanto, $I = R$. Igual sucede con los ideales izquierdos.

2. Se sigue del ítem anterior, puesto que todo campo es un anillo con división.

3. Sea R un anillo simple conmutativo y $0 \neq a \in R$. Como $\langle a \rangle = R$ se sigue que $1 \in \langle a \rangle$. Por lo tanto, existe x in R tal que $ax = xa = 1$.

□

Definición 1.26. $R[x]$ es el conjunto de polinomios en x con coeficientes en el anillo R. Este conjunto forma un anillo bajo la suma y multiplicación de polinomios usuales. Notemos que un elemento de $R[x]$ tiene la forma $f(x) = \sum_{i=0}^{n} a_i x^i$ donde $a_i \in R$.

Teorema 1.27. *Sea K un cuerpo. Entonces $K[x]$ es un dominio de ideales principales.*

Demostración. Sean $f(x) = \sum_{i=0}^{n} a_i x^i$ y $g(x) = \sum_{i=0}^{m} a_i x^i$ elementos de $K[x]$ donde $a_n \neq 0$ y $b_m \neq 0$. Entonces

$$f(x)g(x) = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j x^{i+j}.$$

Como K es un cuerpo se tiene que $a_n b_m \neq 0$. Por lo tanto, $fg \neq 0$. Esto es, $K[x]$ es un dominio entero. Resta demostrar que $K[x]$ es un anillo de ideales principales. Para esto, sea $0 \neq I$ un ideal de $K[x]$ y $g(x) \in I$. Luego, existe un polinomio $f(x)$ de grado mínimo en I. Además, por el algoritmo de la división en $K[x]$ se sigue que $g(x) = f(x)q(x) + r(x)$ donde $\deg(r(x)) < \deg(f(x))$ o $r(x) = 0$. Pero $r(x) = g(x) - f(x)q(x) \in I$, entonces $r(x) = 0$ y $g(x) = f(x)q(x)$. En consecuencia, $I = \langle f(x) \rangle$.

□

Definición 1.28. Sea I un ideal de un anillo R. El conjunto de clases laterales de I en R se define como

$$R/I := \{a + I : a \in R\}.$$

El conjunto R/I se denomina *anillo cociente* o *anillo factor* bajo las siguientes operaciones

$$(a+I)+(b+I) := (a+b)+I.$$
$$(a+I)(b+I) := (ab)+I.$$

Denotamos la clase $a+I$ como $[a]$.

Ejemplo 1.29. El anillo cociente $\mathbb{F}_3[x]/\langle x^2+2\rangle$ esta formado por los siguientes elementos

$$\mathbb{F}_3[x]/\langle x^2+2\rangle = \{[0],[1],[2],[x],[x+1],[x+2],[2x],[2x+1],[2x+2]\}.$$

Los representantes de las clases son determinados por los polinomios de $\mathbb{F}_3[x]$ de grado menor a 2.

Definición 1.30. Sean R y S anillos. Una función $\varphi : R \longrightarrow S$ es un *homomorfismo de anillos* si se cumple

1. $\varphi(x+y) = \varphi(x)+\varphi(y)$ para todo $x, y \in R$.
2. $\varphi(xy) = \varphi(x)\varphi(y)$ para todo $x, y \in R$.

Si φ es inyectiva o sobreyectiva, φ de denomina *monomorfismo* o *epimorfismo* respectivamente. Si φ es biyectiva, decimos que es un *isomorfismo* y escribimos $R \cong S$. Si $R = S$ entonces φ es un *endomorfismo* y si φ es un endomorfismo biyectivo, entonces decimos que es un *automorfismo*.

Definición 1.31. Dado $\varphi : R \longrightarrow S$ un homomorfismo de anillos, definimos el kernel y la imagen de φ como sigue

1. $\mathrm{Ker}(\varphi) := \{x \in R : f(x) = 0\}$.
2. $\mathrm{Im}(\varphi) := \{\varphi(x) : x \in R\}$.

Lema 1.32. *Sea $\varphi : R \longrightarrow S$ un homomorfismo de anillos. Entonces*

1. *φ es un monomorfismo si y solo si $\mathrm{Ker}(\varphi) = \{0\}$.*
2. *φ es un epimorfismo si y solo si $\mathrm{Im}(\varphi) = S$.*
3. *$\mathrm{Ker}(\varphi)$ es un ideal de R.*
4. *Si $\varphi(1_R) = 1_S$, entonces $\mathrm{Im}(\varphi)$ es un subanillo de S.*

Demostración. 1. Notemos que $0 \in \mathrm{Ker}(\varphi)$. Si φ es un monomorfismo, entonces $\mathrm{Ker}(\varphi) = \{0\}$. Recíprocamente, si $x, y \in R$ con $\varphi(x) = \varphi(y)$, se tiene que $\varphi(x - y) = 0$. Como $\mathrm{Ker}(\varphi) = 0$, se sigue que $x = y$. Por lo tanto, φ es un monomorfismo.

2. Se sigue de la definición.

3. Sean $x, y \in \mathrm{Ker}(\varphi)$ y $a \in R$. Entonces $\varphi(x+y) = \varphi(x)+\varphi(y) = 0+0 = 0$ y $\varphi(xa) = \varphi(x)\varphi(a) = 0\varphi(a) = 0$. En consecuencia, $x + y, xa \in \mathrm{Ker}(\varphi)$ para todo $x, y \in \mathrm{Ker}(\varphi)$ y todo $a \in R$.

4. Como $\varphi(1_R) = 1_S$, entonces $1_S \in S$. Además, sean $a, b \in \mathrm{Im}(\varphi)$, entonces existen $x, y \in R$ tales que $\varphi(x) = a$ y $\varphi(y) = b$. Por lo tanto, $\varphi(x - y) = \varphi(x) - \varphi(y) = a - b$ y $\varphi(xy) = \varphi(x)\varphi(y) = ab$. Luego, $a - b, ab \in \mathrm{Im}(\varphi)$ para todo $a, b \in \mathrm{Im}(\varphi)$.

□

Definición 1.33. Dado un ideal I de un anillo R. Definimos $\pi : R \longrightarrow R/I$ como $\pi(a) := a + I$. La función π es un epimorfismo de anillos llamado *proyección canónica* o *epimorfismo canónico*.

Teorema 1.34 (Primer teorema de isomorfía para anillos)**.** *Sea $f : R \longrightarrow S$ un homomorfismo de anillos. Entonces $R/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$.*

Demostración. Definamos $\varphi : R/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ como $\varphi(x + \mathrm{Ker}(f)) = f(x)$. Veamos que φ está bien definida y es inyectiva.

$$\begin{aligned} x + \mathrm{Ker}(f) = y + \mathrm{Ker}(f) &\iff x - y \in \mathrm{Ker}(f) \iff f(x - y) = 0 \\ &\iff f(x) - f(y) = 0 \iff f(x) = f(y) \\ &\iff \varphi(x + \mathrm{Ker}(f)) = \varphi(y + \mathrm{Ker}(f)). \end{aligned}$$

Por otro lado,

$$\begin{aligned} \varphi((x + \mathrm{Ker}(f)) + (y + \mathrm{Ker}(f))) &= \varphi((x + y) + \mathrm{Ker}(f)) \\ &= f(x + y) = f(x) + f(y) \\ &= \varphi(x + \mathrm{Ker}(f)) + \varphi(y + \mathrm{Ker}(f)). \end{aligned}$$

$$\begin{aligned} \varphi((x + \mathrm{Ker}(f))(y + \mathrm{Ker}(f))) &= \varphi((xy) + \mathrm{Ker}(f)) \\ &= f(xy) = f(x)f(y) \\ &= \varphi(x + \mathrm{Ker}(f))\varphi(y + \mathrm{Ker}(f)). \end{aligned}$$

Por lo tanto, φ es un monomorfismo de anillos. Resta verificar que φ es sobreyectiva. Sea $a \in \mathrm{Im}(f)$, entonces existe $x \in R$ tal que $f(x) = a$. Esto implica que $\varphi(x + \mathrm{Ker}(f)) = f(x) = a$. En consecuencia, $R/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. □

Teorema 1.35 (Teorema de correspondencia)**.** *Sea R un anillo y I un ideal de R. Definamos $l(R, I)$ y $l(R/I)$ como*

$$l(R, I) := \{J : I \subseteq J \subseteq R, J \text{ es un ideal de } R\}.$$

$$l(R/I) := \{J' : J' \text{ es un ideal de } R/I\}.$$

Entonces, existe una biyección entre estos conjuntos que preserva la inclusión dada por $\varphi : l(R, I) \longrightarrow l(R/I)$ con $\varphi(J) = \pi(J) = J/I$, donde $\pi : J \longrightarrow J/I$ es la proyección canónica.

Definición 1.36. Sea I un ideal de una anillo R. I es un *ideal maximal derecho* de R si y solo si $I \neq R$ y si $I \subseteq J \subseteq R$ para algún ideal derecho J, entonces $J = R$ o $J = I$.

Teorema 1.37. *Sea R un anillo conmutativo, entonces I es un ideal maximal de R si y solo si R/I es un campo.*

Demostración. Como I es un ideal maximal, no existe otro ideal $J \neq R$ que contenga a I. Luego, por el teorema de correspondencia, no existe un ideal R/J en R/I distinto de $\{I\}$ o R/I. Es decir, R/I es un anillo simple conmutativo. Por lo cual, R/I es un campo. □

Definición 1.38. Dado un anillo R, decimos que R tiene característica positiva si existe al menos un entero positivo n tal que $nx = 0$ para todo $x \in R$. En este caso, llamamos *característica* de R al menor entero positivo que satisface esta propiedad, denotado $\mathrm{char}(R)$. Si no existe n, decimos que $\mathrm{char}(R) = 0$.

Teorema 1.39. *R tiene característica $n > 0$ si y solo si n es el menor entero positivo que satisface $n \cdot 1 = 0$.*

Demostración. Si $\mathrm{char}(R) = n$, entonces $n1 = 0$. Recíprocamente, si $m1 = 0$ para un entero positivo m, entonces $0 = (m1)x = m(1x) = mx$ para todo $x \in R$. □

Teorema 1.40. *Sea K un cuerpo.*

1. *Entonces* $\text{char}(K) = 0$ *o* $\text{char}(K) = p$*, donde* p *es un número primo.*

2. *Si* K *es finito, entonces* $\text{char}(K) = p$*, donde* p *es un número primo.*

Demostración. 1. Sea $\text{char}(K) \neq 0$ y supongamos que $\text{char}(K)$ no es un número primo, entonces $\text{char}(K) = km$ donde $k, m \in \mathbb{N}$. Luego, $0 = (km)1 = (k1)(m1)$. Como K es un cuerpo, $k1 = 0$ o $m1 = 0$, lo cual es una contradicción.

2. Verifiquemos que si K es finito, entonces $\text{char}(K) \neq 0$. Como K es finito, existen $m, n \in \mathbb{N}$ con $m > n$ tales que $m \cdot 1 = n \cdot 1$. Luego, $(m - n) \cdot 1 = 0$ con $m - n \neq 0$.

□

1.3. Espacios vectoriales

Los espacios vectoriales junto con los anillos son esenciales para la definición de álgebras. Por ello, presentaremos algunos conceptos y teoremas relacionados con espacios vectoriales y transformaciones lineales, que son necesarios para la demostración de resultados posteriores.

Definición 1.41. Un *espacio vectorial* V sobre un cuerpo K es un conjunto no vacío con una operación binaria $(+)$ y una operación externa $(\cdot)$ tales que

1. $(V, +)$ es un grupo abeliano.

2. $k(u + v) = ku + kv$ para todo $k \in K$ y todo $u, v \in V$.

3. $(k_1 + k_2)v = k_1u + k_2v$ para todo $k_1, k_2 \in K$ y todo $v \in V$.

4. $(k_1k_2)v = k_1(k_2v)$ para todo $k_1, k_2 \in K$ y todo $v \in V$.

5. $1 \cdot v = v$ para todo $v \in V$.

Ejemplo 1.42. $\mathbb{R}^n$ es un espacio vectorial con la suma y la multiplicación por escalar por componentes.

Definición 1.43. Sea V un espacio vectorial sobre un cuerpo K y sean $v_1, v_2, \ldots, v_n$ elementos de V, también llamados vectores.

1. Decimos que $W \subseteq V$ es un *subespacio vectorial* si y solo si para todo $u, v \in W$ y $k \in K$ se tiene que $u + v \in W$ y $kv \in W$.

2. Sean U, W subespacios de V. Definimos el subespacio

$$U + W := \{u + w : u \in U, w \in W\}.$$

Si $V = U + W$ y $U \cap W = 0$, entonces decimos que V es la *suma directa* de U y W y lo denotamos $V = U \oplus W$.

3. Decimos que $\{v_1, v_2, \ldots, v_n\}$ generan a V si existen $k_1, \ldots, k_n \in K$ tales que $v = k_1 v_1 + \cdots + k_n v_n$ para cada $v \in V$.

4. Decimos que $\{v_1, v_2, \ldots, v_n\}$ son *linealmente dependientes* si existen $k_1, \ldots, k_n \in K$ no todos iguales a 0 tales que $k_1 v_1 + \cdots + k_n v_n = 0$. Si no existen tales números entonces los vectores son *linealmente independientes.*

5. Decimos que $\{v_1, v_2, \ldots, v_n\}$ son una *base* de V si generan a V y son linealmente independientes.

Observación 1.44. Dos bases de V tienen el mismo número de elementos. Así, la *dimensión* de V, denotada $\dim_K(V)$, es el número de elementos de cualquier base.

Teorema 1.45. *Sea V un espacio vectorial de dimensión n y $W \subseteq V$ un subespacio de dimensión n. Entonces $V = W$.*

Demostración. Una base para W también es una base para V. □

Definición 1.46. Sean V y W espacios vectoriales. La función $L : V \longrightarrow W$ es una *transformación lineal* si se cumple

1. $L(u + v) = L(u) + L(v)$ para todo $u, v \in V$.

2. $L(kv) = kL(v)$ para todo $k \in K$ y $v \in V$.

Si $V = W$ decimos que L es un endomorfismo. El conjunto de todos los endomorfismos de V se denota $\mathrm{End}_K(V)$.

Lema 1.47. *Sea $L : V \longrightarrow W$ una transformación lineal. Entonces*

1. $\mathrm{Ker(L)} := \{v \in V : L(v) = 0\}$ *es un subespacio de V.*

2. $\mathrm{Im}(L) := \{L(v) : v \in V\}$ *es un subespacio de W.*

Demostración. 1. Notemos que $0 \in \text{Ker(L)}$. Además, sean $u, v \in \text{Ker}(L)$ y $k \in K$. Entonces $L(u+v) = L(u) + L(v) = 0$ y $L(kv) = kL(v) = k \cdot 0 = 0$.

2. Sean $a, b \in \text{Im}(L)$, entonces existen $u, v \in V$ tales que $L(u) = a$ y $L(v) = b$. Por lo tanto, $L(u+v) = L(u) + L(v) = a + b$ y $L(ku) = kL(u) = ka$.

□

Teorema 1.48. *Sean V un espacio vectorial y $L : V \longrightarrow W$ una transformación lineal de V en W. Entonces*

$$\dim_K(V) = \dim_K(\text{Ker}(L)) + \dim_K(\text{Im}(L)).$$

Demostración. Sea $\{w_1, \ldots, w_s\}$ una base para $\text{Im}(L)$, sean $v_1, \ldots, v_s \in V$ tales que $L(v_i) = w_i$ para todo $i = 1, \ldots, s$ y sea $u_1, u_2, \ldots, u_q$ una base para $\text{Ker}(L)$. Demostremos que $B = \{v_1, \ldots, v_s, u_1, \ldots, u_q\}$ es una base de V. Si $v \in V$, entonces existen $x_1, \ldots, x_s$ tales que

$$\begin{aligned} L(v) &= x_1 w_1 + \cdots + x_s w_s \\ &= x_1 L(v_1) + \cdots + x_s L(v_s) \\ &= L(x_1 v_1 + \cdots + x_s v_s). \end{aligned}$$

Aplicando la linealidad de L tenemos que $L(v - x_1 v_1 - \cdots - x_s v_s) = 0$. Por lo tanto, $v - x_1 v_1 - \cdots - x_s v_s \in \text{Ker}(L)$ y existen $y_1, \ldots, y_q$ tales que

$$v - x_1 v_1 - \cdots - x_s v_s = y_1 u_1 + \cdots + y_q u_q.$$

Entonces $v = x_1 v_1 + \cdots + x_s v_s + y_1 u_1 + \cdots + y_q u_q$. De este modo, V es combinación lineal de los elementos de B. Ahora supongamos que $x_1 v_1 + \cdots + x_s v_s + y_1 u_1 + \cdots + y_q u_q = 0$. Al aplicar L tenemos

$$x_1 L(v_1) + \cdots + x_s L(v_s) + y_1 L(u_1) + \cdots + y_q L(u_q) = 0.$$

Pero $L(u_i) = 0$ para todo $i = 1, \ldots, q$, entonces $x_1 w_1 + \cdots + x_s w_s = 0$. Como $w_1, \ldots, w_s$ es una base para $\text{Im}(L)$ se sigue que $x_1 = \cdots = x_n = 0$. Por ende, $y_1 u_1 + \cdots + y_q u_q = 0$. Similarmente, $u_1, \ldots, u_s$ es una base para $\text{Ker}(L)$, entonces $y_1 = \cdots = y_n = 0$ y se concluye que los elementos de B son linealmente independientes. □

Definición 1.49. El *rango* de una matriz A es el número de columnas (o filas) linealmente independientes y es denotado $\text{rang}(A)$.

Teorema 1.50. *Sea $L : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ una transformación lineal definida como $x \longmapsto Ax^t$ donde A es una matriz de tamaño $m \times n$. Entonces,* $\text{rang}(A) = \dim(\text{Im}(L))$.

Demostración. Veamos que las columnas de A generan la imagen de L.

$$\begin{aligned} Ax^t &= \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} (x_1, \dots, x_n)^t \\ &= (x_1 a_{11} + \cdots + x_n a_{1n}, \dots, x_1 a_{m1} + \cdots + x_n a_{mn})^t \\ &= x_1 A_1 + \cdots + x_n A_n. \end{aligned}$$

Donde $A_1, \dots, A_n$ son las columnas de la matriz A. Por lo tanto, $\text{Im}(L) = \langle A_1, \dots, A_n \rangle$. En consecuencia, $\dim(\text{Im}(L))$ es igual al número de columnas independientes de A, es decir, $\text{rang}(A) = \dim(\text{Im}(L))$. □

Definición 1.51. Sea V un K-espacio vectorial. Decimos que $P \in \text{End}_K(V)$ es una *proyección* si $P^2 = P$.

Lema 1.52. *Sea V un K-espacio vectorial y $P^2 = P \in \text{End}_K(V)$. Entonces $V = \text{Ker}(P) \oplus \text{Im}(P)$.*

Demostración. Sea $v \in V$. Luego,

$$P^2(v) = P(v) \Rightarrow P(v) - P^2(v) = 0 \Rightarrow P(v - P(v)) = 0.$$

Por lo tanto, $v = v - P(v) + P(v) \in \text{Ker}(P) + \text{Im}(P)$. Además, si $v \in \text{Ker}(P) \cap \text{Im}(P)$, entonces $P(v) = 0$ y existe un w tal que $v = P(w)$. Por lo cual, $v = P(w) = P^2(w) = P(v) = 0$. □

Definición 1.53. Sean V un espacio vectorial y K un cuerpo, decimos que $f : V \times V \longrightarrow K$ es una *forma bilineal* si se verifica

1. $f(u, v_1 + v_2) = f(u, v_1) + f(u, v_2)$ para todo $u, v_1, v_2 \in V$.
2. $f(u_1 + u_2, v) = f(u_1, v) + f(u_2, v)$ para todo $u_1, u_2, v \in V$.
3. $f(u, kv) = kf(u, v)$ para todo $k \in K$ y $u, v \in V$.

4. $f(ku, v) = kf(u, v)$ para todo $k \in K$ y $u, v \in V$.

Decimos que f es una forma bilineal *simétrica* si $f(u, v) = f(v, u)$ y decimos que es *no degenerada* o *no singular* si $f(u, V) = 0$ implica que $u = 0$.

Teorema 1.54. *Sea U subespacio vectorial de V con una forma bilineal f no degenerada. Si $U^{\perp} := \{v \in V : f(v, u) = 0$ para todo $u \in U\}$, entonces*

$$\dim U + \dim U^{\perp} = \dim V.$$

1.4. Álgebras

Un álgebra es un tipo especial de anillo. A continuación, estudiaremos conceptos análogos a los descritos anteriormente para anillos, tales como álgebra, subálgebra, ideal, álgebra cociente y homomorfismo de álgebras.

Definición 1.55. Sea K un cuerpo. Un conjunto no vacío A es una *K-álgebra* si y solo si

1. A es un anillo unitario.
2. A es un K-espacio vectorial.
3. $(ka)b = k(ab) = a(kb)$ para todo $k \in K$ y todo $a, b \in A$.

La estructura aditiva de A es la misma como anillo y espacio vectorial. Si A es un anillo conmutativo entonces decimos que A es un *K-álgebra conmutativa* y si $\dim_K(A)$ es finita, decimos que A es un *K-álgebra de dimensión finita.*

Definición 1.56.

1. Sea A un K-álgebra. El conjunto $\emptyset \neq B \subseteq A$ es un *subálgebra* de A si B es también un K-álgebra.
2. Sea A un K-álgebra. El conjunto $\emptyset \neq I \subseteq A$ es un *ideal derecho* de A, denotado $I \leq A$, si y solo si
   a) I es un K-subespacio vectorial de A.
   b) $xa \in I$ para todo $x \in I$ y $a \in A$.

   De forma similar se define el *ideal izquierdo*. Si I es un ideal izquierdo y derecho, entonces I es un *ideal* de A.

3. Sea A un K-álgebra. Un ideal I de A es *maximal* si y solo si $I \neq A$ y si $I \subseteq J \subseteq A$ para algún ideal J de A, entonces $J = A$ o $J = I$.

4. Sea A un K-álgebra. Si $X \subseteq A$. Definimos el *ideal generado* por X, denotado $\langle X \rangle$ como
$$\langle X \rangle := \bigcap_{X \subseteq I \leq A} I.$$
Es decir, $\langle X \rangle$ es la intersección de ideales de A que contienen a X.

5. Sea I un ideal de un K-álgebra A. Entonces A/I es un K-álgebra bajo las operaciones:
$$\begin{aligned}(a+I)+(b+I) &:= (a+b)+I.\\ (a+I)(b+I) &:= (ab)+I.\\ k(a+I) &:= ka+I.\end{aligned}$$
El conjunto A/I se denomina *álgebra cociente*. Además, $\dim_K(A/I) = \dim_K(A) - \dim_K(I)$

Ejemplo 1.57. 1. El cuerpo K es un K-álgebra con $\dim_K(A) = 1$ llamada *álgebra regular*.

2. El conjunto $M_n(K)$ de matrices con entradas en K de tamaño $n \times n$ es un K-álgebra de dimensión n^2. Las matrices triangulares inferiores forman un K-subálgebra de $M_n(K)$. Además, para $n = 2$, $\begin{pmatrix} K & 0 \\ 0 & 0 \end{pmatrix}$ es un ideal derecho y $\begin{pmatrix} K & 0 \\ K & 0 \end{pmatrix}$ y $\begin{pmatrix} 0 & 0 \\ K & K \end{pmatrix}$ son ideales maximales.

3. El conjunto de polinomios $K[x]$ es un álgebra conmutativa, $\langle x^n - 1 \rangle$ donde $n \in \mathbb{N}$ es un ideal de $K[x]$ y $K[x]/\langle x^n - 1 \rangle$ es un álgebra cociente.

Definición 1.58. Sean A y B K-álgebras. Una función $\varphi : A \longrightarrow B$ es un *homomorfismo de K-álgebras* si se cumple

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$ para todo $a, b \in A$.

2. $\varphi(ab) = \varphi(a)\varphi(b)$ para todo $a, b \in A$.

3. $\varphi(ka) = k\varphi(a)$ para todo $k \in K$ y todo $a \in A$.

Si φ es inyectiva o sobreyectiva, φ de denomina *monomorfismo* o *epimorfismo* respectivamente. Si φ es biyectiva, decimos que es un *isomorfismo* y escribimos $A \cong B$.

Lema 1.59. *Dado $\varphi : A \longrightarrow B$ un homomorfismo de K-álgebras, entonces*

1. $\mathrm{Ker}(\varphi) := \{x \in R : \varphi(x) = 0\}$ *es un ideal de A.*
2. $\mathrm{Im}(\varphi) := \{\varphi(x) : x \in R\}$ *es un subálgebra de B.*

Demostración. 1. Sean $x, y \in \mathrm{Ker}(\varphi)$, $a \in R$ y $k \in K$. Entonces

$$\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y) = 0 + 0 = 0, \\ \varphi(kx) &= k\varphi(x) = k \cdot 0 = 0, \text{ y} \\ \varphi(xa) &= \varphi(x)\varphi(a) = 0\varphi(a) = 0. \end{aligned}$$

2. Sean $a, b \in \mathrm{Im}(\varphi)$ y $k \in K$, entonces existen $x, y \in R$ tales que $\varphi(x) = a$ y $\varphi(y) = b$. Por tanto,

$$\begin{aligned} \varphi(x-y) &= \varphi(x) - \varphi(y) = a - b, \\ \varphi(kx) &= k\varphi(x) = ka, \text{ y} \\ \varphi(xy) &= \varphi(x)\varphi(y) = ab. \end{aligned}$$

□

Ejemplo 1.60. 1. Sea V un K-espacio vectorial de dimensión n. Entonces $\mathrm{End}_K(V)$ es un K-álgebra de dimensión n^2 llamada el *álgebra de las transformaciones de V.*

2. Si V es un K-espacio vectorial de dimensión n, entonces que las K-álgebras $\mathrm{End}_K(V)$ y $M_n(K)$ son isomorfas.

