TEORÍA DE CÓDIGOS & ÁLGEBRAS DE GRUPOS

Gerson Leonel Barajas Ávila

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Matemáticas
Bucaramanga
2016

TEORÍA DE CÓDIGOS & ÁLGEBRAS DE GRUPOS

Autor

Gerson Leonel Barajas Ávila

Trabajo de grado como requisito

parcial para optar al título de

Matemático

Director

Alexander Holguín Villa

Doctor en Matemáticas

Codirector

Carlos Arturo Rodríguez Palma

Magister en Matemáticas

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

2016

NOTA DE PROYECTO DE GRADO

NOMBRE DEL ESTUDIANTE: GERSON LEONEL BARAJAS ÁVILA			CODIGO: 2090899
TITULO DEL PROYECTO : "TEORÍA DE CÓDIGOS Y ÁLGEBRAS DE GRUPO"			
REGISTRO N°	FACULTAD : *Ciencias*	CARRERA: *Matemáticas*	
CALIFICACIÓN: TRES, CINCO (3.5)			CREDITOS: *10*
Director: ALEXANDER HOLGUIN V. Codirector: CARLOS ARTURO RODRIGUEZ	FIRMAS: A HOLGUIN VILLA Carlos A. Rodriguez		

CALIFICADORES

F Arnoldo Teherán H ARNOLDO TEHERÁN HERRERA	F WILSON OLAYA LEÓN	FECHA A 16 M 2 D 29

ENTREGA DE TRABAJOS DE GRADO, TRABAJOS DE INVESTIGACION O TESIS Y AUTORIZACIÓN DE SU USO A FAVOR DE LA UIS

Yo, **GERSON LEONEL BARAJAS AVILA**, mayor de edad, vecino de Bucaramanga, identificado con la Cédula de Ciudadanía No. 1098701704 de Bucaramanga, actuando en nombre propio, en mi calidad de autor del trabajo de grado, del trabajo de investigación, o de la tesis denominada(o):

TEORÍA DE CÓDIGOS & ÁLGEBRAS DE GRUPOS,

hago entrega del ejemplar respectivo y de sus anexos de ser el caso, en formato digital o electrónico (CD o DVD) y autorizo a LA UNIVERSIDAD INDUSTRIAL DE SANTANDER, para que en los términos establecidos en la Ley 23 de 1982, Ley 44 de 1993, decisión Andina 351 de 1993, Decreto 460 de 1995 y demás normas generales sobre la materia, utilice y use en todas sus formas, los derechos patrimoniales de reproducción, comunicación pública, transformación y distribución (alquiler, préstamo público e importación) que me corresponden como creador de la obra objeto del presente documento. PARÁGRAFO: La presente autorización se hace extensiva no sólo a las facultades y derechos de uso sobre la obra en formato o soporte material, sino también para formato virtual, electrónico, digital, óptico, uso en red, Internet, extranet, intranet, etc., y en general para cualquier formato conocido o por conocer.

EL AUTOR – ESTUDIANTE, manifiesta que la obra objeto de la presente autorización es original y la realizó sin violar o usurpar derechos de autor de terceros, por lo tanto la obra es de su exclusiva autoría y detenta la titularidad sobre la misma. PARÁGRAFO: En caso de presentarse cualquier reclamación o acción por parte de un tercero en cuanto a los derechos de autor sobre la obra en cuestión, EL AUTOR / ESTUDIANTE, asumirá toda la responsabilidad, y saldrá en defensa de los derechos aquí autorizados; para todos los efectos la Universidad actúa como un tercero de buena fe.

Para constancia se firma el presente documento en dos (02) ejemplares del mismo valor y tenor, en Bucaramanga, a los 2 días del mes de Marzo de Dos Mil Dieciséis 2016.

EL AUTOR / ESTUDIANTE:

(Firma) .....

Nombre: Gerson Leonel Barajas Avila

Agradecimientos

En primer lugar le agradezco a Dios, por acompañarme en cada uno de los caminos de vida, guiándome y llenándome de sabiduría para poder disfrutar de este gran logro, como lo es obtener mi titulo profesional como Matemático, mediante la culminación de mi proyecto de grado.

A mis padres, Carlos y Margarita por ser unos padres ejemplares, pues con sacrificios construyeron un hermoso hogar y lograron darme las cosas necesarias para alcanzar mis sueños, aunque las condiciones no fuera las mejores por algunos momentos, por mostrarme que el único camino para triunfar en nuestro mundo es caminando bajo la sombra de Dios, estudiando y siendo una persona agradable ante los ojos de los demás, por todo esto y mucho más gracias papás, los amo.

A mi director y codirector de tesis, pues valoro el hecho de que dedicaran parte de su tiempo, para con su sabiduría ayudarme a comprender los resultados que se exhibirán en esta tesis, me siento orgulloso de contar con su apoyo, y en especial a mis amigos y hermanos quienes en tiempos difíciles siempre me han animado para seguir adelante. Gracias.

Índice general

Resumen

TITULO: TEORÍA DE CÓDIGOS & ÁLGEBRAS DE GRUPOS. [1]

AUTOR: Gerson Leonel Barajas Avila. [2]

PALABRAS CLAVE: Álgebras de grupos, Cuerpo finito, Código, Ideal, Idempotente.

DESCRIPCIÓN

Estudiaremos la construcción de códigos sobre álgebras de grupo $\mathbb{F}G$ de un grupo G sobre un cuerpo $\mathbb{F}$. En particular, consideraremos $\mathbb{F}$ un cuerpo finito de q elementos y G un grupo finito tal que $mcd(q, |G|) = 1$, para que $\mathbb{F}G$ sea semisimple, pues siendo semisimple todo código en $\mathbb{F}G$ es un ideal y todo ideal de $\mathbb{F}G$ es de la forma $\mathbb{F}Ge$, donde e es un elementos idempotente, es decir, todo ideal es generado por un elemento idempotente. Por lo tanto, nos concentraremos en la construcción de dichos elementos. Además, si G es un grupo cíclico los códigos serán cíclicos y si Ges abeliano los códigos serán abelianos.

Por medio de los resultados obtenidos por Raul Ferraz y Cesar Polcino en el artículo Ïdempotents in group algebras and minimal abelian codes", calcularemos los idempotentes generados por los subgrupos de G, para después ver que son el conjunto de idempotentes primitivos y así los generadores de los códigos cíclicos y abelianos minimales.

Este punto de vista (álgebras de grupo) extendió los resultados de Arora y Pruthi, los cuales fueron obtenidos desde la óptica de anillos de polinomios. Además, permitió calcular la dimensión y el peso de los códigos de manera más fácil.

[1] Tesis.

[2] FACULTAD DE CIENCIAS, MATEMÁTICAS.
DIRECTOR Dr. Alexander Holguín Villa.
CODIRECTOR Mg. Carlos Arturo Rodriguez Palma.

Abstract

TITLE: CODING THEORY & GROUP ALGEBRAS. [3]

AUTHOR: Gerson Leonel Barajas Avila [4]

KEY WORDS: Group algebras, Finite field, Code, Ideal, Idempotent.

DESCRIPTION

We will study construction codes on group algebras $\mathbb{F}G$ of a group G on a field $\mathbb{F}$. In particular, we will consider a finite field $\mathbb{F}$ with q elements and G a finite group such that $gcd(q, |G|) = 1$, so $\mathbb{F}G$ is semisimple, as being semisimple all code $\mathbb{F}G$ is an ideal code and every ideal code of $\mathbb{F}G$ is from the form $\mathbb{F}Ge$, where e is an idempotent element, in other words, every ideal code is generated by an idempotent element. Therefore, we will concentrate on the construction of such elements. Also, if G is a cyclic group, the codes are cyclical and if G is abelian, then the codes are abelian.

By means of the results obtained by Raul Ferraz and Cesar Polcino in the article Ïdempotents in Group Algebras and Minimal Abelian Codes", we will calculate the idempotent generated by the subgroups of G, then we will see which are the set of primitive idempotents and thus the generators of cyclic and abelian minimal codes.

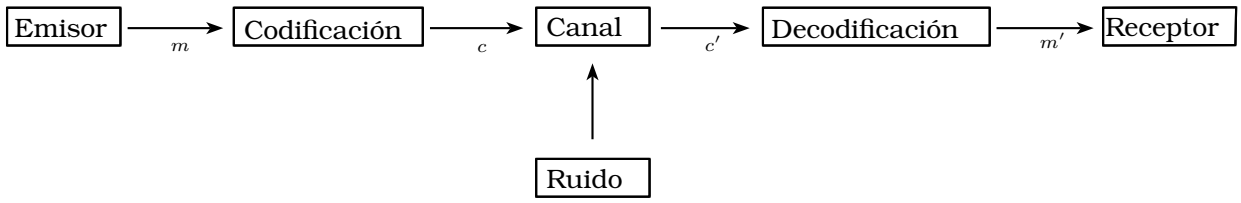
This point of view (group algebras) extended the results of Arora and Pruthi, which were obtained from the viewpoint of polynomial rings. Furthermore, it allowed calculating size and the weight of the codes of easier way.

[3] Thesis.

[4] FACULTY OF SCIENCES, MATHEMATICS.
DIRECTOR Dr. Alexander Holguín Villa.
CODIRECTOR Mg. Carlos Arturo Rodriguez Palma.

Introducción

Supongamos que queremos enviar un mensaje. Este es enviado por un *canal de comunicación*, cuyas características dependen de la naturaleza del mensaje a ser enviado (sonido, imagen, datos). En general hay que hacer una *traducción* entre el mensaje original (o *palabra fuente*) m y el tipo de mensaje c que el canal está capacitado para enviar (*palabras código*). Este proceso se llama *codificación*. Una vez codificado el mensaje lo enviamos a través del canal, y nuestro intermediario (*el receptor*) recibe un mensaje codificado (*palabra recibida*) posiblemente erróneo, ya que en todo este proceso de comunicación hay ruido e interferencias. El mensaje recibido c' es traducido nuevamente a términos originales x', es decir, es *decodificado*. Todo este proceso se resume en el siguiente diagrama:



(1)

Debido a que todos los canales son susceptibles al ruido, es necesario dar respuesta a las siguientes preguntas cada vez que se envíe un mensaje.

(i) ¿Qué tan seguro es el código?

(ii) ¿Qué tan confiable es el código?

Cuando preguntamos ¿qué tan seguro es el código?, estamos pensando en que el código sea inviolable, en el sentido de que una persona ajena a la comunicación no logre decodificar el mensaje, obteniendo así la información que este contiene.

Ahora, cuando hablamos de confiabilidad, hacemos referencia a que el mensaje enviado sea el mismo recibido, puesto que en el proceso de codificación y/o decodificación puede

ocurrir algún error.

Las preguntas aunque parecen similares, cada una pertenece a diferentes campos de investigación, de hecho, la pregunta (i) hace parte de la *criptografía*, mientras que la pregunta (ii) se resuelve desde la teoría de códigos, en particular la *teoría de códigos detectores y correctores de errores*. Es sobre esta última teoría que basaremos el estudio en esta monografía.

El estudio de la teoría de códigos, ha sido abordado desde diferentes puntos de vista, al principio fue usada la teoría de congruencias, la teoría de polinomios y recientemente desde la teoría de álgebras de grupo en el cual se trabaja con un enfoque similar a la teoría de polinomios pero cambiando la estructura algebraica, esto con el fin de que los procesos de codificación y decodificación sean más eficaces.

El objetivo de esta monografía es estudiar la construcción de códigos sobre álgebras de grupo, para ello veremos en principio que todo código es un ideal en álgebra de grupo, lo cuales a su vez son generados por elementos idempotentes. Por tal razón, para construir códigos estudiaremos la construcción de elementos idempotentes en el álgebra de grupo.

Capítulo 1

Preliminares

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

Presentaremos las nociones utilizadas a lo largo del trabajo, la mayoría de ellas serán asumidas sin prueba, más serán indicadas las respectivas referencias bibliográficas. Muchas de las pruebas de las mismas, pueden ser consultadas en [10], [7], referencias que son clásicas en este contexto.

1.1. Teoría de grupos

Definición 1.1. *Un **grupo** es un conjunto no vacío G junto con una operación binaria denotada por "$\cdot$", tal que para todo $a, b, c \in G$, se cumplen las siguientes propiedades.*

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(ii) Existe un elemento identidad, denotado por $1 = 1 \in G$*, tal que* $a \cdot 1 = 1 \cdot a = a$.

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

✓ Dados $a, b \in G$, $a \cdot b$ se denotará por ab.

✓ Si para cada $a, b \in G$ se cumple que $ab = ba$, se dice que el grupo es **abeliano**.

✓ Si $a \in G$, el orden de a, denotado por $o(a)$, es el menor entero positivo m tal que $a^m = 1$.

Además, si G es un conjunto finito, el número de elementos de G es su orden y se denota por $|G|$.

✓ El elemento identidad $1 \in G$ es único y cada $a \in G$ tiene un único inverso a^{-1}.

✓ Para $a, b \in G$, $(a^{-1})^{-1} = a$ y $(ab)^{-1} = b^{-1}a^{-1}$.

✓ Sea p un número primo, se dice que $g \in G$ es un p**-elemento** si su orden es una potencia de p. Además, si para todo g en G, g es un p-elemento, diremos que G es un p**-grupo**.

✓ Si la operación en el grupo es la suma "$+$", diremos que el grupo es "aditivo" y en este caso representamos ab, 1 y a^{-1} por $a+b$, 0 y $-a$, respectivamente. En adelante, consideremos todos los grupos como grupos multiplicativos, a menos que se indique lo contrario.

Definición 1.2. *Un subconjunto no vacío H de un grupo G se llama subgrupo de G y se denota por $H \leq G$, si él mismo es un grupo bajo la operación definida en G restringida a los elementos de H.*

El siguiente teorema debido a J. Lagrange provee una lista de candidatos a ser subgrupos de un grupo finito dado G, basada en los divisores del orden de G.

Teorema 1.1. *(Teorema de Lagrange)*
Si G es un grupo finito y $H \leq G$, entonces el orden de H divide al orden de G.

Demostración. [10, Pág 58]. □

Definición 1.3. *Sea G un grupo,*

*(i) G es llamado **cíclico** si existe un elemento $a \in G$ tal que $G = \langle a \rangle = \{a^n : n \in Z\}$, tal elemento a es llamado un **generador** de G.*

*(ii) Un subgrupo N de un grupo G es llamado **subgrupo normal** de G y denotado por $N \lhd G$, si para todo $g \in G$ se cumple*

$$g^{-1}Ng = \{g^{-1}ng : n \in N\} = N.$$

Ejemplo 1.1.

(a) Sea G un grupo de orden p, donde p es primo, entonces dado $a \in G$, $a \neq 1_G$, por el Teorema 1.1 $o(a) \mid |G| = p$, por lo tanto $o(a) = |\langle a \rangle| = p$ y así G es cíclico.

(b) Sea $S \subseteq G$. El centro de G y el normalizador de S en G se definen respectivamente por:

$$Z(G) = \{g \in G : gh = hg, \forall h \in G\} \quad y \quad N_G(S) = \{g \in G : g^{-1}Sg = S\}.$$

Se puede probar que $Z(G) \lhd G$ y $N_G(S) \leq G$, [7, Teorema 9.1].

Definición 1.4. *Sean G y H dos grupos; una aplicación $\varphi : G \to H$ es llamada un **homomorfismo** si para todos $g_1, g_2 \in G$, $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$.*

Si $\varphi : G \to H$ es un homomorfismo de grupos, entonces:

✓ $\varphi(1_G) = 1_H$ y $\varphi(g^{-1}) = (\varphi(g))^{-1}$.

✓ φ es llamado **Monomorfismo** si es inyectivo, **Epimorfismo** si es sobreyectivo e **Isomorfismo** si es inyectivo y sobreyectivo.

✓ Si para todo $g \in G$, $\varphi(g) = 1_H$, φ se llama el *homomorfismo trivial*.

Definición 1.5. *Sea $\varphi : G \to H$ un homomorfismo de grupos, se definen el **Kernel** y la **Imagen** de φ respectivamente como:*

$$Ker(\varphi) = \{x \in G : \varphi(x) = 1_H\} \quad y \quad Im(\varphi) = \{y \in H : (\exists x \in G)(\varphi(x) = y)\}.$$

Observación 1.1. *Es bien conocido que $Ker(\varphi) \lhd G$, mientras que $Im(\varphi) \leq H$, [10, Teorema 2.5.5].*

Sea N un subgrupo de un grupo G. Definimos una relación de equivalencia en G de la siguiente manera: dados $a, b \in G$, decimos que $a \equiv b \pmod N$, si $b^{-1}a \in N$. Para un elemento $a \in G$ fijo, denotamos su clase de equivalencia por:

$$\bar{a} = \{x \in G : x \equiv a \pmod N\} = \{x \in G : a^{-1}x \in N\} = aN$$

Además, simbolizamos G/N el conjunto de todas las clases de equivalencia de los elementos de G. Definimos el producto de elementos en G/N por

$$\overline{a}\overline{b} = \overline{ab}.$$

En el caso en que N sea un subgrupo normal de G, G/N es un grupo llamado el **grupo factor** de G por N.

Teorema 1.2. *(Primer Teorema del isomorfismo de grupos)*

Sea $\varphi : G \to H$ un homomorfismo de grupos. Entonces

$$G/Ker(\varphi) \simeq Im(\varphi).$$

En particular, si φ es epimorfismo, entonces $G/Ker(\varphi) \simeq H$.

Demostración. [10, Teorema 2.7.1] □

Teorema 1.3. *Sea H un subgrupo normal de un grupo G. Entonces*

(i) Para cada subgrupo K de G que contiene a H, el conjunto $K/H = \{xH : x \in K\}$ es un subgrupo de G/H (Este es normal si y solo si K es normal).

(ii) Recíprocamente, si $\mathcal{K}$ es un subgrupo de G/H, entonces la preimagen $\pi^{-1}(\mathcal{K}) = K = \{x \in G : xH \in \mathcal{K}\}$ es un subgrupo de G que contiene a H, tal que $\mathcal{K} = K/H$.

Finalmente, tenemos dos importantes consecuencias del teorema [1.2].

Teorema 1.4. *(Segundo teorema del isomorfismo de grupos)*

Sea H y K subgrupos de un grupo G y asuma que K es normal. Entonces

$$\frac{H}{H \cap K} \simeq \frac{HK}{K},$$

donde $HK = \{hk : h \in H, k \in K\}$.

Demostración. [10, Teorema 2.7.2] □

Teorema 1.5. *(Tercer teorema del isomorfismo de grupos)*

Sean $H \subset K$ subgrupos normales de un grupo G. Entonces

$$\frac{G/H}{K/H} \simeq \frac{G}{K}.$$

Demostración. [10, Teorema 2.7.3] □

Concluiremos esta sección definiendo unos subgrupos especiales y enunciando algunos resultados de los mismos, los cuales serán necesarios para el desarrollo de esta monografía.

Definición 1.6. *Sea G un grupo finito de orden $p^n m$ donde $p \nmid m$. Un subgrupo de G de orden p^n es llamado un p-**subgrupo de sylow** de G.*

Teorema 1.6. *(Primer teorema de Sylow)*

Sean G un grupo finito y p un número primo. Si p^k divide a $|G|$, entonces G posee al menos un subgrupo de orden p^k.

Demostración. [7, Teorema 24.3] □

Teorema 1.7. *(Segundo teorema de Sylow) Si H es un subgrupo de un grupo finito G y $|H|$ es una potencia de un número primo p, entonces H está contenido en algún p-subgrupo de Sylow de G.*

Demostración. [7, Teorema 24.4] □

Teorema 1.8. *(Tercer teorema de Sylow) Sea G un grupo de orden $p^k m$, donde p es un número primo no divisor de m. Entonces, para cada $r = 0, \ldots, n$, G posee al menos un subgrupo de orden p^r.*

Demostración. [7, Teorema 24.5] □

1.2. Teoría de anillos

En está sección recordaremos algunas definiciones y resultados básicos de la teoría de anillos, anillos de polinomios y cuerpos.

Definición 1.7. *Un **anillo** es un conjunto no vacío R junto con dos operaciones binarias, "$+$" y "$\cdot$", tal que $\langle R, + \rangle$ es un grupo abeliano y para todo $a, b, c \in R$:*

(i) $a(bc) = (ab)c$.

(ii) $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$.

Denotamos por $\langle R, +, \cdot \rangle$ al anillo R bajo las operaciones suma ("$+$") y producto ("$\cdot$"). Si el producto en R es conmutativo, R es llamado **anillo conmutativo**, y si existe $0 \neq 1_R \in R$, tal que $1a = a1 = a$, entonces R es llamado **anillo con unidad**.

Un anillo es llamado un **dominio** si satisface la siguiente condición: $ab = 0$ implica que $a = 0$ o $b = 0$, para todo $a, b \in R$.

Los elementos no ceros a, b de un anillo R tales que $ab = 0$ son llamados **divisores de cero**, por lo tanto, un dominio es un anillo sin divisores de cero.

