Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ciencias

TEORÍA DE LOS GRUPO-ANILLOS Y SUS APLICACIONES

Hugo Allan García Monterrosa
Asesorado por: Ph.D. Sergio Roberto López Permouth
Lic. William Roberto Gutiérrez Herrera

Guatemala, abril de 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

TEORÍA DE LOS GRUPO-ANILLOS Y SUS APLICACIONES

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

HUGO ALLAN GARCÍA MONTERROSA
ASESORADO POR PH.D. SERGIO ROBERTO LÓPEZ PERMOUTH
LIC. WILLIAM ROBERTO GUTIÉRREZ HERRERA

AL CONFERÍRSELE EL TÍTULO DE

LICENCIADO EN MATEMÁTICA APLICADA

GUATEMALA, ABRIL DE 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Lic.
EXAMINADOR	Lic.
EXAMINADOR	Lic.
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

TEORÍA DE LOS GRUPO-ANILLOS Y SUS APLICACIONES

Tema que me fuera asignado por la Dirección de la Escuela de Ciencias, con fecha noviembre de 2012.

Hugo Allan García Monterrosa

OHIO
UNIVERSITY
College of Arts and Sciences

Department of Mathematics
Morton Hall 321
Athens OH 45701-2979

T: 740.593.1254
F: 740.593.9805

Marzo 6, 2014

Ing. Edwin Adalberto Bracamonte
DIRECTOR, ESCUELA DE CIENCIAS
FACULTAD DE INGENIERÍA
USAC, Ciudad.

Estimado Ingeniero Bracamonte:

Me dirijo a usted para informarle que he realizado la revisión al trabajo de graduación **"Teoría de los grupos-anillos y sus aplicaciones"**, presentada por el estudiante **Hugo Allan García Monterrosa**, con carné No. 2007-14466; y considerando que cumple con los objetivos de la carrera de Licenciatura en Matemática Aplicada, le doy mi aprobación como asesor de dicho trabajo.

Muy atentamente,

Dr. Sergio Roberto López Permouth, Asesor de Tesis, y
catedrático del departamento de Matemática de la
Universidad de Ohio, Athens, Ohio, Estados Unidos de América.
A S E S O R

DEPT. OF MATHEMATICS
OHIO UNIVERSITY
ATHENS, OHIO 45701

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería

Guatemala, 25 de marzo del 2014

Ing. Edwin Adalberto Bracamonte
Director de Escuela de Ciencias
Facultad de Ingeniería
Presente

Estimado Ingeniero Bracamonte:

Por este medio me dirijo a usted, para informarle que he realizado la revisión al trabajo de graduación titulado *Teoría de los grupo-anillos y sus aplicaciones*, presentado por el estudiante universitario **Hugo Allan García Monterrosa** con carné No. 2007-14466, y considero que el mismo cumple con el rigor matemático adecuado y es presentado en forma clara y concisa, por lo que en mi calidad de coasesor le doy mi *aprobación.*

Agradeciendo su atención, me suscribo

Id y enseñad a todos.

Lic. William Roberto Gutiérrez Herrera
Asesor

Lic. William R. Gutiérrez H.
MATEMÁTICO
Colegiado No. 8090

ACTO QUE DEDICO A:

Mi familia Por apoyarme incondicionalmente.

AGRADECIMIENTOS A:

Dios	Por darme la vida y la oportunidad de aprender matemática.
Mi familia	Por su apoyo en el estudio de mi universitaria.
Mis amigos	Por compartir conmigo tantos momentos y proyectos dentro y fuera de las aulas universitarias.
Ohio University	Por brindarme la oportunidad de realizar mi trabajo de graduación en su prestigiosa institución.
Mis asesores	Por darme consejos, sugerencias e ideas en la elaboración de este trabajo.
Eva Gramajo	Por brindarme su apoyo para lograr cumplir mis metas personales, y profesionales y compartir conmigo los buenos y malos momentos.
Mis profesores	Por compartir sin recelo sus conocimientos y experiencias académicas.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