Teorema 1.61. *Si A es un K-álgebra, entonces A es isomorfa a un subálgebra de $\mathrm{End}_K(V)$ para algún espacio vectorial V sobre K.*

Demostración. Como A es un espacio vectorial, tomemos $V = A$ y dado $a \in A$ definamos $T_a : V \longrightarrow V$ como $T_a(v) = av$. Veamos que $T_a \in \mathrm{End}_K(V)$. Sea $v_1, v_2 \in V$ y $k \in K$, entonces

$$\begin{aligned} T_a(v_1 + v_2) &= a(v_1 + v_2) = av_1 + av_2 = T(v_1) + T(v_2). \\ T_a(kv_1) &= a(kv_1) = k(av_1) = kT_a(v_1). \end{aligned}$$

Luego, definamos $\varphi : A \longrightarrow \mathrm{End}_K(V)$ como $\varphi(a) = T_a$. Sea $a_1, a_2 \in A$ y $k \in K$, entonces para todo $v \in V$ se sigue que

$$\begin{aligned}\varphi(a_1 + a_2)(v) &= T_{a_1+a_2}(v) = (a_1 + a_2)v = a_1v + a_2v \\ &= T_{a_1}(v) + T_{a_2}(v) = \varphi(a_1)(v) + \varphi(a_2)(v).\end{aligned}$$

$$\begin{aligned}\varphi(a_1a_2)(v) &= T_{a_1a_2}(v) = (a_1a_2)v = a_1(a_2v) \\ &= T_{a_1}(T_{a_2}(v)) = \varphi(a_1)\varphi(a_2)(v).\end{aligned}$$

$$\varphi(ka_1)(v) = T_{ka_1}(v) = (ka_1)v = k(a_1v) = k(T_{a_1}(v)) = k\varphi(a_1)(v).$$

Además, $T_{a_1}(v) = T_{a_2}(v) \iff a_1v = a_2v \iff a_1 = a_2$. Por lo tanto, φ es un monomorfismo y $A \cong \mathrm{Im}(\varphi)$ como álgebras, donde $\mathrm{Im}(\varphi)$ es un subálgebra de $\mathrm{End}_K(V)$. □

1.5. Módulos sobre anillos

Un módulo sobre un anillo es la generalización del concepto de espacio vectorial sobre un cuerpo, en donde la operación externa está dada con elementos de un anillo en lugar de elementos de un cuerpo.

Definición 1.62. Sea $(M, +)$ un grupo aditivo y $(A, +, \cdot)$ un anillo unitario. Entonces M es un *A-módulo derecho* (unitario) si existe una operación binaria $M \times A \longrightarrow M$ definida como $(x, a) \longmapsto xa$ tal que para todo $x, y \in M$ y $a, b \in A$ se tiene que

1. $x(a + b) = xa + xb$.
2. $(x + y)a = xa + ya$.
3. $x(ab) = (xa)b$.
4. $x \cdot 1 = x$.

Para indicar que M es un A-módulo derecho escribimos M_A. De forma similar definimos *módulo izquierdo* y lo denotamos ${}_AM$.

Observación 1.63.
1. Si M es un A-módulo izquierdo donde A un anillo conmutativo, entonces M es un A-módulo derecho con la operación $x * a := ax$. En efecto, $x * (ab) = (ab)x = (ba)x = b(ax) = ax * b = (x * a) * b$.

2. Si A es un K-álgebra, entonces M es también un K-espacio vectorial con la operación $k \cdot x := (k1_A)x$ para todo $k \in K$. Además, $k(ax) = a(kx) = (ka)x$ para todo $a \in A$, $x \in M$ y $k \in K$.

En este capítulo, A siempre denota un K-álgebra.

Ejemplo 1.64. 1. El K-álgebra A es un A-módulo derecho llamado el *A-módulo regular derecho* y denotado ${}_AA$.

2. El conjunto I es un ideal derecho de A si y solo si I es un A-módulo derecho.

3. Sea $(M, +)$ un grupo aditivo. M es un $\mathbb{Z}$-módulo izquierdo donde la operación nx es la definición usual de exponente aditivo. Además, M es un $\mathbb{Z}$-módulo derecho con la operación $x * n = nx$ puesto que $\mathbb{Z}$ es un anillo conmutativo.

Definición 1.65. 1. Sea M un A-módulo derecho. Decimos que $\emptyset \neq N \subseteq M$ es un *A-submódulo* de M, denotado $N \leq M$, si N es también un A-módulo derecho bajo las operaciones de M. Equivalentemente, N es un A-submódulo derecho de M si se verifica que $x + y \in N$ y $xa \in N$ para todo $x \in N$ y todo $a \in A$.

2. Si N es un submódulo de M, entonces

$$M/N := \{x + N : x \in M\}$$

es un A-módulo bajo las operaciones $(x + I) + (x' + I) = (x + x') + I$ y $(x + I)a := (xa) + I$. El conjunto M/N se denomina *módulo cociente*.

3. Sean M y N dos A-módulos. Decimos que $\varphi : M \longrightarrow N$ es un *homomorfismo de A-módulos* si para todo $x, y \in M$ y todo $a \in A$ se cumple

   a) $\varphi(x + y) = \varphi(x) + \varphi(y)$.

   b) $\varphi(xa) = \varphi(x)a$.

   Similarmente a lo descrito para anillos y álgebras se define *monomorfismo*, *epimorfismo* e *isomorfismo*. En caso que $M = N$, decimos que φ es un *endomorfismo*. El conjunto de homomorfismos de M a N se denota $\mathrm{Hom}_A(M, N)$ y si $M = N$, se denota $\mathrm{End}_A(M)$.

Lema 1.66. *Dado $\varphi : M \longrightarrow N$ un homomorfismo de A-módulos, entonces*

1. $\mathrm{Ker}(\varphi) := \{x \in M : \varphi(x) = 0_N\}$ *es un submódulo de* M.
2. $\mathrm{Im}(\varphi) := \{\varphi(x) : x \in M\}$ *es un submódulo de* N.
3. φ *es un monomorfismo si y solo si* $\mathrm{Ker}(\varphi) = \{0\}$.
4. φ *es un epimorfismo si y solo si* $\mathrm{Im}(\varphi) = S$.

Demostración.

1. Sean $x, y \in \mathrm{Ker}(\varphi)$ y $a \in A$. Entonces $\varphi(x + y) = \varphi(x) + \varphi(y) = 0$ y $\varphi(xa) = \varphi(x)a = 0 \cdot a = 0$.
2. Sean $x, y \in \mathrm{Im}(\varphi)$, entonces existen $x', y' \in R$ tales que $\varphi(x') = x$ y $\varphi(y') = y$. Por lo tanto, $\varphi(x' + y') = \varphi(x') + \varphi(y') = x + y$ y $\varphi(x'a) = \varphi(x')a = xa$.
3. Como φ es un monomorfismo y $\varphi(0) = 0$, entonces $\mathrm{Ker}(\varphi) = \{0\}$. Recíprocamente, si $x, y \in M$ con $\varphi(x) = \varphi(y)$, entonces $\varphi(x - y) = 0$. Pero $\mathrm{Ker}(\varphi) = \{0\}$, lo cual implica que $x - y = 0 \Rightarrow x = y$.
4. Se sigue de la definición.

□

Teorema 1.67 (Primer teorema de isomorfía para módulos)**.** *Sea $f : M \longrightarrow N$ un homomorfismo de A-módulos. Entonces $M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$.*

Demostración. Definamos $\varphi : M/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ como $\varphi(x + \mathrm{Ker}(f)) = f(x)$. Veamos que φ está bien definida y es inyectiva. Sean $x, y \in M$ y $a \in A$, entonces

$$\begin{aligned} x + \mathrm{Ker}(f) = y + \mathrm{Ker}(f) &\iff x - y \in \mathrm{Ker}(f) \iff f(x - y) = 0 \\ &\iff f(x) - f(y) = 0 \iff f(x) = f(y) \\ &\iff \varphi(x + \mathrm{Ker}(f)) = \varphi(y + \mathrm{Ker}(f)). \end{aligned}$$

Por otro lado,

$$\begin{aligned} \varphi((x + \mathrm{Ker}(f)) + (y + \mathrm{Ker}(f))) &= \varphi((x + y) + \mathrm{Ker}(f)) \\ &= f(x + y) = f(x) + f(y) \\ &= \varphi(x + \mathrm{Ker}(f)) + \varphi(y + \mathrm{Ker}(f)). \end{aligned}$$

$$\varphi((x+\mathrm{Ker}(f))a) = \varphi((xa)+\mathrm{Ker}(f)) = f(xa) = f(x)a = \varphi(x+\mathrm{Ker}(f))a.$$

Por lo tanto, φ es un monomorfismo de módulos. Resta verificar que es sobreyectiva. Sea $a \in \mathrm{Im}(f)$, entonces existe $x \in R$ tal que $f(x) = a$ y en consecuencia $\varphi(x+\mathrm{Ker}(f)) = f(x) = a$. Por lo tanto, φ es un isomorfismo y $M/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. □

Teorema 1.68 (Teorema de correspondencia para módulos)**.** *Sea $f : M \longrightarrow N$ un epimorfismo de módulos. Entonces existe una correspondencia biyectiva entre los submódulos de M que contienen a $\mathrm{Ker}(\varphi)$ y los submódulos de N.*

Definición 1.69. Sea $0 \neq M$ un A-módulo derecho.

1. Los conjuntos $\{0\} \leq M$ y $M \leq M$ se denominan submódulos triviales. Si estos son los únicos submódulos de M, decimos que M es *simple* o *irreducible*.

2. Sean M_1, M_2 submódulos de M. Decimos que M es la *suma directa* de M_1 y M_2 si y solo si $M = M_1 + M_2$ y $M_1 \cap M_2 = 0$. Además, escribimos $M = M_1 \oplus M_2$ donde M_1 y M_2 son llamados sumandos directos de M.

3. M es llamado *completamente reducible* o *semisimple* si M es la suma directa de A-submódulos irreducibles. A es *semisimple* si el A-módulo regular es semisimple.

4. M es llamado *indescomponible* si no existe una descomposición directa $M = M_1 \oplus M_2$ con A-módulos $M_1 \neq 0 \neq M_2$.

5. Si M es un A-módulo derecho y $x \in M$, entonces $xA := \{xa : a \in A\}$ es un A-submódulo de M llamado *submódulo cíclico*.

6. Un A-submódulo derecho N de M es *maximal* si y solo si $N \neq M$ y si $N \leq L \leq M$ para algún submódulo derecho L de M, entonces $L = M$ o $L = N$.

7. Si $S \subseteq M$, definimos el *submódulo generado* por S, denotado $\langle S \rangle$, como

$$\langle S \rangle := \left\{ \sum_{i=1}^{n} s_i a_i : s_i \in S, a_i \in A, n \in \mathbb{N} \right\}.$$

   En caso que $\langle S \rangle = M$, decimos que S genera a M. Además, si S es finito, decimos que M es *finitamente generado*. Podemos verificar

que $\langle S\rangle = \cap_{S\subseteq N\leq M} N$, es decir, $\langle S\rangle$ es el submódulo más pequeño que contiene a S.

Lema 1.70 (Lema de Schur)**.** *Sea M un A-módulo simple. Luego,* $\mathrm{End}_A(M)$ *es un anillo con división.*

Demostración. Sea $0 \neq f \in \mathrm{End}_A(M)$. Demostremos que f es una biyección y por lo tanto es invertible. Como $0 \neq \mathrm{Im}(f) \leq M$ y M es simple, $\mathrm{Im}(f) = M$. Similarmente, $\mathrm{Ker}(\varphi) \leq M$ y $\mathrm{Ker}(\varphi) \neq M$, entonces $\mathrm{Ker}(\varphi) = 0$. □

Teorema 1.71. *M es un A-módulo simple si y solo si $M = \langle x\rangle$ para todo $0 \neq x \in M$.*

Demostración. Supongamos que M es un A-módulo simple y $0 \neq x \in M$, entonces $\langle x\rangle$ es un submódulo no nulo de M. Como M es simple, $\langle x\rangle = M$. Recíprocamente, supongamos que $M = \langle x\rangle$ para todo $0 \neq x \in M$ y sea $0 \neq N$ un submódulo de M. Luego, existe un $y \in N$ tal que $M = \langle y\rangle \subseteq N$ de donde se sigue que $M = N$. □

Definición 1.72. Sea N un subconjunto de A-módulo derecho M. Definimos el *anulador derecho* de N como

$$\mathrm{Ann}_d(N) := \{a \in A : xa = 0 \text{ para todo } x \in N\}.$$

Similarmente, se puede definir el anulador izquierdo de N.

Observación 1.73. El anulador derecho de N es un ideal derecho de A. Note que $\mathrm{Ann}_d(N) \neq \emptyset$ puesto que $\{0\} \in \mathrm{Ann}_d(N)$. Además, dados $a_1, a_2 \in \mathrm{Ann}_d(N), x \in N$ y $b \in A$ se tiene que $(a_1 + a_2)x = a_1x - a_2x = 0$ y $(a_1b)x = a_1(bx) = 0$.

Definición 1.74. Sea M un A-módulo derecho y $\{x_\alpha\}_I$ un conjunto de elementos de M.

1. $\{x_\alpha\}_I$ es una *base* de M si y solo si $\{x_\alpha\}_I$ genera a M y es linealmente independiente.

2. M es un *A-módulo libre* si y solo si M tiene una base.

Teorema 1.75. *Sea M un A-módulo derecho y $\{x_\alpha\}_I$ un conjunto de elementos de M. Entonces $\{x_\alpha\}_I$ es una base para M si y solo si cada elemento $x \in M$ es escrito de forma única como $\sum_I x_\alpha a_\alpha$.*

Demostración. Sea $\{x_\alpha\}_I$ una base para M entonces $x = \sum_I x_\alpha a_\alpha$. Si además $x = \sum_I x_\alpha b_\alpha$, se concluye que $\sum_I x_\alpha(a_\alpha - b_\alpha) = 0$. Por lo tanto, $a_\alpha = b_\alpha$ para todo $\alpha \in I$ y x es escrito de forma única. Por otro lado, si cada elemento $x \in M$ es escrito de forma única como $\sum_I x_\alpha a_\alpha$, se tiene que $\{x_\alpha\}_I$ genera a M. Además, sea $\sum_I x_\alpha a_\alpha = 0$. Como $\sum_I x_\alpha 0 = 0$, entonces $a_\alpha = 0$ para todo $\alpha \in I$, con lo cual se comprueba la independencia lineal de $\{x_\alpha\}_I$. En consecuencia, $\{x_\alpha\}_I$ es una base para M. □

Definición 1.76.
1. Un elemento $0 \neq e \in A$ se denomina *idempotente* si $e^2 = e$.
2. Dos idempotentes e_1 y e_2 son *ortogonales* si $e_1e_2 = 0 = e_2e_1$.
3. Un idempotente e se denomina *primitivo* si no puede ser escrito como $e = e_1 + e_2$ con e_1, e_2 idempotentes ortogonales.

Lema 1.77. *Sea $0 \neq e = e^2 \in A$. Entonces e es primitivo si y solo si eA es indescomponible.*

Demostración. Supongamos que e no es primitivo, esto es $e = e_1 + e_2$ con e_1, e_2 idempotentes y $e_1e_2 = e_2e_1 = 0$. Entonces $eA = e_1A + e_2A$. Además, sea $x \in e_1A \cap e_2A \Rightarrow x = e_1a_1 = e_2a_2$, para algún a_1 y $a_2 \in A$. Luego, $x = e_1a_1 = e_1^2a_1 = e_1e_2a_2 = 0$. Por lo tanto, $e_1A \cap e_2A = 0$ y $eA = e_1A \oplus e_2A$.

Recíprocamente, supongamos que $eA = M_1 \oplus M_2$. Entonces $e = e_1 + e_2$ y existe $a_1 \in A$ tal que $e_1 = ea_1$. Multiplicando a la izquierda por e tenemos $ee_1 = e^2a_1 = ea_1 = e_1$. Por lo cual, $e_1^2 + e_2e_1 = e_1 \Rightarrow e_1^2 - e_1 = e_2e_1 \in M_1 \cap M_2$. En consecuencia, $e_2e_1 = 0$ y $e_1^2 = e_1$. Similarmente se demuestra que $e_1e_2 = 0$ y $e_2^2 = e_2$. □

1.6. El álgebra de grupo KG

En esta sección definiremos y presentaremos algunos resultados relacionados con el álgebra de grupo KG, debido a que tiene especial importancia en la definición de códigos de grupo.

Definición 1.78. Sea G un grupo finito de orden n y K un cuerpo. Definimos el conjunto KG como

$$KG := \left\{ \alpha = \sum_{g \in G} a_g g : a_g \in K \right\}.$$

Este conjunto es un K-álgebra denominado *álgebra de grupo* bajo las siguientes operaciones

$$\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (a_g + b_g) g.$$

$$b \sum_{g\in G} a_g g = \sum_{g\in G} (b a_g) g.$$

$$\begin{aligned}\left(\sum_{g\in G} a_g g\right)\left(\sum_{h\in G} b_h h\right) &= \sum_{g,h\in G} (a_g b_g)(gh) \\ &= \sum_{g\in G}\left(\sum_{hk=g} a_h b_k\right) g \\ &= \sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right) g.\end{aligned}$$

Observación 1.79. El conjunto $B := \{1g : 1 \in K, g \in G\}$ es una base para el álgebra de grupo KG. En efecto, B genera a KG puesto que $\sum_{g\in G} a_g g = \sum_{g\in G} a_g(1g)$. Adicionalmente, los elementos de B son linealmente independientes dado que si $\sum_{i=1}^{n} a_i(1g_i) = \sum_{i=1}^{n} a_i g_i = 0$, entonces $a_i = 0$ para todo $i = 1, 2, \ldots, n$. Por lo tanto, $\dim_K(KG) = |G| = n$.

Ejemplo 1.80. Sean $G = \langle g \mid g^3 = e\rangle$ y $K = \mathbb{F}_2$. Luego,

$$\begin{aligned}\mathbb{F}_2 G = \{&0e + 0g + 0g^2, 1e + 0g + 0g^2, 0e + 1g + 0g^2, 1e + 1g + 0g^2, \\ &0e + 0g + 1g^2, 1e + 0g + 1g^2, 0e + 1g + 1g^2, 1e + 1g + 1g^2\}.\end{aligned}$$

Si $u = 1e + 0g + 1g^2$ y $v = 0e + 1g + 1g^2$, entonces $u + v = 1e + 1g + 0g^2$ y $uv = 1e + 0g + 1g^2$.

Lema 1.81. *El cuerpo K es un KG-módulo izquierdo con la operación $g\lambda = \lambda$ para todo $g \in G$ y todo $\lambda \in K$. Este KG-módulo se denomina módulo trivial.*

Demostración. Veamos que K satisface las propiedades para KG-módulo.

Sea $\lambda_1, \lambda_2 \in K$ y $\sum_{g\in G} a_g g, \sum_{g\in G} b_g g \in KG$. Luego,

$$\begin{aligned}\left(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\right)\lambda &= \left(\sum_{g\in G}(a_g+b_g)g\right)\lambda = \sum_{g\in G}(a_g+b_g)\lambda \\ &= \sum_{g\in G}(a_g\lambda + b_g\lambda) = \sum_{g\in G} a_g\lambda + \sum_{g\in G} b_g\lambda \\ &= \left(\sum_{g\in G} a_g g\right)\lambda + \left(\sum_{g\in G} b_g g\right)\lambda.\end{aligned}$$

$$\begin{aligned}\left(\sum_{g\in G} a_g g\right)(\lambda_1+\lambda_2) &= \sum_{g\in G} a_g(\lambda_1+\lambda_2) = \sum_{g\in G}(a_g\lambda_1 + a_g\lambda_2) \\ &= \sum_{g\in G} a_g\lambda_1 + \sum_{g\in G} a_g\lambda_2 \\ &= \left(\sum_{g\in G} a_g g\right)\lambda_1 + \left(\sum_{g\in G} a_g g\right)\lambda_2.\end{aligned}$$

$$\begin{aligned}\left(\sum_{g\in G} a_g g \sum_{h\in G} b_h h\right)\lambda &= \left(\sum_{g,h\in G} a_g b_h gh\right)\lambda = \left(\sum_{g,h\in G} a_g b_h \lambda\right) \\ &= \left(\sum_{g\in G} a_g\left(\sum_{h\in G} b_h\lambda\right)\right) \\ &= \sum_{g\in G} a_g g\left(\left(\sum_{h\in G} b_h h\right)\lambda\right).\end{aligned}$$

□

Teorema 1.82. *Si M y N son KG-módulos, entonces* $\mathrm{Hom}_K(M,N)$ *es un KG-módulo mediante la operación $gf(m) = gf(g^{-1}m)$ para $m \in M$, $g \in G$ y $f \in \mathrm{Hom}_k(M,N)$.*

Demostración. Sean $m, m_1, m_2 \in M$, $g \in G$, $f \in \mathrm{Hom}_K(M,K)$ y $\lambda \in K$. Inicialmente probemos que $gf \in \mathrm{Hom}_k(M,N)$. Entonces

$$\begin{aligned}gf(m_1+m_2) &= gf(g^{-1}(m_1+m_2)) = gf(g^{-1}m_1 + g^{-1}m_2) \\ &= g(f(g^{-1}m_1) + f(g^{-1}m_2)) = gf(g^{-1}m_1) + gf(g^{-1}m_2) \\ &= gf(m_1) + gf(m_2).\end{aligned}$$

$$\begin{aligned} gf(\lambda m) &= gf(g^{-1}(\lambda m)) = gf(\lambda g^{-1}m) = g\lambda f(g^{-1}m) \\ &= \lambda gf(g^{-1}m) = \lambda gf(m). \end{aligned}$$

Demostremos ahora que, bajo la acción definida, $\mathrm{Hom}_K(M,N)$ es un KG-módulo. Para esto verifiquemos que la acción es lineal.

$$\begin{aligned} g(f_1+f_2)(m) &= g(f_1+f_2)(g^{-1}m) = gf_1(g^{-1}m) + gf_2(g^{-1}m) \\ &= gf_1(m) + gf_2(m). \end{aligned}$$

$$g(\lambda f)(m) = g(\lambda f)(g^{-1}m) = \lambda gf(g^{-1}m) = \lambda gf(m).$$

Además, $ef(m) = ef(em) = f(m)$ y

$$\begin{aligned} ((g_1g_2)f)(m) &= (g_1g_2)f((g_1g_2)^{-1}m) = (g_1g_2)f(g_2^{-1}g_1^{-1}m)) \\ &= (g_1g_2)f(g_2^{-1}(g_1{-}1m)) = g_1(g_2f(g_2^{-1}(g_1{-}1m))) \\ &= [g_1(g_2f)](m). \end{aligned}$$

□

Teniendo en cuenta este teorema y el Lema 1.81 podemos definir el siguiente KG-módulo.

Definición 1.83. Sea M un KG-módulo. Entonces $M^* := \mathrm{Hom}(M,K)$ es un KG-módulo mediante la operación

$$gf(m) = f(g^{-1}m)$$

para $m \in M$, $g \in G$ y $f \in \mathrm{Hom}(M,K)$. M^* se denomina el *módulo dual* de M y si $M \cong M^*$, decimos que M es un KG-módulo *autodual*.

Teorema 1.84. *Sean K un cuerpo y $G = \langle g \rangle$ el grupo cíclico de orden n. Entonces $K[x]/\langle x^n - 1\rangle \cong KG$ (como K-álgebras).*

Demostración. Sea $\phi : K[x]/\langle x^n-1\rangle \longrightarrow KG$ definida como $\phi(\sum_{i=0}^{n-1} a_ix^i) = \sum_{i=0}^{n-1} a_ig^i$. Entonces ϕ es un homomorfismo de álgebras. En efecto,

$$\begin{aligned} \phi\left(\sum_{i=0}^{n-1} a_ix^i + \sum_{i=0}^{n-1} b_ix^i\right) &= \phi(\sum_{i=0}^{n-1}(a_i+b_i)x^i = \sum_{i=0}^{n-1}(a_i+b_i)g^i \\ &= \phi\left(\sum_{i=0}^{n-1} a_ix^i\right) + \phi\left(\sum_{i=0}^{n-1} b_ix^i\right). \end{aligned}$$

$$\phi\left(\lambda\sum_{i=0}^{n-1}a_ix^i\right)=\phi(\sum_{i=0}^{n-1}(\lambda a_i)x^i=\sum_{i=0}^{n-1}(\lambda a_i)g^i$$
$$=\lambda\sum_{i=0}^{n-1}a_ig^i=\lambda\phi\left(\sum_{i=0}^{n-1}a_ix^i\right).$$

$$\phi\left(\sum_{i=0}^{n-1}a_ix^i\sum_{j=0}^{n-1}b_jx^j\right)=\phi\left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}a_ib_jx^{(i+j)\mod n}\right)=\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}a_ib_ig^{i+j}$$
$$=\sum_{i=0}^{n-1}a_ig^i\sum_{j=0}^{n-1}b_jg^j=\phi\left(\sum_{i=0}^{n-1}a_ix^i\right)\phi\left(\sum_{i=0}^{n-1}b_ix^i\right).$$

Además, ϕ es un monomorfismo puesto que

$$\mathrm{Ker}(\phi)=\left\{\sum_{i=0}^{n-1}a_ix^i:\sum_{i=0}^{n-1}a_ig^i=0\right\}=\{0\}.$$

Por otro lado, dado $\sum_{i=0}^{n-1}a_ig^i\in KG$ se tiene que $\phi(\sum_{i=0}^{n-1}a_ix^i)=\sum_{i=0}^{n-1}a_ig^i$, esto es, ϕ es un epimorfismo. En consecuencia, $K[x]/\langle x^n-1\rangle\cong KG$.