Un anillo con unidad, el cual es un dominio conmutativo es llamado **dominio entero**.

Un elemento no cero de un anillo conmutativo con unidad, no necesariamente tiene inverso multiplicativo, esto motiva la siguiente definición.

Definición 1.8. *Un elemento no cero a de un anillo R es llamado **invertible** si existe un elemento, denotado por a^{-1} y llamado el **inverso** de a, tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. El conjunto*

$$\mathcal{U}(R) = \{a \in R : a \; es \; invertible\},$$

*es llamado **las unidades** de R. Es claro que este conjunto es un grupo con la operación producto.*

*Un anillo es llamado **anillo con división** si todo elemento no cero es invertible, es decir, si $\mathcal{U}(R) = R \backslash \{0\}$. Un anillo con división es conmutativo es llamado **cuerpo**.*

Ejemplo 1.2.

(a) Los conjuntos de los números enteros ($\mathbb{Z}$), racionales ($\mathbb{Q}$), reales ($\mathbb{R}$) y complejos ($\mathbb{C}$), con las operaciones usuales de suma y producto, son de anillos conmutativos. Además, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.

(b) Sea R un anillo. Entonces el conjunto $M_n(R)$ de todas las matrices $n \times n$ con entradas en R, con las operaciones de suma y producto de matrices usual, es un anillo no conmutativo.

Definición 1.9. *Un subconjunto no vacío de un anillo R es llamado un subanillo de R, si es un anillo con respecto a las operaciones de R.*

Definición 1.10. *Un subconjunto no vacío L de un anillo R es un **ideal a izquierda** de R si:*

(i) $(x - y) \in L$ siempre que $x, y \in L$.

(ii) $ax \in L$ siempre que $x \in L$ y $a \in R$.

Análogamente, podemos definir ideales a derecha. Un subconjunto L de un anillo R es llamado ideal de R (algunas veces llamado **ideal bilateral**), si L es tanto ideal a izquierda como ideal a derecha de R. Denotaremos un ideal a izquierda I de R (respectivamente ideal a derecha), por $I \leq_l R$ (respectivamente $I \leq_r R$), en adelante y para nuestros propósitos $I \leq R$ denotará un ideal a izquierda a menos que se indique lo contrario.

Los subconjuntos $\{0\}$ y R son siempre ideales de R. Los ideales $\{0\}$ y R son llamados los ideales triviales. Un ideal L de R diferente de $\{0\}$ y R, es llamado un **ideal propio**.

Un ideal propio I de un anillo conmutativo R, se dice un **ideal primo** de R, si $a, b \in R$ y $ab \in I$, implica $a \in I$ o $b \in I$. Ahora bien, I se dice un **ideal maximal** de R, si siempre que $J \leq R$ y $I \subseteq J \subseteq R$, implica que $J = I$ ó $J = R$, es decir, no existen ideales I de R contenidos estrictamente entre J y R, y se dice **ideal minimal** si para cualquier $I' \subseteq I$ un ideal de R implica que $I' = I$.

Teorema 1.9. *Sea R un anillo conmutativo con unidad e $I \leq R$,*

(i) R/I es dominio entero si y solo si I es un ideal primo.

(ii) R/I es cuerpo si y solo si I es un ideal maximal.

Demostración. [7, Teorema 14.3] □

Así como un homomorfismo grupo preserva la operación del grupo, un homomorfismo de anillos preserva las operaciones de anillo, como veremos a continuación.

Definición 1.11. *Sean R y S anillos. Una aplicación $\phi : R \to S$ es llamada un* ***homomorfismo de anillos*** *si para todo $a, b \in R$ se tiene que:*

(i) $\phi(a + b) = \phi(a) + \phi(b)$.

(ii) $\phi(a \cdot b) = \phi(a) \cdot \phi(a)$

✓ Sea $\phi : R \to S$ un homomorfismo de anillos. Entonces la **Imagen** y el **Kernel** de ϕ son respectivamente los conjuntos:

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

✓ Definimos **monomorfismo**, **epimorfismo** y **isomorfismo** de igual manera que para homomorfismo sobre grupos.

✓ Si dos anillos R y S son isomorfos, abstractamente hablando, estos anillos pueden ser considerados como el mismo. Si $R \simeq S$ entonces $S \simeq R$. Es fácil verificar que composición de isomorfismos es reflexiva, simétrica y transitiva, así isomorfismo define una *relación de equivalencia*, en la clase de los anillos.

Suponga que R y S son anillos con unidad $1 = 1_R$ y $1' = 1_S$ respectivamente. Entonces no necesariamente es verdadero que $\phi(1) = 1'$. Por ejemplo, tomemos $R = M_2(\mathbb{Q})$, $S = M_3(\mathbb{Q})$ y $\phi : R \to S$ definida por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

este es un homomorfismo de anillos y

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

claramente, $\phi(1) \neq 1'$, puesto que la unidad en S es la matriz cuyos elementos en la diagonal son el $1_{\mathbb{Q}}$.

Sea I un ideal de un anillo R. Dado que R es un grupo (abeliano) bajo la suma y así $I \lhd R$, podemos formar el grupo cociente $R/I = \{r + I : r \in R\}$. Veamos que podemos formar un anillo de este grupo de clases laterales.

La suma y producto de dos clases laterales, se defines respectivamente por

$$(r+I)+(s+I)=(r+s)+I=r+s+I$$

$$(r+I)(s+I)=rs+I$$

Ahora bien, si $r+I=r'+I$ y $s+I=s'+I$, entonces $r=r'+a$, $s=s'+b$; $a,b\in I$. Por lo tanto, $rs=(r'+a)(s'+b)=r's'+r'b+as'+ab$ y así $rs+I=(r's'+r'b+as'+ab)+I=r's'+I$, pues $a,b\in I$ e $I\leq R$, es decir, el producto $\{r+I : r\in I\}$ está bien definido cuando $I\leq R$.

El conjunto de clases laterales $\{r+I : r\in R\}$ es un grupo abeliano y es un ejercicio sencillo establecer que el producto es asociativo y distributivo con respecto a la adición dado que sabemos que el producto definido en R lo es, más aún el producto define una operación binaria sobre las clases laterales.

Definición 1.12. *Sea I un ideal bilateral de un anillo R. Entonces el anillo R/I definido anteriormente es llamado **anillo cociente** de R por I.*

Considere la aplicación $\omega : R\to R/I$ dada por:

$$R\ni a\mapsto \omega(a)=\overline{a}=a+I.$$

Claramente, ω es un epimorfismo de anillos, llamado **homomorfismo natural** de R en el anillo cociente R/I tal que $\omega(0)=0+I$ y $Ker(\omega)=I$. Lo cual muestra, que todo ideal bilateral I de R es kernel de algún homomorfismo de anillos.

Análogamente a los Teoremas 1.2, 1.4 y 1.5, tenemos:

Teorema 1.10. *(Primer Teorema del isomorfismo de anillos)*
Sean $\phi : R\to S$ un homomorfismo de anillos de R sobre S y $K=Ker(\phi)$. Entonces $R/K\simeq S$; en realidad la aplicación $\psi : R/K\to S$ definida por $\psi(a+K)=\phi(a)$ es un isomorfismo de R/K sobre S.

Demostración. [10, Teorema 4.3.3] □

Teorema 1.11. *(Segundo teorema del isomorfismo de anillos)*
Sea I y J ideales bilaterales de un anillo R. Entonces

$$\frac{I}{I\cap J}\simeq\frac{I+J}{J},$$

donde $I\cap J\leq I$ y $J\leq I+J$.

Demostración. [10, Teorema 4.3.4] □

Teorema 1.12. *(Tercer teorema del isomorfismo de anillos)*
Sean $I \subset J$ ideales bilaterales de un anillo R. Entonces:

$$\frac{R/I}{J/I} \simeq \frac{R}{J},$$

donde $J/I \leq R/I$ y $J \leq R$.

Demostración. [10, Teorema 4.3.5] □

Anillo de Polinomios. Sea $\mathbb{F}$ un cuerpo; el **anillo de polinomios** con coeficiente en $\mathbb{F}$, denotado por $\mathbb{F}[x]$, es el conjunto de todas las sumas formales finitas $p(x) = a_0 + a_1x + \cdots + a_nx^n$, donde los $a_i \in F$, son llamados los **coeficientes** del polinomio $p(x)$. En $\mathbb{F}[x]$ se definen igualdad, suma y producto de dos polinomios de forma usual, para hacer de $\mathbb{F}[x]$ un anillo conmutativo. Sea $p(x) = a_0 + a_1x + \cdots + a_nx^n$ y $a_n \neq 0$, entonces el grado de $p(x)$, denotado por $grd(p(x))$, es n. Además, $p(x)$ es **mónico** si el coeficiente de su potencia más alta es 1.

Un polinomio $f(x) \in \mathbb{F}[x]$ es llamado **irreducible** si $grd(f(x)) \geq 1$ y siempre que $f(x) = g(x)h(x)$, donde $g(x), h(x) \in \mathbb{F}[x]$, entonces $g(x)$ o $h(x)$ es un polinomio constante. Si un polinomio no es irreducible es llamado **reducible**.

Proposición 1.1. *Recordemos algunas propiedades básicas de $\mathbb{F}[x]$*

(i) Si $f(x) \in \mathbb{F}[x]$ y $0 \neq g(x) \in \mathbb{F}[x]$, entonces existen únicos $q(x), r(x) \in \mathbb{F}[x]$ tales que $f(x) = g(x)q(x) + r(x)$, donde $r(x) = 0$ o $grd(r(x)) \leq grd(g(x))$.

(ii) $\mathbb{F}[x]$ es un dominio de ideales principales.

(iii) Las unidades de $\mathbb{F}[x]$ son los elementos no cero de $\mathbb{F}$.

(iv) Si $p(x)$ es irreducible en $\mathbb{F}[x]$, entonces $\mathbb{F}[x]/\langle p(x)\rangle$ es un cuerpo, y viceversa.

Consideremos el siguiente ejemplo, el cual será fundamental en el desarrollo de esta monografía.

Ejemplo 1.3. *Sea $\mathbb{R}[x]$ el anillo de polinomios con coeficientes reales y $\langle x^2 + 1\rangle$ el ideal principal*[1] *generado por $x^2 + 1$, es decir,*

$$\langle x^2 + 1\rangle = \{f(x)(x^2 + 1) : f(x) \in R[x]\}.$$

[1] Un ideal se dice principal si es generado por un elemento del anillo

Entonces

$$\mathbb{R}[x]/\langle x^2+1\rangle = \{g(x)+\langle x^2+1\rangle\} = \{ax+b+\langle x^2+1\rangle : a,b \in \mathbb{R}\}.$$

Luego, por el algoritmo de la division (Proposición 1.1), $g(x) = q(x)(x^2+1)+r(x)$*, donde* $q(x)$ *es el cociente y* $r(x)$ *es el residuo al dividir* $g(x)$ *por* x^2+1*, donde* $r(x) = 0$ *o el grado de* $r(x)$ *es menor que dos, así que* $r(x) = ax+b$ *para algunos* a *y* b *en* $\mathbb{R}$*. Por lo tanto,* $g(x)+\langle x^2+1\rangle = q(x)(x^2+1)+r(x)+\langle x^2+1\rangle = r(x)+\langle x^2+1\rangle$*, como el ideal* $\langle x^2+1\rangle$ *absorbe el término* $q(x)(x^2+1)$*.*

¿Como se realiza la multiplicación? Dado que

$$x^2+1+\langle x^2+1\rangle = 0+\langle x^2+1\rangle$$

debemos pensar en x^2+1 *como cero, o equivalentemente, que* $x^2 = 1$*. Así, por ejemplo*

$$\begin{aligned}&(x+3+\langle x^2+1\rangle)(2x+5+\langle x^2+1\rangle)\\ &= 2x^2+11x+15+\langle x^2+1\rangle\\ &= 11x+13+\langle x^2+1\rangle.\end{aligned}$$

En vista del hecho que los elementos del anillo cociente tienen la forma $ax+b+\langle x^2+1\rangle$ *donde* $x^2+\langle x^2+1\rangle = -1+\langle x^2+1\rangle$*.*

Proposición 1.2. *Sea* $f(x) \in \mathbb{F}[x]$ *un polinomio de grado mayor que* 1*. Si* $f(\alpha) = 0$ *para algún* $\alpha \in \mathbb{F}$*, entonces* $f(x)$ *es reducible sobre* $\mathbb{F}$*.*

Demostración. Por el algoritmo de la división tenemos que, $f(x) = (x-\alpha)(q(x))+r(x)$. Como $f(\alpha) = 0$, entonces $r(x) = 0$, así $f(x) = (x-\alpha)(q(x))$, $q(x) \notin \mathbb{F}$ puesto que $grd(f(x)) \geq 1$; luego $f(x)$ es reducible en $\mathbb{F}$. □

Definición 1.13. *Sea* $\mathbb{E}$ *un cuerpo que contiene al cuerpo* $\mathbb{F}$*, y sea* $f(x) \in \mathbb{F}[x]$*. Un elemento* $\alpha \in \mathbb{E}$ *es llamado una* ***raíz*** *o* ***Cero*** *de* $f(x)$ *si* $f(\alpha) = 0$*.*

Proposición 1.3. *Sea* $f(x) \in \mathbb{F}[x]$ *un polinomio tal que* $grd(f(x)) = 2$ *o* 3*. Entonces* $f(x)$ *es reducible si y solo si* $f(x)$ *tiene una raíz en* $\mathbb{F}$*.*

Un Polinomio $f(x) \in \mathbb{Z}[X]$ es llamado **primitivo** si el máximo común divisor de los coeficientes de $f(x)$ es 1. Claramente, todo polinomio mónico es primitivo.

Definición 1.14. *Si* $\mathbb{F}$ *es un subcuerpo de un cuerpo* $\mathbb{E}$*, entonces* $\mathbb{E}$ *es llamado una extensión de cuerpos de* $\mathbb{F}$ *o una extensión simple de* $\mathbb{F}$ *y denotaremos este hecho por el siguiente diagrama*

$$\begin{array}{c}\mathbb{E}\\ |\\ \mathbb{F}\end{array}$$

Definición 1.15. *Sea $\mathbb{E}$ un extensión de $\mathbb{F}$. Entonces la dimensión de $\mathbb{E}$ como espacio vectorial sobre $\mathbb{F}$ es llamado el grado de $\mathbb{E}$ sobre $\mathbb{F}$ y es denotado por $[\mathbb{E} : \mathbb{F}]$.*

Teorema 1.13. *Sean $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ cuerpos. Si $[\mathbb{K} : \mathbb{E}] < \infty$ y $[\mathbb{E} : \mathbb{F}] < \infty$, entonces*

(i) $[\mathbb{K} : \mathbb{F}] < \infty$

(ii) $[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}][\mathbb{E} : \mathbb{F}]$.

Demostración. [7, Teorema 21.5] □

Un homomorfismo inyectivo de un cuerpo $\mathbb{F}$ en un cuerpo $\mathbb{E}$ es llamado una **inmersión** de $\mathbb{F}$ en $\mathbb{E}$.

Corolario 1.1. *(Teorema de Kronecker)*
Sea $f(x) \in \mathbb{F}[x]$ un polinomio no constante. Entonces existe un extensión $\mathbb{E}$ de $\mathbb{F}$ en la cual $f(x)$ tiene raíz.

1.3. Módulos y Álgebras

Definición 1.16. *Sean R un anillo y M un grupo abeliano (en notación aditiva). Diremos que M es un **módulo a izquierda**, R-módulo, si existe una aplicación $\mu : R \times M \to M$ donde $\mu(r, m) = rm$ que verifica lo siguiente para todos $a, b \in R$ y para todos $m, m_1, m_2 \in M$,*

(i) $(a + b)m_1 = am_1 + bm_1$,

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

(iii) $a(bm_1) = (ab)m_1$,

(iv) $1m = m$,

donde 1 es la identidad multiplicativa en R.

De manera similar se define un **módulo a derecha**, módulo-R, considerando $\nu : M \times R \to M$ tal que $\nu(m, r) = mr$. Si $\mathbb{K}$ es un cuerpo, entonces el concepto de $\mathbb{K}$-módulo coincide con la definición de espacio vectorial sobre $\mathbb{K}$.

Ejemplo 1.4.

(a) Un grupo abeliano A (en notación aditiva). Con el producto $ma = \underbrace{a + \cdots + a}_{n}$, para $a \in A$ y $m \in \mathbb{Z}$, es un $\mathbb{Z}$-módulo, donde $\mathbb{Z}$ denota el conjunto de los enteros.

(b) Sea L un ideal a izquierda de un anillo R. Como el producto de los elementos de R por elemento e L está en L, se sigue L es un R-módulo izquierdo. De manera similar, ideales derechos, son R-módulos derechos.

En particular, un anillo es siempre un módulo sobre si mismo. Cuando consideremos un anillo R, como un R-módulo derecho o izquierdo sobre si mismo, utilizaremos la notaciones ${}_RR$ y R_R respectivamente.

(c) Sea L un ideal a izquierda de un anillo R y R/L el grupo factor bajo la adición. Entonces R/L se convierte en un R-módulo, bajo la aplicación $\phi : R \times R/L \to R/L$, donde

$$\phi(r, (r + L) = r(a + L) = ra + L, \forall r, a \in R.$$

Definición 1.17. *Sea R un anillo conmutativo y M es un R-módulo, diremos que M es una R-álgebra, si existe una multiplicación en M, definida en M tal que con la misma adición dada y está multiplicación, M es un anillo que satisface:*

$$r(ab) = (ra)b = a(rb),$$

para todos $a, b \in M$

Si M, es un anillo con unidad $1_M = 1$, entonces $R \cdot 1 \simeq R$ está contenido en el centro de M, $\zeta(M)$. Sean $r \in R$ y $m \in M$ arbitrarios, luego,

$$rm = r\underbrace{(m \cdot 1)}_{\in M} = m\underbrace{(r \cdot 1)}_{\in R} = ar$$

Por lo tanto $r \in \zeta(M)$

Definición 1.18. *Sea M un módulo sobre anillo R. Un subconjunto no vacío $N \subset M$ es llamado un R-**submódulo** de M y lo denotaremos por $N \leq M$, si para todo $x, y \in N$ y $r \in R$ se cumplen las siguientes condiciones:*

(i) $x + y \in N$

(ii) $rx \in N$.

Si R es conmutativo y M es una R-álgebra, se dice que N es una R-subálgebra de M y también un submódulo y subanillo de M.

Nota:

(i) Se sigue directamente de la definición que, si V es un K-espacio vectorial entonces los K-submódulos de V son exactamente sus subespacios vectoriales.

Además, si consideramos un anillo R como R-módulo, entonces los submódulos de ${}_RR$ son sus ideales a izquierda.

(ii) Cada módulo no-cero M contiene al menos dos submódulos, (0) y M mismo, los cuales son llamados **triviales**. Un submódulo diferente de estos, es llamado **submódulo propio**. Un módulo no-cero que no contiene submódulos es llamado **simple**.

(iii) Note que, si N_1 y N_2 son dos submódulos de un R-módulo M, entonces el conjunto

$$N_1 + N_2 = \{n_1 + n_2 : n_1 \in N_1, n_2 \in N_2\}$$

es un submódulo de M llamado la **suma** de los submódulos N_1 y N_2.

Sea N un submódulo de un R-módulo M. Como en el caso de anillos, el grupo factor aditivo M/N se convierte en un R módulo vía la $(r, \bar{m}) \mapsto r\bar{m}$, $r \in R$, $m \in M$. Este es llamado el **módulo factor** de M por N. Un análogo de los teoremas de isomorfismo (para grupos) también se cumple para módulos. Solo debemos verificar que los homomorfismos involucrados son también R-homomorfismos.

Finalmente, observemos que si R es un anillo conmutativo y A y B son R-álgebras, entonces la aplicación $\phi : A \to B$ es llamada un homomorfismo de R-álgebras si es un homomorfismo de anillos y un R-homomorfismo. Todos los resultados de homomorfismo de anillos se cumplen exactamente del mismo modo, para homomorfismos de R-álgebras.

Tenemos a continuación la extensión de la noción familiar de una base en un espacio vectorial para el caso de un módulo sobre un anillo dado.

Sea S un subconjunto de R-módulo M. Denotemos por RS el conjunto de todas las sumas finitas de la forma $\sum_{i=1}^{n} x_i s_i$ para algún entero positivo n y $x_i \in R$, $s_i \in S$ para $1 \leq i \leq n$ (es decir, el conjunto de todos las combinaciones R-lineales de elementos de S).