LISTA DE SÍMBOLOS

Símbolo	**Significado**
$\boldsymbol{a \mid b}$	a divide a b
$\boldsymbol{a \equiv b}$	a es congruente con b
$\boldsymbol{A \simeq B}$	A es isomorfo a B
$\boldsymbol{A \to B}$	A se mapea en B
$\boldsymbol{a \nmid b}$	a no divide a b
$\boldsymbol{A \lhd B}$	A es subgrupo normal de B
$\boldsymbol{Ann_d(X)}$	Aniquilador del conjunto X por la derecha
$\boldsymbol{Ann_i(X)}$	Aniquilador del conjunto X por la izquierda
$\mathbf{car}(\boldsymbol{K})$	Característica del campo K
$\mathbb{Z}$	Conjunto de números enteros
$\mathbb{Q}$	Conjunto de números racionales
$\mathbb{R}$	Conjunto de números reales
$\boldsymbol{\emptyset}$	Conjunto vacío
$[\boldsymbol{a}, \boldsymbol{b}]$	Conmutador de a y b
$\mathbf{cos}$	Función trigonométrica coseno
$\mathbf{sin}$	Función trigonométrica seno
$\mathbf{deg}$	Grado de una representación de un polinomio
$\mathbf{hom}_{\boldsymbol{K}}(\boldsymbol{A}, \boldsymbol{A})$	Conjunto de homomorfismos de A en A como K-módulos
$\Longrightarrow$	Implicación
$\boldsymbol{\infty}$	Infinito

$\cap$	Intersección de conjuntos
$\mathbf{ker}(\boldsymbol{f})$	Kernel de la función f
$\neq$	No igual a
$\notin$	No pertenece a
$\|\|\boldsymbol{a}\|\|$	Norma del vector a
$\mathbf{o}(\boldsymbol{p})$	Orden del elemento p
$\in$	Pertenencia
$\subseteq$	Subconjunto
$\subset$	Subconjunto propio
$\oplus$	Suma directa
$\sum$	Sumatoria
$\mathbf{:}$	Tal que
$\mathbf{tr}(\boldsymbol{A})$	Traza de la matriz A
$\cup$	Unión de conjuntos
$\boldsymbol{x} \mapsto \boldsymbol{y}$	x se mapea en y

GLOSARIO

Aplicación Se refiere a una regla que asigna a cada elemento de un primer conjunto, un único elemento de un segundo conjunto.

Campo ciclotómico Es un cuerpo numérico que se obtiene al añadir una raíz primitiva de la unidad compleja a el campo de los números racionales.

Cubierta Es una colección de subconjuntos A de un conjunto X, tal que la unión de los elementos de la colección A es igual a X.

Grupo soluble Es un grupo para el cual existe una cadena finita de subgrupos $\{G_i\}_{i=1}^{n} \subset G$ tal que $\{1_G\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ donde para cada $i = 0, 1, \ldots, n-1$ se cumple que G_i es subgrupo normal en G_{i+1} y el grupo cociente G_{i+1}/G_i es abeliano.

Inducción matemática Es un razonamiento que permite demostrar una infinidad de proposiciones, o una proposición que depende de un parámetro n, que toma una infinidad de valores enteros.

Norma Es la función que determina el tamaño de un elemento de un espacio vectorial.

Registro de desplazamiento	Es un circuito digital secuencial consistente en una serie de biestables, generalmente de tipo D, conectados en cascada que basculan de forma sincrónica con la misma señal de reloj.
Tupla	Es una secuencia ordenada de objetos, esto es, una lista con un número limitado de objetos.

RESUMEN

En el siguiente trabajo de investigación se hace un estudio detallado de la teoría básica de los grupo-anillos, necesaria para el desarrollo de la teoría de códigos, dando énfasis en la relación que tienen con la teoría de grupos y la teoría de anillos, ambas materias de estudio de un pregrado en Matemática.

El trabajo está estructurado en seis capítulos, cuyo contenido se describe a continuación:

El primer capítulo contiene todo el bagaje matemático que sirve de cimiento para un estudio adecuado de los grupo-anillos.