□

Teorema 1.85. *Sea G un grupo finito y K un cuerpo tal que* $\mathrm{char}(K)=0$ *o* $\mathrm{char}(K)\nmid|G|$. *Si M es un KG-módulo y N es un KG-submódulo de M, entonces N es un sumando directo de M como KG-módulo.*

Demostración. El módulo N es un K-subespacio vectorial, por lo tanto existe un K-subespacio L tal que $M=N\oplus L$. Definamos $\pi:M\longrightarrow N$ como $\pi(n+l)=n$ para todo $m=n+l\in M$. La función π es un transformación lineal puesto que

$$\pi(m_1+m_2)=\pi(n_1+l_1+n_2+l_2)=n_1+n_2=\pi(m_1)+\pi(m_2).$$

$$\pi(km_1)=\pi(k(n_1+l_1)=\pi(kn_1+kl_1)=kn_1=k\pi(m_1).$$

Dado que $\mathrm{char}(K)=0$ o $\mathrm{char}(K)\nmid|G|$, podemos definir $P:M\longrightarrow M$ como

$$P(m):=\frac{1}{|G|}\sum_{g\in G}g\pi(g^{-1}m)$$

para todo $m \in M$. Verifiquemos que $P \in \mathrm{End}_K(M)$.

$$\begin{aligned} P(m_1+m_2) &= \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}(m_1+m_2)) \\ &= \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}m_1+g^{-1}m_2) \\ &= \frac{1}{|G|}\sum_{g\in G} g(\pi(g^{-1}m_1)+\pi(g^{-1}m_1)) \\ &= \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}m_1) + \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}m_2) \\ &= P(m_1)+P(m_2). \end{aligned}$$

$$\begin{aligned} P(km) &= \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}(km)) = \frac{1}{|G|}\sum_{g\in G} g(k\pi(g^{-1}m)) \\ &= k\frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}m) = kP(m). \end{aligned}$$

Más aún, P es un KG-homomorfismo puesto que

$$\begin{aligned} P(hm) &= \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}hm) = \frac{1}{|G|}\sum_{g\in G} hh^{-1}g\pi(g^{-1}hm) \\ &= \frac{1}{|G|}h\sum_{g\in G}(h^{-1}g)\pi((h^{-1}g)^{-1}m) \\ &= \frac{1}{|G|}h\sum_{y\in G} y\pi(y^{-1}m) \\ &= hP(m). \end{aligned}$$

Además, como $g^{-1}n \in N$ entonces $g\pi(g^{-1}n) = gg^{-1}n = n$. Luego,

$$P(n) = \frac{1}{|G|}\sum_{g\in G} g\pi(g^{-1}n) = \frac{1}{|G|}\sum_{g\in G} n = \frac{1}{|G|}|G|n = n.$$

Por otro lado, como $g\pi(g^{-1}m) \in N$ se tiene que $P(m) \in N$. Si $P(m) = n'$, entonces

$$P^2(m) = P(P(m)) = P(n') = n' = P(m).$$

Por lo tanto, $\mathrm{Im}(P) = N$ y $P^2 = P$. Por el Lema 1.52, se sigue que

$$M = \mathrm{Ker}(P) \oplus \mathrm{Im}(P) = \mathrm{Ker}(P) \oplus N$$

donde $\mathrm{Ker}(P)$ es un submódulo de M. □

Teorema 1.86 (Maschke)**.** *Sea G un grupo finito y K un cuerpo tal que* $\mathrm{char}(K) = 0$ *o* $\mathrm{char}(K) \nmid |G|$*. Entonces, todo KG-módulo M es semisimple.*

Demostración. Por inducción sobre $\dim_K(M)$ tenemos que si $\dim_K(M) = 1$, entonces M es simple y por lo tanto, semisimple. Supongamos ahora que todo módulo con dimensión menor que n es semisimple y sea M con $\dim_K(M) = n$. Si M es simple entonces M es semisimple. Si M no es simple, entonces existe un KG-submódulo N de M no trivial. Por el teorema anterior, existe otro submódulo L tal que $M = N \oplus L$ con $\dim_K(M) < n$ y $\dim_K(L) < n$. Por la hipótesis de inducción, N y L son semisimples y en consecuencia M es semisimple. □

Capítulo 2

Códigos lineales

Los códigos lineales son una de las clases de códigos más importante y estudiada, puesto que su estructura algebraica facilita su análisis y aplicación. En este capítulo abordaremos este tipo de códigos, basándonos en los resultados establecidos en [3], [7], [14] y [15].

2.1. Conceptos básicos

En esta sección presentaremos una breve introducción a la teoría de códigos lineales. Para esto definiremos algunos conceptos fundamentales, tales como matriz generadora, matriz de control, distancia mínima y código dual.

Definición 2.1.

1. Un *código* C es un subconjunto del espacio vectorial $\mathbb{F}_q^n$ donde $\mathbb{F}_q$ es un cuerpo finito con q elementos y $n \in \mathbb{N}$.
2. Un elemento de C es una secuencia $v = v_1 v_2 \dots v_n$, con $v_i \in \mathbb{F}_q$, denominado *codeword* o *palabra*, la cual también puede ser escrita como n-tupla $v = (v_1, v_2, \dots, v_n)$.

Así, si un código C es un conjunto formado por M palabras q-arias de longitud n, decimos que C es un $[n, M]$-código sobre $\mathbb{F}_q$.

Ejemplo 2.2. $C = \{000, 001, 010, 011, 100, 101, 110, 111\}$ es un $[3, 8]$-código binario.

Definición 2.3. Un *código lineal* C es un subespacio vectorial de $\mathbb{F}_q^n$, denotado $C \leq \mathbb{F}_q^n$. Además, si $\dim_{\mathbb{F}_q}(C) = k$, decimos que C es un $[n, k]$-código lineal sobre $\mathbb{F}_q$.

Observación 2.4. A partir de la definición se sigue que un código lineal contiene q^k palabras.

Definición 2.5. Sea C un $[n,k]$-código sobre $\mathbb{F}_q$.

1. Sea $G \in M_{k\times n}(\mathbb{F}_q)$, esto es, G es una matriz de tamaño $k \times n$ con entradas en $\mathbb{F}_q$. Si $k \geq 1$, decimos que G es una *matriz generadora* de C si y solo si
$$C = \mathbb{F}_q^k G := \{uG : u = (u_1, u_2, \ldots, u_k) \in \mathbb{F}_q^k\}.$$
En caso que $k = 0$, se define $G = (0, \ldots, 0) \in \mathbb{F}_q^n$. Un código lineal puede tener distintas matrices generadoras, entonces si $G = [I_k|A]$, decimos que G está en *forma estándar*.

2. Si $k < n$, decimos que $H \in M_{(n-k)\times n}(\mathbb{F}_q)$ es una *matriz de control* de C si y solo si
$$C = \{v \in \mathbb{F}_q^n : Hv^t = 0\}.$$
En caso que $C = \mathbb{F}_q^n$, se define $H = (0, \ldots, 0) \in \mathbb{F}_q^n$. Así como con la matriz generadora, es posible tener varias matrices de control para un mismo código.

Observación 2.6.

1. Se puede verificar que una matriz generadora de C es una matriz $G \in M_{k\times n}(\mathbb{F}_q)$ cuyas filas forman una base para C. Esto debido a que $\dim_{\mathbb{F}_q}(C) = k$ y a que las filas de G generan a C. Veamos esto último.
$$\begin{aligned} uG &= (u_1, \ldots, u_k) \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \cdots & & \cdots \\ g_{k1} & \cdots & g_{kn} \end{pmatrix} \\ &= (u_1 g_{11} + \cdots + u_k g_{k1}, \ldots, u_1 g_{1n} + \cdots + u_k g_{kn}) \\ &= u_1(g_{11}, \ldots, g_{1n}) + \cdots + u_k(g_{k1}, \ldots, g_{kn}) \end{aligned}$$
Luego, $C = \mathbb{F}_q^k G = \langle (g_{11}, \ldots, g_{1n}), \ldots, (g_{k1}, \ldots, g_{kn}) \rangle$.

2. La matriz de control H de un $[n,k]$-código lineal C tiene $n-k$ filas independientes. En efecto, sea $L : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-k}$ una transformación lineal definida como $L(v) = Hv^t$ con $\mathrm{Ker}(L) = C$. Por los Teoremas 1.48 y 1.50 se sigue que
$$\begin{aligned} \dim(\mathbb{F}_q^n) &= \dim(\mathrm{Ker}(L)) + \dim(\mathrm{Im}(L)) \\ &\Rightarrow n = \dim(C) + \mathrm{rang}(H) \\ &\Rightarrow n = k + \mathrm{rang}(H). \end{aligned}$$

Teorema 2.7. *Si $G = [I_k|A]$ es una matriz generadora de un $[n,k]$-código lineal C, entonces $H = [-A^t|I_{n-k}]$ es una matriz de control para C.*

Demostración. Sea L la transformación lineal $v \longmapsto Hv^t$. Como $HG^t = -A^t + A^t = 0$, se tiene que $C = \mathbb{F}_q^k G \subseteq \mathrm{Ker}(L)$. Por el Teorema 1.50, se concluye que $\dim(\mathrm{Im}(L)) = \mathrm{rang}(H) = n - k$. Entonces $\dim(\mathrm{Ker}(L)) = k = \dim(C)$ y por ende, $C = \mathrm{Ker}(L)$. Por lo tanto, H es una matriz de control para C. □

Definición 2.8. Sean $u = (u_1, u_2, \ldots, u_n)$ y $v = (v_1, v_2, \ldots, v_n)$ dos palabras de longitud n en $\mathbb{F}_q$. Definimos la *distancia de Hamming* entre u y v, denotada $\mathrm{d}(u,v)$, como el número de coordenadas en que estos difieren, esto es

$$\mathrm{d}(u,v) := |\{i : u_i \neq v_i\}|.$$

Además, definimos la *distancia mínima* de un código C como

$$d = \mathrm{d}(C) := \min\{\mathrm{d}(u,v) : u, v \in C, u \neq v\}.$$

En caso que $|C| = 1$ definimos $\mathrm{d}(C) := 0$.

Ejemplo 2.9. Sean $C = \{000, 100, 110\}$. Entonces

$$\mathrm{d}(000,100) = 1,\ \mathrm{d}(000,110) = 2 \text{ y } \mathrm{d}(100,110) = 1.$$

Por lo tanto, $\mathrm{d}(C) = 1$.

Observación 2.10. La distancia de Hamming es una métrica sobre $\mathbf{F}_q^n$ puesto que satisface las siguientes condiciones:

1. $\mathrm{d}(u,v) \geq 0$ para todo $u, v \in \mathbb{F}_q^n$.
2. $\mathrm{d}(u,v) = 0 \iff u = v$.
3. $\mathrm{d}(u,v) = \mathrm{d}(u,v)$ para todo $u, v \in \mathbb{F}_q^n$.
4. $\mathrm{d}(u,v) \leq \mathrm{d}(u,w) + \mathrm{d}(w,v)$ para todo $u, v, w \in \mathbb{F}_q^n$.

Además como $\mathbb{F}_q^n$ es un grupo abeliano con la suma, se sigue que

$$\mathrm{d}(u,v) = \mathrm{d}(u+w, v+w) \text{ para todo } u, v, w \in \mathbb{F}_q^n.$$

En efecto, $u_i \neq v_i \iff u_i + w_i \neq v_i + w_i$, entonces

$$\mathrm{d}(u,v) = |\{i : u_i \neq v_i\}| = |\{i : u_i + w_i \neq v_i + w_i\}| = \mathrm{d}(u+w, v+w).$$

Un $[n,k]$-código lineal con mínima distancia d se denota $[n,k,d]$-código lineal. Esta métrica es importante debido a que cuanto mayor es la distancia mínima d, mayor es el número de errores que un código puede corregir.

Teorema 2.11 (Cota de Singleton)**.** *Sea C un $[n,k,d]$-código lineal sobre $\mathbb{F}_q$. Entonces $d \leq n-k+1$.*

Demostración. Sea $f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n-(d-1)}$ la función definida como

$$f(u_1,\ldots,u_{n-(d-1)},u_{n-d+2},\ldots,u_n) = (u_1,\ldots,u_{n-(d-1)}).$$

Notemos que f es inyectiva. En efecto, si $f(u) = f(v)$ para $u = (u_1,\ldots,u_n)$ y $v = (v_1,\ldots,v_n)$, entonces $(u_1,\ldots,u_{n-(d-1)}) = (v_1,\ldots,v_{n-(d-1)})$. Por lo tanto, u y v son diferentes en máximo $n-(n-(d-1)) = d-1$ coordenadas, esto es, $d(u,v) \leq d-1$, lo cual es una contradicción. Por lo tanto,

$$q^k = |C| = |f(C)| \leq |\mathbb{F}_q^{n-(d-1)}| = q^{n-(d-1)}.$$

En consecuencia, $k \leq n-(d-1)$, es decir, $d \leq n-k+1$. □

Definición 2.12. Los códigos que satisfacen la cota de Singleton se denominan MDS-códigos (maximum distance separable). Por lo cual, decimos que un $[n,k,d]$-código sobre $\mathbb{F}_q$ con $d = n-k+1$ es un MDS-código.

Teorema 2.13. *Sea C un código con mínima distancia d y sea $t = \lfloor \frac{d-1}{2} \rfloor$. Entonces es posible detectar hasta $d-1$ errores y corregir hasta t errores.*

Demostración. Suponga que un palabra es transmitida como x con $d-1$ errores o menos, dado que la distancia mínima del código es d, se tiene que x no es una palabra de C y por lo tanto los errores son detectados. Por otro lado, suponga que una palabra es transmitida como x con t errores o menos y sean u y v dos palabras tales que $\mathrm{d}(u,x) \leq t$ y $\mathrm{d}(x,v) \leq t$. Entonces $\mathrm{d}(u,v) \leq \mathrm{d}(u,x) + \mathrm{d}(x,v) \leq 2t \leq d-1$. Por lo tanto, $u = v$, es decir, u es única y es posible corregir los errores. Esto no se garantiza cuando la palabra es transmitida con más de t errores. □

Definición 2.14. El *peso de una palabra* $v = (v_1, v_2, \ldots, v_n)$ se define como el numero de coordenadas no nulas. Esto es,

$$\mathrm{wt}(v) := |\{i : v_i \neq 0\}|.$$

Además, definimos el *peso mínimo* de un código C como

$$\mathrm{wt}(C) := \mathrm{mín}\{\mathrm{wt}(v) : v \in C, v \neq 0\}.$$

En caso que $C = 0$, se define $\mathrm{wt}(C) := 0$.

Lema 2.15. *Sean* $u, v \in \mathbb{F}_q^n$, *entonces* $\mathrm{d}(u,v) = \mathrm{wt}(u-v)$. *En particular* $\mathrm{d}(u,0) = \mathrm{wt}(u)$.

Demostración. Por la definición de distancia y peso se sigue que

$$\mathrm{d}(u,v) = |\{i : u_i \neq v_i\}| = |\{i : u_i - v_i \neq 0\}| = \mathrm{wt}(u-v).$$

En particular, $\mathrm{d}(u,0) = \mathrm{wt}(u-0) = \mathrm{wt}(u)$. □

Teorema 2.16. *Si* $C \leq \mathbb{F}_q^n$, *entonces* $\mathrm{d}(C) = \mathrm{wt}(C)$.

Demostración. Si $C = \{0\}$ la afirmación es inmediata. Para $C \neq \{0\}$, sean $u, v \in C$. Como C es un subespacio vectorial, se tiene que $w = u - v \in C$. Luego,

$$\begin{aligned}
\mathrm{d}(C) &= \mathrm{mín}\{d(u,v) : u \neq v, u, v \in C\} \\
&= \mathrm{mín}\{\mathrm{wt}(u-v) : u - v \in C, u - v \neq 0\} \\
&= \mathrm{mín}\{\mathrm{wt}(w) : w \in C, w \neq 0\} \\
&= \mathrm{wt}(C).
\end{aligned}$$

□

Definición 2.17. Sea $A_i(C)$ el número de palabras de peso i en el código $C \leq \mathbb{F}_q^n$. El listado de los valores A_i donde $0 \leq i \leq n$ es llamado la *distribución de pesos* de C.

Teorema 2.18. *Sea* C *un* $[n,k,d]$*-código lineal en* $\mathbb{F}_q^n$. *Entonces*

1. $A_0(C) + A_1(C) + \cdots + A_n(C) = q^k$.
2. $A_0(C) = 1$ *y* $A_1(C) = A_2(C) = \cdots = A_{d-1} = 0$.

Demostración. 1. Se sigue de que el código C tiene q^k palabras.

2. El código C tiene un solo elemento con peso 0, entonces $A_0(C) = 1$. Además, si d es la distancia mínima, no existen palabras cuyo peso sea menor que d. Por lo tanto, $A_1(C) = A_2(C) = \cdots = A_{d-1} = 0$.

□

Podemos relacionar la matriz de control y el peso mínimo de un código con el siguiente teorema.

Teorema 2.19. *Sea $C \leq \mathbb{F}_q^n$ un código lineal, entonces* $\mathrm{wt}(C) = d$ *si y solo si la matriz de control H tiene d columnas linealmente dependientes pero no $d-1$ columnas linealmente dependientes.*

Demostración. Si $\mathrm{wt}(C) = d$, entonces existe un vector v con d coordenadas diferentes de 0 que satisface $Hv^t = 0$, por lo tanto H tiene d columnas dependientes pero no $d-1$ columnas dependientes, dado que si así fuera, existiría un vector u con peso $d-1$ tal que $Hu^t = 0$, lo cual es una contradicción. Similarmente, si H tiene d columnas dependientes pero no $d-1$ columnas dependientes, los vectores que satisfacen $Hv^t = 0$ tienen mínimo d coordenadas distintas de 0, por lo tanto $\mathrm{wt}(C) = d$. □

En la Observación 2.6 mostramos que la matriz de control H de un $[n,k]$-código lineal C tiene $n-k$ filas independientes. Estas filas forman una base para otro código que llamamos el código dual y denotamos $C^\perp$. Este código dual también puede ser caracterizado utilizando el producto interior.

Definición 2.20. El *producto interior* de dos vectores $u = (u_1, u_2, \ldots, u_n)$ y $v = (v_1, v_2, \ldots, v_n)$ en $\mathbb{F}_q^n$ es definido como

$$\langle u, v\rangle := uv^t = \sum_{i=1}^{n} u_i v_i \in \mathbb{F}_q.$$

Definición 2.21. Sea $C \leq \mathbb{F}_q^n$ un $[n,k]$-código lineal. Definimos el *código dual* $C^\perp$ de C como

$$C^\perp := \{u \in \mathbb{F}_q^n : \langle u, v\rangle = 0, \text{ para todo } v \in C\}.$$

Decimos que C es *auto-ortogonal* si $C \subseteq C^\perp$ y es *auto-dual* si $C = C^\perp$.

Teorema 2.22. *Si G es la matriz generadora y H es la matriz de control de un $[n,k]$-código lineal C sobre $\mathbb{F}_q$, entonces $C^\perp$ es un $[n, n-k]$-código con matriz generadora H y matriz de control G.*

Demostración. Sean G una matriz generadora para C y $x \in C^\perp$. Entonces

$$\begin{aligned}
x \in C^\perp &\iff \langle x, v\rangle = 0 \text{ para todo } v \in C \\
&\iff xv^t \text{ para todo } v = uG \in C \\
&\iff x(uG)^t = 0 \text{ para todo } u \in \mathbb{F}_q^k \\
&\iff uGx^t = 0 \text{ para todo } u \in \mathbb{F}_q^k \\
&\iff Gx^t = 0.
\end{aligned}$$

Por lo tanto, $C^{\perp} = \{x \in \mathbb{F}_q^n : Gx^t = 0\}$, es decir, G es una matriz de control para $C^{\perp}$. Por otro lado, sea H una matriz de control para C. Dado que $Hv^t = 0$ para todo $v \in C$ y que $\text{rang}(H) = n - k$, se tiene que existen $n - k$ filas independientes en H que pertenecen a $C^{\perp}$. Además, por el Teorema 1.48, si L es la transformación lineal $x \longmapsto Gx^t$, entonces $n = \dim_{\mathbb{F}_q}(\text{Ker}(L)) + \dim_{\mathbb{F}_q}(\text{Im}(L)) = \dim_{\mathbb{F}_q} C^{\perp} + \text{rang}(G)$. Esto implica que $\dim_{\mathbb{F}_q}(C^{\perp}) = n - k$. Por lo tanto, las filas de H forman una base para $C^{\perp}$, es decir, H es una matriz de control para $C^{\perp}$. □

Corolario 2.23. *Sea $C \leq \mathbb{F}_q^n$. Entonces $\dim_{\mathbb{F}_q}(\mathbb{F}_q^n) = \dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp})$.*

Demostración. Si $\dim_{\mathbb{F}_q}(C) = k$, entonces $\dim_{\mathbb{F}_q}(C^{\perp}) = n - k$. Por lo tanto,

$$\dim_{\mathbb{F}_q}(C) + \dim_{\mathbb{F}_q}(C^{\perp}) = k + n - k = n = \dim_{\mathbb{F}_q}(\mathbb{F}_q^n).$$

□

Teorema 2.24. *Sea C un $[n, k]$-código lineal sobre $\mathbb{F}_q$.*

1. *Si C es un código auto-dual, entonces n es par y su dimensión es $n/2$.*
2. *$(C^{\perp})^{\perp} = C$*

Demostración.

1. Como C es un código auto-dual, se tiene que $\dim_{\mathbb{F}_q} C = \dim_{\mathbb{F}_q} C^{\perp}$. Luego, por el Corolario anterior,
$$n = \dim_{\mathbb{F}_q} C + \dim_{\mathbb{F}_q} C^{\perp} = 2\dim_{\mathbb{F}_q} C.$$
2. Sea $x \in C$, entonces $\langle x, y \rangle = 0$ para todo $y \in C^{\perp}$. Por lo tanto, $C \subseteq (C^{\perp})^{\perp}$. Pero $\dim_{\mathbb{F}_q}(C^{\perp})^{\perp} = n - (n - k) = k = \dim_{\mathbb{F}_q}(C)$, con lo cual se tiene la igualdad.

□

El siguiente teorema muestra que, para los códigos autoduales sobre $\mathbb{F}_q$ con $q = 2$ o 3, existe una cota menor que la cota de Singleton.

Teorema 2.25 ([10],[13])**.** *Sea C un $[n, n/2, d]$-código autodual sobre $\mathbb{F}_q$.*

1. *Si $q = 2$, entonces*
$$d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4 \quad si\ n \not\equiv 22 \mod 24$$
$$y \quad d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 6 \quad si\ n \equiv 22 \mod 24.$$

2. Si $q = 3$, entonces

$$d \leq 3 \left\lfloor \frac{n}{12} \right\rfloor + 3.$$

Los códigos autoduales que satisfacen esta cota superior se denominan *códigos extremales*. El código de Golay binario extendido $\mathcal{G}_{24}$ y el código de Golay ternario extendido $\mathcal{G}_{12}$, que serán definidos en la penúltima sección de este capítulo, son códigos extremales.

2.2. Códigos equivalentes

Se requiere encontrar una relación de equivalencia en la que se conserven tanto las propiedades algebraicas como las relacionadas con la distancia y el peso. Se podría considerar que dos códigos C_1 y C_2 son equivalentes si son isomorfos como espacio vectorial, es decir, si existe una matriz del grupo lineal general $\mathrm{GL}_n(\mathbb{F}_q) := \{A \in \mathbb{F}_q^{n\times n} : A \text{ es invertible}\}$ tal que $C_1A = C_2$. Sin embargo, con esta acción, una palabra de un peso podría ser enviada a una palabra de diferente peso. Una manera de evitar esto es utilizar matrices de permutación.

Definición 2.26. Una *matriz de permutación* P es una matriz $n \times n$ con un 1 en cada fila y columna y 0 en las demás posiciones.

Definición 2.27. Los códigos lineales C_1 y C_2 son *permutacionalmente equivalentes* si existe una matriz de permutación P tal que si G_1 es matriz generadora de C_1, G_1P es matriz generadora de C_2. También podemos decir que dos códigos son permutacionalmente equivalentes si existe una matriz de permutación P tal que $C_1P = C_2$ donde $C_1P = \{u : u = vP, \text{ para todo } v \in C_1\}$.

Ejemplo 2.28. Sean C_1 y C_2 códigos lineales en $\mathbb{F}_2^5$ con matrices generadoras

$$G_1 = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ y } G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

respectivamente. Entonces $G_1P = G_2$ con

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

Por lo tanto, C_1 y C_2 son permutacionalmente equivalentes.

Observación 2.29. La acción de una matriz de permutación sobre la matriz generadora es la reorganización de sus columnas, del mismo modo, la acción sobre las palabras del código es la reorganización de sus coordenadas. Por lo tanto, las matrices de permutación son elementos de $\mathrm{GL}_n(\mathbb{F}_q)$ que conservan las relaciones de distancia y peso.

Teorema 2.30. *Sea $C \leq \mathbb{F}_q^n$ un $[n,k]$-código lineal. Entonces C es permutacionalmente equivalente a un código C' con una matriz generadora en forma estándar.*

Demostración. Sea G una matriz generadora de C. Aplicando operaciones elementales en G se obtiene una matriz con las columnas de I_k pero en diferente orden. Luego, existe una matriz de permutación que reorganiza las columnas de forma que $G' = [I_k|A]$. Si C' es el código generado por G', entonces C y C' son permutacionalmente equivalentes. □

Con frecuencia es más conveniente expresar las matrices de permutación en forma cíclica, es decir, como elementos del grupo simétrico de grado n, denotado $\mathrm{Sym}(n)$.

Definición 2.31. Sean $\sigma \in \mathrm{Sym}(n)$ y $v = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$. Definimos la acción de $\mathrm{Sym}(n)$ sobre v como

$$\sigma(v) := (w_1, w_2, \ldots, w_n) \text{ donde } w_i = v_{\sigma^{-1}(i)}.$$

Entonces $\sigma(v) = vP_\sigma$, donde la matriz de permutación $P_\sigma = [p_{ij}]$ es definida como

$$p_{ij} = \begin{cases} 1 & \text{si } j = \sigma(i) \\ 0 & \text{otro caso} \end{cases}$$

Ejemplo 2.32. Sean $v = (v_1, v_2, v_3)$ una palabra de longitud 3 sobre $\mathbb{F}_q$ y $\sigma = (1,2,3)$. Note que $\sigma^{-1}(1) = 3$, $\sigma^{-1}(2) = 1$, y $\sigma^{-1}(3) = 2$. Luego, $\sigma(v) = (v_3, v_1, v_2)$. Además,

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

En particular, dado $v = (0,1,2)$, se sigue que $\sigma(v) = (0,1,2)P_\sigma = (2,0,1)$.