Definición 1.19. *Sea $S = \{s_i\}_{i \in I}$, un conjunto de elementos de un R-módulo M.*

*(i) S es llamado un **conjunto de generadores** de M si $M = RS$; es decir, cada elemento de M puede ser escrito como una combinación lienal (finita) de elementos de S con coeficientes en R.*

(ii) S *es llamado* ***linealmente independiente*** *(o algunas veces* R*-libre) si, para cada combinación lineal finita de elementos de* S *con coeficientes en* R*:*

$$r_{i_1}s_{i_1} + r_{i_2}s_{i_2} + \cdots + r_{i_t}s_{i_t} = 0$$

implica que $r_{i_1} = r_{i_2} = \cdots = r_{i_t} = 0$*.*

(iii) S *es llamado una* ***base*** *de* M *sobre* R *(o por brevedad una* R***-base****), si es linealmente independiente y un conjunto de generadores.*

Como en el caso de los espacios vectoriales, tenemos la siguiente caracterización de bases.

Proposición 1.4. *Un conjunto* $S = \{s_i\}_{i\in I}$*, de elementos de un* R*-módulo* M *es una base, si y solo si cada elemento* $m \in M$ *puede ser expresado de manera única como una combinación lineal (finita)*

$$m = r_{i_1}s_{i_1} + r_{i_2}s_{i_2} + \cdots + r_{i_t}s_{i_t},$$

donde $r_{i_j} \in R$*,* $s_{i_j} \in S$*,* $1 \leq i \leq t$*.*

Observación 1.2. *Desafortunadamente, no todo* R*-módulo* M *tiene una base. Considere, por ejemplo, el conjunto* $\mathbb{Z}_6$ *como un* $\mathbb{Z}$*-módulo. Para cada elemento* $\bar{a} \in \mathbb{Z}_6$ *tenemos que* $6\bar{a} = \bar{0}$ *y* $6 \neq 0$ *en* $\mathbb{Z}$*. Esto muestra que ningún subconjunto de* $\mathbb{Z}_6$ *es linealmente independiente sobre* $\mathbb{Z}$*, así este módulo no puede tener base.*

Aquellos R*-módulos que tienen base son llamados* R*-módulos* ***libres****.*

Proposición 1.5. *Sea* R *un anillo. Cada* R*-módulo* M *es imagen epimorfica de un* R*-módulo libre.*

Terminaremos esta sección, con el siguiente lema clásico, conocido como el *Lema de Zorn*, el cual hace parte de los denominados *Principios Maximales*, y que son ampliamente usados en matemáticas para demostrar teoremas por métodos "no constructivos".

Una cadena $\mathcal{C}$ en conjunto parcialmente ordenado $(A, \leq)$ es un subconjunto de A tal que, para todo $a, b \in \mathcal{C}$, $a \leq b$ o $b \leq a$. Un elemento $u \in A$ es **cota superior** de $\mathcal{C}$, si $a \leq u$ para todo $a \in C$; un elemento $m \in A$ es un **elemento maximal** de $(A, \leq)$ si $m \leq a$, $a \in A$, implica que $m = a$.

Ahora, tenemos las herramientas necesarias para enunciar el Lema de Zorn.

Lema 1.1. *(Lema de Zorn)*
Si toda cadena $\mathcal{C}$ *en un conjunto parcialmente ordenado* $(A, \leq)$ *tiene una cota superior en* A*, entonces* $(A, \leq)$ *tiene un elemento maximal.*

1.4. Anillos de grupo

Ahora, introduciremos la definición de un anillo de grupo RG de un grupo G sobre un anillo R. Como su nombre lo indica, su estudio es un lugar de encuentro de la teoría de grupos y de la teoría de anillos.

Dado un grupo G y un anillo R, deseamos construir un R-módulo, teniendo los elementos de G como base, y usando conjuntamente las operaciones de G y R para definir una estructura de anillo sobre él. Denotaremos por RG al siguiente conjunto:

$$RG = \left\{ \sum_{g\in G} \alpha_g g : \alpha_g \in R \text{ y } \alpha_g \neq 0 \text{ para un número finito de } \alpha_g \right\}.$$

Note que los elementos en RG son sumas finitas sin importar el orden de G. Dado un elemento $\alpha = \sum_{g\in G} \alpha_g g$ el **soporte de** α es el conjunto,

$$supp(\alpha) = \{g \in G : \alpha_g \neq 0\}.$$

Dos elementos $\sum_{g\in G} \alpha_g g$ y $\sum_{g\in G} \beta_g g$ de RG son iguales si y solo si, $\alpha_g = \beta_g$ para todo $g \in G$.

Sean $\alpha_g, \beta_g \in R$ y $g, h \in G$, definimos las operaciones de suma "$+$" y producto "$\cdot$", de la siguiente forma

(+) $(\sum_{g\in G} \alpha_g g) + (\sum_{g\in G} \beta_g g) = \sum (\alpha_g + \beta_g) g,$

(·) $\sum_{g\in G} \alpha_g g \sum_{h\in G} \beta_h h = \sum_{g,h\in G} (\alpha_g \beta_h) gh = \sum_{u\in G} c_u u$, donde $c_u = \sum_{gh=u} \alpha_g \beta_h$.

RG con la operaciones definidas anteriormente, es un anillo con unidad, donde la unidad esta dada por $1_{RG} = \sum_{g\in G} \alpha_g g$, donde $\alpha_{g_0} = 1$ para algún $g_0 \in G$ y $\alpha_g = 0$, para todo $g \neq g_0$. Además, $0_{RG} = \sum_{g\in G} 0_g g$ es el cero en RG y $-\alpha = \sum_{g\in G} (-\alpha_g) g$ es el inverso aditivo de $\alpha \in RG$.

Notemos que RG tiene estructura de R-módulo, con el producto $\mu : R \times RG \to RG$ definido por la expresión:

$$(\lambda, \sum_{g\in G} \alpha_g g) \overset{\mu}{\mapsto} \sum_{g\in G} (\lambda \alpha_g) g.$$

Si R es un anillo conmutativo tenemos que RG es un R-álgebra. En particular, si tomamos $R = \mathbb{F}$ un cuerpo, $\mathbb{F}G$ es un $\mathbb{F}$-álgebra, más aún $\mathbb{F}G$ es un $\mathbb{F}$-espacio vectorial.

Definición 1.20. *El conjunto RG con las operaciones anteriormente definidas es llamado el* ***anillo de grupo del grupo*** *G* ***sobre el anillo*** *R. Además, si R es un anillo conmutativo, entonces RG también es llamado el* ***álgebra de grupo de*** *G* ***sobre*** *R.*

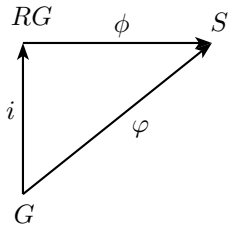
Observación 1.3. *La aplicación $i : G \to RG$ dada por $x \mapsto i(x) = \sum_{g\in G} \alpha_g g$ donde $\alpha_x = 1$ y $\alpha_g = 0$ si $g \neq x$, nos permite ver a G inmerso en RG, que denotaremos por $G \overset{i}{\hookrightarrow} RG$. Esta inmersión muestra claramente que G resulta ser una R-base para RG.*

Ahora, consideremos $v : R \to RG$ la función dada por $v(r) = \sum_{g\in G} \alpha_g g$ donde $\alpha_{1_G} = r$ y $\alpha_g = 0$ si $g \neq 1_G$. Así, v define un monomorfismo de anillos y R un subanillo de RG.

Dados $r \in R$ y $g \in G$, se tiene que $rg = gr$ en RG. Por tanto, si R es conmutativo, $R \subseteq Z(RG)$, dado que para $g \in G$, $r(\alpha_g g) = (r\alpha_g)g = (\alpha_g r)g = \alpha_g(rg) = (\alpha_g g)r$, esto implica que, $r(\sum \alpha_g g) = (\sum \alpha_g g)r$.

Enunciaremos a continuación, una importante propiedad ("Propiedad Universal"), para los anillos de grupo:

Proposición 1.6. *Sean G un grupo y R un anillo. Dado cualquier anillo S tal que $R \subset S$ y cualquier función $\varphi : G \to S$ tal que $\phi(gh) = \phi(g)\phi(h)$, para todos $g, h \in G$, existe un único homomorfismo de anillos $\phi : RG \to S$, el cual es $R-$lineal y tal que $\phi \circ i = \varphi$ donde $i : G \hookrightarrow RG$ es la inclusión dada arriba. Es decir, tenemos el siguiente diagrama conmutativo:*



Corolario 1.2. *Sea $\varphi : G \to H$ un homomorfismo de grupos. Entonces,*

(i) Existe un único homomorfismo de anillos $\phi : RG \to RH$ tal que $\phi(g) = \varphi(g)$, para todo $g \in G$,

(ii) Si R es un anillo conmutativo, ϕ es un homomorfismo de R-álgebras

(iii) Si φ es un monomorfismo (epimorfismo) entonces ϕ es un monomorfismo (epimorfismo).

Si $H = \{1\}$, entonces del Corolario 1.2, la aplicación $G \to \{1\}$ induce un homomorfismo de anillos $\varepsilon : RG \to R$ dado por:

$$\varepsilon\Big(\sum_{g\in G} \alpha_g g\Big) = \sum_{g\in G} \alpha_g,$$

llamada la **aplicación de aumento** de RG. Naturalmente, ε tiene asociado un núcleo denotado por $\Delta(G)$ y llamado el **ideal de aumento** de RG.

Considere $\alpha = \sum_{g\in G} \alpha_g g \in RG$. Si $\alpha \in \Delta(G)$ entonces $\varepsilon(\sum_{g\in G} \alpha_g g) = \sum_{g\in G} \alpha_g = 0$. Luego, obtenemos que:

$$\alpha = \sum_{g\in G} \alpha_g g - \sum_{g\in G} \alpha_g = \sum_{g\in G} \alpha_g (g-1).$$

Claramente, todos los elementos de la forma $g-1$ con $g \in G$, pertenecen a $\Delta(G)$, es decir, $\{g-1 : g \in G \text{ y } g \neq 1\}$ es un conjunto de generadores de $\Delta(G)$ sobre R. Además, es posible mostrar que este conjunto es linealmente independiente. Por lo tanto, tenemos:

Proposición 1.7. *El conjunto $\{g-1 : g \in G, \quad g \neq 1\}$ es una base para $\Delta(G)$ sobre R y, por tanto:*

$$\Delta(G) = \langle g-1 : g \in G\backslash\{1\}\rangle_R = \Big\{ \sum_{g\in G} \alpha_g (g-1) : g \in G,\, \alpha_g \in R \Big\},$$

donde $\alpha_g \neq 0$ para un número finito de α_g.

Notemos que si R es un anillo conmutativo y G es un grupo finito, entonces $\Delta(G)$ es un $R-$módulo libre de rango $rank(\Delta(G)) = |G| - 1$.

A continuación exhibimos una función Φ del conjunto $\mathcal{S}(G)$ de todos los subgrupos de G en el conjunto $\mathcal{I}(RG)$ de todos los ideales a izquierda de RG, estableciendo una relación entre estos dos conjuntos.

En efecto, dado $H \in \mathcal{S}(G)$, denotaremos por $\Delta_R(G,H)$ al ideal a izquierda de RG generado por el conjunto $\{h-1 : h \in H\}$, es decir,

$$\Delta_R(G,H) = \{ \sum_{h\in H} \alpha_h (h-1) : \alpha_h \in RG \}.$$

Cuando el anillo R es fijado, omitiremos el subíndice y denotaremos tal ideal izquierdo simplemente por $\Delta(G,H)$. Note que el ideal $\Delta(G,G)$ coincide con el ideal de aumento $\Delta(G)$ en RG.

A continuación describiremos un conjunto generador y una base para $\Delta(G,H)$ como ideal a izquierda de RG

Lema 1.2. *Sean H un subgrupo de G y S un conjunto generador de H. Entonces, el conjunto $\{s-1 : s \in S\}$ es un conjunto de generadores de $\Delta(G,H)$ como ideal a izquierda de RG.*

Demostración. Como $\langle s \rangle = H$, cada elemento $a \neq h \in H$ puede ser escrito en la forma

$$h = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_r^{\epsilon_r},$$

con $s_i \in S$, $\epsilon_i = \pm 1$, $1 \leq i \leq r$, para algún entero positivo r.

Ahora bien, la siguiente aplicación repetitiva

$$x^{-1} - 1 = x^{-1}(1-x) \quad y \quad xy - 1 = x(y-1) + (x-1)$$

muestra que todos los elementos de la forma $h-1$, $h \in H$ pertenecen al ideal a izquierda generado por el conjunto $\{s-1 : s \in S\}$. □

Para obtener una mejor descripción de $\Delta(G,H)$, consideremos un transversal $\tau = \{q_i\}_{i\in I}$ de H en G, donde tomamos como representante de la clase lateral H en τ, precisamente al elemento identidad de G. Así, cada elemento $g \in G$ puede ser escrito de manera única en la forma $g = q_i h_j$ con $q_i \in \tau$ y $h_j \in H$, $G = \bigcup_{i\in I} q_i H$. Así obtenemos una R-base para $\Delta(G,H)$.

Proposición 1.8. *El conjunto $B_H = \{q(h-1) : q \in \tau, 1 \neq h \in H\}$ es una base de $\Delta(G,H)$ sobre R.*

Demostración. [12, Proposición 3.3.3] □

Ahora bien, si $H \lhd G$, el epimorfismo canónico $\pi_H : G \to G/H$ puede ser extendido al epimorfismo.

$\pi_H^* : RG \to R(G/H)$, donde $\sum_{g\in G} \alpha_g g \mapsto \sum_{g\in G} \alpha_g \pi_H(g)$.

Si consideramos $\tau = \{q_i\}_{i\in I}$ una transversal de H en G, cada elemento $\alpha \in RG$ tiene la presentación

$$\alpha = \sum_{g\in G} \alpha_g g = \sum_{i,j} \alpha_{ij} q_i h_j, \quad \alpha_{ij} \in R, q_i ß \tau, h_j \in H$$

si $\bar{q}$ es la imagen de q_i en el grupo factor, entonces tenemos

$$\pi_H^*(\alpha) = \sum_i (\sum_j \alpha_{ij}) \bar{q},$$

por tanto, $\alpha \in Ker(\pi_H^*)$ si y solo si $\sum_j r_{ij} = 0$ para cada valor de i. Así, si $\alpha \in Ker(\pi_H^*)$ (luego de adicionar algunos ceros) tenemos que:

$$\alpha = \sum_{i,j} r_{ij} + q_i h_j = \sum_{i,j} r_{ij} q_i h_j - \sum_i (\sum_j r_{ij}) q_i = \sum_{i,j} r_{ij} q_i (h_j - 1) \in \Delta(G,H)$$

Por lo cual $Ker(\pi_H^*) \subset \Delta(G,H)$, la otra inclusión es clara; por tanto, $Ker(\pi_H^*) = \Delta(G,H)$.

Finalmente, por el Teorema 1.2, tenemos que

$$\frac{RG}{\Delta(G,H)} \simeq R\left(\frac{G}{H}\right),$$

en particular, $RG/\Delta(G,H) \simeq R$.

Así, hemos construido $\Phi : \mathcal{S} \to \mathcal{I}(RG)$ tal que subgrupos normales de H en G son enviados a ideales bilaterales de RG.

Capítulo 2

Semisimplicidad y Álgebras de Grupo de Grupos Abelianos

En este capítulo estudiaremos algunos conceptos y resultados de semisimplicidad para módulos y álgebras de grupo, los cuales son importantes para el desarrollo de esta monografía. Estos resultados pueden ser consultados en [12, Sección 2.5, Sección 2.6, Sección 3.4 y Sección 3.5]

2.1. Semisimplicidad

Como es bien sabido cada subespacio de un espacio vectorial finitamente generado es un sumando directo del mismo. Esta idea ya no es cierta para en el caso más general de los módulos sobre un anillo arbitrario, por ejemplo, $\mathbb{Z}$ no es un sumando directo de $\mathbb{Q}$ como un $\mathbb{Z}$-módulo. Estaremos particularmente interesado en los módulos que sí tienen esta propiedad.

Definición 2.1. *Sea $\{M_i\}_{i\in I}$ una familia de submódulos de un R-módulo M. Decimos que M es **suma directa** de los submódulos de esta familia y escribimos $M = \bigoplus_{i\in I} M_i$, si se cumplen las siguientes condiciones:*

(i) Para todo $i \in I$, se tiene que $M_i \bigcap (\sum_{j\neq i} m_j) = 0$

(ii) $M = \sum_{i\in I} M_i$.

Las dos condiciones de la definición son equivalentes a:

(iii) Todo elemento $m \in M$ puede ser escrito manera única como $m = m_{i_1} + m_{i_2} + \cdots + m_{i_t}$, con $m_{i_j} \in M_{i_j}$, $1 \leq j \leq t$.

En particular, si $\{m_i\}_{i \in I}$ es una R-base de M, entonces M es la suma directa $M = \bigoplus_{i \in I} Rm_i$.

Definición 2.2. *Un submódulo N de un R-módulo M es llamado **sumando directo** si existe otro módulo N' tal que $M = N \oplus N'$. Un módulo el cual no contiene un sumando directos no trivial es llamada **indescomponible**.*

Estaremos particularmente interesados en aquellos módulos en los que cada uno de sus sudmódulos es un sumando directo.

Definición 2.3. *Un R-módulo M es llamado **semisimple** si cada submódulo de M es un sumando directo.*

Proposición 2.1. *Sea $N \neq (0)$ un submódulo de un módulo semisimple M. Entonces N es semisimple y contiene un módulo simple.*

Demostración. Primero mostraremos que N es semisimple. Sea S un submódulo arbitrario de N, entonces S también es un submódulo semisimple de M, y pon tanto existe otro submódulo S' tal que $M = S \oplus S'$.

Afirmamos: $N = S \oplus (S' \bigcap N)$.

De hecho, es claro que $S \bigcap (S' \bigcap N) \subset S \bigcap S' = (0)$. Por otro lado, dado $n \in N$, él puede ser escrito como $n = x + y$ con $x \in S$ y $y \in S'$. Pero $y = n - x \in N$, así $y \in N \bigcap S'$, probando así nuestra afirmación.

Para probar que N contiene un submódulo simple, elegimos un elemento $x \in N, x \neq 0$. Note que la familia de submódulos de N que contiene a x es no vacía (s' es uno de ellos) y es parcialmente ordenada por inclusión, por lo cual tiene cota superior, entonces por el Lema de Zorn, existe un elemento maximal N_1. Como N es semisimple, existe otro submódulo N_2 de N tal que $N = N_1 \oplus N_2$, nuestro argumento está completo si N_2 es simple.

Si N_2 no es simple, él contiene un un submódulo propio W y existe W' tal que $N_2 = W \oplus W'$. Se sigue que $N = N_1 \oplus W \oplus W'$ y además $N_1 = (N_1 + W) \bigcap (N_1 + W')$. Como $x \notin N_1$ tenemos que o bien $x \in N_1 + W$ o bien $x \notin N_1 + W'$, contradiciendo la maximalidad de N_1. □

Veamos algunas caracterizaciones de semisimplicidad.

Teorema 2.1. *Sea M un $R-$módulo, entonces las siguientes condiciones son equivalentes:*

(i) M es semisimple.

(ii) M *es suma directa de submódulos simples.*

(iii) M *es suma (no necesariamente directa) de submódulos simples.*

Demostración. $(i) \Rightarrow (ii)$ Sea $\mathcal{F}$ la colección de todos los submódulos los cuales pueden ser escritos como suma directa de submódulos simples (existen submódulos simples de M, debido a la Proposición 2.1). Podemos definir un orden en $\mathcal{F}$ de la siguiente forma. Dados dos elementos $\oplus_{i\in I}M_i$ y $\oplus_{i\in J}M_i$ en $\mathcal{F}$, decimos que $\oplus_{i\in I}M_i \prec \oplus_{i\in J}M_i$ si y solo si $I \subset J$.

Ahora, dado que $(\mathcal{F}, \prec)$ satisface las condiciones del Lema de Zorn, así existe un elemento maximal $M_0 \in \mathcal{F}$, el cual puede ser escrito de la siguiente forma $M_0 = \oplus_{i\in I}M_i$ con M_i simple, $i \in I$.

La implicación será probada, si mostramos que $M_0 = M$. Razonando por el absurdo, supongamos que $M_0 \neq M$, de la hipótesis, existe un submódulo N de M tal que $M = M_0 \oplus N$. Por la Proposición 2.1, N contiene un módulos simple S. Pero $M_0 \oplus S = \oplus_{i\in I}M_i \oplus S \supset M_0$, contradiciendo la maximalidad de M_0.

$(ii) \Rightarrow (iii)$ Es clara, ya que la condición (ii) asegura que M es suma de submódulos simples.

$(iii) \Rightarrow (i)$ Asuma que $M = \sum_{i\in I} M_i$, donde cada M_i, $i \in I$, es simple. Sea N un submódulo propio arbitrario de M. Probemos que N es un sumando directo de M.