En el segundo capítulo se da la definición de un grupo-anillo y una grupo-álgebra, caso especial del anterior. Posteriormente, se establecen las condiciones necesarias y suficientes para que un grupo-anillo sea semisimple.

En el tercer capítulo se estudia la teoría de representación de grupos y su relación con los módulos de los grupo-anillos.

En el cuarto capítulo se estudian algunos elementos algebraicos de un grupo-anillo como los elementos nilpotentes, los idempotentes y las unidades de torsión.

En el quinto capítulo se da una breve introducción al estudio de las unidades de un grupo-anillo, mostrando algunas construcciones de unidades no triviales para los mismos.

Finalmente en el sexto capítulo se da una introducción a la teoría de códigos correctores, dando relevancia a los códigos cíclos y mostrando que dichos códigos tienen una fuerte conexión con las grupo-álgebras.

OBJETIVOS

General

Describir las características fundamentales de los grupo-anillos y su relación con la teoría de representación de grupos.

Específicos

1. Identificar los elementos fundamentales que dan paso al estudio de los grupo-anillos.
2. Identificar las condiciones necesarias y suficientes para la semisimplicidad.
3. Mostrar ejemplos de unidades en los grupo-anillos en casos particulares.
4. Documentar algunas aplicaciones de los grupo-anillos en la teoría algebraica de códigos.

INTRODUCCIÓN

Los grupo-anillos son una estructura muy interesante por sus propiedades algebraicas y su importancia surgió aparentemente, después de los trabajos de T. Molien, G. Frobenius, I. Schur y H. Maschke en los inicios del siglo XX. La importancia de esta estructura en la teoría de la representación de grupos fue establecida por E. Noether y R. Brauer y a partir de ese punto los grupo-anillos comenzaron a ser estudiados como materia aparte por derecho propio.

El estudio de los grupo-anillos involucra el conocimiento de diversas ramas de la matemática (teoría de campos, el álgebra lineal y la teoría algebraica de números), además de estar ampliamente relacionados con la topología algebraica, el álgebra homológica y la K-teoría algebraica. En la última década, también se ha encontrado que los grupo-anillos tienen aplicaciones en la teoría algebraica de codificación.

Dentro de la teoría de códigos es muy importante el estudio de los códigos correctores, los cuales están explícitamente diseñados para evitar la pérdida de información debido a problemas de ruido en la transmisión. En este sentido los primeros diseños de códigos correctores fueron los de bloque, los cuales construyen bloques de información para luego ser transformados en otro tipo de bloques mediante una aplicación llamada diccionario.

El coste computacional de la codificación es excesivo, así que se hace necesario introducir una estructura algebraica que permita simplicar los procesos de codificación.

De esta forma los grupo-anillos juegan un papel importante en la teoría algebraica de la codificación, permitiendo conocer el código cíclico y su estructura sin necesidad de una implementación.

1. CONCEPTOS PRELIMINARES

En este capítulo se presentará la teoría básica del álgebra abstracta necesaria para la comprensión del contenido a desarrollar más adelante. Dicha exposición no pretende ser una guía de estudios del álgebra, más bien refresca resultados básicos de teoría de grupos, anillos y álgebras. En la medida de lo posible se evitará dar demostraciones de los resultados de estos conceptos, a menos que no sean materia de estudio de la licenciatura en Matemática.

1.1. Antecedentes

La *teoría de grupos* como la conocemos actualmente tiene sus orígenes en los trabajos de Ruffini, Abel, Lagrange y Galois a inicios siglo XIX, quienes trabajaron con el concepto de **permutación** (en su tiempo Cauchy las llamaba sustituciones, ver (18:104)). Con Cayley (1: 104) se formalizó el concepto de **grupo** y además se dieron muchos avances significativos que impulsaron la investigación de este tema. Entre los avances hechos por Cayley figuran:

- Definición formal de grupo usando la notación de multiplicación.
- Utilizar una *tabla* para mostrar como actúa una operación.
- Demostración de existencia de dos grupos no isomorfos de orden cuatro, dando ejemplos explícitos.
- Demostración de existencia de dos grupos no isomorfos de orden seis, uno de los cuales es conmutativo y el otro es isomorfo a $\mathcal{S}_3$, el grupo de permutaciones de tres elementos.
- Demostración de que el orden de todo elemento es divisor del orden del grupo, cuando éste es finito.