Definición 2.33. El conjunto de permutaciones de coordenadas que envían un código C a el mismo forman un grupo llamado el *grupo de automorfismos permutacional* de C, denotado $\mathrm{PAut}(C)$. Esto es,

$$\mathrm{PAut}(C) := \{\sigma \in \mathrm{Sym}(n) : \sigma(C) = C\}.$$

Notemos que $\mathrm{PAut}(C) \subseteq \mathrm{Sym}(n)$. Además, el grupo $\mathrm{PAut}(C)$ también puede ser definido con matrices de permutación como

$$\mathrm{PAut}(C) = \{P_\sigma : CP_\sigma = C, \sigma \in \mathrm{Sym}(n)\}.$$

Teorema 2.34. *Sea $C \leq \mathbb{F}_q^n$ y $P = P_\sigma$, donde $\sigma \in \mathrm{Sym}(n)$.*

1. $(CP)^\perp = C^\perp P$.
2. $\mathrm{PAut}(C) = \mathrm{PAut}(C^\perp)$.

Demostración. 1. Recordemos que $u \in C^\perp$ si $\langle u, v\rangle = 0$, para todo $v \in C$. Entonces

$$\begin{aligned} C^\perp P &= \{uP \in \mathbb{F}_q^n : \langle u, v\rangle = 0, \text{ para todo } v \in C\} \\ &= \{uP \in \mathbb{F}_q^n : uv^t = 0, \text{ para todo } v \in C\} \\ &= \{uP \in \mathbb{F}_q^n : uPP^tv^t = 0, \text{ para todo } v \in C\} \\ &= \{uP \in \mathbb{F}_q^n : uP(vP)^t = 0, \text{ para todo } v \in C\} \\ &= \{x \in \mathbb{F}_q^n : \langle x, vP\rangle = 0, \text{ para todo } v \in C\} \\ &= (CP)^\perp. \end{aligned}$$

2. Supongamos que $P \in \mathrm{PAut}(C)$, entonces $C = CP$. Por el ítem anterior,

$$C = CP \iff C^\perp = (CP)^\perp \iff C^\perp = C^\perp P.$$

En consecuencia, $\mathrm{PAut}(C) = \mathrm{PAut}(C^\perp)$.

□

Podemos definir una relación de equivalencia mas general utilizando matrices monomiales. Los siguientes resultados muestran que estás matrices forman el grupo de transformaciones lineales que conserva la distancia entre dos vectores.

Definición 2.35. Una matriz $A \in \mathrm{GL}_n(\mathbb{F}_q)$ es una *isometría lineal* de $\mathbb{F}_q^n$ si se verifica

$$\mathrm{d}(uA, vA) = \mathrm{d}(u, v) \text{ para todo } u, v \in \mathbb{F}_q^n.$$

En particular, $\mathrm{wt}(uA) = \mathrm{d}(uA, 0) = \mathrm{d}(u, 0) = \mathrm{wt}(u)$. Por lo tanto, A es una isometría si y solo si $\mathrm{wt}(uA) = \mathrm{wt}(u)$ para todo $u \in \mathbb{F}_q^n$.

Observación 2.36.

1. Si A es un isometría lineal, A^{-1} también es una isometría puesto que $\mathrm{wt}(uA^{-1}) = \mathrm{wt}(uA^{-1}A) = \mathrm{wt}(u)$ para todo $u \in \mathbb{F}_q^n$.

2. El conjunto de isometrías lineales de $\mathbb{F}_q^n$ forma un subgrupo de $\mathrm{GL}_n(\mathbb{F}_q)$. Note que I_n es una isometría y si A y B son isometrías lineales de $\mathbb{F}_q^n$, entonces AB^{-1} también es una isometría lineal.

Definición 2.37. Una *matriz monomial* es de la forma $M = DP_\sigma$ donde $D = \mathrm{diag}(a_{11}, \ldots, a_{nn})$ es una matriz diagonal de tamaño $n \times n$ con $0 \neq a_{ii} \in \mathbb{F}_q$ y $\sigma \in \mathrm{Sym}(n)$. El conjunto de matrices monomiales $n \times n$ con entradas en $\mathbb{F}_q$ se denota $\mathrm{Mon}(n, \mathbb{F}_q)$.

Ejemplo 2.38.

1. La siguiente matriz es monomial.

$$M = \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ c & 0 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}}_{D} \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}}_{P_\sigma} = DP_\sigma.$$

   Estas matriz también pueden ser descrita de forma más compacta como $M = \mathrm{diag}(a, b, c)(1, 2, 3)$ donde $\mathrm{diag}(a, b, c)$ es la matriz diagonal y $\sigma = (1, 2, 3)$.

2. Sea $v = (v_1, v_2, v_3)$ y $M = \mathrm{diag}(a, b, c)(1, 3, 2)$ una matriz monomial. Entonces

$$vM = vDP_\sigma = (av_1, bv_2, cv_3)(1, 3, 2) = (bv_2, cv_3, av_1).$$

Notemos que la acción de una matriz monomial sobre un vector es la multiplicación de sus coordenadas por un escalar diferente de cero y la reorganización de dichas coordenadas.

Teorema 2.39. $\mathrm{Mon}(\mathrm{n}, \mathbb{F}_\mathrm{q})$ *es el grupo de isometrías lineales de* $\mathbb{F}_q^n$.

Demostración. Sea $M = DP_\sigma$ una matriz monomial y $v \in \mathbb{F}_q^n$, entonces $vDP_\sigma = u$. Notemos que u es el vector resultante de multiplicar las coordenadas de v por un escalar diferente de cero y permutarlas. Con lo cual podemos concluir que u y v tienen el mismo número de coordenadas distintas de cero. Por lo tanto, M es una isometría de $\mathbb{F}_q^n$.
Recíprocamente, Sea $\{e_1, \ldots, e_n\}$ la base canónica de $\mathbb{F}_q^n$ y A una isometría de $\mathbb{F}_q^n$. Entonces

$$1 = \mathrm{wt}(e_i) = \mathrm{wt}(e_i A) \text{ para } i = 1, \ldots, n.$$

Por lo tanto, $e_i A = a_i e_{i'}$ donde $0 \neq a_i \in \mathbb{F}_q$ y $i' \in \{1, \ldots, n\}$. Veamos que la función σ dada por $i \longmapsto i'$ es biyectiva. Para esto solo probaremos que σ es sobreyectiva puesto que es una función que va de $\{1, \ldots, n\}$ a si mismo. Como A es invertible, si $i' \in \{1, \ldots, n\}$, entonces existe i tal que $e_{i'} A^{-1} = b_i e_i$ y por ende,

$$e_i A = b_i^{-1} e_{i'} A^{-1} A = b_i^{-1} e_{i'}, \text{ es decir, } \sigma(i) = i'.$$

Por ello, $\sigma \in \mathrm{Sym}(n)$. En consecuencia, $A = \mathrm{diag}(a_1, \ldots, a_n) P_\sigma$ es una matriz monomial. □

Definición 2.40. Sean $C_1, C_2 \leq \mathbb{F}_q^n$. Decimos que C_1 y C_2 son *monomialmente equivalentes* si existe una matriz $M \in \mathrm{Mon(n, \mathbb{F}_q)}$ tal que si G_1 es matriz generadora de C_1, entonces $G_1 M$ es matriz generadora de C_2. Esto es, C_1 y C_2 son equivalentes si existe una matriz monomial M tal que $C_1 M = C_2$.

Definición 2.41. El conjunto de matrices monomiales que envían el código C a el mismo forman un grupo llamado el *grupo de automorfismos monomial* de C, denotado $\mathrm{MAut}(C)$. Note que $\mathrm{MAut}(C) \subseteq \mathrm{Mon}(n, \mathbb{F}_q)$.

Teorema 2.42. *Sea C un código lineal sobre $\mathbb{F}_q$.*

1. $(CD)^\perp = C^\perp D^{-1}$.
2. $\mathrm{MAut}(C^\perp) = \{D^{-1}P : DP \in \mathrm{MAut}(C)\}$.

Demostración. 1. Recordemos que $u \in C^\perp$ si $\langle u, v \rangle = 0$ para todo $v \in C$.

Entonces

$$\begin{aligned} C^{\perp}D^{-1} &= \{uD^{-1} \in \mathbb{F}_q^n : \langle u, v\rangle = 0, \text{ para todo } v \in C\} \\ &= \{uD^{-1} \in \mathbb{F}_q^n : uv^t = 0, \text{ para todo } v \in C\} \\ &= \{uD^{-1} \in \mathbb{F}_q^n : uD^{-1}Dv^t = 0, \text{ para todo } v \in C\} \\ &= \{uD^{-1} \in \mathbb{F}_q^n : uD^{-1}(vD)^t = 0, \text{ para todo } v \in C\} \\ &= \{x \in \mathbb{F}_q^n : \langle x, vD\rangle = 0, \text{ para todo } v \in C\} \\ &= (CD)^{\perp}. \end{aligned}$$

2. Sea $DP \in \mathrm{MAut}(C)$. Por el ítem anterior, se tiene que

$$\begin{aligned} CDP = C &\iff (CDP)^{\perp} = C^{\perp} \iff (CD)^{\perp}P = C^{\perp} \\ &\iff C^{\perp}D^{-1}P = C^{\perp}. \end{aligned}$$

Con lo cual se comprueba la igualdad.

□

También consideraremos la equivalencia semilineal de códigos. Esta es una equivalencia más general en la que, además de la acción de las matrices monomiales, se incluye la acción de los automorfismos del cuerpo $\mathbb{F}_q$. El grupo de automorfismos de cuerpo $\mathbb{F}_q$ es denotado $\mathrm{Aut}(\mathbb{F}_q)$.

Definición 2.43. Una función $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ es *semilineal* si se cumple

1. $f(x + y) = f(x) + f(y)$ para todo $x, y \in \mathbb{F}_q^n$.
2. Existe algún $\sigma_f \in \mathrm{Aut}(\mathbb{F}_q)$ tal que $f(\lambda x) = \sigma_f(\lambda)f(x)$ para todo $\lambda \in \mathbb{F}_q$ y $x \in \mathbb{F}_q^n$.

El conjunto de funciones semilineales invertibles forman un grupo llamado el grupo general semilineal denotado $\Gamma\mathrm{L}_n(\mathbb{F}_q)$. Notemos que $\mathrm{GL}_n(\mathbb{F}_q) \subseteq \Gamma\mathrm{L}_n(\mathbb{F}_q)$, puesto que $\mathrm{GL}_n(\mathbb{F}_q)$ es el grupo de funciones semilineales para las cuales el automorfismo σ_f es la identidad.

Lema 2.44. *1.* $\mathrm{GL}_n(\mathbb{F}_q)$ *es un subgrupo normal de* $\Gamma\mathrm{L}_n(\mathbb{F}_q)$.

2. Sea B *una base de* $\mathbb{F}_q^n$ *y* $H := \{h_\sigma : \sigma \in \mathrm{Aut}(\mathbb{F}_q)\}$ *donde* $h_\sigma : \mathbb{F}_q^n \to \mathbb{F}_q^n$ *es definida como* $h_\sigma(\sum_{b\in B} \lambda_b b) = \sum_{b\in B} \sigma(\lambda_b)b$. *Entonces* H *es un subgrupo de* $\Gamma\mathrm{L}_n(\mathbb{F}_q)$ *isomorfo a* $\mathrm{Aut}(\mathbb{F}_q)$.

3. *El subgrupo H es un complemento de* $\mathrm{GL}_n(\mathbb{F}_q)$*, esto es,* $\Gamma\mathrm{L}_n(\mathbb{F}_q) = \mathrm{GL}_n(\mathbb{F}_q)H$ *y* $H \cap \mathrm{GL}_n(\mathbb{F}_q) = 1$.

Demostración. 1. Definamos $\varphi : \Gamma\mathrm{L}_n(\mathbb{F}_q) \longrightarrow \mathrm{Aut}(\mathbb{F}_q)$ como $\varphi(f) = \sigma_f$. Primero veamos que el automorfismo asociado a una función semilineal es único. Para $f \neq 0$, existe $x \in \mathbb{F}_q^n$ tal que $f(x) \neq 0$, si suponemos que $f(\lambda x) = \sigma(\lambda)f(x) = \theta(\lambda)f(x)$ para $\sigma, \theta \in \mathrm{Aut}(\mathbb{F}_q)$, entonces

$$\begin{aligned} &\sigma(\lambda)f(x) - \theta(\lambda)f(x) = 0 \text{ para todo } \lambda \in \mathbb{F}_q \\ \Rightarrow\ &(\sigma(\lambda) - \theta(\lambda))f(x) = 0 \text{ para todo } \lambda \in \mathbb{F}_q \\ \Rightarrow\ &\sigma(\lambda) - \theta(\lambda) = 0 \text{ para todo } \lambda \in \mathbb{F}_q \\ \Rightarrow\ &\sigma(\lambda) = \theta(\lambda) \text{ para todo } \lambda \in \mathbb{F}_q. \end{aligned}$$

Por lo tanto, si $f = g$, entonces $\sigma_f = \sigma_g$. Por otro lado,

$$\begin{aligned} fg(\lambda x) &= f(g(\lambda x)) = f(\sigma_g(\lambda)g(x)) = \sigma_f(\sigma_g(\lambda))f(g(x)) \\ &= \sigma_f\sigma_g(\lambda)fg(x). \end{aligned}$$

Esto implica que $\varphi(fg) = \sigma_f\sigma_g = \varphi(f)\varphi(g)$ y demuestra que φ es un homomorfismo de grupos. Más aún,

$$\mathrm{Ker}(\varphi) = \{f \in \Gamma\mathrm{L}_n(\mathbb{F}_q) : \sigma_f(\lambda) = \lambda \text{ para todo } \lambda \in \mathbb{F}_q\} = \mathrm{GL}_n(\mathbb{F}_q).$$

Como el kernel de un homomorfismo de grupos es un subgrupo normal, tenemos que $\mathrm{GL}_n(\mathbb{F}_q)$ es un subgrupo normal de $\Gamma\mathrm{L}_n(\mathbb{F}_q)$.

2. Claramente h_σ es semilineal e invertible. Demostremos entonces que H es un subgrupo de $\Gamma\mathrm{L}_n(\mathbb{F}_q)$. Sean $h_\sigma, h_\theta \in H$. Luego,

$$\begin{aligned} h_\sigma h_{\theta^{-1}} \left(\sum_{b\in B} \lambda_b b\right) &= h_\sigma \left(\sum_{b\in B} \theta^{-1}(\lambda_b)b\right) = \sum_{b\in B} \sigma(\theta^{-1}(\lambda_b))b \\ &= \sum_{b\in B} \sigma\theta^{-1}(\lambda_b)b = h_{\sigma\theta^{-1}} \left(\sum_{b\in B} \lambda_b b\right) \in H. \end{aligned}$$

Definamos ahora $\varphi : H \longrightarrow \mathrm{Aut}(\mathbb{F}_q)$ como $\varphi(h_\sigma) = \sigma$. Notemos que $h_\sigma h_\theta = h_{\sigma\theta}$, entonces

$$\varphi(h_\sigma h_\theta) = \varphi(h_{\sigma\theta}) = \sigma\theta = \varphi(h_\sigma)\varphi(h_\theta).$$

Por lo tanto, φ es un homomorfismo de grupos. Además, se tiene que φ es inyectiva, puesto que $h_\sigma = h_\theta \iff \sigma = \theta$. Más aún, φ es sobreyectiva, dado que para todo $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ existe h_σ tal que $\varphi(h_\sigma) = \sigma$. En consecuencia, φ es un isomorfismo.

3. Sea $f \in \Gamma\mathrm{L}_n(\mathbb{F}_q)$. Definamos $g : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ como

$$g(\sum_{b\in B} \lambda_b b) := \sum_{b\in B} f(\sigma_f^{-1}(\lambda_b)b) = \sum_{b\in B} \sigma_f(\sigma_f^{-1}(\lambda_b))f(b) = \sum_{b\in B} \lambda_b f(b).$$

Entonces $g \in \mathrm{GL}_n(\mathbb{F}_q)$. Más aún, $gh_{\sigma_f} = f$. En efecto,

$$g(h_{\sigma_f}(\sum_{b\in B} \lambda_b b)) = g(\sum_{b\in B} \sigma_f(\lambda_b)b) = \sum_{b\in B} \sigma_f(\lambda_b)f(b) = f(\sum_{b\in B} \lambda_b b).$$

Por lo tanto, $\Gamma\mathrm{L}_n(\mathbb{F}_q) = \mathrm{GL}_n(\mathbb{F}_q)H$. Sea ahora $h_\sigma \in H \cap \mathrm{GL}_n(\mathbb{F}_q)$. Como $h_\sigma \in \mathrm{GL}_n(\mathbb{F}_q)$ se tiene que $\sigma(\lambda) = \lambda$ para todo $\lambda \in \mathbb{F}_q$. Así, $h_\sigma(\sum_{b\in B} \lambda_b b) = \sum_{b\in B} \lambda_b b$, es decir, h_σ es la función identidad.

□

Recordemos que para un grupo G dado y $N, V \leq G$, decimos que $G = N \rtimes U$ si y solo si N es un subgrupo normal de G y $U \cong V$, con V un complemento de N en G.

Teorema 2.45. $\Gamma\mathrm{L}_n(\mathbb{F}_q) = \mathrm{GL}_n(\mathbb{F}_q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$.

Demostración. Se sigue del Lema 2.44. □

Definición 2.46. Un función $f \in \Gamma\mathrm{L}_n(\mathbb{F}_q)$ es una *isometría semilineal* si se verifica $\mathrm{d}(f(u), f(v)) = \mathrm{d}(u, v)$ para todo $u, v \in \mathbb{F}_q^n$.

Teorema 2.47. $\mathrm{Mon}(n, \mathbb{F}_q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$ *es el grupo de isometrías semilineales de* $\mathbb{F}_q^n$.

Demostración. Este resultado se sigue de que $\mathrm{Mon}(n, \mathbb{F}_q)$ son la matrices de $\mathrm{GL}_n(\mathbb{F}_q)$ que conservan las distancia y de que los elementos de $H \cong \mathrm{Aut}(\mathbb{F}_q)$ preservan la distancia. □

Definición 2.48. 1. Dos códigos lineales C_1 y C_2 de longitud n sobre $\mathbb{F}_q$ son *semilinealmente equivalentes* si existe una función $f \in \mathrm{Mon}(n, \mathbb{F}_q) \rtimes \mathrm{Aut}(\mathbb{F}_q)$ tal que $f(C_1) = C_2$.

2. El conjunto de isometrías semilineales que envían un código C a si mismo se denomina el *grupo de automorfismos* de C y se denota $\Gamma\mathrm{Aut}(C)$.

Observación 2.49. Note que para cualquier código lineal $C \leq \mathbb{F}_q^n$ dado, $\mathrm{PAut}(C) \subseteq \mathrm{MAut}(C) \subseteq \Gamma\mathrm{Aut}(C)$. Un caso especial ocurre cuando q es primo, debido a que el grupo de automorfismos del cuerpo $\mathbb{F}_q$ es trivial. Por lo cual, $\mathrm{MAut}(C) = \Gamma\mathrm{Aut}(C)$. En particular, si $q = 2$, entonces $\mathrm{PAut}(C) = \mathrm{MAut}(C) = \Gamma\mathrm{Aut}(C)$.

2.3. Códigos cíclicos

Los códigos cíclicos son una clase especial de los códigos lineales. En esta sección estudiaremos principalmente la identificación de estos códigos como ideales del álgebra $\mathbb{F}_q[x]/\langle x^n - 1\rangle$.

Definición 2.50. Un código lineal de longitud n sobre $\mathbb{F}_q$ se denomina *cíclico* si y solo si para todo $(c_0, c_1 \ldots, c_{n-1}) \in C$ se tiene que $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$.

Observación 2.51. El siguiente lema muestra que el estudio de códigos cíclicos de longitud n sobre $\mathbb{F}_q$ es equivalente al estudio de ideales del álgebra cociente $\mathcal{R}_n := \mathbb{F}_q[x]/\langle x^n - 1\rangle$. Para esto, definamos la función $f : \mathbb{F}_q^n \longrightarrow \mathcal{R}_n$ como

$$f(c_0, c_1 \ldots, c_{n-1}) = c(x) + \langle x^n - 1\rangle$$

donde $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$. Esta función es un isomorfismo de $\mathbb{F}_q$-espacios vectoriales.

Lema 2.52. *Un código $C \leq \mathbb{F}_q^n$ es cíclico si y solo si $C(x) := \{c(x) + \langle x^n - 1\rangle : c \in C\}$ es un ideal de $\mathcal{R}_n$.*

Demostración. Sea C un código cíclico y $c(x) = c_0 + \cdots + c_{n-1}x^{n-1} \in C(x)$. Entonces $xc(x) \in C(x)$ puesto que $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. En general, $x^i c(x) \in C(x)$ para $i = 1, \ldots, n-1$. Por lo tanto, si $p(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathcal{R}_n$, entonces $p(x)c(x) = \sum_{i=0}^{n-1} a_i x^i c(x) \in C(x)$. Recíprocamente, si $C(x)$ es un ideal de $\mathcal{R}_n$, entonces $xc(x) \in C(x)$ para todo $c(x) \in C(x)$. En consecuencia, para todo $(c_0, c_1 \ldots, c_{n-1}) \in C$ se tiene que $(c_{n-1}, c_0, \ldots, c_{n-2}) \in C$. □

Ahora podemos identificar cada palabra c de un código cíclico $C \leq \mathbb{F}_q^n$ como $c(x) + \langle x^n - 1\rangle$ en $\mathcal{R}_n$, notación que simplificaremos como $c(x)$. Por otro lado, como $\mathbb{F}_q[x]$ es un dominio de ideales principales, entonces los ideales

del álgebra $\mathcal{R}_n$ también son ideales principales. En consecuencia, los códigos cíclicos son ideales generados por un polinomio.

Teorema 2.53. *Sea C un código cíclico no nulo en $\mathcal{R}_n$. Existe un polinomio $g(x) \in C$ con las siguientes propiedades*

1. *$g(x)$ es el único polinomio mónico de grado mínimo en C.*
2. *$C = \langle g(x) \rangle$.*
3. *$g(x) \mid (x^n - 1)$.*

Demostración. 1. Como C es no nulo y es un subespacio vectorial se tiene que existe un polinomio mónico de grado mínimo n en C, sea este polinomio $g(x)$. Verifiquemos que este polinomio es único. Sea $f(x)$ otro polinomio mónico de grado mínimo n. Luego, $\deg(f(x) - g(x)) < n$ o $f(x) - g(x) = 0$. Como $f(x) - g(x) \in C$, se sigue que $f(x) - g(x) = 0$, es decir, $f(x) = g(x)$.

2. Sea $c(x) \in C$. Por el algoritmo de división en $\mathbb{F}_q[x]$, existe $h(x)$ y $r(x)$ tales que $c(x) = g(x)h(x) + r(x)$ donde $r(x) = 0$ o $\deg(r(x)) < \deg(g(x))$. Como C es un ideal, $r(x) = c(x) - g(x)h(x) \in C$, pero $g(x)$ es de grado mínimo en C, entonces $r(x) = 0$.

3. Por el algoritmo de división en $\mathbb{F}_q[x]$ tenemos que $x^n - 1 = g(x)h(x) + r(x)$ donde $r(x) = 0$ o $\deg(r(x)) < \deg(g(x))$. Como $r(x) \in C$, entonces $r(x) = 0$.

□

Corolario 2.54. *Sea C un código cíclico no nulo en $\mathcal{R}_n$. Si $C = \langle g(x) \rangle$, $g(x)$ es mónico y $g(x) \mid (x^n - 1)$, entonces $g(x)$ es el único polinomio mónico de grado mínimo en C.*

Demostración. Suponga que $C = \langle g(x) \rangle$, $g(x)$ es mónico y $g(x) \mid (x^n - 1)$ y sea $g_1(x)$ el único polinomio mónico de grado mínimo en C. Como $g_1 \in C = \langle g(x) \rangle$ se sigue que $g_1(x) \equiv g(x)a(x) \mod (x^n - 1)$, esto es $g_1(x) = g(x)a(x) + (x^n - 1)b(x)$ en $\mathbb{F}_q[x]$. Luego, $g(x) \mid g_1(x)$. Como $C = \langle g_1(x) \rangle$, entonces $g_1(x) \mid g(x)$. Puesto que $g_1(x)$ y $g(x)$ son polinomios mónicos, se tiene que $g_1(x) = g(x)$. □

Observación 2.55. Con este corolario mostramos que existe un único polinomio mónico que genera el código cíclico C y divide a $(x^n - 1)$. Este polinomio se denomina el *polinomio generador* del código cíclico C.

Teorema 2.56. *Sea $g(x)$ el polinomio generador del código cíclico no nulo C en $\mathcal{R}_n$. Sea $k = n - \deg(g(x))$ y $g(x) = \sum_{i=0}^{n-k} g_i x^i$ donde $g_{n-k} = 1$ entonces*

1. *Cada elemento de C es expresado de manera única como $g(x)h(x)$ con $h(x) = 0$ o $\deg(h(x)) < k$.*
2. *$\dim_{\mathbb{F}_q}(C) = k$ y $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ es una base para C.*
3. *La matriz G es una matriz generadora para C, donde*

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & \\ & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & & g_0 & & \cdots & & g_{n-k} \end{pmatrix}.$$

Demostración.

1. Si $c(x) \in C$, entonces $c(x) = 0$ o $c(x) = g(x)h(x) \in \mathbb{F}_q[x]$ con $\deg(c(x)) < n$. Si $c(x) = 0$, entonces $h(x) = 0$ y si $c(x) \neq 0$, entonces $\deg(h(x)) < k$. Por lo tanto, $C = \{g(x)h(x) \mid h(x) = 0 \text{ o } \deg(h(x)) < k\}$.

2. Del ítem anterior, cada elemento $c(x) \in C$ puede ser escrito como $g(x)h(x)$ donde $h(x) = \sum_{i=0}^{k-1} h_i x^i$. Luego, Los polinomios $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ son polinomios linealmente independientes que generan a C.