Consideremos la familia:

$$\mathcal{J} = \left\{ \sum_{i\in J} M_i : J \subset I, \left(\sum_{i\in J} M_i\right) \bigcap N = (0) \right\}$$

Note que, como M_i, es simple, si $N \bigcap M_i \neq (0)$ entonces $M_i \subset N$. Como $N \neq M$, se sigue que existe al menos un submódulo M_i tal que $N \bigcap M_i = (0)$ y $\mathcal{J}$ es no vacío. Por el Lema de Zorn, podemos encontrar un submódulo maximal en $\mathcal{J}$, digamos $M_0 = \sum_{i\in J_0} M_i$. De la definición de la familia $\mathcal{J}$ es claro que $(\sum i \in J_0 M_i) \cap N = (0)$.

Ahora, si para cada $i \in I$, tenemos que $M_i \subset M_0 + N$, entonces $\sum_{i\in I} M_i = M \subset M_0 + N \subset M$, es decir, $M = M_0 + N$ que era lo que queríamos demostrar.

Supongamos que existe un índice i_0 tal que $M_{i_0} \not\subset M_0 + N$. Como M_{i_0} es simple, tenemos que $M_{i_0} \cap (M_0 + N) = (0)$, luego $(M_{i_0} + M_0) \cap N = (0)$, caso contrario, existe $x \in (M_{i_o} + M_0) \cap N$ con $x = m_{i_o} + \sum_{i\in J_0} m_i$; $m_i \in M_i$, $i \in J_0$ y $x = n; n \in N$. Por lo tanto $(m_{i_0} + \sum_{i\in J_0} m_i) \in N$, m_0 y $m_{i_0} = n + \sum_{i\in J_0} \bar{m}_i \in M_{i_0}$ una contradicción del hecho que $M_{i_0} \cap (M_0 + N) = (0)$. Por tanto $(M_{i_0} + M_0) \cap N = (0)$ y así $m_{i_0} + m_o \in J$, contradicción pues $M_0 \in \mathcal{J}$ maximal. □

Así, dado un submódulo N de un módulo semisimple M siempre podemos encontrar un subconjunto de índices $J_0 \subset I$ tal que $M = N \oplus N_0$ con $N_0 = \oplus_{i\in J_0} M_i$. Luego

$$N \simeq \frac{M}{N_0} = \frac{\bigoplus_{i\in I} M_i}{\bigoplus_{i\in J_0} M_i} \simeq \bigoplus_{i\in I\setminus J_0} M_i$$

nos lleva al siguiente resultado:

Corolario 2.1. *Sean $M = \oplus_{i\in I} M_i$ una descomposición de módulos semisimples M como suma directa de submódulos simples y N un submódulo de M. Entonces existe un subconjunto $J \subset I$ tal que $N \simeq \oplus_{j\in J} M_j$.*

Corolario 2.2. *Un módulo factor L de un módulo semisimple M es isomorfo a un submódulo de M por lo que también es semisimple.*

Demostración. Sean L un módulo factor de M, $\pi : M \to L$ el homomorfismo natural y $N = Ker(\pi)$. Entonces, existe un submódulo N' de M tal que $M = N \oplus N'$, luego $N' \simeq M/Ker(\pi) \simeq L$, el resultado se sigue del corolario anterior. □

Análogamente tenemos la noción de anillos semisimple.

Definición 2.4. *Un anillo R es semisimple si el módulo a izquierda sobre si mismo ${}_RR$ es semisimple.*

Como los submódulos de ${}_RR$ son los ideales a izquierda de R, entonces R es semisimple si y solo si cada ideal a izquierda de R es un sumando directo de R.

Teorema 2.2. *Sea R un anillo. Entonces, las siguientes condiciones son equivalente:*

(i) Cada R-módulo es semisimple.

(ii) R es un anillo semisimple.

(iii) R es suma directa un número finito de ideales minimales a izquierda.

Demostración.
$(i) \Rightarrow (ii)$ Como todo anillo R es un R-módulo sobre si mismo, el resultado es claro.
$(ii) \Rightarrow (iii)$ Como los submódulos simples de ${}_RR$ son precisamente los ideales minimales a izquierda de R, se sigue del Teorema 2.1 que R puede ser escrito de la forma $R = \oplus_{i\in I} L_i$ donde cada L_i es un ideal minimal a izquierda. Así, para concluir esta implicación, necesitamos mostrar solamente que esta suma es finita.

En particular, el elemento $1 \in R$ puede ser escrito como una suma finita: $1 = x_{i_1} + \cdots + x_{i_n}$, con $x_{i_j} \in L_{i_j}$, entonces para un elemento arbitrario $r \in R$, tenemos que $r = r \cdot 1 = rx_{i_1} + \cdots + rx_{i_n}$, donde $rx_{i_j} \in L_{i_j}$, $1 \leq j \leq n$. Lo cual muestra que $R \subset L_{i_1} \oplus L_{i_2} \oplus \cdots \oplus L_{i_n}$, y así $R = L_{i_1} \oplus L_{i_2} \oplus \cdots \oplus L_{i_n}$.

Note que el Teorema 2.1 tomando como R-módulo a R, nos dá que $(iii) \Rightarrow (ii)$, por tanto, solo necesitamos establecer $(ii) \Rightarrow (i)$. Supongamos que R es semisimple y sea M cualquier R-módulo. Sabemos por la Proposición 1.5 que M es una imagen epimorfica de un R-módulo libre F. Entonces F puede ser escrito de la formar $F = \oplus_i Ra_i$ donde $Ra_i \simeq R$ es semisimple. Así, F es semisimple y el Corolario 2.2 implica que M es semisimple. □

Corolario 2.3. *Si ${}_RR$ es semisimple, entonces R es de longitud finita, es decir, existe una cadena de submódulos*

$$R = J_0 \supset J_1 \supset \cdots \supset J_n = (0) \tag{2.1}$$

tal que J_i/J_{i+1} es simple, para todo $i \in I$.

Demostración. Como se mostró en Teorema 2.2, si R es semisimple, podemos escribirlo como una suma directa finita $R = L_1 \oplus L_2 \oplus \cdots \oplus L_t$, donde L_i es un ideal minimal a izquierda, $1 \leq i \leq t$. Por tanto

$$R = (L_1 \oplus L_2 \oplus \cdots \oplus L_t) \supset (L_2 \oplus L_2 \oplus \cdots \oplus L_t) \supset \cdots \supset L_t \supset (0).$$

Así, existe una cadena tal que satisface la condición 2.1, por lo tanto, R es de longitud finita. □

La siguiente es un caracterización de semisimplicidad en términos de elementos idempotentes, es decir, elementos $e \in R$ tales que $e^2 = e$.

Teorema 2.3. *Un anillo R es semisimple si y solo si cada ideal de R es de la forma Re donde e es un elemento idempotente.*

Demostración. Asuma que R es semisimple. Sea L un ideal a izquierda de R. Entonces L es un sumando directo, así existe un ideal a izquierda L', tal que $R = L \oplus L'$, de donde, $1 = x + y$ con $x \in L$ y $y \in L'$, entonces $x = x \cdot 1 = x^2 + x \cdot y$, así $xy = x - x^2 \in L$ y como L' es ideal a izquierda, tenemos que $xy \in L'$. Dado que $L \bigcap L' = (0)$ entonces se sigue que $xy = 0$, así $x = x^2$, esto es, x es idempotente. Claramente $Rx \subset L$. Dado un elemento $a \in L$ tenemos que $a = a \cdot 1 = ax + ay$ así $a - ax = ay \in L \cap L' = (0)$ y por lo tanto $a = ax \in Rx$ demostrando así la otra inclusión. Por lo cual $L = Rx$.

Recíprocamente, asumamos que los ideales a izquierda son como en el enunciado. Necesitamos mostrar que cualquier ideal a izquierda L de R es sumando directo. Por hipótesis, el ideal L es de la forma $L = Re$ donde $e \in R$ es un idempotente. Sea $L' = R(1-e)$. Es claro que L' es un ideal a izquierda y que dado $x \in R$ podemos escribirlo como $x = xe + x(1-e)$, así tenemos que $R = Re + R(1-e)$. Además, si $x \in R \bigcap R(1-e)$, tenemos que $x = re = s(1-e)$

para algunos $r, s \in R$, entonces, $xe = re \cdot e = re^2 = re = x$ y, por otro lado, tenemos que $xe = s(1-e)e = 0$ así $x = 0$ y se sigue que $Re \bigcap R(1-e) = (0)$. Esto muestra que $R = L \oplus L'$ y así L es un sumando directo. □

Podemos usar los idempotentes para caracterizar la descomposición de un anillo semisimple como suma directa de ideales minimales a izquierda.

Teorema 2.4. *(Teorema de descomposición de Peirce)*
Sea $R = \oplus_{i=1}^{t} L_i$ una descomposición de anillos semisimples como suma directa de ideales minimales. Entonces existe una familia $\{e_1, e_2, \ldots, e_t\}$ de elementos de R tales que:

(i) $e_i \neq 0$ *es idempotente,* $1 \leq i \leq t$.

(ii) Si $i \neq j$, *entonces* $e_i e_j = 0$.

(iii) $e_1 + e_2 + \cdots + e_t = 1$.

(iv) e_i *no puede escribirse como* $e_i = e_i' + e_i''$ *donde* e_i' *y* e_i'' *son idempotentes tales que* e_i', $e_i'' \neq 0$ *y* $e_i' e_i'' = 0$, $1 \leq i \leq t$.

Recíprocamente, si existe una familia de idempotentes $\{e_1, e_2, \ldots, e_t\}$ la cual satisface las condiciones anteriores, entonces los ideales $L_i = Re_i$ son minimales y $R = \oplus_{i=1}^{t} L_i$.

Demostración. Supongamos que $R = \oplus_{i=1}^{t} L_i$ es una descomposición de un anillo semisimple R como suma directa de ideales minimales a izquierda y escribimos $1 = e_1 + e_2 + \cdots + e_t$ con $e_i \in L_i$. Entonces se sigue del Teorema 2.3, que cada e_i es un idempotente, $L_i = Re_i$, $1 \leq i \leq t$, y que $i \neq j$ implica que $e_i e_j = 0$. Ahora, si para algún índice i, se puede escribir $e_i = e_i{}' + e_i{}''$ donde $e_i{}', e_i{}''$ son idempotentes tales que $e_i{}' e_i{}'' = 0$ entonces, de nuevo por el Teorema 2.3, tenemos que $L_i = Re_i{}' \oplus Re_i{}''$, con $Re_i{}', Re_i{}'' \neq 0$, contradiciendo así que L_i sea minimal.

Recíprocamente, supongamos que existe una familia de idempotentes $\{e_1, e_2, \ldots, e_t\}$ la cual satisface todas la condiciones dadas. Probaremos primero que un ideal $L_i = Re_i$ es minimal, $1 \leq i \leq t$. Para ello, digamos que no es minimal, es decir, existe un ideal a izquierda J y, dado que ${}_R R$ es semisimple, L_i también es semisimple, así existe un ideal J' en L_i tal que $L_i = J \oplus J'$ y aplicando una vez más el Teorema 2.3, esto implica que $e_i = e_i{}' + e_i{}''$ donde $e_i{}', e_i{}''$ son idempotentes tales que $e_i{}', e_i{}'' \neq 0$ y $e_i{}' e_i{}'' = 0$, contradicción con (iv).

El hecho que $R = L_1 + \cdots L_t$ se sigue inmediatamente de la condición (iii). Para probar que la suma es directa, supongamos que $x \in L_j \bigcap \left(\sum_{i \neq j} L_i \right)$. Entonces podemos escribir $x = r_j e_j = \sum_{i \neq j} r_i e_i$. Multiplicando por e_j tenemos que $r_j {e_j}^2 = x = \sum_{i \neq j} r_i e_i e_j = 0$, lo cual implica que $x = 0$. □

Definición 2.5. *Sea R un anillo, La familia de idempotentes $\{e_1, e_2, \ldots, e_t\}$ del Teorema 2.4 se denomina **familia ortogonal de idempotentes** si satisface las condiciones $(i), (ii)$ y (iii). Si además, satisface la última condición diremos que es una **familia ortogonal de idempotentes primitivos**.*

Lema 2.1. *Sea L un ideal a izquierda minimal de un anillo semisimple R y M un R-módulo simple. Entonces, $LM \neq (0)$ si y solo si $L \simeq M$ como R-módulos; en este caso $LM = M$.*

Demostración. Supongamos que $LM \neq (0)$. Entonces, existe un elemento $x \in L$ y un elemento $m \in M$ tales que $xm \neq 0$, así $Lm \neq (0)$. Como Lm es un submódulo de M el cual es simple, tenemos que $Lm = LM = M$. Ahora, considere la aplicación $f : L \to M$ dada por $L \ni x \mapsto xm$. Claramente, $Im(f) = Lm = LM = M$, por lo cual, f es un epimorfismo y como $Ker(f) \neq L$ es un ideal de R contenido en L y L es minimal, por lo cual $Ker(f) = (0)$. Así, f también es inyectiva y tenemos que $L \simeq M$.

Recíprocamente, asumiendo que $L \simeq M$ como R-módulos y $f : L \to M$ un isomorfismo. Como R es semisimple existe un idempotente $e \in R$ tal que $L = Re$. Sea $m_0 = f(e)$. Como $f(re) = rf(e) = rm_0$ para todo $r \in R$ se sigue que $m_0 \neq 0$. Como $m_0 = f(e) = f(e^2) = ef(e) = em_0$, se sigue que $LM \neq (0)$. El hecho que $LM = M$ es trivial. □

Proposición 2.2. *Sea $R = \oplus_{i=1}^{t} L_i$ una descomposición de un anillo semisimple como suma directa de ideales minimales a izquierda. Entonces cada R-módulo simple es isomorfo a un de los ideales L_i en la descomposición dada.*

Demostración. Sea $R = \oplus_{i=1}^{t} L_i$ una descomposición de R como suma directa de ideales minimales a izquierda y M un R-módulo simple. Entonces, como $0 \neq RM$ es un submódulo de M y como M es simple, tenemos que $RM = M$. Pero $RM = \oplus_{i=1}^{t} L_i M$ así existe un índice j tal que $L_j M \neq (0)$ y por el lema anterior $L_j \simeq M$. □

2.2. El Teorema de Wedderburn-Artin

En esta sección, describiremos la estructura de los anillo semisimples. Empezaremos obteniendo resultados acerca de sus ideales bilaterales.

Lema 2.2. *Sea L un ideal minimal a izquierda de un anillo semisimple R. Entonces la suma de todos los ideales a izquierda de R isomorfos a L es un ideal bilateral de R.*

Demostración. Sea $A = \sum_{J \simeq L} J$. Como la suma de ideales izquierdos es un ideal izquierdo, A es un ideal a izquierda. Veremos que A también es un ideal a izquierda. Escribimos $R = \oplus_{i=1}^{t} L_i$, como suma directa de ideales minimales a izquierda. Entonces $AR = \sum_{J \simeq L} JR =$

$\sum_{J\simeq L}\sum_{i=1}^{t} JL_i$. Pero $JL_i = (0)$ o bien $JL_i = L_i$. Por el Lema 2.1 tenemos que $JL_i = L_i$ solo sucede si $J \simeq L_i$, es decir, cuando $L_i \simeq L$ y esto implicaría que $L_i \subset A$. Por tanto, $AR = \sum_{J\simeq L} JR = \sum_{J\simeq L}\sum JL_i$, luego, tenemos que $AR \subset A$. □

Lema 2.3. *Sea I un ideal bilateral de un anillo semisimple R que contiene un ideal minimal a izquierda L. Entonces I contiene todos los ideales isomorfos a L.*

Demostración. Sea $L \subset I$ un ideal minimal a izquierda y J un ideal isomorfo a L. Entonces, del Lema 2.1, tenemos que $J = LJ \subset IJ \subset I$. □

Ya con esta información, podemos pasar a expresar anillos semisimples como suma directa de un tipo especial de anillos.

Proposición 2.3. *Sea L un ideal minimal a izquierda de un anillo semisimple R y B la suma de todos los ideales a izquierda de R isomorfos a L. Entonces, B es un ideal bilateral minimal de R.*

Demostración. Por el Lema 2.2, B es un ideal bilateral de R, veamos que además es minimal.

Sea B_1 un ideal bilateral de R contenido en B y L_1 un ideal minimal a izquierda de R contenido en B_1. Si $L_1 \not\simeq L$, de donde obtenemos que $L_1J = (0)$, para todo $J \simeq L$ Lema 2.1, por lo tanto, $L_1B = (0)$ lo cual implica, en particular, que $L_1L_1 = (0)$. Esto no sucede, ya que L_1 contiene un elemento idempotente, como lo muestra el Teorema 2.3. El argumento implica que $L_1 \simeq L$ así, por el Lema 2.3, se sigue que $B_1 = B$, por lo tanto B es minimal. □

Dada una descomposición de un anillo semisimple R como suma directa de ideales minimales a izquierda, reordenando de ser necesario, podemos agrupar ideales de la siguiente forma:

$$R = \underbrace{L_{11} \oplus \cdots \oplus L_{1r_1}} \oplus \underbrace{L_{21} \oplus \cdots \oplus L_{2r_2}} \oplus \cdots \oplus \underbrace{L_{s1} \oplus \cdots \oplus L_{sr_s}} \tag{2.2}$$

donde $L_{ij} \simeq L_{ik}$ y $L_{ij}L_{kh} = (0)$, si $i \neq k$, esto por el Lema 2.1. Además, se sigue de la Proposición 2.2 que todo ideal minimal a izquierda es isomorfo a un ideal en la descomposición de R dada anteriormente.

Teorema 2.5. *Con la notación anterior, sea A_i la suma de todos los ideales isomorfos a L_{i_1}, $1 \leq i \leq s$. Entonces:*

(i) Cada A_i es un ideal bilateral minimal de R.

(ii) $A_iA_j = (0)$ si $i \neq j$.

(iii) $R \oplus \oplus_{i=1}^{s} A_i$ *como anillos, donde* s *es el número de clases isomorfas de los ideales minimales a izquierda de* R.

Demostración. (i) Se sigue de la Proposición 2.3.

Para probar (ii), escribimos

$$R = (L_{11} \oplus \cdots \oplus L_{1r_1}) \oplus (L_{21} \oplus \cdots \oplus L_{2r_2}) \oplus \cdots \oplus (L_{s1} \oplus \cdots \oplus L_{sr_s})$$

como lo hicimos anteriormente. Entonces para todo elemento $x \in R$ puede ser escrito de la forma $x = x_{11} + \cdots + x_{1r_1} + \cdots + x_{s1} + \cdots + x_{sr_s}$, con $x_{ij} \in L_{ij}$. Sea $y_i = x_{i1} + \cdots + x_{ir_i}$, $1 \leq i \leq s$. Entonces $y_i \in A_i$, $1 \leq i \leq s$ y $x = y_i + \cdots + y_s$. Esto muestra que $R = A_1 + \cdots + A_s$. Note que (ii) se sigue directamente de la definición de los A_i y del Lema 2.1. Por (i), $R = A_1 + A_2 + \cdots + A_s$, además de (ii) si $i \neq j$, $A_i A_j = \{0\}$, luego de la definición de suma directa se sigue (iii). □

Definición 2.6. *Un anillo* R *es llamado* ***simple****, si sus únicos ideales bilaterales son* (0) *y* R.

Corolario 2.4. *Los ideales* A_i, $1 \leq i \leq s$, *definidos en el Teorema 2.5 son anillos simples.*

Demostración. Dado que A_i, $1 \leq i \leq s$, es un ideal bilateral minimal de R, es suficiente probar que cualquier ideal bilateral B_i de A_i es también un ideal de R. Esto implicaría inmediatamente que $B_i = (0)$ o bien $B_i = A_i$.

Sea $b \in B_i$ y $r \in R$. Claramente $r = x_1 + \cdots + x_s$, con $x_j \in A_j$, $1 \leq j \leq s$. Entonces, $rb = \sum_{j=1}^{s} x_j b$ y como $x_j b = 0$ si $j \neq i$, tenemos que $rb = x_j b \in B_j$, pues B_j es ideal de A_i. De forma similar se prueba que $br \in B_i$, así $B_i \leq R$. □

Debemos resaltar que los ideales bilaterales construidos anteriormente determinan completamente todos los ideales bilaterales de R.

Proposición 2.4. *Sea* $R = \oplus_{i=1}^{s} A_i$ *la descomposición de un anillo semisimple* R *como suma directa de ideales bilaterales minimales, entonces*

(i) Todo ideal bilateral I *de* R *puede ser escrito de la forma* $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, $1 \leq i_1 \leq \cdots \leq i_t \leq s$.

(ii) Si $R = \oplus_{i=1}^{s} B_i$ *otra descomposición de* R *como suma directa ideales bilaterales minimales, entonces* $r = s$ *y después de una reordenamiento de los índices,* $A_i = B_i$, $i = 1, 2, \ldots, s$.