1.2. Teoría de grupos

Definición 1.2.1. Un **grupo** es un conjunto no vacío G junto con una operación binaria, denotada como $\cdot$, tal que para cada $a, b \in G$ se cumplen las siguientes condiciones:

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- Existe un elemento único $1 \in G$, tal que $a \cdot 1 = 1 \cdot a = a$.
- Para cada $a \in G$ existe un elemento único $a^{-1} \in G$, tal que

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Si, además de las tres propiedades anteriores, se cumple

$$a \cdot b = b \cdot a, \text{ para cada } a, b \in G$$

entonces se dice que el grupo es **abeliano** o **conmutativo**. Si el conjunto G es finito, entonces el número de elementos de G es llamado el **orden** de G y se denota como $\circ(G)$.

Ejemplo 1.2.1. Sea M un conjunto finito. El lector deberá recordar que una aplicación biyectiva de M a M es llamada *permutación* de M. Es claro entonces que la aplicación identidad de M a M es una permutación, que la composición de dos permutaciones es una permutación y la inversa de una permutación también es permutación.

A partir de estos hechos, es evidente que dado un conjunto M se puede construir conjunto de permutaciones y que este constituye un grupo respecto a la composición de funciones. Este grupo usualmente es denotado como $\mathcal{S}_M$ y es llamado el **grupo**

de permutaciones de M. Si $M = \{1, 2, \ldots, n\}$ entonces $\mathcal{S}_M$ es llamado el *grupo de simetrías de grado* n y se denotada como $\mathcal{S}_n$. Dado un elemento $\psi \in \mathcal{S}_n$, si se elige que $i_k = \psi(k),\ 1 \leq k \leq n$, entonces se puede representar ψ en la forma:

$$\psi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix},$$

la cual es una notación introducida por Cauchy en 1845 (4:64-90). Usando esta notación, la inversa de ψ se representa como:

$$\psi^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

Dadas, por ejemplo,

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \qquad \text{y} \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix},$$

se tiene que $(\phi \circ \psi)(1) = \phi(2) = 5$. Haciendo el cálculo para el resto de los números se obtiene

$$\phi \circ \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}.$$

De la misma manera

$$\psi \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}.$$

Este simple cálculo demuestra que, en general, $\mathcal{S}_n$ no es conmutativo. De hecho, es fácil demostrar que $\mathcal{S}_n$ es conmutativo si y sólo si $n \leq 2$.

Definición 1.2.2. Un subconjunto no vacío H de un grupo G es llamado **subgrupo de** G si es cerrado bajo la operación de G y H, con la restricción de la operación de G, es un grupo por sí mismo.

Ejemplo 1.2.2 (Subgrupos cíclicos). Sea a un elemento del grupo G. Para un exponente entero n se definen las potencias de a como

$$a^n = \begin{cases} \underbrace{a \cdot a \cdots a}_{n \text{ veces}} & \text{si } n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{|n| \text{ veces}} & \text{si } n < 0 \\ 1 & \text{si } n = 0. \end{cases}$$

Como $a^m \cdot a^n = a^{m+n}$, se sigue que el conjunto

$$\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$$

es un subgrupo de G, llamado **subgrupo cíclico de** G generado por a. Si este grupo es finito, entonces existen enteros positivos n, m distintos tales que $a^n = a^m$, de esta cuenta, se tiene $a^{n-m} = a^{m-n} = 1$. El entero positivo más pequeño n tal que $a^n = 1$ se le llama **orden de** a y se denota como $\circ(a)$. Si $\langle a \rangle$ es infinito se dice que a es de **orden infinito**. Si existe un elemento a en G tal que $G = \langle a \rangle$, entonces se dice que G es un **grupo cíclico** y que a es un **generador** de G. Nótese que $\circ(a) = |\langle a \rangle|$.