3. Se sigue del ítem anterior al escribir la base $\{g(x), xg(x), \ldots, x^{k-1}g(x)\}$ como n-tuplas.

□

Teorema 2.57. *Sean C_1 y C_2 códigos cíclicos de longitud n en $\mathbb{F}_q$ con polinomio generador $g_1(x)$ y $g_2(x)$ respectivamente. $C_1 \subseteq C_2$ si y solo si $g_2(x) \mid g_1(x)$.*

Demostración. Supongamos que $C_1 \subseteq C_2$, entonces $g_1(x) \in C_2$. Por lo tanto, $g_2(x) \mid g_1(x)$. Recíprocamente, suponga que $g_2(x) \mid g_1(x)$, entonces cada $c(x) \in C_1$ puede ser escrito como $c(x) = g_2(x)h(x)$, esto es, $c(x) \in C_2$. Luego, $C_1 \subseteq C_2$. □

En el Teorema 1.84 se demostró que $\mathbb{F}_q[x]/\langle x^n-1\rangle \cong \mathbb{F}_q G$, donde G es el grupo cíclico de orden n. Entonces, por el teorema de Maschke, $\mathcal{R}_n$ es semisimple si $\mathrm{char}(\mathbb{F}_q) = \mathrm{p} \nmid \mathrm{n}$. En lo que resta de esta sección asumiremos que $\mathcal{R}_n$ es semisimple, por ende, cada ideal será generado por un único elemento idempotente llamado *generador idempotente*.

Teorema 2.58. *Sea C un código cíclico no nulo en $\mathcal{R}_n$. Si $e(x)$ es un idempotente distinto de 0, entonces $C = \langle e(x)\rangle$ si y solo si $e(x)$ es una unidad de C.*

Demostración. Si $e(x)$ es una unidad de C, entonces $\langle e(x)\rangle \subseteq C$. Por otro lado, $c(x) = e(x)c(x) \in \langle e(x)\rangle$ implica que $C \subseteq \langle e(x)\rangle$. Por lo tanto, $C = \langle e(x)\rangle$. Recíprocamente, si $C = \langle e(x)\rangle$, entonces cada elemento $c(x) \in C$ puede ser escrito como $c(x) = h(x)e(x)$. Por lo cual, $c(x)e(x) = h(x)e(x)^2 = h(x)e(x) = c(x)$. Es decir, $e(x)$ es una unidad. □

Observación 2.59. Notemos que el generador idempotente es único. Por el Teorema anterior se tiene que si $e_1(x)$ y $e_2(x)$ son generadores idempotentes de C, entonces $e_1(x) = e_1(x)e_2(x) = e_2(x)$.

Teorema 2.60. *Sea C un código cíclico en $\mathcal{R}_n$ con generador idempotente $e(x)$. Entonces el polinomio generador de C es $g(x) = \gcd(e(x), x^n - 1)$ calculado en $\mathbb{F}_q[x]$.*

Demostración. Sea $d(x) = \gcd(e(x), x^n - 1)$ en $\mathbb{F}_q[x]$ y sea $g(x)$ es polinomio generador de C. Como $d(x) \mid e(x)$, entonces cada $c(x) \in C$ es un múltiplo de $d(x)$ y $C \subseteq \langle d(x)\rangle$. Por otro lado, $g(x) \mid x^n - 1$ y $g(x) \mid e(x)$, de donde se sigue que $g(x) \mid d(x)$. Por lo tanto, $d(x) \in C$ y por ende, $\langle d(x)\rangle \subseteq C$. En consecuencia, $C = \langle d(x)\rangle$. Por el Corolario 2.54 y dado que $d(x)$ es mónico, se concluye que $d(x) = g(x)$. □

Teorema 2.61. *Sea C un $[n, k]$-código en $\mathcal{R}_n$ con generador idempotente $e(x) = \sum_{i=0}^{n-1} e_i x^i$. Entonces la matriz G de tamaño $n \times k$ es una matriz generadora de C, donde*

$$G = \begin{pmatrix} e_0 & e_1 & e_2 & \cdots & e_{n-2} & e_{n-1} \\ e_{n-1} & e_0 & e_1 & \cdots & e_{n-3} & e_{n-2} \\ & & & \vdots & & \\ e_{n-k+1} & e_{n-k+2} & e_{n-k+3} & \cdots & e_{n-k-1} & e_{n-k} \end{pmatrix}.$$

Demostración. Debemos probar que $\{e(x), xe(x), \ldots, x^{k-1}e(x)\}$ es una base para C. Como C es generado por $e(x)$, es suficiente probar que si $a(x)e(x) = 0$ con $\deg(a(x)) < k$, entonces $a(x) = 0$. Sea $a(x)e(x) = 0$ y $g(x)$ el polinomio generador de C. Notemos que $0 = a(x)e(x)g(x) = a(x)g(x)$. Luego, por el Teorema 2.56, se sigue que $a(x) = 0$. □

2.4. Códigos resto-cuadráticos

Los códigos resto-cuadráticos son una familia de códigos cíclicos de longitud prima p, entre los cuales se encuentran los códigos de Golay.

Definición 2.62. Sea p un número primo impar. Dado $\gcd(a, p) = 1$, decimos que a es un *residuo cuadrático módulo p* si existe un número x tal que $x^2 \equiv a$ mód p. Si no existe x que satisfaga esta congruencia, decimos que a es un *no-residuo cuadrático módulo p*.

Observación 2.63. Notemos que cualquier a es congruente con un elemento del conjunto $\mathbb{Z}_p^* := \{1, 2, \ldots, p-1\}$. Así, el conjunto de residuos cuadráticos módulo p que pertenecen a $\mathbb{Z}_p^*$ los denotaremos QR y el conjunto de los no-residuos cuadráticos módulo p que pertenecen a $\mathbb{Z}_p^*$ lo denotaremos NQR.

Teorema 2.64. *Sea p un número primo impar. Entonces*

1. $|QR| = |NQR| = \frac{(p-1)}{2}$
2. *El producto de dos residuos cuadráticos o dos no-residuos cuadráticos es un residuo cuadrático y el producto de un residuo cuadrático y un no-residuo cuadrático es un no-residuo cuadrático.*
3. $\text{QR} = \{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$ *donde todos los números son módulo p.*

Demostración.

1. Es conocido que $\mathbb{Z}_p^*$ es un grupo cíclico de orden $p-1$ bajo la multiplicación. Si α es un generador de $\mathbb{Z}_p^*$, entonces $QR = \{\alpha^{2i} : 0 \leq i < (p-1)/2\}$. Por lo tanto, QR tiene $(p-1)/2$ elementos y en consecuencia, NQR tiene $(p-1)/2$ elementos.

2. Se sigue de que $NQR = QR\alpha$. De este modo, el producto de dos residuos cuadráticos y dos no-residuos cuadráticos tienen orden par, es decir es un residuo cuadrático y el producto de un residuo cuadrático y un no-residuo cuadrático tiene orden impar, es decir, es un no-residuo cuadrático.

3. Note que $(p-x)^2 \equiv p^2 - 2px - x^2 \equiv x^2 \mod p$. Luego, los $(p-1)/2$ elementos distintos de QR son $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$.

□

Ejemplo 2.65. Si tenemos $p = 11$, entonces $1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16 \equiv 5 \mod p, 5^2 = 25 \equiv 3 \mod p$. Luego, QR $= \{1, 4, 9, 5, 3\}$ y NQR $= \{2, 6, 7, 8, 10\}$.

Recordemos que si n y q son primos relativos entonces $(x^n - 1)$ tiene n raíces distintas en $\mathbb{F}_{q^s}$, donde s es el entero positivo más pequeño tal que $q^s \equiv 1 \mod n$. Estás raíces son llamadas n-ésimas raíces de la unidad sobre $\mathbb{F}_q$, el conjunto formado por ellas se denota $E^{(n)}$ y es un subgrupo cíclico de tamaño n del grupo multiplicativo $\mathbb{F}_{q^s}^*$. Una n-ésima raíz de la unidad sobre $\mathbb{F}_q$ que genere a $E^{(n)}$ es denominada n-ésima raíz primitiva sobre $\mathbb{F}_q$. De este modo, si ω es un raíz primitiva se tiene que $E^{(n)} = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$. A partir de esto, podemos factorizar $x^n - 1$ como

$$x^n - 1 = \prod_i m_i(x)$$

donde $m_i(x)$ son los polinomios mínimos. Estos polinomios están dados por

$$m_i(x) = \prod_{j \in C_i} (x - \omega^j)$$

donde $C_i = \{i, iq, \ldots, iq^{d-1}\}$ con d el entero positivo más pequeño para el cual $iq^d \equiv 1 \mod n$. El conjunto C_i es llamado i-ésima clase ciclotómica módulo q y es el conjunto formado por los exponentes de los conjugados de ω^i. Por lo tanto, un código cíclico puede ser definido por un conjunto completo de ceros $\mathcal{Z} = \{w^i : i \in Z\}$, donde Z la unión de clases ciclotómicas módulo q. Esta última condición garantiza que el polinomio generador divida a $x^n - 1$ en $\mathbb{F}_q[x]$.

Nuestra intención es definir los códigos resto-cuadráticos. Por ello, sea $n = p$ con p es un número primo y sea ω la p-ésima raíz primitiva de la unidad sobre $\mathbb{F}_q$, entonces las p-ésimas raíces de la unidad son $\{1, \omega, \omega^2, \ldots, \omega^{p-1}\}$. Para tener un código cíclico, se requiere que $\mathcal{Z} = \{w^i : i \in \text{QR}\}$ sea un conjunto completo de ceros. Para esto, QR debe ser la unión de clases ciclotómicas módulo q, es decir,

$$i \in \text{QR} \Longrightarrow C_i = \{i, iq, \ldots, iq^{d-1}\} \subseteq QR.$$

Por el Teorema 2.64, para $i \in \mathrm{QR}$, se sigue que $iq \in \mathrm{QR}$ si y solo si $q \in \mathrm{QR}$. Similarmente, dado $\mathcal{U} = \{w^i : i \in \mathrm{NQR}\}$ se tiene que NQR es la unión de clases ciclotómicas módulo q si y solo si $q \in \mathrm{QR}$. Por lo tanto, para q un número primo que es residuo cuadrático módulo p, los polinomios

$$q(x) = \prod_{r \in \mathrm{QR}} (x - \omega^r) \quad \text{y} \quad n(x) = \prod_{u \in \mathrm{NQR}} (x - \omega^u)$$

tienen coeficientes en $\mathbb{F}_q$. Por lo cual, $x^p - 1 = (x-1)q(x)n(x)$.

Definición 2.66. Sea p un primo impar y sea q un primo que es residuo cuadrático módulo p. Los códigos cíclicos

$$\mathcal{Q}(p) = \langle q(x) \rangle, \ \overline{\mathcal{Q}}(p) = \langle (x-1)q(x) \rangle,$$

$$\mathcal{N}(p) = \langle n(x) \rangle \quad \text{y} \quad \overline{\mathcal{N}}(p) = \langle (x-1)n(x) \rangle$$

de longitud p en $\mathcal{R}_p := \mathbb{F}_q[x]/\langle x^p - 1 \rangle$ son llamados *códigos resto-cuadráticos.*

Teorema 2.67. *Para los códigos resto cuadráticos de longitud p tenemos*

$$\dim(\mathcal{Q}(p)) = \dim(\mathcal{N}(p)) = (p+1)/2$$

$$\dim(\overline{\mathcal{Q}}(p)) = \dim(\overline{\mathcal{N}}(p)) = (p-1)/2.$$

Demostración. Como $|QR| = |NQR| = (p-1)/2$ se tiene que $\deg(q(x)) = \deg(n(x)) = (p-1)/2$. Entonces, por el Teorema 2.56,

$$\dim(\mathcal{Q}(p)) = p - \deg(q(x)) = p - \frac{(p-1)}{2} = \frac{(p+1)}{2}$$

$$\text{y} \quad \dim(\overline{\mathcal{Q}}(p)) = p - \deg((x-1)q(x)) = p - (\frac{p-1}{2} + 1) = \frac{(p-1)}{2}.$$

Similarmente, $\dim(\mathcal{N}(p)) = (p+1)/2$ y $\dim(\overline{\mathcal{N}}(p)) = (p-1)/2$. □

Observación 2.68. Notemos que 2 es un residuo cuadrático módulo 23 puesto que $5^2 \equiv 2 \mod 23$. Por ello, existe la factorización

$$x^{23} - 1 = (x-1)q(x)n(x)$$

sobre $\mathbb{F}_2$. Más aún, esta factorización es

$$x^{23}-1 = (x-1)(x^{11}+x^9+x^7+x^6+x^5+x+1)(x^{11}+x^{10}+x^6+x^5+x^4+x^2+1).$$

Por lo tanto, llamamos *código de Golay binario* $\mathcal{G}_{23}$ a el código resto cuadrático binario $\mathcal{Q}(23)$.

Del mismo modo, 3 es un residuo cuadrático módulo 11. Entonces la factorización $x^{11} - 1 = (x-1)q'(x)n'(x)$ sobre $\mathbb{F}_3$ esta dada por

$$x^{11} - 1 = (x-1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 - x - 1).$$

Así, el *código de Golay ternario* $\mathcal{G}_{11}$ es el código resto-cuadrático ternario $\mathcal{Q}(11)$.

Estos códigos también pueden ser definidos de forma alternativa como se muestra a continuación.

Definición 2.69. Definimos el *código de Golay binario* $\mathcal{G}_{23}$ como el $[23, 12, 7]$-código sobre $\mathbb{F}_2$ cuya matriz generadora es $G_{23} = [I_{12} \mid A']$, donde

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

Es posible crear un código más largo a partir de un código inicial dado. La forma más común de extender un código es agregar una columna a la matriz generadora de tal modo que la suma de las coordenadas de cada fila de la nueva matriz sea 0. Si extendemos el código de Golay binario $\mathcal{G}_{23}$ de esta manera, obtenemos un nuevo código llamado *código de Golay binario extendido* $\mathcal{G}_{24}$, de parámetros $[24, 12, 8]$, cuya matriz generadora es $G_{24} =$

$[I_{12} \mid A]$, donde

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

Con los siguientes resultados mostramos que el código de Golay binario extendido $\mathcal{G}_{24}$ es autodual y tiene mínima distancia 8.

Teorema 2.70. *1. El código de Golay binario extendido $\mathcal{G}_{24}$ es un código autodual.*

2. El código de Golay binario extendido $\mathcal{G}_{24}$ también es generado por $[A|I_{12}]$.

3. El peso de cada palabra del código de Golay binario extendido $\mathcal{G}_{24}$ es divisible por 4.

4. El código de Golay binario extendido $\mathcal{G}_{24}$ no tiene palabras de peso 4.

5. El código de Golay binario extendido $\mathcal{G}_{24}$ tiene mínima distancia 8.

Demostración. 1. Es sencillo verificar que el producto interior de dos filas cualesquiera de G_{24} es 0. Por lo tanto, $\mathcal{G}_{24} \subseteq \mathcal{G}_{24}^{\perp}$. Pero $\dim(\mathcal{G}_{24}) = \dim(\mathcal{G}_{24}^{\perp}) = 12$. En consecuencia, $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

2. Note que $A^t = A$ y como el código de Golay binario extendido $\mathcal{G}_{24}$ es autodual, se tiene que la matriz de control $[A^t \mid I_{12}] = [A \mid I_{12}]$ es también una matriz generadora del código.

3. El peso de cada fila de G_{24} es divisible por 4 puesto su peso es 8 o 12. Si r y s son filas de G_{24}, definimos $r \cap s$ como el vector de $\mathbb{F}_2^{24}$

que tiene 1 solo en las coordenadas donde r y s tienen 1. Entonces $\mathrm{wt}(r+s) = \mathrm{wt}(r) + \mathrm{wt}(s) - 2\mathrm{wt}(r \cap s)$, pero $\mathrm{wt}(r \cap s) \equiv r \cdot s = 0$ mód 2. Por lo tanto, $\mathrm{wt}(r+s)$ es divisible por 4. Por inducción, la suma de cualquier número de filas de la matriz generadora es divisible por 4 y por ende, cada palabra del código es divisible por 4.

4. Se tienen dos matrices generadoras $G_1 = [I_{12} \mid A]$ y $G_2 = [A \mid I_{12}]$. Supongamos que $c = (a, b)$ es una palabra del código de Golay binario extendido $\mathcal{G}_{24}$ de peso 4 donde a es la mitad izquierda y b es la mitad derecha de c. Como c es combinación lineal de las filas de G_1, entonces $\mathrm{wt}(a) \geq 1$. Note que si $\mathrm{wt}(a) = 1$, se tiene que c es una fila de G_1 y ninguna de ellas tiene peso 4. Luego, $\mathrm{wt}(a) \geq 2$. Como c también es combinación lineal de las filas de G_2, se concluye que $\mathrm{wt}(b) \geq 2$. Por lo que la única opción es $\mathrm{wt}(a) = \mathrm{wt}(b) = 2$, pero esto no es posible porque si $\mathrm{wt}(a) = 2$, entonces c es la suma de dos filas de G_1 y no hay dos filas en esta matriz cuya suma sea tal que $\mathrm{wt}(b) = 2$.

5. Como el peso de cada palabra es divisible por 4 y en la matriz generadora hay vectores con peso 8, la mínima distancia es 4 o 8. Por el ítem anterior sabemos que el código de Golay binario extendido $\mathcal{G}_{24}$ no tiene palabras de peso 4, entonces la mínima distancia es 8.

□

Definición 2.71. El *código de Golay ternario* $\mathcal{G}_{11}$ es un $[11, 6, 5]$-código sobre $\mathbb{F}_3$ cuya matriz generadora es $G_{11} = (I_6 \mid A')$, donde

$$A' = \begin{pmatrix} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

También podemos extender el código de Golay ternario $\mathcal{G}_{11}$, para obtener un $[12, 6, 6]$-código llamado *código de Golay ternario extendido* $\mathcal{G}_{12}$ cuya

matriz generadora es $G_{12} = (I_6 \mid A)$, donde

$$A = \begin{pmatrix} 0 & 1 & -1 & -1 & 1 & -1 \\ 1 & 0 & 1 & -1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 & -1 \\ -1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & -1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Observación 2.72. Similar al Teorema 2.70, podemos demostrar que el código de Golay ternario extendido $\mathcal{G}_{12}$ es un código autodual con mínima distancia 6.

El siguiente teorema muestra que los códigos de Golay $\mathcal{G}_{24}$ y $\mathcal{G}_{12}$ son únicos.

Teorema 2.73 ([12])**.** *1. Cualquier* $[24, 12, 8]$*-código sobre* $\mathbb{F}_2$ *es equivalente al código de Golay binario extendido* $\mathcal{G}_{24}$*.*

2. Cualquier $[12, 6, 6]$*-código sobre* $\mathbb{F}_3$ *es equivalente al código de Golay ternario extendido* $\mathcal{G}_{12}$*.*

2.5. Códigos de Hamming

En esta sección definiremos los códigos de Hamming, estos códigos junto con los códigos de Golay son las familias de códigos lineales más conocidas.

Definición 2.74. El código de Hamming $\mathcal{H}_{q,r}$ tiene una matriz de control $H_{q,r}$ cuyas columnas consisten en vectores distintos de cero de cada subespacio unidimensional de $\mathbb{F}_q^r$. Si $q = 2$, el código de Hamming es denotado $\mathcal{H}_r$.

Observación 2.75. 1. El espacio $\mathbb{F}_q^r$ tiene $q^r - 1$ elementos distintos de cero que pueden generar un subespacio unidimensional. Además, dos subespacios son iguales si son generados por múltiplos escalares. Como hay $q-1$ escalares en $\mathbb{F}_q$ distintos de cero, se tiene que el número de espacios unidimensionales en $\mathbb{F}_q^r$ es $\frac{q^r-1}{q-1}$. Entonces el código de Hamming $\mathcal{H}_{q,r}$ tiene longitud $n = \frac{q^r-1}{q-1}$.

2. La matriz de control $H_{q,r}$ tiene r filas. Por lo cual, la dimensión del código de Hamming $\mathcal{H}_{q,r}$ es $k = n - r = \frac{q^r-1}{q-1} - r$.

3. En la matriz $H_{q,r}$ no hay dos columnas que sean múltiplos una de la otra y al sumar dos columnas cualesquiera obtenemos un vector de otro espacio unidimensional, entonces por el Lema 2.19, se tiene que el mínimo peso de $\mathcal{H}_{q,r}$ es 3.

4. El código de Hamming $\mathcal{H}_{q,r}$ es un $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$-código.

Ejemplo 2.76. La siguiente es una matriz de control para $\mathcal{H}_3$, el cual es un $[7, 4, 3]$-código binario.

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Para definir $H_{q,r}$ se establece un orden para los subespacios unidimensionales y se elige un representante para cada uno de estos subespacios. Si se tiene una matriz de control $H'_{q,r}$ con otro orden para los subespacios y con representantes distintos, se generará un nuevo código monomialmente equivalente al código descrito por la matriz de control $H_{q,r}$.

Teorema 2.77. *Cualquier $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$-código sobre $\mathbb{F}_q$ es monomialmente equivalente al código de Hamming $\mathcal{H}_{q,r}$.*

Demostración. Sea H' la matriz de control del $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$-código. H' es un matriz con r filas, $\frac{q^r-1}{q-1}$ columnas y entradas en $\mathbb{F}_q$. Además, como $d = 3$, dos columnas cualesquiera de H' son independientes. Para que dos columnas sean independientes, estas deben ser vectores distintos de cero de diferentes subespacios unidimensionales de $\mathbb{F}_q^r$. Como hay $\frac{q^r-1}{q-1}$ columnas, cada columna es un vector distinto de cero de cada subespacio unidimensional de $\mathbb{F}_q^r$, esto es, el $[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1} - r, 3]$-código es equivalente al código de Hamming $\mathcal{H}_{q,r}$. □

Capítulo 3

Códigos de grupo

Los códigos de grupo son ideales del álgebra de grupo $\mathbb{F}_q G$, para algún grupo finito G. En esta sección definiremos estos códigos, presentaremos algunos resultados sobre el dual de un código de grupo y caracterizaremos los códigos lineales que son códigos de grupo en términos de su grupo de automorfismos permutacional.

Anteriormente se demostró que el estudio de códigos cíclicos de longitud n sobre $\mathbb{F}_q$ es equivalente al estudio de ideales del álgebra $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Asimismo, se verificó que $\mathbb{F}_q[x]/\langle x^n - 1\rangle \cong \mathbb{F}_q G$ como $\mathbb{F}_q$-álgebras, donde G es el grupo cíclico de orden n. Podemos ahora identificar cada elemento $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ con $c' = \sum_{i=0}^{n-1} c_i g^i \in \mathbb{F}_q G$ y definir el conjunto $C' := \{c' \in \mathbb{F}_q G : c \in C\}$ para concluir lo siguiente.

Lema 3.1. *Un código $C \leq \mathbb{F}_q^n$ es cíclico si y solo si C' es un ideal de $\mathbb{F}_q G$, donde G es el grupo cíclico de orden n.*

Demostración. Por el Lema 2.52 se tiene que C es cíclico si y solo si $C(x)$ es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Pero $\mathbb{F}_q[x]/\langle x^n - 1\rangle \cong \mathbb{F}_q G$, entonces $C(x)$ es un ideal de $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ si y solo si C' es un ideal de $\mathbb{F}_q G$. □

En consecuencia, el estudio de códigos cíclicos en $\mathbb{F}_q^n$ es equivalente al estudio de ideales de $\mathbb{F}_q G$, donde G es el grupo cíclico de orden n. Generalizando esta idea para cualquier grupo G, podemos fijar un orden para los elementos del grupo $\{g_1, g_2, \ldots, g_n\}$ y a cada palabra $(c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$ asignarle un elemento de la forma $c_1 g_1 + c_2 g_2 + \cdots + c_n g_n \in \mathbb{F}_q G$. Teniendo esto en cuenta, definimos los códigos de grupo como se muestra a continuación.

Definición 3.2. Sea G un grupo finito. Un *código de grupo* es un ideal derecho de $\mathbb{F}_q G$. Equivalentemente, un código $C \leq \mathbb{F}_q^n$ es un código de grupo para G si existe una biyección $\varphi : E \longrightarrow G$ donde $E := \{e_1, e_2, \ldots, e_n\}$ es la base canónica de $\mathbb{F}_q^n$, tal que la extensión lineal de φ a un isomorfismo $\varphi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q G$ envía C a un ideal derecho de $\mathbb{F}_q G$. Si C es un código de grupo, lo denotamos $C \leq \mathbb{F}_q G$.

En esta definición solo consideramos los ideales derechos. Sin embargo, los siguientes resultados pueden ser igualmente demostrados para ideales izquierdos.

Ejemplo 3.3.

1. Los códigos cíclicos en $\mathbb{F}_q^n$ son códigos de grupo en $\mathbb{F}_q G$, donde G es el grupo cíclico de orden n.
2. El código lineal $C = \{(c_1, c_2, \ldots, c_n) : c_i \in \mathbb{F}_q, \sum_{i=1}^n c_i = 0\}$ es un código de grupo para cualquier grupo G con $|G| = n$. En efecto, si definimos $\varphi : \mathbb{F}_q G \longrightarrow \mathbb{F}_q$ como $\varphi(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g$, entonces φ es un homomorfismo de álgebras cuyo kernel es un ideal de $\mathbb{F}_q G$ isomorfo a C.

En este nuevo ambiente podemos definir los siguientes conceptos asociados a códigos.

Definición 3.4.

1. Sean $a = \sum_{g \in G} a_g g$ y $b = \sum_{g \in G} b_g g$ dos elementos de $\mathbb{F}_q G$. La *distancia de Hamming* entre a y b se define como

$$\mathrm{d}(a, b) := |\{g \in G : a_g \neq b_g\}|.$$

El *peso* de un elemento a se define como

$$\mathrm{wt}(a) := |\{g \in G : a_g \neq 0\}|.$$

Entonces $\mathrm{d}(a, b) = \mathrm{wt}(a - b)$. En particular, $d(a, 0) = \mathrm{wt}(a)$.

2. En el álgebra $\mathbb{F}_q G$ definimos una *forma bilineal* $\langle \cdot, \cdot \rangle$ como

$$\langle a, b \rangle := \sum_{g \in G} a_g b_g \in \mathbb{F}_q.$$

Esta forma bilineal es simétrica y no degenerada. Además, $\langle \cdot, \cdot \rangle$ es G-invariante, esto es, $\langle ag, bg \rangle = \langle a, b \rangle$ para todo $g \in G$ y todo $a, b \in \mathbb{F}_q G$.