Demostración. Sea I un ideal bilateral de R. Entonces $I = \oplus_{i=1}^{s} (A_i \bigcap I)$. Como los A_i son minimales, se cumple (i). Por la misma razón cada B_j es igual a algún A_i y viceversa, luego necesariamente, $r = s$ y $A_i = B_i$ (reordenando de ser necesario), para todo i. □

Definición 2.7. *Los únicos ideales bilaterales minimales de un anillo semisimple R son llamados las* ***componentes simples*** *de R.*

Nota: La idea es relacionar la descomposición de R como suma directa de ideales bilaterales a una familia de idempotentes.

De la ecuación (2.2), tenemos que

$$R = \bigoplus_{j_1=1}^{r_1} L_{1j_1} \bigoplus_{j_2=1}^{r_2} L_{2j_2} \bigoplus \cdots \bigoplus_{j_s=1}^{r_s} L_{sj_s},$$

$L_{ij} = Re_{ij}$, donde L_{ij} ideales minimales a izquierda y e_{ij} una familia completa de idempotentes ortogonales primitivos $1 \leq i \leq r$, $1 \leq j \leq r_i$.

Para todo índice i, $e_i = e_{i1} + e_{i2} + \cdots + e_{ir_i}$, entonces

$$1 = (e_{11} + e_{12} + \cdots + e_{1r_1}) + (e_{21} + e_{22} + \cdots + e_{2r_2}) + \cdots + (e_{s1} + e_{s2} + \cdots + e_{sr_s}),$$

por tanto,

$$1 = e_1 + e_2 + \cdots + e_s.$$

Además,

$$\begin{aligned} e_i^2 &= e_i e_i \\ &= (e_{i1} + e_{i2} + \cdots + e_{ir_i})(e_{i1} + e_{i2} + \cdots + e_{ir_i}) \\ &= (e_{i1}^2 + e_{i1}e_{i2} + \cdots + e_{ir_1}e_{ir_i}) + \cdots + (e_{ir_i}e_{i1} + e_{ir_i}e_{i2} + \cdots + e_{ir_i}^2) \\ &= (e_{i1} + e_{i2} + \cdots + e_{ir_i}) \\ &= e_i. \end{aligned}$$

Esto es, $e_i^2 = e_i$

$$\begin{aligned} e_i e_j &= (e_{i1} + e_{i2} + \cdots + e_{ir_i})(e_{j1} + e_{j2} + \cdots + e_{jr_j}) \\ &= (e_{i1}e_{j1} + e_{i1}e_{j2} + \cdots + e_{ir_1}e_{jr_j}) + \cdots + (e_{ir_i}e_{j1} + e_{ir_i}e_{j2} + \cdots + e_{ir_i}e_{jr_j}) \\ &= (0 + 0 + \cdots + 0) \\ &= 0, \end{aligned}$$

luego, $e_i e_j = 0$, si $i \neq j$.

Afirmación:

$$Re_i = \oplus_{j=1}^{r_i} Re_{ij}, 1 \leq i \leq s$$

En efecto, tenemos que $x \in \bigoplus_{j=1}^{r_i} Re_{ij}$, entonces $x = x_{i1}e_{i1} + \cdots + x_{ir_i}e_{ir_i}$, así

$$\begin{aligned} xe_i &= (x_{i1}e_{i1} + \cdots + x_{ir_i}e_{ir_i})(e_{i1} + e_{i2} + \cdots + e_{ir_i}) \\ &= (x_{i1}e_{i1} + \cdots + x_{ir_i}e_{ir_i}) \\ &= x. \end{aligned}$$

esto es, $xe_i = x$.

Teorema 2.6. *Sea $R = \oplus_{i=1}^{s} A_i$ la descomposición de un anillo semisimple R como suma directa de ideales bilaterales minimales. Entonces, existe una familia $\{e_1, \ldots, e_s\}$ de elementos de R tal que:*

(i) $e_i \neq 0$ *es un idempotente central,* $1 \leq i \leq s$.

(ii) Si $i \neq j$ *entonces* $e_i e_j = 0$.

(iii) $1 = e_1 + \cdots + e_s$

(iv) e_i *no puede ser escrito como* $e_i = e_i{}' + e_i i''$, *donde* $e_i{}', e_i{}''$ *son idempotentes centrales tales que* $e_i{}', e_i{}'' \neq 0$ *y* $e_i{}' e_i{}'' = 0$, $1 \leq i \leq s$.

Demostración. La prueba de este resultado es análoga a la del Teorema 2.4 excepto por el hecho que además son idempotentes centrales. Para cada $x \in R$ tenemos, de (iii), que $x = \sum_{i=1}^{s} xe_1 = \sum_{i=1}^{s} e_i x$. Recordemos que los A_i son ideales bilaterales y que la suma es directa , así $xe_i = e_i x$, como deseábamos. □

Definición 2.8. *Los elementos $\{e_1, \ldots, e_s\}$ del teorema anterior son llamados los* ***idempotentes centrales primitivos*** *de R.*

Como vimos en la Proposición 2.4, todo anillo semisimple R puede ser escrito como la suma directa de sus componentes simples, es decir,

$$R = \bigoplus_{i=1}^{s} A_i, \tag{2.3}$$

donde para cada $i = 1, 2, \ldots, s$, es un ideal bilateral minimal único.

El siguiente teorema clásico en la teoría de anillos y álgebras, llamado Teorema de Wedderbunr-Artin[1], nos permite dar una descripción exacta de los anillos simples dados en la ecuación (2.3).

[1]Resultado original de J. Wedderburn (1882-1948), y extendido luego a anillos artinianos por E. Artin (1898-1962).

Teorema 2.7. *(Teorema de Wedderburn-Artin)*
Un anillo R es semisimple si y solo si es un suma directa de álgebras de matrices sobre anillos de división, es decir

$$R \simeq M_{n_1}(D_1) \bigoplus \cdots \bigoplus M_{n_s}(D_s).$$

Mas aún, si

$$M_{n_1}(D_1) \bigoplus \cdots \bigoplus M_{n_s}(D_s \simeq R \simeq M_{m_1}(D'_1) \bigoplus \cdots \bigoplus M_{m_r}(D'_r)$$

donde D_i, D'_j son anillos de división con $1 \leq i \leq s$ y $1 \leq j \leq r$. Entonces, $s = r$ y, para una permutación adecuada de índices, se tiene que $n_i = m_i$ y $D_i \simeq D'_i$.

Demostración. [12, Teorema 2.6.18] □

2.3. Semisimplicidad en RG

Ahora, queremos determinar las condiciones necesarias y suficientes sobre R y G para que el anillo de grupo RG sea semisimple.

Definición 2.9. *Sea X un subconjunto de un anillo de grupo RG, el **anulador izquierdo** de X es el conjunto*

$$Ann_l(X) = \{\alpha \in RG : \alpha x = 0, \forall x \in X\}$$

*Análogamente, definimos el **anulador derecho** de X como*

$$Ann_l(X) = \{\alpha \in RG : x\alpha = 0, \forall x \in X\}$$

Definición 2.10. *Dado un anillo de grupo RG y un subconjunto finito X del grupo G, denotaremos por $\widehat{X}$ el siguiente elemento de RG:*

$$\widehat{X} = \sum_{x \in X} x.$$

Lema 2.4. *Sean H un subgrupo de un grupo G y R un anillo. Entonces $Ann_r(\triangle(G,H)) \neq (0)$ si y solo si H es finito. En este caso, tenemos que*

$$Ann_r(\triangle(G,H)) = \widehat{H} \cdot RG.$$

Además, si $H \lhd G$ entonces el elementos $\widehat{H}$ es central en RG y tenemos

$$Ann_r(\triangle(G,H)) = Ann_l(\triangle(G,H)) = RG \cdot \widehat{H}.$$

Demostración. Supongamos que $Ann_r(\triangle(G,H)) \neq (0)$ y escojamos $\alpha = \sum_{g\in G} a_g g \neq 0$ en $Ann_r(\triangle(G,H))$. Para cada elemento $h \in H$ tenemos que $(h-1)\alpha = 0$, luego $h\alpha = \alpha$. Esto es,

$$\alpha = \sum_{g\in G} \alpha_g g = \sum_{g\in G} \alpha_g hg.$$

Tomemos $g_0 \in supp(\alpha)$. Entonces $\alpha_{g_0} \neq 0$ y así la ecuación anterior muestra que $hg_0 \in supp(\alpha)$ para todo $h \in H$. Dado que $supp(\alpha)$ es finito, esto claramente implica que H debe ser finito.

Note que el argumento anterior muestra que, cada vez que $g_0 \in supp(\alpha)$ el coeficiente de cada elemento de la forma hg_0 es igual al coeficiente de g_0, por lo cual podemos escribir α de la siguiente forma:

$$\alpha = a_{g_0}\widehat{H}g_0 + a_{g_1}\widehat{H}g_1 + \cdots + a_{g_t}\widehat{H}g_t = \widehat{H}\beta,\ \beta \in RG.$$

Esto muestra que, si H es finito, entonces $Ann_r(\triangle(G,H)) \subset \widehat{H} \cdot RG$. La otra contenencia es inmediata ya que $h\widehat{H} = \widehat{H}$ implica que $(h-1)\widehat{H} = 0$ para todo $h \in H$.

Finalmente, si $H \lhd G$, $\forall g \in G$ tenemos que $g^{-1}Hg = H$; por consiguiente $g^{-1}\widehat{H}g = \sum_{x\in H} g^{-1}xg = \sum_{x\in H} x = \widehat{H}$. Por lo tanto, $\widehat{H}g = g\widehat{H}$, para todo $g \in G$, lo cual muestra que $\widehat{H}$ es central en G. Consecuentemente $RG \cdot \widehat{H} = \widehat{H} \cdot RG$ y el resultado se sigue. □

Corolario 2.5. *Sea G un grupo finito. Entonces:*

(i) $Ann_l(\Delta(G)) = Ann_r(\Delta(G)) = R \cdot \widehat{G}$.

(ii) $Ann_r(\Delta(G)) \bigcap \Delta(G) = \{a\widehat{G} : a \in R, a|G| = 0\}$.

Demostración. Po lo anterior con $H = G$

$$Ann_l(\Delta(G)) = Ann_r(\Delta(G)) = RG \cdot \widehat{G}.$$

además, si $g \in G$ entonces $g \cdot \widehat{G} = \widehat{G}$, por tanto $RG \cdot \widehat{G} = R \cdot \widehat{G}$. Luego, (i) se sigue.

Para probar (ii) notemos que $\alpha = a\widehat{G} \in \Delta(G)$ si y solo si

$$\epsilon(\alpha) = \epsilon(a\sum_{i=1}^{l} g_i) = a\epsilon(\sum_{i=1}^{l} g_i) = a\epsilon(\widehat{G}) = a|G| = 0.$$

□

Lema 2.5. *Sea I un ideal bilateral de un anillo R. Suponga que existe un ideal a izquierda J tal que $R = I \oplus J$ (como R-módulos). Entonces $J = Ann_r(I)$ y es por lo tanto J un ideal bilateral.*

Demostración. Tomemos elementos arbitrario $x \in J$, $y \in J$. Dado que J es un ideal a izquierda e I es bilateral, tenemos que $yx \in J \bigcap I = (0)$. Lo cual implica que $yx = 0$ y por lo tanto $x \in Ann_r(I)$.

Recíprocamente, sea $x \in Ann_r(I)$. Escribimos $1 = e_1 + e_2$, con $e_1 \in I$, $e_2 \in J$. Entonces $x = 1 \cdot x = e_1x + e_2x$. Dado que $x \in Ann_r(I)$, sabemos que $e_1x = 0$, por lo cual $x = e_2x \in J$, así $Ann_r(I) = J$. □

Lema 2.6. *Si el ideal de aumento $\triangle(G)$ es sumando directo de RG como un R-módulo entonces G es finito y $|G|$ es invertible in R.*

Demostración. Supongamos que $\triangle(G)$ es sumando directo de RG. Entonces, el Lema 2.5 muestra que $Ann_r(\triangle(G)) \neq 0$ y por lo tanto G es finito, además $Ann_r(\triangle(G)) = \widehat{G}RG = \widehat{G}R$.

Escribiremos $RG = \triangle(G) \oplus Ann_r(\triangle(G))$ y $1 = e_1 + e_2$ con $e_1 \in \triangle(G)$ y $e_2 \in Ann_r(\triangle(G))$. Entonces $1 = \epsilon(1) = \epsilon(e_1) + \epsilon(e_2)$. Dado que $e_2 = a\widehat{G}$, para algún $a \in R$, tenemos que $a\epsilon(\widehat{G}) = 1$; por lo tanto $a|G| = 1$, esto muestra que $|G|$ es invertible en R y que $|G|^{-1} = a$. □

De lo anterior podemos determinar las condiciones necesarias y suficientes sobre R y G para el anillo de grupo RG sea semisimple.

Teorema 2.8. *(Teorema de Maschke)*
Sea G un grupo y R un anillo. Entonces, el anillo de grupo RG es semisimple si y solo si se cumplen las siguiente condiciones.

(i) R es semisimple.

(ii) G es finito.

(iii) $|G|$ es una unidad en R.

Demostración. Sunpongamos que RG es semisimple. Sabemos que $R \simeq RG/\triangle(G)$. Dado que los anillos factores de anillos semisimples son también semisimples, se sigue inmediatamente que R es semisimple. Como la semisimplicidad de RG implica que $\triangle(G)$ es sumando directo, el Lema 2.6 muestra que se cumplen las condiciones (ii) y (iii).

Recíprocamente, asumiendo que la condiciones (i), (ii) y (iii) se cumplen y tomando M un RG-submódulo de RG. Dado que R es semisimple, se sigue que RG es semisimple como un R-módulo. Por lo cual, existe un R-submódulo N de RG tal que

$$RG = M \oplus N.$$

Sea $\pi : RG \to M$ la proyección natural asociada a la suma directa. Definimos $\pi^* : RG \to M$ mediante un proceso de promedio,

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx), \forall x \in RG.$$

Si probamos que π^* es un RG-homomorfismo tal que $(\pi^*)^2 = \pi^*$ y $Im(\pi^*) = M$, entonces $Ker(\pi^*)$ sera un RG-submódulo tal que $RG = M \oplus Ker(\pi^*)$ y el teorema quedaría probado.

Como π^* es un R-homomorfismo, para mostrar que también es un RG-homomorfismo, será suficiente probar que

$$\pi^*(ax) = a\pi^*(x),\ \forall x \in RG,\ \forall a \in G.$$

Tenemos que

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Cuando g recorre todo los elemento de G, el producto ga también recorre todos estos elementos, por lo tanto

$$\pi^*(ax) = a\frac{1}{|G|} \sum_{t \in G} t^{-1}\pi(tx) = a\pi^*(x) :$$

Como π es una proyección sobre M, sabemos que $\pi(m) = m$, para todo $m \in M$. Además, dado que M es un RG-módulo, tenemos que $gm \in M$, para todo $g \in G$. Por lo tanto

$$\pi^*(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gm) = \frac{1}{|G|} \sum_{g \in G} g^{-1}gm = m.$$

Dado un elemento arbitrario $x \in RG$, tenemos que $\pi(gx) \in M$, luego $\pi^*(x) \in M$ y e sigue que $Im(\pi^*) \subset M$. Consecuentemente, $\pi^*(\pi^*(x)) = \pi^*(x)$ para todo $x \in RG$, esto es, $(\pi^*)^2 = \pi^*$.

Finalmente, el hecho que $\pi^*(m) = m$, para todo $m \in M$ también muestra que $M \subset Im(\pi^*)$. □

El caso en el que $R = \mathbb{F}$, F es siempre semisimple y $|G|$ es invertible en $\mathbb{F}$ si y solo si $|G| \neq 0$ en $\mathbb{F}$, es decir, si y solo si $char(\mathbb{F}) \nmid |G|$ [2]. Como consecuencia directa del teorema anterior establecemos el siguiente resultado.

Corolario 2.6. *Sea G un grupo finito y $\mathbb{F}$ un cuerpo. Entonces, $\mathbb{F}G$ es semisimple si y solo si $char(\mathbb{F}) \nmid |G|$.*

Una interpretación del Teorema de Wedderburn-Artin, en este contexto nos dará gran de información sobre la estructura del álgebra de grupo.

Teorema 2.9. *Sea G un grupo finito y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Entonces:*

(i) FG es suma directa de un número finito de ideales bilaterales $\{B_i\}_{1 \leq i \leq r}$, las componentes simples de $\mathbb{F}G$. Cada B_i es un anillo simple.

(ii) Cualquier ideal bilateral de $\mathbb{F}G$ es suma directa de algunos de los miembro de la familia $\{B_i\}_{1 \leq i \leq r}$.

(iii) Cada componente simple B_i es isomorfa a un anillo de matrices de la forma $M_{n_i}(D_i)$, donde D_i es un anillo con división que contiene una copia isomorfa de $\mathbb{F}$ en su centro, y el isomorfismo

$$FG \overset{\phi}{\simeq} \oplus_{i=1}^{r} M_{n_i}(D_i)$$

es un isomorfismo de $\mathbb{F}$-álgebras.

(iv) En cada anillo de matrices $M_{n_i}(D_i)$, el conjunto

$$I_i = \left\{ \begin{bmatrix} x_1 & 0 & \dots & 0 \\ x_2 & 0 & \dots & 0 \\ & & \dots & \\ x_{n_i} & 0 & \dots & 0 \end{bmatrix} : x_1, x_2, \dots, x_{n_i} \in D_i \right\} \simeq D_i^{n_i}$$

es un ideal a izquierda.

Dado $x \in \mathbb{F}G$, consideremos $\phi(x) = (\alpha_1, \dots, \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$ y definimos el producto de x por un elemento $m_i \in I_i$ por $xm_i = \alpha_i m_i$. Con esta definición, I_i se convierte en un $\mathbb{F}G$-módulo simple, entonces

(v) $I_i \not\simeq I_j$, si $i \neq j$.

(vi) Cualquier $\mathbb{F}G$-módulo simple es isomorfo a algún I_i, $1 \leq i \leq r$.

[2] La característica de un cuerpo $\mathbb{F}$ ($char(\mathbb{F})$) se define como el menor entero positivo n tal que $n \cdot 1 = 0$, o cero si tal entero n no existe.

Corolario 2.7. *Sea G un grupo finito y $\mathbb{F}$ un cuerpo algebraicamente cerrado, es decir, $\bar{\mathbb{F}} = \mathbb{F}$, tal que $char(\mathbb{F}) \nmid |G|$. Entonces:*

$$\mathbb{F}G \simeq \oplus_{i=1}^{r} M_{n_i}(\mathbb{F})$$

y $n_1^2 + n_2^2 + \cdots + n_r^2 = |G|$.

Demostración. Dado que $char(\mathbb{F}) \nmid |G|$, tenemos que

$$KG \simeq \oplus_{i=1}^{r} M_{n_i}(D_i),$$

donde D_i es un anillo con división que contiene una copia de $\mathbb{F}$ en su centro.

Si calculamos la dimension sobre $\mathbb{F}$ en ambos lados de la última expresión, tenemos que

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : \mathbb{F}],$$

y se sigue que cada anillo con división es de dimensión finita sobre $\mathbb{F}$. Como $\mathbb{F}$ es algebraicamente cerrado, tenemos que $D_i = \mathbb{F}$, $1 \leq i \leq r$. □

2.4. Álgebras de grupos abelianos

Ahora haremos una descripción de los anillos de grupos abelianos finitos G sobre un cuerpo $\mathbb{F}$ tal que $char(\mathbb{F}) \nmid |G|$. Esta caracterización fue introducida por S. Perlis y G. Walker. Empezaremos por el caso cuando G es cíclico, asumiendo que $G = \langle a : a^n = 1 \rangle$ y que $\mathbb{F}$ es un cuerpo tal que $char(\mathbb{F}) \nmid |G|$. Considere la siguiente aplicación $\phi : \mathbb{F}[X] \to \mathbb{F}G$ dada por:

$$f \in \mathbb{F}[X] \mapsto f(a) \in \mathbb{F}G.$$

Claramente, ϕ es un epimorfismo de anillos, entonces por el Teorema 1.10

$$\mathbb{F}G \simeq \frac{\mathbb{F}[X]}{Ker(\phi)},$$

donde $Ker(\phi) = \{f \in \mathbb{F}[X] : f(a) = 0\}$. Dado que $\mathbb{F}[X]$ es un dominio de ideales principales, $Ker(\phi)$ es un ideal generado por un polinomio mónico f_0; de menor grado tal que $f(a) = 0$. Como $a^n = 1$, entonces $(x^n - 1) \in Ker(\phi)$. Note que si $f(x) = \sum_{i=0} r k_i x^i$ es un polinomio de grado $r < n$, tenemos que $f(a) = \sum_{i=0}^{r} k_i a^i \neq 0$ puesto que los elementos $\{1, a, a^2, \ldots, a^r\}$ son

linealmente independientes sobre $\mathbb{F}$. Por lo tanto $Ker(\phi) = \langle x^n - 1 \rangle$, así tenemos que

$$\frac{\mathbb{F}[x]}{< x^n - 1 >} \simeq \mathbb{F}G \tag{2.4}$$

Sea $x^n - 1 = f_1 f_2 \cdots f_t$ la descomposición de $x^n - 1$ como producto de polinomio irreducibles en $\mathbb{F}[X]$. Como asumimos que $char(\mathbb{F}) \nmid n$, este polinomio es separable y por lo tanto, $f_i \neq f_j$ si $i \neq j$. Luego podemos escribir:

$$KG \simeq \frac{\mathbb{F}[X]}{(f_1)} \bigoplus \frac{\mathbb{F}[X]}{(f_2)} \bigoplus \cdots \bigoplus \frac{\mathbb{F}[X]}{(f_t)}. \tag{2.5}$$

Bajo este isomorfismo, el generador a enviado al elemento

$$(x + (f_1), \ldots, x + (f_t)$$

Ahora, si ζ_i denota una raíz de f_i, $1 \leq i \leq t$, entonces tenemos que $\frac{\mathbb{F}[X]}{(f_i)} \simeq \mathbb{F}(\zeta_i)$, consecuentemente:

$$\mathbb{F}G \simeq \mathbb{F}(\zeta_1) \oplus \mathbb{F}(\zeta_2) \oplus \cdots \oplus \mathbb{F}(\zeta_t). \tag{2.6}$$

Como todos lo elementos ζ_i, $1 \leq i \leq t$, son raíces de $x^n - 1$, tenemos mostrado que $\mathbb{F}G$ es isomorfo a la suma directa de la extensiones ciclotómicas de $\mathbb{F}$; bajo este isomorfismo, el elemento a será enviado al elemento $(\zeta_1, \zeta_2, \ldots, \zeta_t)$.