Ejemplo 1.2.3. Sea X un subconjunto no vacío de un grupo G. Se define el **subgrupo generado por** X como la intersección de todos los subgrupos de G que contienen a X. Esta familia de subgrupos es no vacía, ya que por lo menos G

pertenece a ella.

Es fácil demostrar que esta intersección definida previamente es un subgrupo de G. Este subgrupo es denotado como $\langle X \rangle$. Se propone al lector demostrar que

$$\langle X \rangle = \{x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} : x_i \in X,\ \epsilon_i = \pm 1,\ k \geq 1\} \cup \{1\}.$$

Si $\langle X \rangle = G$ se dice que X es un **conjunto de generadores de** G. Si X es finito, entonces se dice que G es un **grupo finitamente generado**.

Lema 1.2.1. Un subconjunto no vacío H de un grupo G es un subgrupo de G si y sólo si para cualesquiera $x, y \in H$ se tiene que $x^{-1}y \in H$.

Definición 1.2.3. El **centro** de un grupo G es el subgrupo

$$\mathcal{Z}(G) = \{a \in G : ax = xa,\ \text{para cada } x \in G\}.$$

Dado un subgrupo H de un grupo G, se puede definir una **partición** de G, es decir una cubierta de G hecha de subconjuntos disjuntos.

Definición 1.2.4. Sea H un subgrupo de un grupo G. Dado un elemento $a \in G$, los subconjuntos de la forma

$$\begin{aligned} aH &= \{ah : h \in H\}, \\ Ha &= \{ha : h \in H\} \end{aligned}$$

son llamados **clases lateral izquierda y derecha del subgrupo** H determinadas por a, respectivamente.

Proposición 1.2.1. Sea H un subgrupo de un grupo G y a, b elementos arbitrarios de G. Entonces se cumple:

1. Si $b \in aH$ entonces $bH = aH$.
2. Si $b \notin aH$ entonces $aH \cap bH = \emptyset$.

Corolario 1.2.1. Sea H un subgrupo de un grupo G. Dados $a, b \in G$ se cumple que $b \in aH$ si y sólo si $aH = bH$.

Todo elemento en una clase lateral es un **representante** de la misma. Un conjunto completo de representantes de un clase lateral izquierda (derecha) es llamado **transversal izquierdo (derecho) de H en G**.

Definición 1.2.5. Sea H un subgrupo de un grupo G. Si el numero de clases izquierdas (derechas) de H en G es finito, entonces este número es llamado **índice** de H en G y se denota como $(G : H)$.

Teorema 1.2.1 (Lagrange). Sea H un subgrupo de un grupo finito G. Entonces, el orden de H divide a el orden de G. Más aún, de manera más formal, se tiene

$$\mid G \mid = (G : H) \mid H \mid .$$

Corolario 1.2.2. Sea a un elemento de un grupo finito G. Entonces $\circ(a)$ es un divisor de $\mid G \mid$.

Ejemplo 1.2.4. Considérese nuevamente a $\mathcal{S}_3$, el grupo de simetrías de grado tres. Se sabe que $|\mathcal{S}_3| = 6$. Explícitamente, este grupo se expresa como

$$\mathcal{S}_3 = \{I, (12), (13), (23), (123), (132)\}, \text{ donde } I = (1).$$

Sea $H = \{I, (12)\}$ y $\alpha = (123)$. Entonces

$$\alpha H = \{(123), (13)\} \text{ y } H\alpha = \{(123), (23)\},$$

con esto se demuestra que, en general, las clases laterales derechas e izquierdas determinadas por el mismo elemento no son iguales.