3. Sea $C \leq \mathbb{F}_q G$. Definimos el *código dual* de C como

$$C^{\perp} := \{x \in \mathbb{F}_q G : \langle x, c\rangle = 0, \text{ para todo } c \in C\}.$$

Decimos que C es *auto-ortogonal* si $C \subseteq C^{\perp}$ y es *auto-dual* si $C = C^{\perp}$. Notemos que $C^{\perp}$ también es un ideal de $\mathbb{F}_q G$ puesto que $\langle c, c^{\perp} g\rangle = \langle cg^{-1}, c^{\perp}\rangle = 0$, esto es, $c^{\perp} g \in C^{\perp}$ para todo $g \in G$.

4. Definimos el *adjunto* de $a = \sum_{g\in G} a_g g \in \mathbb{F}_q G$, denotado $\widehat{a}$, como

$$\widehat{a} := \sum_{g\in G} a_g g^{-1}.$$

Dado $C \leq \mathbb{F}_q G$, definimos el adjunto de C como $\widehat{C} := \{\widehat{c} : c \in C\}$. Si $C = \widehat{C}$, decimos que C es *auto-adjunto*.

3.1. Códigos de grupo y su dualidad

En esta sección mostraremos que el código dual de un código de grupo $C \leq \mathbb{F}_q G$, para algún grupo finito G, es también un ideal derecho del álgebra de grupo $\mathbb{F}_q G$.

Lema 3.5. *Si C es un ideal derecho de $\mathbb{F}_q G$, entonces $\widehat{C}$ es un ideal izquierdo de $\mathbb{F}_q G$.*

Demostración. Sea $f : \mathbb{F}_q G \longrightarrow \mathbb{F}_q G$ definido como $f(a) = \widehat{a}$. Entonces f es un anti-isomorfismo. Esto es, f es claramente lineal y biyectiva y dados $a = \sum_{g\in G} a_g g \in \mathbb{F}_q G$ y $h \in G$ se sigue que

$$\begin{aligned} f(ah) = f(\sum_{g\in G} a_g gh) &= \sum_{g\in G} a_g (gh)^{-1} = \sum_{g\in G} a_g h^{-1} g^{-1} \\ &= h^{-1} \sum_{g\in G} a_g g^{-1} = f(h) f(a) \end{aligned}$$

Luego, si C es un ideal derecho de $\mathbb{F}_q G$, entonces $f(C) = \widehat{C}$ es un ideal izquierdo de $\mathbb{F}_q G$. En efecto, $f(cg^{-1}) = f(g^{-1}) f(c) = g\widehat{c} \in \widehat{C}$. □

Teorema 3.6. *Si $C \leq \mathbb{F}_q G$, entonces $C^{\perp} = \widehat{\mathrm{Ann}_l(C)}$.*

Demostración. Sea $a \in \mathrm{Ann}_l(C) = \{a \in \mathbb{F}_q G : aC = 0\}$, entonces para todo $c \in C$ se sigue que

$$0 = \langle ac, 1\rangle = \sum_{g\in G} a_{g^{-1}} c_g = \langle \hat{a}, c\rangle.$$

Por lo tanto, $\hat{a} \in C^\perp$. Luego, $\widehat{\mathrm{Ann}_l(C)} \subseteq C^\perp$. Por otro lado, si $a \in C^\perp$, entonces $0 = \langle a, c\rangle = \langle \hat{a}c, 1\rangle$ para todo $c \in C$. Como la forma bilineal es G-invariante y no degenerada se tiene que

$$0 = \langle \hat{a}c, 1\rangle = \langle \hat{a}cb, b\rangle \text{ para todo } b \in \mathbb{F}_q G \Longrightarrow \hat{a}cb = 0.$$

En particular, $\hat{a}c = 0$ para todo $c \in C$. Entonces $\hat{a} \in \mathrm{Ann}_l(C)$ o equivalentemente $a \in \widehat{\mathrm{Ann}_l(C)}$ lo cual implica que $C^\perp \subseteq \widehat{\mathrm{Ann}_l(C)}$. □

Similar a la Definición 1.83 podemos definir el módulo dual de un código de grupo C.

Definición 3.7. Sea $C \leq \mathbb{F}_q G$, entonces $C^* := \mathrm{Hom}_{\mathbb{F}_q}(C, \mathbb{F}_q)$ es un $\mathbb{F}_q G$-módulo con operación $fg(c) = f(cg^{-1})$ para $c \in C$, $g \in G$, y $f \in C^*$.

Observación 3.8. Verifiquemos que $\dim_{\mathbb{F}_q}(C) = \dim_{\mathbb{F}_q}(C^*)$. Sea $\{e_1, e_2, \ldots e_k\}$ una base para C y definamos $\delta_i : C \to \mathbb{F}_q$ como $\delta_i(\sum_{j=1}^k a_j e_j) := a_i$, entonces $B = \{\delta_i : i = 1, \ldots, k\}$ es una base para C^*. En efecto, estas funciones son linealmente independientes y dado un homomorfismo $\alpha \in C^*$, se tiene que $\alpha(c) = \sum_{i=1}^k a_i \alpha(e_i) = \sum_{i=1}^k \alpha(e_i)\delta_i(c)$ para todo $c \in C$, es decir, $\alpha = \sum_{i=1}^k \alpha(e_i)\delta_i$.

Lema 3.9. *Si $C \leq \mathbb{F}_q G$, entonces $\mathbb{F}_q G/C^\perp \cong C^*$ como $\mathbb{F}_q G$-módulos.*

Demostración. Sea $\alpha : \mathbb{F}_q G \longrightarrow C^*$ definida como $\alpha(a) = f_a$ donde $f_a(c) := \langle a, c\rangle$. Veamos que $f_a \in C^*$. Sean $c_1, c_2 \in C$ y $k \in \mathbb{F}_q$, entonces

$$f_a(c_1 + c_2) = \langle a, c_1 + c_2\rangle = \langle a, c_1\rangle + \langle a, c_2\rangle = f_a(c_1) + f_a(c_2).$$
$$f_a(kc_1) = \langle a, kc_1\rangle = k\langle a, c_1\rangle = kf_a(c_1).$$

Por otro lado, α está bien definida dado que si $a = b$, entonces $f_a(c) = \langle a, c\rangle = \langle b, c\rangle = f_b(c)$ para todo $c \in C$. La función α es además un homomorfismo de módulos. En efecto,

$$\begin{aligned}\alpha(a + b)(c) = f_{a+b}(c) &= \langle a + b, c\rangle = \langle a, c\rangle + \langle b, c\rangle \\ &= f_a(c) + f_b(c) = \alpha(a)(c) + \alpha(b)(c),\end{aligned}$$

$$\alpha(ka)(c) = f_{ka}(c) = \langle ka, c\rangle = k\langle a, c\rangle = kf_a(c) = k\alpha(a)(c)$$

y como $\langle\cdot,\cdot\rangle$ es G-invariante se tiene que

$$\begin{aligned}\alpha(ag)(c) = f_{ag}(c) = \langle ag, c\rangle = \langle a, cg^{-1}\rangle = f_a(cg^{-1})\\ = \alpha(a)(cg^{-1}) = (\alpha(a)g)(c).\end{aligned}$$

Por otro lado,

$$\begin{aligned}\ker(\alpha) &= \{a \in \mathbb{F}_qG : \alpha(a) = 0\}\\ &= \{a \in \mathbb{F}_qG : f_a(c) = 0 \text{ para todo } c \in C\}\\ &= \{a \in \mathbb{F}_qG : \langle a, c\rangle = 0 \text{ para todo } c \in C\}\\ &= C^{\perp}.\end{aligned}$$

Entonces por el primer teorema de isomorfía, $\mathbb{F}_qG/C^{\perp} \cong \mathrm{Im}(\alpha) \leq C^*$. Resta probar que $\mathrm{Im}(\alpha) = C^*$. Para esto veamos que $\dim_{\mathbb{F}_q}(C^*) = \dim_{\mathbb{F}_q}(\mathbb{F}_qG/C^{\perp})$. En efecto,

$$\dim_{\mathbb{F}_q}(\mathbb{F}_qG/C^{\perp}) = \dim_{\mathbb{F}_q}(\mathbb{F}_qG) - \dim_{\mathbb{F}_q} C^{\perp} = \dim_{\mathbb{F}_q} C = \dim_{\mathbb{F}_q}(C^*).$$

□

3.2. Códigos de grupo y su grupo de automorfismos

A continuación presentaremos un criterio para determinar cuando un código lineal es un código de grupo. Para esto notemos que la acción de $\mathrm{Sym}(n)$ en la base de $\mathbb{F}_q^n$ está dada por $\sigma(e_i) = e_{\sigma(i)}$, para todo $\sigma \in \mathrm{Sym}(n)$ y $i \in \mathbb{N}_n$. Además, recordemos que un subgrupo G de $\mathrm{Sym}(n)$ es llamado regular si G actúa regularmente sobre $\{1, \ldots, n\}$.

Teorema 3.10 ([1])**.** *Sea $C \leq \mathbb{F}_q^n$ y G un grupo de orden n. Entonces C es un código de grupo para G si y solo si G es isomorfo a un subgrupo regular de* $\mathrm{PAut}(C)$.

Demostración. Dada una biyección $\phi : E \longrightarrow G$, también denotamos su extensión lineal $\phi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_qG$ y definimos $f = f_\phi : G \longrightarrow \mathrm{Sym}(n)$ como

$e_{f(g)(i)} = \phi^{-1}(\phi(e_i)g^{-1})$ para $g \in G$ y $i \in \mathbb{N}_n$. Entonces f es un homomorfismo de grupos. En efecto,

$$\begin{aligned} e_{f(gh)(i)} &= \phi^{-1}(\phi(e_i)(gh)^{-1}) = \phi^{-1}(\phi(e_i)h^{-1}g^{-1}) \\ &= \phi^{-1}(\phi(e_{f(h)(i)})g^{-1}) = e_{f(g)f(h)(i)}. \end{aligned}$$

Más aún, f es inyectiva puesto que

$$\begin{aligned} f(g)(i) = i &\iff \phi^{-1}(\phi(e_i)g^{-1}) = e_i \iff \phi(e_i)g^{-1} = \phi(e_i) \\ &\iff \phi(e_i) = \phi(e_i)g \iff g = 1. \end{aligned}$$

De esta manera, se sigue que $H = f(G)$ es isomorfo a G y por ende, $|H| = |G| = n$. Además, si $f(g)(i) = i$, entonces $f(g) = 1$. Por lo cual, H es libre y por el Lema 1.10, H es un subgrupo regular de $\mathrm{Sym}(n)$.

Supongamos ahora que C es un código de grupo para G y sea $\phi : E \longrightarrow G$ la biyección tal que $\phi(C)$ es un ideal derecho de $\mathbb{F}_q G$ y $f = f_\phi$. Entonces $H = f(G)$ es un subgrupo regular de $\mathrm{Sym}(n)$. Por otro lado, si $h \in H$, se tiene que existe $g \in G$ tal que $h = f(g)$. Luego,

$$e_{h(i)} = e_{f(g)(i)} = \phi^{-1}(\phi(e_i)g^{-1}) = \phi^{-1}(\phi(e_i)(f^{-1}(h))^{-1}).$$

Por lo tanto, dados $h \in H$ y $\alpha = \sum a_i e_i \in \mathbb{F}_q^n$, se sigue que

$$\begin{aligned} h(\alpha) &= \sum a_i h(e_i) = \sum a_i e_{h(i)} = \sum a_i \phi^{-1}(\phi(e_i) \cdot (f^{-1}(h))^{-1}) \\ &= \phi^{-1}(\phi(\alpha) \cdot (f^{-1}(h))^{-1}). \end{aligned}$$

Entonces, como $\phi(C)$ es un ideal derecho de $\mathbb{F}_q G$, se concluye que

$$h(C) = \phi^{-1}(\phi(C) \cdot (f^{-1}(h))^{-1}) = \phi^{-1}(\phi(C)) = C.$$

En consecuencia, $H \subseteq \mathrm{PAut}(C)$.

Recíprocamente, supongamos que G es isomorfo a un subgrupo regular H de $\mathrm{PAut}(C)$. Sin perdida de generalidad, podemos suponer que $G = H$. Sea $\phi : E \longrightarrow G$ una biyección tal que $\phi^{-1}(g^{-1}) = e_{g(1)}$. Entonces

$$\phi(e_{g(1)})h = g^{-1}h = (h^{-1}g)^{-1} = \phi(e_{(h^{-1}g)(1)}) = \phi(h^{-1}(e_{g(1)}))$$

para cada $h, g \in G$. Como G es transitiva, existe $g \in G$ tal que $g(1) = i$ para cada $i \in \mathbb{N}_n$. Por ello, $\phi(e_i)h = \phi(h^{-1}(e_i))$ para cada $i \in \mathbb{N}_n$. Luego, $\phi(C)h = \phi(h^{-1}(C)) = \phi(C)$ puesto que $G \subseteq \mathrm{PAut}(C)$. En consecuencia, $\phi(C)$ es un ideal derecho de $\mathbb{F}_q G$. □

Ejemplo 3.11. El código de Golay binario extendido $[24, 12, 8]$ es un código de grupo autodual en $\mathbb{F}_2\mathrm{Sym}(4)$ ([2]) o en $\mathbb{F}_2 D_{24}$ ([11]), donde $\mathrm{Sym}(4)$ y D_{24} son subgrupos regulares de $M_{24} = \mathrm{PAut}(C)$ ([9]). Por lo tanto, un código puede ser código de grupo para diferentes grupos.

Con el siguiente teorema verificamos que no todos los códigos lineales son códigos de grupo.

Teorema 3.12 ([16])**.** *El álgebra $\mathbb{F}_q G$ contiene un código de grupo autodual si y sólo si $2 \mid |G|$ y $\mathbb{F}_q$ tiene característica 2.*

Observación 3.13. Por el teorema anterior, el código de Golay ternario extendido $[12, 6, 6]$ no es un código de grupo puesto que es un código autodual con característica diferente de 2. Sin embargo, como mostraremos en el siguiente capítulo, este código sí es un ideal de un álgebra de grupo torcido $\mathbb{F}_3\mathrm{Alt}(4)$.

Capítulo 4

Códigos de grupo torcidos

El objetivo de este capítulo es presentar un resultado análogo al Teorema 3.10 con el cual caracterizaremos los códigos lineales que son códigos de grupo torcidos. También mostraremos que códigos muy conocidos, tales como el código de Golay ternario extendido $\mathcal{G}_{12}$ y los códigos de Hamming existen como códigos de grupo torcidos. Iniciaremos este análisis definiendo estos códigos y exponiendo algunos resultados con relación a su código dual.

Definición 4.1. 1. Un función $\alpha : G \times G \to \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ se denomina *2-cociclo* si

$$\alpha(g_1, g_2g_3)\alpha(g_2, g_3) = \alpha(g_1g_2, g_3)\alpha(g_1, g_2) \text{ para todo } g_1, g_2, g_3 \in G.$$

El conjunto de los 2-cociclo de G forman un grupo denotado $\mathrm{Z}^2(G, \mathbb{F}_q^*)$.

2. Una función $\alpha \in \mathrm{Z}^2(G, \mathbb{F}_q^*)$ es llamada *coborde* si existe una función $\beta : G \longrightarrow \mathbb{F}_q^*$ con $\beta(1) = 1$ tal que

$$\alpha(g, h) = \beta(g)^{-1}\beta(h)^{-1}\beta(gh) \text{ para todo } g, h \in G.$$

El conjunto de los coborde de G forman un grupo denotado $\mathrm{B}^2(G, \mathbb{F}_q^*)$.

Observación 4.2. Podemos reemplazar un 2-cociclo α por un 2-cociclo normalizado α', donde

$$\alpha'(g, h) = \frac{\alpha(g, h)}{\alpha(1, 1)}.$$

Notemos que $\alpha'(g, 1)\alpha'(1, 1) = \alpha'(g, 1 \cdot 1)\alpha'(1, 1) = \alpha'(g, 1)\alpha'(g, 1)$. Por lo tanto, $\alpha'(g, 1) = \alpha'(1, 1) = 1$. Similarmente, $\alpha'(1, h) = \alpha'(1, 1) = 1$. En adelante, asumimos que $\alpha \in \mathrm{Z}^2(G, \mathbb{F}_q^*)$ esta normalizado.

Definición 4.3. Sea $\alpha \in \mathrm{Z}^2(G, \mathbb{F}_q^*)$ y G un grupo finito. El *álgebra de grupo torcido* $\mathbb{F}_q^\alpha G$ es definida como

$$\mathbb{F}_q^\alpha G := \left\{ a = \sum_{g \in G} a_g \overline{g} : a_g \in \mathbb{F} \right\}.$$

Donde la multiplicación está dada por $\overline{g}\overline{h} = \alpha(g,h)\overline{gh}$ para todo $g, h \in G$ extendida linealmente. Además, la suma y la multiplicación por escalares es similar a las definidas para $\mathbb{F}_q G$, donde $g \in G$ es reemplazada por $\overline{g}$. Así, el conjunto $\{\overline{g} : g \in G\}$ es una base de $\mathbb{F}_q^\alpha G$ y $\dim(\mathbb{F}_q^\alpha G) = |G|$.

Observación 4.4. Tanto el álgebra de grupo como el álgebra de grupo torcido tienen aplicación en criptografía de clave pública. En particular, [5] define un 2-cociclo α_λ para el grupo dihedral D_{2n}, con el cual propone un cifrado de clave pública que aprovecha las propiedades del álgebra de grupo torcido $\mathbb{F}_q^{\alpha_\lambda} D_{2n}$. Similarmente, [4] propone un cifrado de clave publica en el álgebra de grupo sesgada $\mathbb{F}_{q^2}^\theta D_{2n}$ donde $\theta : D_{2n} \to \mathrm{Aut}(\mathbb{F}_{q^2})$ es un homomorfismo de grupos.

Teorema 4.5. *Sea $\alpha, \beta \in \mathrm{Z}^2(G, \mathbb{F}_q^*)$. Entonces $\Gamma : \mathbb{F}_q^\alpha G \longrightarrow \mathbb{F}_q^\beta G$ definido por $\overline{g} \mapsto \gamma(g)\overline{g}$ donde $\gamma(g) \in \mathbb{F}_q^*$ es un isomorfismo de álgebras si y solo si*

$$\alpha(g,h) = \beta(g,h)\gamma(g)\gamma(h)\gamma(gh)^{-1}.$$

Demostración. La función Γ es claramente lineal. Entonces Γ es un isomorfismo si y solo si $\Gamma(\overline{g}\overline{h}) = \Gamma(\overline{g})\Gamma(\overline{h})$. Note que

$$\begin{aligned} \Gamma(\overline{g}\overline{h}) &= \Gamma(\overline{g})\Gamma(\overline{h}) \\ \iff \Gamma(\alpha(g,h)\overline{gh}) &= \gamma(g)\overline{g}\gamma(h)\overline{h} \\ \iff \alpha(g,h)\gamma(gh)\overline{gh} &= \beta(g,h)\gamma(g)\gamma(h)\overline{gh} \\ \iff \alpha(g,h) &= \beta(g,h)\gamma(g)\gamma(h)\gamma(gh)^{-1} \end{aligned}$$

□

Observación 4.6. Notemos que si $\beta(g,h) = 1$ para todo $g, h \in G$, entonces $\mathbb{F}_q^\beta G = \mathbb{F}_q G$. Luego, por el teorema anterior, $\mathbb{F}_q^\alpha G \cong \mathbb{F}_q G$ si y solo si $\alpha(g,h) = \gamma(g)\gamma(h)\gamma(gh)^{-1}$. Es decir, $\mathbb{F}_q^\alpha G \cong \mathbb{F}_q G$ si α es coborde.

Definición 4.7. Un *código de grupo torcido* C es un ideal derecho de $\mathbb{F}_q^\alpha G$, denotado $C \leq \mathbb{F}_q^\alpha G$.

Definimos los códigos de grupo torcidos como ideales derechos por conveniencia. Los siguientes resultados pueden ser igualmente demostrados para ideales izquierdos.

Ejemplo 4.8. Los ideales del álgebra $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ donde $\lambda \in \mathbb{F}_q^*$ son llamados códigos λ-constacíclicos. Notemos que en $\mathbb{F}_q[x]/\langle x^n - \lambda\rangle$,

$$x^n \equiv \lambda \text{ y } x^i x^j = \begin{cases} 1x^{i+j} & \text{si } 0 \leq i+j < n \\ \lambda x^{i+j \mod n} & \text{si } n \leq i+j \leq 2(n-1) \end{cases}$$

Sea ahora $G = \langle g\rangle$ el grupo cíclico de orden n y definamos el 2-cociclo α_λ de G como

$$\alpha_\lambda(g^i, g^j) = \begin{cases} 1 & \text{si } 0 \leq i+j < n \\ \lambda & \text{si } n \leq i+j \leq 2(n-1) \end{cases}$$

Si definimos la función $f : \mathbb{F}_q^{\alpha_\lambda} G \longrightarrow \mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ como $f(\overline{g}) = x + \langle x^n - \lambda\rangle$, entonces $\mathbb{F}_q^{\alpha_\lambda} G \cong \mathbb{F}_q[x]/\langle x^n - \lambda\rangle$ como $\mathbb{F}_q$-álgebras. En efecto, f es lineal, biyectiva y

$$f(\overline{g^i} \cdot \overline{g^j}) = f(\alpha_\lambda(g^i, g^j)\overline{g^{i+j}}) = \alpha_\lambda(g^i, g^j) f(\overline{g^{i+j}}) = x^i x^j = f(g^i) f(g^j).$$

Por lo tanto, los códigos λ-constacíclicos son ideales derechos de $\mathbb{F}_q^{\alpha_\lambda} G$, es decir, son códigos de grupo torcidos para $G = \langle g\rangle$ el grupo cíclico de orden n y el 2-cociclo α_λ.

Definición 4.9. En este nuevo ambiente, tenemos lo siguiente definiciones

1. Sean $a = \sum_{g\in G} a_g \overline{g}$ y $b = \sum_{g\in G} b_g \overline{g}$ dos elementos de $\mathbb{F}_q^\alpha G$. El *peso* de a se define como $\mathrm{wt}(a) := |\{g \in G : a_g \neq 0\}$ y la *distancia* entre a y b se define como $\mathrm{d}(a, b) := \mathrm{wt}(a - b) = |\{g \in G : a_g \neq b_g\}|$.

2. En el álgebra $\mathbb{F}_q^\alpha G$ se define una *forma bilineal* simétrica y no degenerada $\langle \cdot, \cdot \rangle$ dada por

   $$\langle \overline{g}, \overline{h}\rangle := \delta_{g,h} \text{ para todo } g, h \in G.$$

   Entonces el *código dual* de $C \leq \mathbb{F}_q^\alpha G$ es

   $$C^\perp := \{x \in \mathbb{F}_q^\alpha G : \langle x, c\rangle = 0 \text{ para todo } c \in C\}.$$

3. Dado $a = \sum_{g\in G} a_g \overline{g} \in \mathbb{F}_q^\alpha G$, definimos el adjunto de a como

   $$\widehat{a} := \sum_{g\in G} a_g \alpha(g, g^{-1}) \overline{g^{-1}}.$$

Lema 4.10. *Sea G un grupo finito y $\alpha \in \mathrm{Z}^2(G, \mathbb{F}_q^*)$. Entonces*

1. *$\alpha(g, g^{-1}) = \alpha(g^{-1}, g)$ para todo $g \in G$.*
2. *Si $\alpha(g, g^{-1})\alpha(g^{-1}, g) = 1$ para todo $g \in G$, entonces $\widehat{\widehat{a}} = a$ para todo $a \in \mathbb{F}_q^\alpha G$.*

Demostración. 1. Por definición del 2-cociclo α y la Observación 4.2 se sigue que

$$\alpha(g, g^{-1}) = \alpha(g^{-1}, 1)\alpha(g, g^{-1}) = \alpha(1, g^{-1})\alpha(g^{-1}, g) = \alpha(g^{-1}, g).$$

2. Sea $\alpha(g, g^{-1})\alpha(g^{-1}, g) = 1$ para todo $g \in G$ y $a = \sum_{g\in G} a_g \overline{g} \in \mathbb{F}_q^\alpha G$. Entonces $\widehat{a} = \sum_{g\in G} a_g \alpha(g, g^{-1})\overline{g^{-1}}$. Luego,

$$\widehat{\widehat{a}} = \sum_{g\in G} a_g \alpha(g, g^{-1})\alpha(g^{-1}, g)\overline{(g^{-1})^{-1}} = \sum_{g\in G} (a_g \cdot 1)\overline{g} = \sum_{g\in G} a_g \overline{g} = a.$$

□

Teorema 4.11. *Para cualquier 2-cociclo α de G, la función $\varphi : \mathbb{F}^\alpha G \longrightarrow \mathbb{F}^{\alpha^{-1}} G$ definida como $a \longmapsto \widehat{a}$ es un anti-isomorfismo de álgebras.*

Demostración. La función φ es claramente $\mathbb{F}_q$-lineal.Por otro lado, note que

$$\overline{g}^{-1} = \alpha(g, g^{-1})\overline{g^{-1}}.$$

Entonces $\varphi(\sum_{g\in G} a_g \overline{g}) = \sum_{g\in G} a_g \overline{g}^{-1}$. Luego, para $g, h \in G$ se sigue que

$$\begin{aligned}\varphi(\overline{g}\overline{h}) &= \varphi(\alpha(g, h)\overline{gh}) = \alpha(g, h)\overline{(gh)}^{-1} = \alpha(g, h)(\alpha(g, h)\overline{g}\overline{h})^{-1} \\ &= \overline{h}^{-1}\overline{g}^{-1} = \varphi(\overline{h})\varphi(\overline{g}).\end{aligned}$$

Por lo tanto, $\varphi(\overline{g}\overline{h}) = \varphi(\overline{h})\varphi(\overline{g})$. □

Corolario 4.12. *Si $\alpha = \alpha^{-1}$ es un 2-cociclo de G entonces $a \longmapsto \widehat{a}$ define un anti-isomorfismo de $\mathbb{F}_q^\alpha G$ de orden 2.*

Demostración. Del Teorema anterior se sigue que si $\alpha = \alpha^{-1}$, entonces $a \longmapsto \widehat{a}$ es un anti-isomorfismo del álgebra $\mathbb{F}_q^\alpha G$. Además,

$$\alpha(g, g^{-1})\alpha(g^{-1}, g) = \alpha(g, g^{-1})\alpha(g, g^{-1}) = \alpha(g, g^{-1})\alpha^{-1}(g, g^{-1}) = 1.$$

Entonces por el Lema 4.10, se concluye que $\widehat{\widehat{a}} = a$. □

4.1. Códigos de grupo torcidos y su dualidad

En esta sección comprobaremos que, a diferencia de los códigos de grupo, el dual de un código de grupo torcido $C \leq \mathbb{F}_q^\alpha G$ no es siempre un ideal del álgebra de grupo torcida $\mathbb{F}_q^\alpha G$. Inicialmente, revisaremos algunos resultados de $\mathbb{F}_q$-álgebras, relacionados con la definición de álgebra de frobenius y álgebra simétrica.