Ejemplo 2.1.

(a) Sea $G = \langle a : a^7 = 1 \rangle$ y $\mathbb{F} = \mathbb{Q}$ En este caso, la descomposición de $x^7 - 1$ en $\mathbb{Q}[x]$ es

$$x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

Por lo tanto, si ζ denota un raíz primitiva de la unidad de orden 7, tenemos que

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta)$$

(b) Sea $G = \langle a : a^6 = 1 \rangle$ y $\mathbb{F} = \mathbb{Q}$ La descomposición de $x^6 - 1$ como producto de polinomios irreducibles en $\mathbb{Q}[x]$ es

$$x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1).$$

Por lo tanto

$$\mathbb{Q}G \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(\frac{-1 + i\sqrt{3}}{2}) \oplus \mathbb{Q}(\frac{1 + i\sqrt{3}}{2})$$

Queremos dar una descripción más precisa de $\mathbb{F}G$ en el caso general. Para esto, calcularemos todos los sumandos directos en la descomposición de $\mathbb{F}G$.

Recordemos que, para un entero positivo d, el **polinomio ciclotómico**, denotado por Φ_d, es el producto $\Phi_d = \prod_j (x - \zeta_j)$, donde ζ_j recorre todas las raíces primitivas de la unidad de orden d. Además, sabemos que $x^n - 1 = \prod_{d|n} \Phi_d$, el producto de todos los polinomios ciclotómicos Φ_d en $\mathbb{F}[x]$, donde d es divisor de n. Para cada d, sea $\Phi_d = \prod_{i=1}^{a_d} f_{d_i}$ la descomposición de Φ_d como producto de polinomios irreducibles en $\mathbb{F}[x]$.

Entonces, la descomposición de $\mathbb{F}G$ puede ser escrita como:

$$\mathbb{F}G \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \frac{\mathbb{F}[x]}{(f_{d_i})} \simeq \bigoplus_{d|n} \bigoplus_{i=1}^{a_d} \mathbb{F}(\zeta_{d_i}),$$

donde ζ_{d_i} denota una raíz de f_{d_i}, $1 \leq i \leq a_d$. Para d fijo, todos los elementos ζ_{d_i} son raíces primitivas de la unidad de orden d. Por consiguiente, todo cuerpo de la forma $\mathbb{F}(\zeta_{d_i})$, $1 \leq i \leq a_d$, son iguales entre sí y podemos escribir

$$\mathbb{F}G \simeq \bigoplus_{d|n} a_d \mathbb{F}(\zeta_d),$$

donde ζ_d es un raíz primitiva de la raíz de orden d y $a_d K(\zeta_d)$ denota la suma directa de a_d cuerpos diferentes, todos los cuerpos isomorfos a $\mathbb{F}(\zeta_d)$.

Además, como $grd(f_{d_i}) = [\mathbb{F}(\zeta_d) : \mathbb{F}]$, veamos que todos los polinomios f_{d_i}, $1 \leq i \leq a_d$, tienen el mismo grado. Por lo tanto,

$$\phi(n) = a_d[\mathbb{F}(\zeta_d) : \mathbb{F}],$$

donde ϕ denota la función de Euler; definida por

$$\phi(d) = |\{n \in \mathbb{Z} : 1 \leq n < d, gcd(n, d) = 1\}|.$$

Como G es un grupo cíclico de orden n, para cada divisor d de n, el número de elementos de orden d en G, que denotaremos por n_d, es precisamente $\phi(d)$. Luego, podemos escribir

$$a_d = \frac{n_d}{[\mathbb{F}(\zeta_d) : \mathbb{F}]}.$$

Ejemplo 2.2. *Sea $\langle a : a^n = 1 \rangle$ un grupo cíclico de orden n y tomemos $\mathbb{F} = \mathbb{Q}$. Es bien sabido*

que el polinomio $x^n - 1$ se descompone en $\mathbb{Q}[x]$ como el producto de polinomios ciclotómicos

$$x^n - 1 = \prod_{d|n} \Phi(x)$$

y estos son irreducible. Por lo tanto, en este caso, la descomposición de $\mathbb{Q}\langle a\rangle$ es

$$\mathbb{Q}\langle a\rangle \simeq \bigoplus_{d|n} \mathbb{Q}(\zeta_d).$$

Note que, como antes, en este isomorfismo el generador a corresponde a la tupla cuyas entradas son raíces primitivas de la unidad de orden d, donde d recorre todos los divisores de n.

Finalizaremos esta sección mostrando que la descripción obtenida anteriormente puede ser extendida a anillos de grupo de un grupo abeliano finito arbitrario.

Teorema 2.10. *(Perlis-Walker)*
Sea G u grupo abeliano finito, de orden n, y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid n$, entonces

$$KG \simeq \bigoplus_{d|n} a_d K(\zeta_d)$$

donde ζ_d denota una raíz primitiva de la unidad de orden d y $a_d = \frac{n_d}{[\mathbb{F}(\zeta_d):\mathbb{F}]}$, donde n_d denota el número de elemento de orden d en G.

Demostración. Procederemos por inducción sobre el orden de G. Asumamos que el resultado se verifica para todo los grupo abelianos de orden menos que n. Si G es cíclico, ya lo tendríamos mostrado el teorema. En caso contrario, podemos usar el Teorema fundamental de los grupos abelianos finitos, para escribir $G = G_1 \times H$, donde H es cíclico y $|G_1| = n_1 < n$. Por hipótesis de inducción, podemos escribir $\mathbb{F}G_1 = \oplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})$, donde $a_d = \frac{n_{d_1}}{[\mathbb{F}(\zeta_{d_1}):\mathbb{F}]}$ y n_{d_1} denota el número de elementos de orden d_1 en G_1. Además, dado que $G = G_1 \times H$ tenemos que

$$\mathbb{F}G \simeq \mathbb{F}(G_1 \times H) \simeq (\mathbb{F}G_1)H \simeq \left(\bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})\right) H \simeq \bigoplus_{d_1|n_1} a_{d_1}\mathbb{F}(\zeta_{d_1})H.$$

Ahora, descomponiendo cada sumando directo, tenemos que

$$\mathbb{F}G \simeq \bigoplus_{d_1|n_1} \bigoplus_{d_2||H|} a_{d_1}a_{d_2}\mathbb{F}(\zeta_{d_1}, \zeta_{d_2}),$$

donde $a_{d_2} = \frac{n_{d_2}}{[\mathbb{F}(\zeta_{d_1},\zeta_{d_2}):\mathbb{F}(\zeta_{d_1})]}$ y n_{d_2} denota el número de elementos de orden d_2 en H.

Si tomamos $d = lmc(d_1, d_2)$, tenemos que $\mathbb{F}(\zeta_{d_1}, \zeta_{d_2}) = \mathbb{F}(\zeta_d)$. Por lo tanto

$$\mathbb{F}G \simeq \bigoplus_{d|n} a_d \mathbb{F}(\zeta_d),$$

con $a_d = \sum a_{d_1} a_{d_2}$, donde la suma es tomada sobre los pares d_1, d_2 tales que $lcm(d_1, d_2) = d$. Como $[\mathbb{F}(\zeta_d) : \mathbb{F}] = [\mathbb{F}(\zeta_{d_1}, \zeta_{d_2}) : \mathbb{F}(\zeta_{d_1})][\mathbb{F}(\zeta_{d_1}) : \mathbb{F}]$, tenemos que

$$a_d[\mathbb{F}(\zeta_{d_1}) : \mathbb{F}] = \sum_{d_1, d_2} a_{d_1} a_{d_2} [\mathbb{F}(\zeta_{d_1}, \zeta_{d_2}) : \mathbb{F}(\zeta_{d_1})][\mathbb{F}(\zeta_{d_1}) : \mathbb{F}] = \sum_{d_1, d_2} n_{d_1} n_{d_2}.$$

Finalmente, como $G = G1 \times H$, cada elemento $g \in G$ puede ser escrito como $g = g_1 h$, con $g_1 \in G_1$ y $h \in H$. Además, es fácil ver que $o(g) = lcm(o(g_1), h)$. Por lo tanto, $\sum_{d_1, d_2} n_{d_1} n_{d_2} = n_d$, el número de elemento de orden d en G, así se tiene

$$a_d = \frac{n_d}{[\mathbb{F}(\zeta_d) : \mathbb{F}]}.$$

□

Corolario 2.8. *Sea G un grupo abeliano finito de orden n, entonces*

$$\mathbb{Q}G \simeq \bigoplus_{d|n} a_d \mathbb{Q}(\zeta_d)$$

donde ζ_d denota una raíz primitiva de la unidad de orden d y a_d es el número de subgrupos cíclicos de G.

Demostración. Tenemos que mostrar que $\frac{a_d}{[\mathbb{Q}(\zeta_d):\mathbb{Q}]}$ donde n_d es el número de elemento de orden d en G.

Ahora, $[\mathbb{Q}(\zeta_d) : \mathbb{Q}] = \phi(d)$. Note que el número de generadores de un grupo cíclico de orden d es precisamente $\phi(d)$, así $\frac{n_d}{\phi(d)}$ es el número de subgrupos cíclicos de orden d en G. □

Corolario 2.9. *Sea G un grupo abeliano finito de orden n y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid n$. Si $\mathbb{F}$ contiene un raíz primitiva de la unidad de orden n, entonces:*

$$\mathbb{F}G \simeq \underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{n}$$

Demostración. Si $\mathbb{F}$ contiene una raíz primitiva de la unidad de orden n, entonces $\mathbb{F}(\zeta_d) = \mathbb{F}$, para todo $d \mid n$ y el corolario se sigue directamente del teorema anterior. Además, dado que la dimensiones de $\mathbb{F}G$ y $\underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{n}$ son iguales, el número de sumandos directos es n. □

Si G y H son grupos isomorfos, es evidente que las álgebras de grupo RG y RH sobre un anillo R son isomorfas. Sin embargo, el recíproco no es del todo cierto. Ahora, estamos listo para dar un contra ejemplo de esta declaración. Si G y H son grupo abelianos no isomorfos de igual orden n y $\mathbb{F}$ un cuerpo tal que $char(\mathbb{F}) \nmid n$, el cual contiene una raíz primitiva de la unidad de orden n, entonces del lema procedente se tiene que

$$\mathbb{F}G \simeq \underbrace{\mathbb{F} \oplus \cdots \oplus \mathbb{F}}_{n} \simeq \mathbb{F}H.$$

Por ejemplo, si C_2 y C_4 denota los grupos cíclicos de orden 2 y 4 respectivamente, entonces para el álgebra compleja de grupos tenemos que

$$\mathbb{C}(C_2 \times C_2) \simeq \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \simeq \mathbb{C}C_4$$

Capítulo 3

Códigos

Tal vez un código, no nos parezca ser familiar, sin embargo continuamente estamos en contacto con ellos, un ejemplo sencillo de un código lo podemos apreciar en nuestros computadores, con el editor de texto Microsoft Word, cuando al escribir la palabra “Rati” y el procesador de texto detecta que esta no es un palabra del código (lengua Española), este subraya la palabra con color rojo indicando así que se encontró un error (código detector) y pide que sea escrito de nuevo (retransmitido) para lo cual se habilita una la lista de sugerencias al dar click derecho sobre la palabra, en este caso serían *Rato, Rata*, dando así solución al error. Las palabras en la lista son palabras que pertenecen al código y las más “cercanas” [1] a la palabra introducida inicialmente. Ahora si introducimos la palabra “Accion”, al dar *espacio* o *enter* el procesador de texto corrige inmediatamente a “Acción"(código corrector), puesto que “accion” no pertenece al código se detecta el error y a su vez se reemplaza por la palabra “Acción” la cual si pertenece al código.

La teoría de códigos correctores tuvo inicio en los años 40 del siglo pasado y actualmente es un campo ampliamente investigado en diversas áreas del conocimiento tales como Matemática, Ciencias de la Computación, Ingeniería Eléctrica y Estadística. El mayor objetivo es detectar cuando un mensaje, enviado mediante un canal fue recibido con algún error como lo describimos anteriormente y además ser capaz de corregirlo.

Un nombre a destacar en la teoría de códigos es Richard W. Hamming. Él se interesó por los errores que ocurrían internamente en los computadores y desarrolló un código corrector

[1] Al hablar de cercanía claramente nos referimos a una métrica entre los códigos, la cual definiremos más adelante

de un único error y códigos que detectaban hasta dos errores y corregían un único error. Su trabajo fue publicado en 1950 en *The Bell System Thechnical Journal* [9], publicación que ocurrió dos años después de la culminación de su trabajo, debido a la solicitud de una patente presentada por los Laboratorios Bell y durante los años en que tales códigos fueron elaborados, él publicó algunas notas a medida que su investigación evolucionaba. Hamming quería desarrollar un código más eficiente y se preguntó, si era posible desarrollar un código corrector de un único error donde las palabras tendrían cuatro dígitos de información y a los cuales se le adicionaban otros cuatro dígitos, llamados redundancia:

Su idea consistió, en dada una información $a_1a_2a_3a_4$ a ser trasmitida, esta es dispuesta en una matriz de 2×2, de la siguiente forma:

$$\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}.$$

Esta última matriz es ampliada a una matriz de 3×3 (sin la entrada en la posición $(3,3)$), de tal forma que cada fila y cada columna tenga un número par de elementos iguales a 1. Por ejemplo, si la información inicial es 1101, obtenemos luego del proceso respectivamente las matrices,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \rightsquigarrow \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & \end{pmatrix}.$$

La información del arreglo 3×3 puede ser escrita como una "palabra", escribiéndola por filas, como 11001110. El computador, la recibe y escribe nuevamente en forma matricial (donde los primeros tres dígitos son la primera fila, los tres siguientes la segunda y los dos últimos la tercera, faltando la posición $(3,3)$) y verifica la paridad. Si hay un error en alguno de los dígitos de información, habrán una fila y una columna erróneas. Por ejemplo, supongamos que el mensaje fue recibido con un error, llegando el mensaje 10001110, ahora al disponerlo en la matriz obtenemos:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & \end{pmatrix}$$

y verificamos inmediatamente que la paridad en la primera fila y segunda columna están erradas. Así, sabemos que el error está en la posición (1,2) y podemos corregirlo. Es fácil ver que si el error estuviera en alguno de los dígitos de redundancia, la paridad estará errada tan solo en una fila o en una columna, y también será posible detectar el error y corregirlo.

En estas mismas notas, él se pregunta si sería posible detectar y corregir un error, en una palabra con cuatro dígitos de información, usando solo tres dígitos de redundancia.

Esta pregunta fue respondida por C.E Shannon, en el artículo *A Mathematical Theory of communication* publicado también en *The Bell System Thechnical Journal* en el año 1948. Un año después J.E. Golay quien trabajaba en *Signal Corps Enginneering Laboratories at Fort Monmouth* extendió los resultados de Shannon y Hamming en su artículo titulado *Notes on Digital Coding*. Posteriormente Golay desarrolló un código que fue utilizado por la nave espacial Voyager para la transmisión de fotografías a color de Júpiter y Saturno.

3.1. Conceptos Básicos

De cierta forma, podemos decir que la construcción de códigos está inspirada en aquellos utilizados comúnmente por los seres humanos: los idiomas. En español, por ejemplo, usamos un alfabeto de 27 letras y las palabras son secuencias de letras. Es claro que el idioma español no está compuesto por todas las posibles palabras formadas a partir de las letras, de ahí que algunas de estas hacen parte del idioma y otras no.

De igual manera que en el lenguaje español, para la construcción de códigos son necesarios los siguientes elemento básicos:

(i) Un conjunto finito $\mathcal{A}$ que llamaremos *alfabeto*. Denotaremos por q al número de elementos de $\mathcal{A}$, y en este caso diremos que el códigos es q-ario.

(ii) Secuencias finitas de símbolos del alfabeto, que llamaremos *palabras*. El número de letras de una palabra es su *longitud*. Los códigos en bloque son aquellos en los que todas sus palabras tienen la misma longitud. Como todos los códigos que estudiaremos serán de esta forma, omitiremos la palabra bloque.

Un *Código q-ario de lo longitud n* será un subconjunto cualquiera de palabras de longitud n, es decir, un código $\mathcal{C}$ es un subconjunto de $\mathcal{A}^n = \underbrace{\mathcal{A} \times \mathcal{A} \times \cdots \mathcal{A}}_{n-veces}$.

El número M de elementos del código también es importante, pues cuanto mayor sea M, mayor es la cantidad de información que puede ser trasmitida. Así, un código q-ario, de longitud n que contiene M palabras es llamado (n, M)-código q-ario.

Note que, si $c \in \mathcal{C} \subset \mathcal{A}^n$, es de la forma $c = (a_1, a_2, \ldots, a_n)$, donde $a_i \in \mathcal{A}$, $1 \leq i \leq n$. Con el objetivo de no sobrecargar la notación, escribiremos a c como una secuencia de elementos en $\mathcal{A}$, es decir, de la forma $c = a_1 a_2 \ldots a_n$.

Ejemplo 3.1. *El conjunto*

$$\mathcal{C}_1 = \{00000, 01011, 10110, 11101\}$$

es un código en bloque, binario, de longitud 5 *o brevemente un* $(5, 4)$*-código binario.*

Consideremos como alfabeto $\mathbb{Z}_3 = \{0, 1, 2\}$*. El conjunto*

$$\mathcal{C}_2 = \{00012, 11022, 10101, 10201, 20202\}$$

es un código $(5, 5)$*-código ternario.*

En el diagrama (1, pág. 4), observamos que un mensaje puede ser recibido con errores, lo cual es producido por un ruido. Una forma de corregir una palabra con un error, es observando que palabra del código está más cercana a ella. Por esta razón es necesaria la siguiente definición.

Definición 3.1. *Sean* $x = x_1x_2 \dots x_n$ *y* $y = y_1y_2 \dots y_n$ *dos palabras de un código* $\mathcal{C} \subset \mathcal{A}^n$*. La* distancia de Hamming *entre* x *e* y*, denotada por* $d(x, y)$*, se define como el número de componentes en que* x *difiere de* y*, es decir,*

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

La siguiente proposición muestra que $(\mathcal{C}, d)$ es un espacio métrico.

Proposición 3.1. *La función* d *es una métrica en* $\mathcal{C}$*, es decir que para todo* x, y, z *en* $\mathcal{C}$*, satisface las siguientes propiedades.*

(i) $d(x, y) \geq 0$*.*

(ii) $d(x, y) = 0$ *si y solo si* $x = y$

(iii) $d(x, y) = d(y, x)$

(iv) $d(x, y) \leq d(x, z) + d(z, y)$

Demostración.

(i) Por definición tenemos que $d(x, y) \geq 0$.

(ii) Si $d(x, y) = 0$ entonces de la definición tenemos que x e y no difieren en ninguna de sus componentes, lo cual ocurre si y solo si $x = y$.

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

(iv) Sean $A = \{1 \leq i \leq n : x_i = y_i\}$, $B = \{1 \leq i \leq n : x_i = z_i\}$ y $C = \{1 \leq i \leq n : z_i = y_i\}$, es claro que $d(x, y) = |A^c|$, $d(x, z) = |B^c|$ y $d(z, y) = |C^c|$. Como $B \cap C \subseteq A$, $B^c \cup C^c \supseteq A^c$; por lo tanto, $|A^c| \leq |B^c| + |C^c|$.

□

Definición 3.2. *Dado un código $\mathcal{C}$ se define la distancia de $\mathcal{C}$, y se le denota por $d(\mathcal{C})$ ó $d_{\mathcal{C}}$, como la menor distancia no-nula entre sus palabras código, es decir,*

$$d(\mathcal{C}) = d_{\mathcal{C}} = \min_{x,y \in \mathcal{C}} \{d(x, y) : x, y \in \mathcal{C}, x \neq y\}$$

Veamos el siguiente ejemplo.

Ejemplo 3.2. *Sea $\mathcal{C} = \{001, 011, 111\}$ un código y supongamos que un emisor envía el mensaje 111, pero en la trasmisión de dicho mensaje, un ruido altera el mensaje, cambiando un 1 por un 0, permitiendo así que el emisor reciba el mensaje 110.*

En este caso el receptor se da cuenta que el mensaje recibido es erróneo, puesto que $110 \notin \mathcal{C}$ (Código detector), ahora puesto que $d((110), (111)) < d((110), (011)) < d((110), (001))$ el mensaje que realmente se había enviado fue 111 (Código corrector).

Pero este método no siempre nos ayuda a corregir, consideremos la situación en que el emisor envía el mensaje 111, pero en su trasmisión se altera, recibiendo así el receptor el mensaje 101, este último detecta el error puesto que $101 \notin \mathcal{C}$. Ahora veamos que:

$d((101), (001)) = 1 = d((101), (111))$*. Por tal razón, a pesar que se puede detectar el error, este no puede ser corregido.*

Para codificar y decodificar de manera más práctica y eficiente es útil dotar al alfabeto $\mathcal{A}$ de cierta estructura algebraica. Es común considerar a $\mathcal{A}$ como un cuerpo finito aunque también se le puede considerar como un anillo. De ahora en adelante, fijaremos $\mathcal{A} = \mathbb{F}_q$, el cuerpo finito de q elementos, donde q es una potencia de un primo p. El conjunto de n-cadenas $\mathcal{A}^n = \mathbb{F}_q^n$ es un espacio n-dimensional sobre $\mathbb{F}_q$, donde

$$\mathbb{F}_q^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{F}_q, 1 \leq i \leq n\}.$$

Introducimos a continuación una familia (respectivamente subfamilia) de códigos, llamados lineales (respectivamente cíclicos).

3.2. Códigos Lineales y Cíclicos

Definición 3.3.

Sea $\mathcal{A} = \mathbb{F}_q$ un alfabeto. Diremos que $\mathcal{C}$ es un (n, q^m)-código lineal q-ario, si $\mathcal{C} \subset \mathbb{F}_q^n$ es un subespacio vectorial de dimensión m.

Un código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ es cíclico si es cerrado bajo desplazamientos cíclicos, es decir,

$$c_0 c_1 \dots c_{n-1} \in \mathcal{C} \quad \Rightarrow \quad c_{n-1} c_0 \dots c_{n-2} \in \mathcal{C}$$

Uno de los objetivos de este trabajo es dar una caracterización de la construcción de los códigos cíclicos, para ello empezaremos definiendo la siguiente correspondencia:

Consideremos $\mathbb{F}_q[x]$ el anillo de polinomios con coeficientes en $\mathbb{F}_q$. Si $\mathcal{C} \subset \mathbb{F}_q^n$ es un código lineal q-ario, a cada palabra código le podemos asignar un polinomio con coeficientes en $\mathbb{F}_q$, mediante la siguiente función.

$$\begin{array}{rccc} \phi: & \mathcal{C} \subset \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q[x] \\ & c = (c_0, c_1, c_2, \dots, c_{n-1}) & \mapsto & \phi(c) = \sum_{i=0}^{n-1} c_i x^i. \end{array}$$

Consideremos $p(x) = x^n - 1 \in \mathbb{F}_q[x]$ y sea $R_n = \mathbb{F}_q[x]/\langle x^n - 1 \rangle$ el anillo cociente usual.

Sea $(c_0, c_1, \dots, c_{n-1}) \in \mathcal{C}$. Entonces

$$\begin{aligned} x(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}) &= c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n \pmod{x^n - 1} \\ &= c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1}. \end{aligned}$$

Lo cual demuestra el siguiente resultado.

Proposición 3.2. *Un código $\mathcal{C}$ es cíclico si y solo si $\phi(\mathcal{C})$ es un ideal en R_n.*

Sean $\mathbb{F}_q$ un cuerpo, C_n un subgrupo cíclico de orden n un entero positivo primo relativo con q. Dado que $\mathbb{F}_q[x]/\langle x^n - 1 \rangle \simeq \mathbb{F}C_n$, (ver ecuación 2.4, pág. 61), los códigos cíclicos pueden ser vistos como ideales en $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$ o ideales en el álgebra de grupo $\mathbb{F}C_n$.

Observación 3.1. *De la Proposición 3.2, podemos concluir que los códigos cíclicos de longitud n pueden ser vistos como ideales en FC_n. En adelante el estudio de esta monografía se basará en encontrar la forma de generar todos los códigos que existen en FC_n.*

Inicialmente Arora y Pruthi en [1], calcularon los idempotentes generadores de códigos de longitud p^n en el caso cuando $p^n = 2$, $p^n = 4$ o p es impar y el orden multiplicativo de q, módulo p^n, es $\Phi(p^n)$[2]. Y además, estudiaron el caso cuando la longitud es $2p^n$.

De forma más general, un **código abeliano** sobre un cuerpo $\mathbb{F}$ es cualquier ideal I en el álgebra de grupo $\mathbb{F}A$ de un grupo abeliano finito A ([2],[3, Section 4.8]). Un **código abeliano minimal** es un ideal I minimal en el conjunto de los ideales de $\mathbb{F}A$.

Ahora, queremos dar una construcción similar de los códigos abelianos minimales bajo las mismas condiciones. Para realizar esto, empezaremos primero por calcular el número de componentes simples de un álgebra de grupo finita FA y luego determinar las condiciones para que este número sea minimal. Tal cálculo puede obtenerse desde el Teorema de Berman y Witt (ver [4, Teoremas 21.5 & 21.25]).

3.3. Número de componentes simples

Sean $\mathbb{F}_q$ un cuerpo finito y A un grupo abeliano finito tal que $mcd(q, |A|) = 1$.[3] Entonces $\mathbb{F}A$ es semisimple, (ver Teorema 2.8). Si $\{e_1, e_2, \ldots, e_r\}$ es el conjunto de los idempotentes primitivos de $\mathbb{F}A$, se tiene que,

$$\mathbb{F}A = \bigoplus_{i=1}^{r} (\mathbb{F}A)e_i \simeq \bigoplus_{i=1}^{r} \mathbb{F}_i$$

donde $\mathbb{F}_i \simeq (\mathbb{F}A)e_i$, $1 \leq i \leq r$, son cuerpos los cuales son extensiones finitas de $\mathbb{F}$.

En [6], Ferraz dio un método general para calcular el número r de componentes simples de un álgebra de grupo semisimple. En el presente caso de álgebras de grupos finitas de grupos abelianos, presentamos una forma más simple de determinar tal número, [5, Teorema 2.1]. Tomemos

$$\mathcal{B} = \bigoplus_{i=1}^{r} \mathbb{F}e_i. \tag{3.1}$$

Note que $\mathbb{F}e_i \simeq \mathbb{F}$ como cuerpos en forma natural (via el isomorfismo $1 \mapsto 1 \cdot e_i$), el número r de componentes simples es también la dimensión de $\mathcal{B}$ como espacio vectorial sobre $\mathbb{F}$.

Lema 3.1. *Sea α un elemento de $\mathbb{F}A$. Entonces $\alpha \in \mathcal{B}$ si y solo si $\alpha^q = \alpha$*

Demostración. Tomemos $\alpha \in \mathbb{F}A$, entonces $\alpha = \sum_{i=1}^{r} \alpha_i$, con $\alpha_i = \alpha e_i \in \mathbb{F}_i, 1 \leq i \leq r$. Ahora

[2] $\Phi(n)$ determina la cantidad de números menores o iguales a n que son primos relativos con el
[3] mcd(a,b) denota el máximo común divisor entre a y b

α es un elemento de $\mathcal{B}$ si y solo si cada elemento α_i está en $\mathbb{F}e_i$ para cada índice i, como $\mathbb{F}e_i \simeq \mathbb{F}$, esto sucede si y solo si $\alpha_i^q = \alpha_i$ para todo i; es decir, si y solo si $\alpha^q = \alpha$. □

Sea g un elemento del grupo abeliano finito A. Las clases q-ciclotómicas de g es el conjunto,

$$S_g = \{g^{q^j} | 0 \leq j \leq t_g - 1\},$$

donde t_g es el menor entero positivo tal que

$$q^{t_g} \equiv 1 \pmod{o(g)},$$

y $o(g)$ denota el orden de g. Dado que $(q,\, o(g)) = 1$, siempre existirá tal número t_g. Además, si $S_g \neq S_h$, entonces $S_g \cap S_h = \emptyset$. Denotemos por $T = \{g_1, g_2, \ldots, g_s\}$ al conjunto de representantes de las clases q-ciclotómicas.

Teorema 3.1. *Sean $\mathbb{F}_q$ un cuerpo finito y A un grupo abeliano finito tal que $mcd(q, |A|) = 1$. Entonces el número de componentes simples de $\mathbb{F}A$ es igual al número de clases q-ciclotómicas de A.*

Demostración. Dado que el número de componentes simples de $\mathbb{F}A$ es igual a la dimensión de $\mathcal{B}$ como espacio vectorial sobre $\mathbb{F}$, (ver ecuación 3.1), exhibamos una base de esta subálgebra con s elementos.

Sabemos que $A \hookrightarrow \mathbb{F}A$, luego cada elemento de S_g, pertenece a $\mathbb{F}A$. Por tanto, dada una clase q-ciclotómica S_g definimos $\eta_g = \sum_{h \in S_g} h \in \mathbb{F}A$.

Afirmamos que $\mathfrak{B} = \{\eta_{g_i} : 1 \leq i \leq s\}$ es una $\mathbb{F}$-base de $\mathcal{B}$. En efecto, como A es una $\mathbb{F}$-base para $\mathbb{F}A$, y cada $S_g \subset A$, se sigue que $\mathfrak{B}$ es un conjunto linealmente independiente. Así, solo nos resta mostrar que también genera a $\mathcal{B}$. De la definición de η_{g_i}, tenemos que $\eta_{g_i}^q = \eta_{g_i}$, $1 \leq i \leq s$, y así $\mathfrak{B} \subset \mathcal{B}$.

Sea $\alpha \in \mathcal{B} = \oplus_{i=1}^{r} \mathbb{F}e_i$. Se sigue del Lema 3.1 que $\alpha^q = \alpha$. Luego, si $\alpha = \sum_{g \in A} \alpha_g g$, se tiene que

$$\alpha = \sum_{g \in A} \alpha_g g = \left(\sum_{g \in A} \alpha_g g \right)^q = \sum_{g \in A} \alpha_g^q g^q.$$

Como $\alpha_g \in \mathbb{F}$, tenemos que $\alpha_g^q = \alpha_g$ y por lo tanto

$$\alpha = \sum_{g \in A} \alpha_g g = \sum_{g \in A} \alpha_g g^q.$$

Así, para cada $g \in A$, se tiene que $\alpha_g = \alpha_{g^q} = \cdots = \alpha_{g^{q^{t_g-1}}}$ y en consecuencia

$$\alpha = \sum_{g \in T} \alpha_g \eta_g.$$

□

Perlis y Walker probaron que el número de componentes simples de un álgebra de grupo racional de un grupo abeliano finito A es igual tanto al número de subgrupos cíclicos de A como al número de sus factores cíclicos, ver [12, Corolario 3.5.5], [13].

Notemos que, si $h \in S_g$, entonces $h = g^{q^j}$ para algún j y así $h \in \langle g \rangle$, es decir, $\langle h \rangle \subset \langle g \rangle$. Como $mcd(q,\, o(g)) = 1$, tenemos que $1 = qs + o(g)r$ con $r, s \in \mathbb{Z}$. Sea $x \in \langle g \rangle$, entonces x es de la forma $x = g^t = g^{t(qs+o(g)r)} = g^{tq} = g^{q^t}$, de ahí que, $\langle h \rangle \subset \langle g \rangle$, lo que prueba que $\langle g \rangle = \langle h \rangle$. Por tanto, si $\mathcal{G}_g$ denota el conjunto de todos los generadores del grupo cíclico $\langle g \rangle$, entonces para cada clase q-ciclotómica S_g, tenemos que $S_g \subset \mathcal{G}_g$, luego es claro que el número de subgrupos cíclicos de A es una cota inferior del número de componentes simples y que esta cota es alcanzada si y solo si $S_g = \mathcal{G}_g$, para todo $g \in A$.

Para enteros positivos r y m, denotamos por $\bar{r} \in \mathbb{Z}_m$ la imagen de r en el anillo de enteros módulo m, entonces

$$\mathcal{G}_g = \{g^r | mcd(r,\, o(g)) = 1\} = \{g^r | \overline{r} \in U(\mathbb{Z}_{o(g)})\}$$

Y se tiene el siguiente resultado.

Teorema 3.2. *Sean $\mathbb{F}$ un cuerpo finito, con $|\mathbb{F}| = q$, y A un grupo abeliano finito, de exponente e, tal que $mcd(q, |A|) = 1$. Entonces $S_g = \mathcal{G}_g$, para todo $g \in A$ si y solo si $U(\mathbb{Z}_e)$ es un grupo cíclico generado por $\bar{q} \in \mathbb{Z}_e$.*

Demostración. Supongamos que $U(\mathbb{Z}_e) = \langle \bar{q} \rangle$. Para un elemento $g \in A$, por el Teorema 1.1 tenemos que $o(g)|e$ y por lo tanto $\bar{q} \in \mathbb{Z}_{o(g)}$ es un generador de $U(\mathbb{Z}_{o(g)})$. Para todo elemento h de $\mathcal{G}_g$ se tiene que $h = g^r$ para algún entero positivo r tal que $\overline{r} \in U(\mathbb{Z}_{o(g)})$, así $\overline{r} = \overline{q}^j$ para algún entero positivo j y $h = g^{q^j} \in S_g$. Esto muestra que $S_g = \mathcal{G}_g$.

Recíprocamente, supongamos que $S_g = \mathcal{G}_g$ para todo $g \in A$. Recordemos que si A es u grupo abeliano finito de exponente e entonces, existe un elemento $g_o \in A$ de orden e y, en particular, $S_{g_o} = \mathcal{G}_{g_o}$. Por lo tanto para cada entero r tal que $\overline{r}r \in U(\mathbb{Z}_e)$, tendremos que $g_o^r \in S_{g_0}$ y existe algún entero j tal que $\overline{r} = \overline{q}^j$. Luego $\overline{q}$ genera $U(\mathbb{Z}_e)$. □

Dado que $U(\mathbb{Z}_e)$ es cíclico si y solo si $e = 2, 4, p^n$, o $2p^n$, donde p es primo impar, y $n \in \mathbb{N}$, [11, Teorema 5.64 y Teorema 5.66], si q es impar entonces $\bar{q}$ es un generador de $U(\mathbb{Z}_2)$; $\bar{q}$ es

un generador para $e = 4$ si $q \equiv 3 \pmod 4$ y $\bar{q}$ es un generador de $U(\mathbb{Z}_e)$ para $e = p^n$ o $2p^n$, si y solo si $o(q) = \Phi(p^n)$ en $U(\mathbb{Z}_{2p^n})$.

Así, en virtud del Teorema 3.2 tenemos:

Corolario 3.1. *Sea $\mathbb{F}$ un cuerpo finito con $|\mathbb{F}| = q$, y sea A un grupo abeliano finito, de exponente e. Entonces $\mathcal{G}_g = S_g$ para todo $g \in A$ si y solo si se cumple una de la siguiente condiciones:*

(i) $e = 2$ *y* q *es impar*

(ii) $e = 4$ *y* $q \equiv 3(md\,4)$

(iv) $e = p^n$ *y* $o(q) = \Phi(p^n)$ *en* $U(\mathbb{Z}_{p^n})$

(iv) $e = 2p^n$ *y* $o(q) = \Phi(p^n)$ *en* $U(\mathbb{Z}_{p^n})$

3.4. Códigos cíclicos minimales

Sean $\mathbb{F}_q$ y H un subgrupo finito de un grupo G. Si $mcd(q, |H|) = 1$, tomemos

$$\widehat{H} = \frac{1}{|H|} \sum_{g \in H} g,$$

un elemento en $\mathbb{F}G$. Además,

$$\begin{aligned}
\widehat{H}^2 &= \left(\frac{1}{|H|}\sum_{g\in H} g\right)\left(\frac{1}{|H|}\sum_{g\in H} g\right) \\
&= \frac{1}{|H|^2}\left(\sum_{g\in H} g\right)\left(\sum_{g\in H} g\right) \\
&= \frac{1}{|H|^2}\underbrace{\left(\sum_{g\in H} g + \sum_{g\in H} g + \cdots + \sum_{g\in H} g\right)}_{|H|-veces} \\
&= \frac{1}{|H|^2}|H|\left(\sum_{g\in H} g\right) \\
&= \frac{1}{|H|}\left(\sum_{g\in H} g\right) \\
&= \widehat{H}
\end{aligned}$$

$\widehat{H}$ es un idempotente de $\mathbb{F}G$.

Lema 3.2. *Sean $\mathbb{F}_q$ un cuerpo, p un primo, $A = \langle a \rangle$ un grupo cíclico de orden p^n, con $n \geq 1$, y*

$$A = A_0 \supset A_1 \supset \cdots \supset A_n = \{1\}$$

la cadena decreciente de todos los subgrupos de A. Entonces los elementos

$$e_0 = \widehat{A} \quad y \quad e_i = \widehat{A_i} - \widehat{A_{i-1}}, \quad 1 \leq i \leq n$$

forman un conjunto de idempotentes en $\mathbb{F}A$ tales que $e_0 + e_1 + \cdots + e_n = 1$.

Una prueba de este resultado la encontramos en [8, Lema VII.1.2].

Ejemplo 3.3. *Sea A un grupo cíclico de orden 3^3 y $\mathbb{F}$ un cuerpo. Entonces utilizaremos el resultado anterior para determinar los elementos idempotentes.*

$$\begin{aligned}
A_0 &= \langle a \rangle = \{1, a, a^2, \ldots, a^{26}\} \\
A_1 &= \langle a^3 \rangle = \{1, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}, a^{21}, a^{24}\} \\
A_2 &= \langle a^9 \rangle = \{1, a^9, a^{18}\} \\
A_3 &= \langle a^{27} \rangle = \{1\}.
\end{aligned}$$

Luego,

$$\begin{aligned}
e_0 &= \frac{1}{27}\left(1 + a + a^2 + \cdots + a^{26}\right) \\
\widehat{A_1} &= \frac{1}{9}\left(1 + a^3 + a^6 + a^9 + a^{12} + a^{15} + a^{18} + a^{21} + a^{24}\right) \\
\widehat{A_2} &= \frac{1}{3}\left(1 + a^9 + a^{18}\right) \\
\widehat{A_3} &= 1
\end{aligned}$$

Así,

$$e_1 = \widehat{A_1} - \widehat{A_0} = \frac{1}{27}\left(2 - a - a^2 + 2a^3 - a^4 - \cdots - a^{23} + 2a^{24} - a^{25} - a^{26}\right)$$
$$e_2 = \widehat{A_2} - \widehat{A_1} = \frac{1}{9}\left(2 - a^3 - a^6 + 2a^9 - a^{12} - a^{15} + 2a^{18} - a^{21} - a^{24}\right)$$
$$e_3 = \widehat{A_3} - \widehat{A_2} = \frac{1}{3}\left(2 - a^9 - a^{18}\right)$$

Además, $e_0 + e_1 + e_2 + e_3 = 1$.

Posterior al resultado anterior, los autores observaron que este método permite obtener todos los idempotentes primitivos en $\mathbb{Q}A$, pero en general, no funciona sobre cuerpos finitos. Para ilustrar esto, consideremos el polinomio $f(x) = x^3 - 1$ sobre el cuerpo de 7 elementos $\mathbb{F}_7$, el cual se expresa como

$$x^3 - 1 = (x-1)(x-2)(x-4),$$

y así,

$$\mathbb{F}_7 C_3 \simeq \frac{\mathbb{F}[x]}{(x^3-1)} \simeq \frac{\mathbb{F}[x]}{(x-1)} \oplus \frac{\mathbb{F}[x]}{(x-2)} \oplus \frac{\mathbb{F}[x]}{(x-4)}$$

Por otro lado sobre $\mathbb{Q}[x]$, el polinomio $(x^3 - 1)$ se descompone como $(x-1)(x^2+x+1)$. Por tanto si ζ denota una raíz primitiva de la unidad de orden 3 tenemos que

$$\mathbb{Q}C_3 \simeq \mathbb{Q} \oplus \mathbb{Q}(\zeta).$$

Así, el grupo cíclico de orden 3 sobre $\mathbb{Q}$ contiene solo dos idempotentes centrales primitivos no triviales, mientras el álgebra de grupo del mismo grupo sobre $\mathbb{F}_7$ contiene tres de tales elementos.