Definición 4.13. Sea A un $\mathbb{F}_q$-álgebra de dimensión finita.

1. A es llamada *álgebra de frobenius* si existe una forma bilineal no singular $\langle \cdot, \cdot \rangle_{Frob} : A \times A \longrightarrow \mathbb{F}_q$ tal que $\langle ab, c \rangle_{Frob} = \langle a, bc \rangle_{Frob}$ para todo $a, b, c \in A$.

2. A es llamada *álgebra simétrica* si existe una forma bilineal simétrica no singular $\langle \cdot, \cdot \rangle$ tal que $\langle ab, c \rangle = \langle a, bc \rangle$ para todo $a, b, c \in A$.

Ejemplo 4.14. $\mathbb{F}_q G$ es un álgebra simétrica. En efecto, para $g_1, g_2 \in G$ definimos la forma bilineal

$$\langle g_1, g_2 \rangle = \begin{cases} 0 & \text{si } g_1 g_2 \neq 1 \\ 1 & \text{si } g_1 g_2 = 1 \end{cases}$$

extendida en $\mathbb{F}_q G$. Entonces $\langle \cdot, \cdot \rangle$ es claramente simétrica. Más aún, $\langle ab, c \rangle = \langle a, bc \rangle$ para todo $a, b, c \in A$, puesto que $\langle g_1 g_2, g_3 \rangle = \langle g_1, g_2 g_3 \rangle$ para todo $g_1, g_2, g_3 \in G$. Resta mostrar que la forma bilineal es no singular. Supongamos que $a = \sum_{g \in G} a_g g$ y que $\langle a, b \rangle = 0$ para todo $b \in \mathbb{F}_q G$. Luego, para todo $h \in G$ se tiene que $0 = \langle a, h^{-1} \rangle = a_h$. Por lo tanto, $a = 0$, esto es, $\langle \cdot, \cdot \rangle$ es no singular.

Teorema 4.15. *Sea A un $\mathbb{F}_q$-álgebra de dimensión finita. Entonces*

1. *A es un álgebra de frobenius si y solo si existe $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q)$ tal que el kernel de λ no contiene ideales derechos de A diferentes de cero.*

2. *A es un álgebra simétrica si y solo si existe $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q)$ tal que el kernel de λ no contiene ideales derechos de A diferentes de cero y $\lambda(xy) = \lambda(yx)$ para todo $x, y \in A$.*

Demostración. 1. Supongamos que A es un álgebra de frobenius con la forma bilineal $\langle\cdot,\cdot\rangle_{Frob}$ y definamos $\lambda : A \to \mathbb{F}_q$ como $\lambda(x) = \langle x, 1\rangle_{Frob}$. Claramente $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q)$. Si I es un ideal de A tal que $\lambda(I) = 0$ y $a \in I$, entonces

$$0 = \langle ab, 1\rangle_{Frob} = \langle a, b\rangle_{Frob} \text{ para todo } b \in A.$$

Por lo tanto, como f es no singular, $a = 0$. Recíprocamente, supongamos $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q)$ y definamos $\langle a, b\rangle_{Frob} = \lambda(ab)$. Entonces $\langle\cdot,\cdot\rangle_{Frob}$ es claramente bilineal y

$$\langle ab, c\rangle_{Frob} = \lambda(abc) = \langle a, bc\rangle_{Frob} \text{ para todo } a, b, c \in A.$$

La no singularidad se sigue de que el kernel de λ no contiene ideales derechos diferentes de cero dado que

$$\langle x, A\rangle_{Frob} = 0 \Rightarrow \lambda(xA) = 0 \Rightarrow x = 0.$$

2. Supongamos que A es un álgebra simétrica con la forma bilineal $\langle\cdot,\cdot\rangle_{Frob}$ y definamos $\lambda : A \to \mathbb{F}_q$ como $\lambda(x) = \langle x, 1\rangle_{Frob}$. Por el ítem anterior $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q)$ y su kernel no contiene ideales derechos de A diferentes de cero. Resta mostrar que $\lambda(xy) = \lambda(yx)$ para todo $x, y \in A$. En efecto,

$$\lambda(xy) = \langle xy, 1\rangle_{Frob} = \langle x, y\rangle_{Frob} = \langle y, x\rangle_{Frob} = \langle yx, 1\rangle_{Frob} = \lambda(yx).$$

Recíprocamente, supongamos que $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q)$. Como en el ítem anterior, definamos $\langle x, y\rangle_{Frob} = \lambda(xy)$. Entonces solo debemos demostrar que

$$\langle x, y\rangle_{Frob} = \lambda(xy) = \lambda(yx) = \langle y, x\rangle_{Frob} \text{ para todo } x, y \in A.$$

□

Teorema 4.16. *Sea $A = \mathbb{F}_q^{\alpha}G$. Entonces A es un álgebra de frobenius y simétrica.*

Demostración. Definamos $\lambda : A \longrightarrow \mathbb{F}_q$ como $\lambda(a) = a_1$ donde $a = a_1\overline{1} + \sum_{1\neq g\in G} a_g\overline{g}$. Claramente se tiene que $\lambda \in \mathrm{Hom}_{\mathbb{F}_q}(A, \mathbb{F}_q)$. Supongamos que I es un ideal de A tal que $\lambda(I) = 0$. Si $a = \sum_{g\in G} a_g\overline{g} \in I$, entonces para cualquier $h \in G$

$$\lambda(a\overline{h^{-1}}) = \alpha(h, h^{-1})a_h = 0$$

puesto que $a\overline{h^{-1}} \in I$. Luego, $a_h = 0$ y por ende, $a = 0$. Es decir, el kernel de λ no contiene ideales derechos de A diferentes de cero. En consecuencia, A es un álgebra de frobenius. Finalmente, para todo $a, b \in A$ se tiene que

$$\lambda(ab) = \sum_{g \in G} a_g b_{g^{-1}} \alpha(g, g^{-1}) = \sum_{g \in G} b_{g^{-1}} a_g \alpha(g^{-1}, g) = \lambda(ba).$$

Por lo tanto, A es simétrica. □

Recordemos que para un álgebra A y un ideal izquierdo I de A, el ideal $\mathrm{Ann}_l(I) = \{a \in A : aI = 0\}$ es llamado el aniquilador izquierdo de I en A.

Teorema 4.17. *Si C es un ideal derecho de un álgebra de frobenius A, entonces*

1. $\mathrm{Ann}_l(C) = \{a \in A : \langle a, c\rangle_{Frob} = 0 \ \ \textit{para todo } c \in C\}$.
2. $\dim_{\mathbb{F}_q} C + \dim_{\mathbb{F}_q}(\mathrm{Ann}_l(C)) = \dim_{\mathbb{F}_q} A$.

Demostración. 1. Sea $C^{\perp}_{Frob} = \{a \in A : \langle a, c\rangle_{Frob} = 0 \ \text{ para todo } c \in C\}$. Por definición, $\mathrm{Ann}_l(C) = \{a \in A, aC = 0\}$. Mostraremos que $\mathrm{Ann}_l(C) = C^{\perp}_{Frob}$. Supongamos que $x \in C^{\perp}_{Frob}$, entonces para todo $c \in C$ y $a \in A$ se tiene

$$0 = \langle x, ca\rangle_{Frob} = \langle xc, a\rangle_{Frob}.$$

Como $\langle \cdot, \cdot \rangle_{Frob}$ es no singular, se sigue que $xc = 0$ para todo $c \in C$. De este modo, $x \in \mathrm{Ann}_l(C)$ y $C^{\perp}_{Frob} \subseteq \mathrm{Ann}_l(C)$. Por otro lado, supongamos que $x \in \mathrm{Ann}_l(C)$, luego

$$0 = \langle xc, 1\rangle_{Frob} = \langle x, c\rangle_{Frob}.$$

Por lo tanto, $x \in C^{\perp}_{Frob}$ y por ello, $\mathrm{Ann}_l(C) \subseteq C^{\perp}_{Frob}$.

2. Como $\langle \cdot, \cdot \rangle_{Frob}$ es una forma bilineal no singular se tiene

$$\dim_{\mathbb{F}_q} A = \dim_{\mathbb{F}_q} C + \dim_{\mathbb{F}_q}(C^{\perp}_{Frob}) = \dim_{\mathbb{F}_q} C + \dim_{\mathbb{F}_q}(\mathrm{Ann}_l(C)).$$

□

Lema 4.18. *Sea $A = \mathbb{F}_q^{\alpha} G$ y C un código de grupo torcido de A. Entonces* $\dim_{\mathbb{F}_q}(C^{\perp}) = \dim_{\mathbb{F}_q}(\widehat{\mathrm{Ann}_l(C)})$

Demostración. Como $C^\perp$ es definido con una forma bilineal no degenerada, se tiene que $\dim_{\mathbb{F}_q}(C^\perp) = \dim_{\mathbb{F}_q} A - \dim_{\mathbb{F}_q} C$. Además, $\dim_{\mathbb{F}_q}(\widehat{\mathrm{Ann}_l(C)}) = \dim_{\mathbb{F}_q}(\mathrm{Ann}_l(C))$ puesto que $\widehat{\ }\colon \mathbb{F}^\alpha G \to \mathbb{F}^{\alpha^{-1}} G$ es un anti-isomorfismo. Entonces, por el Teorema 4.17, se concluye que

$$\dim_{\mathbb{F}_q}(\mathrm{Ann}_l(C)) = \dim_{\mathbb{F}_q} A - \dim_{\mathbb{F}_q} C = \dim_{\mathbb{F}_q}(C^\perp).$$

□

Teorema 4.19. *Sea $C \leq \mathbb{F}_q^\alpha G$ un código de grupo torcido. Entonces*

$$C^\perp = \widehat{\mathrm{Ann}_l(C)}.$$

Demostración. Sea $a = \sum_{g\in G} a_g \overline{g} \in \mathrm{Ann}_l(C)$ y $c = \sum_{g\in G} c_{g^{-1}} \overline{g^{-1}} \in C$. Por el Lema 4.10, se concluye que

$$0 = \langle ac, \overline{1}\rangle = \sum_{g\in G} a_g c_{g^{-1}} \alpha(g, g^{-1}) = \sum_{g\in G} c_{g^{-1}} a_g \alpha(g^{-1}, g) = \langle c, \hat{a}\rangle.$$

Por lo tanto, $\widehat{\mathrm{Ann}_l(C)} \subseteq C^\perp$. Además, por el Lema 4.18, se sigue que $\dim_{\mathbb{F}_q} C^\perp = \dim_{\mathbb{F}_q}(\widehat{\mathrm{Ann}_l(C)})$. En consecuencia, $C^\perp = \widehat{\mathrm{Ann}_l(C)}$. □

Observación 4.20. Teniendo en cuenta el Teorema anterior y dado que $\widehat{\ }\colon \mathbb{F}_q^\alpha G \to \mathbb{F}_q^{\alpha^{-1}} G$ es un anti-isomorfismo, se deduce que $C^\perp$ es un ideal de $\mathbb{F}_q^{\alpha^{-1}} G$. En general, $C^\perp$ no es un ideal de $\mathbb{F}_q^\alpha G$ puesto que la forma bilineal $\langle\cdot,\cdot\rangle$ no es G-invariante. Note que

$$\begin{aligned}\langle \overline{g}\ \overline{x}, \overline{h}\ \overline{x}\rangle &= \alpha(g,x)\alpha(h,x)\delta_{gx,hx} = \alpha(g,x)\alpha(h,x)\delta_{g,h} \\ &= \langle \overline{g}, \overline{h}\rangle \alpha(g,x)\alpha(h,x)\end{aligned}$$

para $g, h, x \in G$. Sin embargo, en caso que $\alpha = \alpha^{-1}$, se sigue que $C^\perp$ es un ideal derecho de $\mathbb{F}_q^\alpha G$.

Corolario 4.21. *Suponga que $\alpha = \alpha^{-1}$ y sea $e^2 = e \in \mathbb{F}_q^\alpha G$ un idempotente. Si $C = e\mathbb{F}_q^\alpha G$, entonces $C^\perp = (\overline{1} - \hat{e})\mathbb{F}_q^\alpha G$.*

Demostración. Verifiquemos que $\mathrm{Ann}_l(C) = \mathbb{F}_q^\alpha G(\overline{1} - e)$. Supongamos que $a = b(\overline{1} - e) \in \mathbb{F}_q^\alpha G(\overline{1} - e)$ para algún $b \in \mathbb{F}_q^\alpha G$. Entonces

$$a(e\mathbb{F}_q^\alpha G) = b(\overline{1} - e)(e\mathbb{F}_q^\alpha G) = be\mathbb{F}_q^\alpha G - be^2\mathbb{F}_q^\alpha G = be\mathbb{F}_q^\alpha G - be\mathbb{F}_q^\alpha G = 0.$$

Por lo tanto, $a \in \mathrm{Ann}_l(e\mathbb{F}_q^\alpha G)$ y por ende, $\mathbb{F}_q^\alpha G(\overline{1}-e) \subseteq \mathrm{Ann}_l(C)$. Ahora, supongamos $a \in \mathrm{Ann}_l(e\mathbb{F}_q^\alpha G)$. Luego,

$$a = a(e+\overline{1}-e) = ae + a(\overline{1}-e) = a(\overline{1}-e) \in \mathbb{F}_q^\alpha G(\overline{1}-e).$$

Por ello, $\mathrm{Ann}_l(C) \subseteq \mathbb{F}_q^\alpha G(\overline{1}-e)$ y se comprueba la igualdad. Finalmente, aplicando el Teorema 4.19 y el Corolario 4.12 se tiene que

$$C^\perp = \widehat{\mathrm{Ann}_l(C)} = \mathbb{F}_q^\alpha \widehat{G(\overline{1}-e)} = (\overline{1}-\hat{e})\mathbb{F}_q^\alpha G.$$

□

Teorema 4.22. *Suponga que $\alpha = \alpha^{-1}$ y sea $C = e\mathbb{F}_q^\alpha G$ un código de grupo torcido donde $e = e^2$. Entonces las siguientes afirmaciones son equivalentes*

1. $C = C^\perp$.
2. $\hat{e}e = 0$ *y* $\overline{1}-\hat{e} = e(\overline{1}-\hat{e})$.

En particular, si $e = \overline{1}-\hat{e}$, entonces $C = C^\perp$.

Demostración. Si $C = C^\perp$, entonces $C = e\mathbb{F}_q^\alpha G = (\overline{1}-\hat{e})\mathbb{F}_q^\alpha G$ donde $(\overline{1}-\hat{e})$ es también un idempotente. Por ello, $e = (\overline{1}-\hat{e})a$ y $(\overline{1}-\hat{e}) = eb$ para algún $a, b \in \mathbb{F}_q^\alpha G$. Luego,

$$(\overline{1}-\hat{e})e = (\overline{1}-\hat{e})((\overline{1}-\hat{e})a) = (\overline{1}-\hat{e})a = e$$

$$\text{y} \quad e(\overline{1}-\hat{e}) = e(eb) = eb = (\overline{1}-\hat{e}).$$

Notemos que $(\overline{1}-\hat{e})e = e$ implica que $\hat{e}e = 0$. Recíprocamente, si $\overline{1}-\hat{e} = e(\overline{1}-\hat{e})$, entonces $(\overline{1}-\hat{e})\mathbb{F}_q^\alpha G = e(\overline{1}-\hat{e})\mathbb{F}_q^\alpha G$. Por lo tanto, $(\overline{1}-\hat{e})\mathbb{F}_q^\alpha G \leq e\mathbb{F}_q^\alpha G$. Además, $\hat{e}e = 0$ es equivalente a $(\overline{1}-\hat{e})e = e$. Por lo cual, $e\mathbb{F}_q^\alpha G = (\overline{1}-\hat{e})e\mathbb{F}_q^\alpha G$, de donde se sigue que $e\mathbb{F}_q^\alpha G \leq (\overline{1}-\hat{e})\mathbb{F}_q^\alpha G$. En consecuencia, $C = C^\perp$. □

4.2. Códigos de grupo torcidos y su grupo de automorfismos

Los siguientes resultados permiten establecen las condiciones necesarias y suficientes para que un código lineal dado exista como un código de grupo torcido, para cierto grupo G.

Definición 4.23. La función $\pi : \mathrm{Mon}(n, \mathbb{F}_q) \longrightarrow \mathrm{Sym}(n)$ definida como $M = DP \longmapsto P$, donde D es la matriz diagonal y P es la matriz de permutación que conforman la matriz monomial M, es llamada *epimorfismo natural*.

Lema 4.24. *Sea α un 2-cociclo de G. Luego, $G(\alpha) = \mathbb{F}_q^* \times G$ es un grupo con $(\lambda, g) \cdot (\mu, h) = (\alpha(g, h)\lambda\mu, gh)$ para $\lambda, \mu \in \mathbb{F}_q^*$ y $g, h \in G$.*

Demostración. Verifiquemos las tres propiedades requeridas para que $G(\alpha)$ sea un grupo. Sea $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{F}_q^*$ y $g_1, g_2, g_3 \in G$. Entonces

1. Asociativa.

$$\begin{aligned}((\lambda_1, g_1)(\lambda_2, g_2))(\lambda_3, g_3) &= (\alpha(g_1, g_2)\lambda_1\lambda_2, g_1g_2)(\lambda_3, g_3) \\ &= (\alpha(g_1g_2, g_3)\alpha(g_1, g_2)\lambda_1\lambda_2\lambda_3, g_1g_2g_3) \\ &= (\alpha(g_1, g_2g_3)\alpha(g_2, g_3)\lambda_1\lambda_2\lambda_3, g_1g_2g_3) \\ &= (\lambda_1, g_1)(\alpha(g_2, g_3)\lambda_2\lambda_3, g_2g_3) \\ &= (\lambda_1, g_1)((\lambda_2, g_2)(\lambda_3, g_3)).\end{aligned}$$

2. Elemento neutro.

$$(\lambda, g)(1, 1) = (\alpha(g, 1)\lambda 1, g1) = (\lambda, g).$$

3. Inverso.

$$(\lambda, g)(\lambda^{-1}\alpha(g, g^{-1})^{-1}, g^{-1}) = (\alpha(g, g^{-1})\lambda\lambda^{-1}\alpha(g, g^{-1})^{-1}, gg^{-1}) = (1, 1).$$

□

Observación 4.25.

1. Sea $N := \{(\lambda, 1) : \lambda \in \mathbb{F}_q^*\}$. Entonces $N \cong \mathbb{F}_q^*$ puesto que la función $(\lambda, 1) \longmapsto \lambda$ es un isomorfismo de grupos. Además, la función $(\lambda, g) \longmapsto g$ es un epimorfismo cuyo kernel es N. Por lo tanto, N es un subgrupo normal de $G(\alpha)$ y $G(\alpha)/N \cong G$.

2. Notemos que $G(\alpha)$ permite una acción monomial en $\mathbb{F}_q^\alpha G$ dada por

$$\overline{g}(\lambda, h) = (\lambda\overline{g})\overline{h} = \lambda\alpha(g, h)\overline{gh}.$$

Entonces, si definimos la permutación $\sigma_h(i) := j$ si y solo si $g_ih = g_j$ para todo $i, j \in \{1, \ldots, n\}$, se tiene que el grupo de matrices correspondientes a la acción de $G(\alpha)$ es

$$H_{G(\alpha)} = \{\mathrm{diag}(\lambda\alpha(g_1, h), \ldots, \lambda\alpha(g_n, h))\sigma_h : (\lambda, h) \in G(\alpha)\}.$$

Así, las matrices diagonales ocurren cuando $h = 1$, es decir, están dadas por la acción de N sobre $\mathbb{F}_q^\alpha G$ puesto que $\overline{g}(\lambda, 1) = \lambda\alpha(g, 1)\overline{g1} = \lambda\overline{g}$. Por lo tanto, las únicas matrices diagonales de la acción de $G(\alpha)$ en $\mathbb{F}_q^\alpha G$ son matrices escalares.

Lema 4.26. *Sea C un código de grupo torcido en $\mathbb{F}_q^\alpha G$ para un 2-cociclo α de G donde $|G| = n$. Entonces existe un subgrupo $H \leq \mathrm{MAut}(C)$ tal que las únicas matrices diagonales son las matrices escalares y $G \cong \pi(H)$ actúa regularmente en el conjunto $\{1, \ldots, n\}$.*

Demostración. Sea $c = \sum_{g\in G} c_g\overline{g} \in C$ y $(\lambda, h) \in G(\alpha)$. Entonces

$$c(\lambda, h) = \sum_{g\in G} c_g\overline{g}(\lambda, h) = \sum_{g\in G} c_g\lambda\alpha(g, h)\overline{gh} = \sum_{g\in G} c_g\lambda\overline{g}\overline{h} = \lambda c\overline{h}.$$

Como C es un ideal derecho de $\mathbb{F}_q^\alpha G$, se sigue que $\lambda c\overline{h} \in C$ y por lo tanto, $C(\lambda, h) = C$. Luego, si H es el grupo de matrices correspondientes a la acción de $G(\alpha)$, entonces H es un subgrupo de $\mathrm{MAut}(C)$ tal que las únicas matrices diagonales son las matrices escalares.
Sea ahora $\pi(H) := \{\sigma_h : h \in G\}$ donde $\sigma_h(i) = j \iff g_ih = g_j$ y definamos $\varphi : G \longrightarrow \pi(H)$ como $h \longmapsto \sigma_{h^{-1}}$. Notemos que

$$\begin{aligned}\sigma_{(gh)^{-1}}(i) = j &\iff g_i(gh)^{-1} = g_j \iff (g_ih^{-1})g^{-1} = g_j\\ &\iff \sigma_{g^{-1}}\sigma_{h^{-1}}(i) = j.\end{aligned}$$

Esto es, $\sigma_{(gh)^{-1}} = \sigma_{g^{-1}}\sigma_{h^{-1}}$. Luego,

$$\varphi(gh) = \sigma_{(gh)^{-1}} = \sigma_{g^{-1}}\sigma_{h^{-1}} = \varphi(g)\varphi(h).$$

De este modo, φ es un homomorfismo que es claramente sobreyectivo. Por lo tanto, $G \cong \pi(H)$. Resta probar que la acción de $\pi(H)$ es regular. Sea $i \in \{1, \ldots, n\}$ tal que $\sigma_h(i) = \sigma_g(i)$, entonces $g = h$ y así, $\sigma_h = \sigma_g$. En consecuencia, la acción de $\pi(H)$ es libre y por ende, regular. □

Teorema 4.27. *Sea $C \leq \mathbb{F}_q^n$ un código lineal. Entonces C es un código de grupo torcido en $\mathbb{F}_q^\alpha G$ para un 2-cociclo α adecuado si y solo si existe un subgrupo $H \leq \mathrm{MAut}(C)$ tal que $G \cong \pi(H)$ actúa regularmente en $\{1, \ldots, n\}$ y las únicas matrices diagonales en H son matrices escalares.*

Demostración. El Lema 4.26 muestra que si $C \leq \mathbb{F}_q^{\alpha} G$ entonces existe $H \leq \mathrm{MAut}(C)$ tal que $G \cong \pi(H)$ actúa regularmente en $\{1, \ldots, n\}$ y las únicas matrices diagonales en H son matrices escalares. Resta probar que si existe H con las características descritas, entonces $C \leq \mathbb{F}_q^{\alpha} G$.

Sea $B = \{e_1, \ldots, e_n\}$ la base estándar de $\mathbb{F}_q^n$. Como G actúa regularmente en $\{1, \ldots, n\}$ se tiene que para todo $i \in \{1, \ldots, n\}$ existe un único $x \in G$ tal que $1x = i$. Por lo tanto, $B = \{e_x : x \in G\}$. Además, para cada $y \in G$ se sigue que $iy = (1x)y = 1(xy)$ entonces iy corresponde con xy. Ahora sea

$$e_x \tilde{y} = a_x(\tilde{y}) e_{xy}$$

donde $\tilde{y} \in H$ es tal que $\pi(\tilde{y}) = y$ y $a_x(\tilde{y})$ es la coordenada i correspondiente a x de la matriz diagonal de $\tilde{y}$.

Notemos que si $\tilde{y}' = D_1 P$ y $\tilde{y} = D_2 P$ son elementos de H con la misma matriz de permutación P, entonces $D_1 P P^{-1} D_2^{-1} = D_1 D_2^{-1}$ es una matriz diagonal en H. Como las únicas matrices diagonales en H son matrices escalares se tiene que $D_1 D_2^{-1} = \lambda I$, esto es, $D_1 = \lambda D_2$. Es decir, si $\tilde{y}', \tilde{y} \in H$ son tales que $\pi(\tilde{y}') = \pi(\tilde{y}) = y$, entonces $\tilde{y}' = \lambda \tilde{y}$ para algún $\lambda \in \mathbb{F}_q^*$. En consecuencia, para cada $y \in G$ podemos escoger un único $\tilde{y} \in H$ tal que $a_1(\tilde{y}) = 1$.