Así, los $n+1$ idempotentes dados en el Lema 3.2, serán el conjunto de idempotentes primitivos de $\mathbb{F}A$, siempre que $\mathbb{F}A$ tenga exactamente $n+1$ componentes. Dado que el exponente de A es p^n, tenemos que esto sucede si y solo si q y p^n están relacionados como en el Corolario 3.1, por tanto tenemos lo siguiente

Corolario 3.2. *Sea $\mathbb{F}_q$ un cuerpo finito y A un grupo cíclico de orden p^n. Entonces, el conjunto de idempotentes definidos en el lema anterior es el conjunto de idempotentes primitivos de A si y solo si una de las siguientes condiciones se cumple*

(i) $p = 2$, *o bien* $n = 1$ *y* q *es impar o* $n = 2$ *y* $q \equiv 3 \pmod 4$.

(ii) p *es un número primo impar y* $o(q) = \Phi(p^n)$ *en* $U(\mathbb{Z}_{p^n})$.

Como una consecuencia inmediata, tenemos el siguiente resultado de Pruthi y Arora [14].

Teorema 3.3. *Sean $\mathbb{F}_q$ un cuerpo finito y A un grupo cíclico de orden p^n tal que $o(q) = \Phi(p^n)$ en $U(\mathbb{Z}_{p^n})$. Sea*

$$A = A_0 \supset A_1 \supset \cdots \supset A_n$$

la cadena decreciente de todos los subgrupos de A. Entonces, el conjunto de idempotentes primitivos de $\mathbb{F}A$ esta dado por

$$e_0 = \frac{1}{p^n}\left(\sum_{a\in A} a\right) \quad y \quad e_i = \widehat{A_i} - \widehat{A_{i-1}} \quad 1 \leq i \leq n$$

Claramente, estos idempotentes determinan el conjunto de ideales minimales en $\mathbb{F}A$ y por tanto, los códigos cíclicos minimales de longitud p^n sobre $\mathbb{F}$.

Podemos establecer un resultado similar para grupos cíclicos de orden $2p^n$, sin embargo, para tal fin es necesario describir el siguiente isomorfismo:

Sean R es un anillo conmutativo con unidad, H y G grupos, entonces la siguiente aplicación

$$\begin{array}{ccc} R(G\times H) & \xrightarrow{\phi} & (RG)H \\ \displaystyle\sum_{(g,h)\in G\times H} \alpha_{(g,h)}(g,h) & \longmapsto & \displaystyle\sum_{h\in H}(\alpha_{(g,h)}g)h \end{array},$$

es un isomorfismo. Esto es, $R(G \times H) \simeq (RG)H$

Los idempotentes generadores de ideales minimales en el caso de los grupos cíclicos de orden $2p^n$, [1, Teorema 2.6] se siguen ahora fácilmente a partir de los resultados anteriores.

Teorema 3.4. *Sea $\mathbb{F}$ un cuerpo con q elementos y G un grupo cíclico de orden $2p^n$, p un primo impar, tal que $o(q) = \Phi(p^n)$ en $U(\mathbb{Z}_{2p^n})$. Escribimos $G = C \times A$ donde A es el p-subgrupo de Sylow de G y $C = \{1, t\}$ es su 2-subgrupo de Sylow. Si e_i, $0 \leq i \leq n$, denotan los idempotentes primitivos de $\mathbb{F}A$ entonces, los idempotentes primitivos de $\mathbb{F}G$ son*

$$\frac{1+t}{2}e_i \quad y \quad \frac{1-t}{2}e_i, \quad 0 \leq i \leq n.$$

Demostración. De las ecuaciones 2.4, 2.5 y 2.6, sabemos que:

$$FC \simeq \frac{F[x]}{\langle x^2-1\rangle} \simeq \frac{F[x]}{\langle x-1\rangle} \bigoplus \frac{F[x]}{\langle x+1\rangle} \simeq F \bigoplus F$$

Por tanto,

$$\mathbb{F}G \simeq \mathbb{F}(C \times A) \simeq (\mathbb{F}C)A \simeq (\mathbb{F} \oplus \mathbb{F})A.$$

Ahora, calculemos los idempotentes de $\mathbb{F}C$ como en el Teorema 3.3, para ellos tenemos primero que $A_0 = A$ y $A_1 = \{1\}$, además

$$\widehat{A_0} = \frac{1}{|A_0|} \sum_{a \in A_0} a = \frac{1}{2}(1+t)$$

$$\widehat{A_1} = \frac{1}{|A_1|} \sum_{a \in A_1} a = \frac{1}{1}(1) = 1,$$

luego los idempotentes serán:

$$e_0 = \frac{1}{p^n}\left(\sum_{a \in A} a\right) = \frac{1}{2}(1+t) = \frac{1+t}{2}$$

$$e_1 = \widehat{A_1} - \widehat{A_0} = 1 - \frac{1}{2}(1+t) = \frac{2-1-t}{2} = \frac{1-t}{2}$$

Así, los idempotentes de $\mathbb{F}G$ son:

$$\frac{1+t}{2}e_i \quad y \quad \frac{1-t}{2}e_i, \quad 0 \leq i \leq n.$$

□

3.5. Códigos abelianos minimales

Ahora, queremos extender estos resultados para grupos abelianos finitos. Comenzaremos considerando el caso de p-grupos.

Sea A un p-grupo abeliano. Para cada subgrupo H de A tal que $A/H \neq \{1\}$ es cíclico, construiremos un idempotente de $\mathbb{F}A$. Recordemos que, dado que A/H es un grupo cíclico de orden una potencia de p, solo existe un subgrupo H^* de A que contiene a H, tal que $|H^*/H| = p$. Definimos $e_H = \widehat{H} - \widehat{H^*}$. Claramente $e_H \neq 0$ y tenemos el siguiente resultado

Lema 3.3. *Los elementos e_H, definidos anteriormente, junto con $e_A = \widehat{A}$, forman un conjunto de idempotentes dos a dos ortogonales de $\mathbb{F}A$ cuya suma es igual a 1.*

Demostración. Veamos primero que dichos elemento son idempotentes, de hecho, en virtud

del Teorema 3.3 tenemos que $\widehat{A}$, $\widehat{H}$ y $\widehat{H^*}$ son idempotentes y además

$$\begin{aligned} e_H^2 &= \left(\widehat{H} - \widehat{H^*}\right)\left(\widehat{H} - \widehat{H^*}\right) \\ &= \widehat{H}^2 + \widehat{H}\widehat{H^*} - \widehat{H}\widehat{H^*} - \widehat{H^*}^2 \\ &= \widehat{H} - \widehat{H^*} \\ &= e_H. \end{aligned}$$

Ahora, probaremos que estos idempotente son ortogonales dos a dos, es decir, $e_H e_K = 0$ para $H \neq K$. Iniciamos suponiendo que existen H y K subgrupos de A diferentes, tales que A/H y A/K son cíclicos y diferentes de $\{1\}$, sean H^* y K^* los subgrupos de A que contienen a H y K, respectivamente, tales que H^*/H y K^*/K son cíclicos de orden p. Consideremos primero el caso cuando $H \subset K$. En este caso, $H^* \subset K$ y por lo tanto

$$e_H e_K = (\widehat{H} - \widehat{H^*})(\widehat{K} - \widehat{K^*}) = \widehat{K} - \widehat{K^*} - \widehat{K} + \widehat{K^*} = 0.$$

Si ninguno de estos subgrupos está contenido en el otro, entonces ambos H y K están propiamente contenidos en HK, así también H^* y K^* están contenido en HK por tanto $H^*K^* \subset HK$ y claramente $HK \subset H^*K^*$, por consiguiente $HK = H^*K^*$. Ahora, dado que $HK \subset HK^* \subset H^*K^*$ se sigue que también $HK^* = HK$ y, de modo similar, tenemos que $H^*K = HK$. Por lo tanto

$$e_H e_K = (\widehat{H} - \widehat{H^*})(\widehat{K} - \widehat{K^*}) = 0$$

De forma análoga se muestra que $e_A e_H = 0$.

Finalmente, mostraremos que la suma de dichos idempotentes es igual a 1. Para cada subgrupo cíclico C de A denotamos por $\mathcal{G}(C)$ el conjunto de los elementos de C que generan este subgrupo.

$$\mathcal{G}(C) = \{c \in C : mcd(o(c), |C|) = 1\}$$

Si $\mathcal{C}$ denota la familia de todos los subgrupos cíclicos de A entonces, $|A| = \sum_{C\in\mathcal{C}} |\mathcal{G}(C)|$ y, dado que A es un p-grupo, $|\mathcal{G}(C)| = |C| - \frac{|C|}{P}$.

Sea $\mathcal{S}$ el conjunto de todos los subgrupos H de A tal que A/H es cíclico y denotemos por $e = \sum_{H\in\mathcal{S}} e_H$. Afirmemos que $e = 1$. Para probar esto, es suficiente mostrar que $(\mathbb{F}A)e = \mathbb{F}A$. Como hemos demostrado que estos idempotentes son ortogonales dos a dos, tenemos que

$$(\mathbb{F}A)e = \bigoplus_{H\in\mathcal{S}} (\mathbb{F}A)e_H.$$

Por tanto

$$dim_{\mathbb{F}}((\mathbb{F}A)e) = \sum_{H\in\mathcal{S}} dim_{\mathbb{F}}((\mathbb{F}A)e_H).$$

Note que $\widehat{H} = \widehat{H^*} + e_H$ y que $\widehat{H^*}e_H = 0$ así

$$(\mathbb{F}A)\widehat{H} = (\mathbb{F}A)\widehat{H^*} \bigoplus (\mathbb{F}A)e_H.$$

Luego,

$$dim_{\mathbb{F}}((\mathbb{F}A)e_H) = dim_{\mathbb{F}}(\mathbb{F}A)\widehat{H} - dim_{\mathbb{F}}(\mathbb{F}A)\widehat{H^*}.$$

De la prueba de [12, Proposición 3.6.7] tenemos que

$$dim_{\mathbb{F}}((\mathbb{F}A)e_H) = dim_{\mathbb{F}}\mathbb{F}(A/H) - dim_{\mathbb{F}}\mathbb{F}(A/H^*),$$

claramente,

$$dim_{\mathbb{F}}\mathbb{F}(A/H) = |A/H| \quad y \quad dim_{\mathbb{F}}\mathbb{F}(A/H^*) = |A/H^*|.$$

sabemos que subgrupos de un grupo cíclicos son cíclico, y del teorema de la correspondencia,(ver Lema 1.3), existe una biyección $\Phi : \mathcal{C} \to \mathcal{S}$, tal que $|X| = |A/\Phi(X)|$ para todo $X \in \mathcal{C}$. Si denotamos por $C \in \mathcal{C}$ el subgrupo tal que $\Phi(C) = H$. Usando el Teorema 1.4 y el hecho que la

$$dim_{\mathbb{F}}\mathbb{F}[A/H] = |C|.$$

Tenemos,

$$dim_{\mathbb{F}}\mathbb{F}[A/H^*] = |A/H^*| = |A/H|/|H^*/H| = \frac{|C|}{P}.$$

Así,

$$dim_{\mathbb{F}}((\mathbb{F}A)e_H) = |C| - \frac{|C|}{p} = |\mathcal{G}(C)|$$

y por tanto

$$\sum_{H\in\mathcal{S}} dim_{\mathbb{F}}((\mathbb{F}A)e_H) = \sum_{C\in\mathcal{C}} |\mathcal{G}(C)| = |A|$$

y el resultado se sigue. □

Ejemplo 3.4. *Encontremos los idempotentes del álgebra de grupo $\mathbb{F}_3C_8$ utilizando el resultado anterior.*

Los subgrupos de C_8 son: $C_8 = \langle a\rangle$, $C_4 = \langle a^2\rangle$, $C_2 = \langle a^4\rangle$ y $C_1 = \langle a^8\rangle = \{1\}$. Además, tenemos

$$|C_8/C_4| = |C_4/C_2| = |C_2/C_1| = 2.$$

Así, por el lema anterior, los idempotentes de $\mathbb{F}_3C_8$ *son:*

$$\begin{aligned}
e_1 &= \widehat{C_8} = 2 + 2a + 2a^2 + 2a^3 + 2a^4 + 2a^5 + 2a^6 + 2a^7,\\
e_2 &= \widehat{C_4} - \widehat{C_8} = 2 + a + 2a^2 + a^3 + 2a^4 + a^5 + 2a^6 + a^7,\\
e_3 &= \widehat{C_2} - \widehat{C_4} = 1 + 2a^2 + a^4 + 2a^6,\\
e_4 &= \widehat{C_1} - \widehat{C_2} = 2 + a^4.
\end{aligned}$$

El siguiente resultado es una consecuencia inmediata del Lema anterior y el Corolario 3.1.

Teorema 3.5. *Sea* p *un primo impar y* A *un* p*-grupo abeliano de exponente* p^r*. Entonces, el conjunto de los idempotentes definidos anteriormente es el conjunto de idempotentes primitivos de* $\mathbb{F}A$ *si y solo si una de las siguientes condiciones se cumple*

(i) $p^r = 2$*, y* q *es impar.*

(ii) $p^r = 4$*, y* $q \equiv 3 \pmod 4$*.*

(iii) p *es un primo impar o* $o(q) = \Phi(p^n)$ *en* $U(\mathbb{Z}_{p^n})$*.*

Además, tenemos el siguiente resultado

Teorema 3.6. *Sea* p *un primo impar y* A *un* p*-grupo abeliano de exponente* $2p^r$*. Escribimos* $A = E \times B$*, donde* E *es un* 2*-grupo abeliano elemental y* B *un* p*-grupo. Entonces los idempotentes primitivos de* $\mathbb{F}A$ *son productos de la forma* $e \cdot f$*, donde* e *es un idempotente primitivo de* $\mathbb{F}E$ *y* f *un idempotente de* $\mathbb{F}B$*.*

Note que los idempotentes primitivos de $\mathbb{F}B$ son dados por el Toerema 3.5 anterior y, escribimos $E = \langle a_i \rangle \times \cdots \times \langle a_n \rangle$, un producto de grupos cíclicos de orden 2, entonces los idempotentes primitivos de $\mathbb{F}E$ son productos de la forma $e = e_1 e_2 \cdots e_n$, donde

$$e_i = \frac{1 + a_i}{2} \quad o \quad e_i = \frac{1 - a_i}{2}, \quad 1 \leq i \leq n.$$

Vale la pena señalar que, en vista de Corolario 3.1, estos son los únicos casos en los que idempotentes primitivos de álgebras de grupos abelianos finitos se pueden calcular de esta manera.

Capítulo 4

Conclusiones

El propósito principal de esta tesis es estudiar la construcción de códigos sobre álgebras de grupo, para ciertos grupos, como los grupos cíclicos y abelianos, teniendo en cuenta los resultados obtenidos por C. Polciono & R. Ferraz en [5].

Para lo cual es fundamental el estudio de está "nueva" estructura algebraica. Por tanto en la Sección 1.4, establecemos algunos de los resultados más relevantes de esta estructura para el desarrollo de esta tesis, sin embargo, para poder entrar en detalle, es necesario recordar algunas de las nociones y resultados de las teorías de grupos y anillos (Secciones 1.1 y 1.2, respectivamente), puesto que esta nueva estructura algebraica es el lugar de encuentro de estas dos teorías. Los resultados allí presentados, son asumidos sin demostración ya que hacen parte de los cursos básicos de *álgebra*.

Por otro lado, dado que las Secciones 2, 2.2 y 2.3, correspondientes a semisimplicidad, son de vital importancia y no forman parte de algún curso de pregado, es necesario mostrar detalladamente sus resultados, los cuales en su mayoría son presentados con demostración o en caso contrario tienen la respectiva referencia bibliográfica.

Ahora bien, ya solo nos resta conocer que es un código, para ello en el Capítulo 3, inicialmente presentamos los conceptos básicos y algunos ejemplos sencillos. Luego, procedemos a relacionar los códigos con una subestructura del álgebra de grupo, pues al lograr esto tendríamos las suficientes herramientas para trabajar desde este enfoque con los códigos.

En principio vemos que los códigos van a estar relacionados con la subestructura de

ideal, y estos a su vez por los preliminares están relacionados con una familia de idempotentes. Luego, la construcción de los códigos está basada en la construcción de dicha familia.

En las Secciones 3.4 y 3.5, mostramos el método de construcción de la familia de idempotentes, concluyendo así los objetivos planteados.

Referencias

[1] Arora S., y Pruthi M. (1999). *Minimal cyclic codes of length* $2p^n$. Finite Fields Appl, 5, 177-187.

[2] Berman S.(1987). *Semisimple cyclic and abelian code II*. Cybernetics, 3(3), 17-23.

[3] Blake I., y Mullin R. (1975). *The Mathematical Theory of Coding*. New York: Academic Press.

[4] Curtis C., y Reiner I. (1981). *Methods of Representation Theory*. New York: Wiley-Interscience.

[5] Ferraz, R., y Polcino, C. (2007). *Idempotents in group algebras and minimal abelian codes*. Finite Fields and Their Applications, 13, 382-393.

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

[7] Gallian J. (2010). *Contemporary Abstract Algebra*. Seventh Edition. University of Minnesota, Duluth: CENGAGE Learning.

[8] Goodaire, E., Jespers, E., y Polcino Milies, C. (1996). *Alternative Loop Rings*. Amsterdam: Elsevier, North-Holland Math. Stud., vol. 184.

[9] Hamming R. (1948). *Error Detecting and Error Correcting Codes*. The Bell System Thechnical Journal, XXVI , 379-423, 623-656.

[10] Herstein I.N. (1986). *Algebra Abstrata*. México: Grupo Editorial Iberoamérica. (Versión original en inglés: *Abtract Algebra*. USA: Macmillan Publishing Company).

[11] Jimenez, R., Gordiilo, E., y Rubiano, G. (2004). *Teoría de números [Para principiantes]*. Segunda Edición. Bogotá: Universidad Nacional de Colombia.

[12] Polcino, C., y Sehgal, S. (2002). *A Course in Group Rings*. Dordrecht: Kluwer Academic Publishers.

[13] Perlis S., y Walker G. (1950) *Abelian group algebras*. USA: Trans. Amer. Math. Soc. 68, 420-426.

[14] Pruthi, M., y Arora S. (1997). *Minimal codes of prime power length*. Finite Fields Appl. 3, 99-113.

Bibliografía

Arora S., y Pruthi M. (1999). *Minimal cyclic codes of length* $2p^n$. Finite Fields Appl, 5, 177-187.

Berman S.(1987). *Semisimple cyclic and abelian code II*. Cybernetics, 3(3), 17-23.

Blake I., y Mullin R. (1975). *The Mathematical Theory of Coding*. New York: Academic Press.

Curtis C., y Reiner I. (1981). *Methods of Representation Theory*. New York: Wiley-Interscience.

Ferraz, R., y Polcino, C. (2007). *Idempotents in group algebras and minimal abelian codes*. Finite Fields and Their Applications, 13, 382-393.

Ferraz, R. (2004). *Simple components and central units in group algebras*. J. Algebra, 279, 191-203.

Gallian J. (2010). *Contemporary Abstract Algebra*. Seventh Edition. University of Minnesota, Duluth: CENGAGE Learning.

Goodaire, E., Jespers, E., y Polcino Milies, C. (1996). *Alternative Loop Rings*. Amsterdam: Elsevier, North-Holland Math. Stud., vol. 184.

Hamming R. (1948). *Error Detecting and Error Correcting Codes*. The Bell System Thechnical Journal, XXVI , 379-423, 623-656.

Herstein I.N. (1986). *Algebra Abstrata*. México: Grupo Editorial Iberoamérica. (Versión original en inglés: *Abtract Algebra*. USA: Macmillan Publishing Company).

Jimenez, R., Gordiilo, E., y Rubiano, G. (2004). *Teoría de números [Para principiantes]*. Segunda Edición. Bogotá: Universidad Nacional de Colombia.

Ling S. (2004). *Coding Theory A Firts Course*. New York: Cambridge University Press.

Polcino, C., y Sehgal, S. (2002). *A Course in Group Rings*. Dordrecht: Kluwer Academic Publishers.

Polcino, C. (2010). *Introduçiòn á Teoria algebraica de códigos*. Notas de clase-Aula. São Paulo: IME-USP.

Polcino, C., y Sehgal, S. (2002). *An introduction to group rings*. Dordrecht: Kluwer Academic Publishers. Algebras and Applications.

Perlis S., y Walker G. (1950) *Abelian group algebras*. USA: Trans. Amer. Math. Soc. 68, 420-426.

Pruthi, M., y Arora S. (1997). *Minimal codes of prime power length*. Finite Fields Appl. 3, 99-113.

Podestá, R. (2006).*Introducción a la Teoría de Códigos Autocorrectores*. Mathematics Subject Classification. CONICET y SecytUNC.