Ahora, definamos $\alpha : G \times G \longrightarrow \mathbb{F}_q^*$ como

$$\alpha(x, y) = a_x(\tilde{y}).$$

Veamos que α es un 2-cociclo. Debemos probar que

$$\alpha(xy, z)\alpha(x, y) = \alpha(x, yz)\alpha(y, z) \text{ para todo } x, y, z \in G.$$

Esto es equivalente a demostrar que

$$a_{xy}(\tilde{z}) a_x(\tilde{y}) = a_x(\widetilde{yz}) a_y(\tilde{z}).$$

Como $(e_x \tilde{y})\tilde{z} = e_x(\tilde{y}\tilde{z})$ entonces

$$a_x(\tilde{y}) e_{xy} \tilde{z} = a_x(\tilde{y}\tilde{z}) e_{xyz} \Longrightarrow a_x(\tilde{y}) a_{xy}(\tilde{z}) e_{xyz} = a_x(\tilde{y}\tilde{z}) e_{xyz}.$$

Por lo tanto,

$$a_{xy}(\tilde{z}) a_x(\tilde{y}) = a_x(\tilde{y}\tilde{z}).$$

Además, de esta última ecuación se tiene que si $x = 1$, entonces $a_y(\tilde{z}) = a_1(\tilde{y}\tilde{z})$. Por ello, debemos probar que

$$a_x(\tilde{y}\tilde{z}) = a_x(\widetilde{yz})a_y(\tilde{z}) = a_x(\widetilde{yz})a_1(\tilde{y}\tilde{z}).$$

Y esto es cierto puesto que

$$\frac{1}{a_1(\tilde{y}\tilde{z})}\tilde{y}\tilde{z} = \widetilde{yz}.$$

En consecuencia, α es un 2-cociclo.

Finalmente, consideremos el isomorfismo $\gamma : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^\alpha G$ definido como

$$\gamma(e_x) := \overline{x}.$$

Para $\tilde{y} \in H$ se tiene que

$$\gamma(e_x\tilde{y}) = \gamma(a_x(\tilde{y})e_{xy}) = a_x(\tilde{y})\overline{xy}$$

y

$$\gamma(e_x)\overline{y} = \overline{x} \cdot \overline{y} = \alpha(x, y)\overline{xy} = a_x(\tilde{y})\overline{xy}.$$

Es decir, $\gamma(e_x)\overline{y} = \gamma(e_x\tilde{y})$. Luego, como $\tilde{y} \in H$ con $H \leq \mathrm{MAut}(C)$, entonces $\gamma(C)\overline{y} = \gamma(C\tilde{y}) = \gamma(C)$. En consecuencia, $\gamma(C)$ es un ideal derecho de $\mathbb{F}_q^\alpha G$. □

Ejemplo 4.28. Sea C el $[4, 2, 3]$-código ternario de Hamming $\mathcal{H}_{3,2}$, también llamado tetracódigo. Su matriz generadora en forma estándar está dada por

$$G = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \end{array}\right).$$

Es conocido que $\mathrm{PAut}(C)$ es un grupo de orden 3 generado por la permutación $(1, 3, 4)$ y $\mathrm{MAut}(C)$ es un grupo de orden 48 generado por las matrices monomiales $\mathrm{diag}(1, 1, 1, -1)(1, 2, 3, 4)$ y $\mathrm{diag}(1, 1, 1, -1)(1, 2)$. Teniendo en cuenta el Teorema 3.10, tenemos que C no puede ser un código de grupo puesto que no hay un subgrupo de $\mathrm{PAut}(C)$ que tenga orden $n = 4$. Sin embargo, si definimos

$$H := \langle \mathrm{diag}(1, -1, -1, 1)(1, 2)(3, 4), \mathrm{diag}(1, 1, -1, -1)(1, 3)(2, 4) \rangle,$$

entonces H es un subgrupo de $\mathrm{MAut}(C)$ cuyas únicas matrices diagonales son los múltiplos escalares de la identidad. Además,

$$\pi(H) = \langle (1,2)(3,4), (1,3)(2,4) \rangle \cong V_4,$$

donde V_4 el grupo de Klein, el cual actúa regularmente en $\{1, \ldots, 4\}$. Por lo tanto, del Teorema 4.27 se sigue que C es un código de grupo torcido en $\mathbb{F}_3^\alpha V_4$ para un 2-cociclo α adecuado.

4.3. Código de Golay ternario extendido como código de grupo torcido

A continuación mostraremos que el código de Golay ternario extendido $\mathcal{G}_{12}$ puede ser visto como un ideal del álgebra de grupo torcido $\mathbb{F}_3^\alpha \mathrm{Alt}(4)$ para un 2-cociclo de $\mathrm{Alt}(4)$ adecuado.

Definición 4.29. El *grupo lineal especial* $\mathrm{SL}(2,3)$ es el grupo de matrices 2×2 con entradas en un campo de 3 elementos y determinante igual a 1. También podemos definir este grupo con los siguientes generadores

$$\mathrm{SL}(2,3) = \langle a, b, c : a^4 = c^3 = 1, b^2 = a^2, bab^{-1} = a^{-1}, c^{-1}ac = b, c^{-1}bc = ab \rangle.$$

Teorema 4.30. *Sea* $\mathrm{Alt}(4)$ *el grupo de permutaciones pares de 4 elementos de orden* 12. *Entonces* $\mathrm{SL}(2,3)/\{\pm E\} \cong \mathrm{Alt}(4)$*, donde* E *denota la matriz identidad de tamaño* 2×2.

Demostración. Sean $[a], [b], [c]$ las clases de los generadores a, b, c de $\mathrm{SL}(2,3)$. La función $\varphi : \mathrm{SL}(2,3)/\{\pm E\} \longrightarrow \mathrm{Alt}(4)$ definida como $[a] \mapsto (12)(34)$, $[b] \mapsto (13)(24)$ y $[c] \mapsto (234)$ es un isomorfismo de grupos. □

Teorema 4.31. *El código de Golay ternario extendido* C *es un código de grupo torcido para el grupo* $\mathrm{Alt}(4)$*. Más aún,* C *es generado por un idempotente.*

Demostración. Partimos de las siguientes matrices

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; Y = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \; A = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \text{y} \; Z = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Notemos que $Z = XY$, $X^2 = Y^2 = -E$, $X^4 = A^3 = 1$, $A^{-1}XA = Y$, $A^{-1}YA = Z$ y $A^{-1}ZA = X$. Por lo tanto, $\mathrm{SL}(2,3) = \langle X, Y, A\rangle$.

Sea $\widetilde{\ }$ el epimorfismo natural de grupos $\mathrm{SL}(2,3) \longrightarrow \mathrm{SL}(2,3)/\{\pm E\}$. Si definimos $x = \widetilde{X}, y = \widetilde{Y}$ y $a = \widetilde{A}$, entonces $G = \langle x, y, a\rangle \cong \mathrm{Alt}(4)$. Luego, la multiplicación en el álgebra de grupo torcido $\mathbb{F}_3^\alpha G$ está dada por el Cuadro 4.1.

	$\overline{1}$	$\overline{x}$	$\overline{y}$	$\overline{z}$	$\overline{a}$	$\overline{xa}$	$\overline{ya}$	$\overline{za}$	$\overline{a^2}$	$\overline{xa^2}$	$\overline{ya^2}$	$\overline{za^2}$
$\overline{1}$	$\overline{1}$	$\overline{x}$	$\overline{y}$	$\overline{z}$	$\overline{a}$	$\overline{xa}$	$\overline{y}$	$\overline{za}$	$\overline{a^2}$	$\overline{xa^2}$	$\overline{ya^2}$	$\overline{za^2}$
$\overline{x}$	$\overline{x}$	$-\overline{1}$	$\overline{z}$	$-\overline{y}$	$\overline{xa}$	$-\overline{a}$	$\overline{za}$	$-\overline{ya}$	$\overline{xa^2}$	$-\overline{a^2}$	$\overline{za^2}$	$-\overline{ya^2}$
$\overline{y}$	$\overline{y}$	$-\overline{z}$	$-\overline{1}$	$\overline{x}$	$\overline{ya}$	$-\overline{za}$	$-\overline{a}$	$\overline{xa}$	$\overline{ya^2}$	$-\overline{za^2}$	$-\overline{a^2}$	$\overline{xa^2}$
$\overline{z}$	$\overline{z}$	$\overline{y}$	$-\overline{x}$	$-\overline{1}$	$\overline{za}$	$\overline{ya}$	$-\overline{xa}$	$-\overline{a}$	$\overline{za^2}$	$\overline{ya^2}$	$-\overline{xa^2}$	$-\overline{a^2}$
$\overline{a}$	$\overline{a}$	$\overline{za}$	$\overline{xa}$	$\overline{ya}$	$\overline{a^2}$	$\overline{za^2}$	$\overline{xa^2}$	$\overline{ya^2}$	$\overline{1}$	$\overline{z}$	$\overline{x}$	$\overline{y}$
$\overline{xa}$	$\overline{xa}$	$-\overline{ya}$	$-\overline{a}$	$\overline{za}$	$\overline{xa^2}$	$-\overline{ya^2}$	$-\overline{a^2}$	$\overline{za^2}$	$\overline{x}$	$-\overline{y}$	$-\overline{1}$	$\overline{z}$
$\overline{ya}$	$\overline{ya}$	$\overline{xa}$	$-\overline{za}$	$-\overline{a}$	$\overline{ya^2}$	$\overline{xa^2}$	$-\overline{za^2}$	$-\overline{a^2}$	$\overline{y}$	$\overline{x}$	$-\overline{z}$	$-\overline{1}$
$\overline{za}$	$\overline{za}$	$-\overline{a}$	$\overline{ya}$	$-\overline{xa}$	$\overline{za^2}$	$-\overline{a^2}$	$\overline{ya^2}$	$-\overline{xa^2}$	$\overline{z}$	$-\overline{1}$	$\overline{y}$	$-\overline{x}$
$\overline{a^2}$	$\overline{a^2}$	$\overline{ya^2}$	$\overline{za^2}$	$\overline{xa^2}$	$\overline{1}$	$\overline{y}$	$\overline{z}$	$\overline{x}$	$\overline{a}$	$\overline{ya}$	$\overline{za}$	$\overline{xa}$
$\overline{xa^2}$	$\overline{xa^2}$	$\overline{za^2}$	$-\overline{ya^2}$	$-\overline{a^2}$	$\overline{x}$	$\overline{z}$	$-\overline{y}$	$-\overline{1}$	$\overline{xa}$	$\overline{za}$	$-\overline{ya}$	$-\overline{a}$
$\overline{ya^2}$	$\overline{ya^2}$	$-\overline{a^2}$	$\overline{xa^2}$	$-\overline{za^2}$	$\overline{y}$	$-\overline{1}$	$\overline{x}$	$-\overline{z}$	$\overline{ya}$	$-\overline{a}$	$\overline{xa}$	$-\overline{za}$
$\overline{za^2}$	$\overline{za^2}$	$-\overline{xa^2}$	$-\overline{a^2}$	$\overline{ya^2}$	$\overline{z}$	$-\overline{x}$	$-\overline{1}$	$\overline{y}$	$\overline{za}$	$-\overline{xa}$	$-\overline{a}$	$\overline{ya}$

Cuadro 4.1: Multiplicación en $\mathbb{F}_3^\alpha G$

Note que, por ejemplo, $\overline{x}\ \overline{za} = -\overline{ya}$ puesto que $X(ZA) = -YA$. Por eso $\alpha(x, za) = -1$. De esta manera, definimos el 2-cociclo α de G que se muestra en el Cuadro 4.2.

	1	x	y	z	a	xa	ya	za	a^2	xa^2	ya^2	za^2
1	1	1	1	1	1	1	1	1	1	1	1	1
x	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
y	1	−1	−1	1	1	−1	−1	1	1	−1	−1	1
z	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1
a	1	1	1	1	1	1	1	1	1	1	1	1
xa	1	−1	−1	1	1	−1	−1	1	1	−1	−1	1
ya	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1
za	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
a^2	1	1	1	1	1	1	1	1	1	1	1	1
xa^2	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1
ya^2	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
za^2	1	−1	−1	1	1	−1	−1	1	1	−1	−1	1

Cuadro 4.2: 2-cociclo α de G

Con GAP también encontramos el siguiente idempotente.

$$e = -\overline{1} + \overline{z} - \overline{xa} + \overline{za} + \overline{xa^2} - \overline{ya^2}.$$

Sea ahora $C = e\mathbb{F}_3^{\alpha}G$. Es sencillo comprobar que $e^2 = e$. Más aún,

$$\widehat{e} = -\overline{1} - \overline{z} + \overline{ya^2} - \overline{xa^2} - \overline{za} + \overline{xa} \quad \text{y} \quad e = \overline{1} - \widehat{e}.$$

Luego, por el Teorema 4.22, se concluye que $C = C^{\perp}$. Como C es un código autodual de longitud 12 entonces $\dim_{\mathbb{F}_3} C = 12/2 = 6$. Además, con GAP también verificamos que $\mathrm{d}(C) = 6$ (ver Apéndice A). Por lo tanto, C es un $[12, 6, 6]$-código autodual que, por el Teorema 2.73, es el código de Golay ternario extendido $\mathcal{G}_{12}$. □

4.4. Códigos de Hamming como códigos de grupo torcidos

En el ejemplo 4.28 comprobamos que el código de Hamming $\mathcal{H}_{3,2}$ es un código de grupo torcido. En esta sección demostraremos que cualquier código de Hamming $\mathcal{H}_{q,r}$ es un código de grupo torcido. Para esto, recordemos que $\mathrm{GL}(n, \mathbb{F}_q)$ es el grupo de transformaciones lineales invertibles de un espacio vectorial de dimensión n sobre $\mathbb{F}_q$. Además, $Z(\mathrm{GL}(n, \mathbb{F}_q))$ es el centro de $\mathrm{GL}(n, \mathbb{F}_q)$, esto es, es el grupo formado por los múltiplos escalares de la función identidad y definimos $\mathrm{PGL}(n, q)$ como el grupo cociente $\mathrm{GL}(n, \mathbb{F}_q)/Z(\mathrm{GL}(n, \mathbb{F}_q))$.

Teorema 4.32. *Para todo q y r, el código de Hamming $\mathcal{H}_{q,r}$ es un código de grupo torcido.*

Demostración. Sea $V := \mathbb{F}_{q^r}$ el espacio vectorial de dimensión r sobre $\mathbb{F}_q$ y sea $\alpha \in \mathbb{F}_{q^r}^*$. Consideremos ahora la función $s_\alpha : V \longrightarrow V$ definida como $s_\alpha(x) := \alpha x$ para todo $x \in V$. Notemos que $s_\alpha \in \mathrm{GL}(r, \mathbb{F}_q)$ para cada $\alpha \in \mathbb{F}_{q^r}^*$. Luego, si γ es un generador del grupo multiplicativo $\mathbb{F}_{q^r}^*$, entonces

$$S := \langle s_\gamma \rangle = \{s_\alpha \in \mathrm{GL}(r, \mathbb{F}_q) : \alpha \in \mathbb{F}_{q^r}^*\}.$$

Más aún, S es un subgrupo cíclico de $\mathrm{GL}(r, \mathbb{F}_q)$ isomorfo a $\mathbb{F}_{q^r}^*$ que actúa regularmente en $V \backslash \{0\}$ (El grupo S es llamado grupo de Singer y el generador s_γ es llamado ciclo de Singer). Definamos ahora

$$\overline{S} := S/Z(\mathrm{GL}(r, \mathbb{F}_q)) = \langle s_\gamma Z(\mathrm{GL}(r, \mathbb{F}_q)) \rangle.$$

Entonces $\overline{S}$ es un subgrupo cíclico de $\mathrm{PGL}(r,q)$ de orden $n = \frac{q^r-1}{q-1}$. Además, dado que $\mathbb{P}^{r-1}(q)$ es el conjunto de subespacios unidimensionales de $\mathbb{F}_{q^r}$, se sigue que $\overline{S}$ actúa sobre el espacio proyectivo $\mathbb{P}^{r-1}(q)$ bajo la acción $[s_\gamma^i]\langle x\rangle = \langle s_\gamma^i(x)\rangle$ para todo $[s_\gamma^i] \in \overline{S}$ donde $i = 1, \ldots, n$. Más aún, esta acción es regular debido a que

$$\begin{aligned}
[s_\gamma^i]\langle x\rangle = \langle x\rangle &\iff \langle \gamma^i x\rangle = \langle x\rangle \\
&\iff \gamma^i x = \lambda x \text{ para algún } \lambda \in \mathbb{F}_q^* \\
&\iff \gamma^i = \lambda \text{ para algún } \lambda \in \mathbb{F}_q^* \\
&\iff s_\gamma^i \in Z(\mathrm{GL}(r,\mathbb{F}_q)) \\
&\iff [s_\gamma^i] = Z(\mathrm{GL}(r,\mathbb{F}_q)).
\end{aligned}$$

Sea ahora H una matriz de control para $C = \mathcal{H}_{q,r}$ y definamos el isomorfismo $f : \mathrm{MAut}(C^\perp) \longrightarrow \mathrm{GL}(r,\mathbb{F}_q)$ como $M \longmapsto f(M)$, donde $f(M)H = HM$. Si $D \in G := f^{-1}(S)$ es una matriz diagonal, entonces $s_\gamma^i H = HD$ de donde se sigue que D es una matriz escalar. Por otro lado, $\pi(G) \cong \overline{S}$ actúa regularmente en $\{1, \ldots, n\}$. Entonces, por el Teorema 4.27, $C^\perp \leq \mathbb{F}_q^\alpha\langle\overline{S}\rangle$ para algún 2-cociclo α. En consecuencia, $C \leq \mathbb{F}_q^{\alpha^{-1}}\langle\overline{S}\rangle$ para algún 2-cociclo α. □

Apéndice A

GAP

A continuación, presentamos el código GAP utilizado para demostrar el Teorema 4.31. Con este código verificamos el cociclo dado, encontramos el idempotente generador del código y demostramos que el ideal generado por este idempotente tiene mínima distancia 6.

```
#Código de Golay Extendido como ideal de código de grupo
#torcido con G=Alt(4) generado por un idempotente e.

#Instalar paquete para error-corrección de códigos
LoadPackage( "guava" );

#Definir G ( grupo alternante 4)
A:= Elements(AlternatingGroup(4));
ADos:= Filtered(A, x->Order(x)= 2);
ATres:= Filtered(A, x->Order(x)= 3);

# Definir e, x, y, z, a
e:= Identity(A);
x:= ADos[1];
y:= ADos[2];
z:= x*y;
a:= ATres[1];

# Ordenar elementos de G como en tabla 2
G:=[];
```

```
G[1]:=e; G[2]:=x; G[3]:=y; G[4]:=z;
G[5]:=a; G[6]:=x*a; G[7]:=y*a; G[8]:=z*a;
G[9]:=a*a; G[10]:=x*(a*a); G[11]:=y*(a*a); G[12]:=z*(a*a);

#Definir F3 u = 1, m = -1
F:=Set(GF(3));
u:=F[2]; m:=F[3];

#Tabla cociclo alfa
H:=[[]];
H[1]:=[u,u,u,u,u,u,u,u,u,u,u,u];
H[2]:=[u,m,u,m,u,m,u,m,u,m,u,m];
H[3]:=[u,m,m,u,u,m,m,u,u,m,m,u];
H[4]:=[u,u,m,m,u,u,m,m,u,u,m,m];
H[5]:=[u,u,u,u,u,u,u,u,u,u,u,u];
H[6]:=[u,m,m,u,u,m,m,u,u,m,m,u];
H[7]:=[u,u,m,m,u,u,m,m,u,u,m,m];
H[8]:=[u,m,u,m,u,m,u,m,u,m,u,m];
H[9]:=[u,u,u,u,u,u,u,u,u,u,u,u];
H[10]:=[u,u,m,m,u,u,m,m,u,u,m,m];
H[11]:=[u,m,u,m,u,m,u,m,u,m,u,m];
H[12]:=[u,m,m,u,u,m,m,u,u,m,m,u];
Display(H);

#Calcular alpha(a,b)
Alp := function (a,b)
    local i, j;
    for i in [1..12] do
    for j in [1..12] do
    if a = G[i] and b = G[j] then
    return H[i][j];
    fi;
    od;
    od;
end;

#Calcular alpha(ab,c)alpha(a,b)
t1:= function (a,b,c)
```

```
    return Alp(a*b,c)*Alp(a,b);
end;

#Calcular alpha(a,bc)alpha(b,c)
t2:= function (a,b,c)
    return Alp(a,b*c)*Alp(b,c);
end;

#Alpha es un cociclo (True)
cc:=F[2];
for i in [1..12] do
for j in [1..12] do
for k in [1..12] do
if t1(G[i],G[j],G[k])<>t2(G[i],G[j],G[k]) then
cc:=F[1];
fi;
od;
od;
od;
cc=F[2];

#Definir elementos del algebra F_3^(alpha)G en T
K:=Cartesian(F,F,F,F,F,F,F,F,F,F,F,F);;
T:=[[]];

for i in [1..Size(K)] do
T[i]:=[[K[i,1],G[1]],[K[i,2],G[2]],[K[i,3],G[3]],
[K[i,4],G[4]],[K[i,5],G[5]],[K[i,6],G[6]],
[K[i,7],G[7]],[K[i,8],G[8]],[K[i,9],G[9]],
[K[i,10],G[10]],[K[i,11],G[11]],[K[i,12],G[12]]];;
od;

#Multiplicación de una constante a por un elemto g en G
#por b=sum a_gg (L no tiene el mismo orden de G en T)
Mult1:=function (a, g, b)
    local L, i;
    L :=[[]];
    for i in [1..12] do
```

```
    L[i]:= [Alp(g,G[i])*a*(b[i][1]),g*G[i]];
    od;
    return L;
end;

#Multiplicación a = sum a_gg y b = sum b_hh (termino a termino)
Mult2:=function (a,b)
    local L, i;
    L:=[[]];
    for i in [1..12] do
    L[i]:=Mult1(a[i][1],a[i][2],b);
    od;
    return L;
end;

#Organiza los coeff de c= sum a_gg en igual orden que G en T
Org:= function(c)
    local V2,i,j;
    V2:=[[]];
    for i in [1..12] do
    for j in [1..12] do
    if c[i][2]=G[j] then
    V2[j]:=c[i][1];
    fi;
    od;
    od;
    return V2;
end;

#Escribir sum a_gg a partir de los coeficientes a_g
Esc:= function(S)
    local c;
    c:=[[]];
    for i in [1..12] do
    c[i]:=[S[i],G[i]];
    od;
    return c;
end;
```

```
#Multiplicación (Resultado final en igual orden que G en T)
Multf:=function(a,b)
    local V, L, i, j, k, c, S;
    V:=[[]];
    L:=Mult2(a,b);
    # organiza coeficientes en el orden de G
    for k in [1..12] do
    V[k]:=Org(L[k]);
    od;
    #sumar los coeficientes
    S:=[[]];
    for i in [1..12] do
    S[i]:=0;
    for j in [1..12] do
    S[i]:=S[i]+V[j][i];
    od;
    od;
    # Escribir el resultado
    c:=Esc(S);
    return c;
end;

#suma de dos elementos a y b en F_3^alphaG
suma:= function(a,b)
    local c;
    c:=[[]];
    for i in [1..12] do
    c[i]:=[a[i][1]+b[i][1], G[i]];
    od;
    return c;
end;

#Calcular peso
wt:=function(a)
    local w;
    w:=0;
    for i in [1..12] do
```

```
    if a[i][1] <> F[1] then
    w:=w+1;
    fi;
    od;
    return w;
end;

#encontrar adjunto
ad:=function (a)
    local c;
    c:=[[]];
    for i in [1..12] do
    c[i]:=[a[i][1]*Alp(a[i][2],Inverse(a[i][2])),
            Inverse(a[i][2])];
    od;
    return Esc(Org(c));
end;

#definir uno y cero del álgebra
cero:=T[1];
uno:=[[F[2], G[1]], [F[1], G[2]], [F[1], G[3]], [F[1],G[4]],
[F[1], G[5]], [F[1], G[6]], [F[1], G[7] ], [F[1], G[8]],
[F[1], G[9]], [F[1], G[10]],[F[1], G[11]], [F[1], G[12]]];

#encontrar idempotente (e = -1 + z - x*a + z*a + x*a^2 - y*a^2)
for e in T do
    if Multf(e,e)=e and e <> uno and e<>cero
    and wt(e)=6 and suma(e,ad(e))=uno then
    return e;
    fi;
od;
e;

#ideal generado por e, denotado SA
eFG:=[];
for i in [1..Size(T)] do
    eFG[i]:=Multf(e, T[i]);
od;
```

```
SA:=Set(eFG);;

#Vectores con peso i en SA
WD:=function (i)
    local L;
    L:=Filtered(SA, x->wt(x)=i);
    return Size(L);
end;

#Distribucion de pesos de SA (minima distancia = 6)
W:=[];
for i in [1..13] do
    W[i]:=WD(i-1);
od;
W;
```

Bibliografía

[1] J. J. Bernal, Á. del Río, and J. J. Simón. An intrinsical description of group codes. *Designs, Codes and Cryptography*, 51(3):289–300, 2009.

[2] F. Bernhardt, P. Landrock, and O. Manz. The extended golay codes considered as ideals. *Journal of Combinatorial Theory, Series A*, 55(2):235–246, 1990.

[3] J. de la Cruz. Ánillos y sus módulos, 2018.

[4] J. de la Cruz, E. Martínez-Moro, and R. Villanueva-Polanco. Public key protocols over skew dihedral group rings. *Mathematics*, 2022.

[5] J. de la Cruz and R. Villanueva-Polanco. Public key cryptography based on twisted dihedral group algebras. *Advances in Mathematics of Communications*, 2022.

[6] J. de la Cruz and W. Willems. Twisted group codes. *IEEE Transactions on Information Theory*, 67(8):5178–5184, 2021.

[7] W. C. Huffman and V. Pless. *Fundamentals of Error Correcting Codes*. Cambridge University Press, 2003.

[8] S. Lang. *Introducción al Álgebra Lineal*. Addison-Wesley Iberoamericana, 1990.

[9] M. W. Liebeck, C. E. Praeger, and J. Saxl. *Regular subgroups of primitive permutation groups*. American Mathematical Soc., 2010.

[10] C. L. Mallows and N. J. Sloane. An upper bound for self-dual codes. *Information and Control*, 22(2):188–200, 1973.

[11] I. McLoughlin and T. Hurley. A group ring construction of the extended binary golay code. *IEEE transactions on information theory*, 54(9):4381–4383, 2008.

[12] V. Pless. On the uniqueness of the golay codes. *Journal of Combinatorial theory*, 5(3):215–228, 1968.

[13] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Transactions on Information Theory*, 44(1):134–139, 1998.

[14] S. Roman. *Coding and information theory*, volume 134. Springer Science & Business Media, 1992.

[15] W. Willems. *Codierungstheorie*. de Gruyter, 1999.

[16] W. Willems. A note on self-dual group codes. *IEEE Transactions on Information Theory*, 48(12):3107–3109, 2002.