Los subgrupos cuyas clases laterales derechas e izquierdas generadas por el mismo elemento son iguales son de especial importancia. Nótese que para un elemento a y un subgrupo H de un grupo G, se tiene que $aH = Ha$ si y sólo si $a^{-1}Ha = H$. Esto sugiere la siguiente

Definición 1.2.6. Sea H un subgrupo de un grupo G. Se dice que H es **normal** en G, y se escribe $H \triangleleft G$ si $a^{-1}Ha = H$ para cualquier $a \in G$.

1.2.1. Homomorfismos y grupos cocientes

Definición 1.2.7. Sean G_1 y G_2 grupos. Una aplicación $f\colon G_1 \to G_2$ es llamada un **homomorfismo de grupos** si para cada $g, h \in G$ se cumple que

$$f(g \cdot h) = f(g) \cdot f(h).$$

Definición 1.2.8. Sea $f\colon G_1 \to G_2$ un homomorfismo de grupos. Entonces, la **imagen de** f es el conjunto

$$\mathrm{Im}(f) = \{y \in G_2\colon \text{ existe } x \in G_1, f(x) = y\}.$$

El **kernel de** f es el conjunto

$$\ker(f) = \{x \in G_1 \colon f(x) = 1\}.$$

Definición 1.2.9. Un homomorfismo de grupos $f \colon G_1 \to G_2$ es llamado un **epimorfismo** si es sobreyectivo. Se llama a f un **monomorfismo** si es inyectivo. Por último, se dice que f es un **isomorfismo** si es sobreyectivo e inyectivo. Dados dos grupos G_1 y G_2, se dice que son **isomorfos**, y se denota como $G_1 \simeq G_2$ si existe un isomorfismo $f \colon G_1 \to G_2$.

Un homomorfismo de un grupo G en sí mismo es llamado un **endomorfismo** y si a su vez es un isomorfismo se llama **automorfismo** de G. El siguiente resultado se debe al famoso matemático británico Arthur Cayley, el cual demuestra la relevancia de los grupos de permutación en la teoría de grupos.

Teorema 1.2.2 (Cayley). Todo grupo G es isomorfo a un grupo de permutaciones.

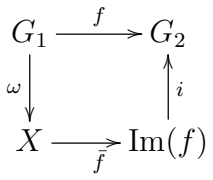
Definición 1.2.10. Sea H un subgrupo normal de un grupo G y $a, b \in G$. Se dice que $a \equiv b \pmod{H}$ si $b^{-1}a \in H$. Es fácil demostrar que esta relación es de equivalencia. Para un elemento $a \in G$ se denota su clase de equivalencia como

$$\bar{a} = \{x \in G \colon x \equiv a \pmod{H}\} = \{x \in G \colon a^{-1}x \in H\} = aH.$$

Se denota como G/H al conjunto de clases de equivalencia de los elementos de G. Se define el producto de elementos en G/H como

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

Figura 1: Primer teorema de isomorfía de grupos



Fuente: elaboración propia con paquete **xymatrix** para LaTeX.

Esta operación es bien definida y G/H es un grupo, llamado **grupo cociente**.

Considérese la aplicación $\omega\colon G \to G/H$ dada por:

$$G \ni a \mapsto \omega(a) = \bar{a} = aH.$$

Es evidente que ω es un epimorfismo de grupos, llamado **homomorfismo canónico** de G hacia el grupo cociente G/H. Este homomorfismo satisface que $\omega(1) = 1H = H$ y $\ker(\omega) = H$.

Teorema 1.2.3 (Primer teorema de isomorfía de grupos). Sea $f\colon G_1 \to G_2$ un homomorfismo de grupos, ω el homomorfismo canónico de G_1 hacia el grupo cociente $X = G_1/\ker(f)$ e i la inclusión de $\mathrm{Im}(f)$ en G_2. Entonces existe un homomorfismo único $\bar{f}\colon G_1/\ker(f) \to \mathrm{Im}(f)$ tal que $f = i \circ \bar{f} \circ \omega$, es decir que diagrama de la figura 1 conmuta. Además $\bar{f}$ es un isomorfismo.

Corolario 1.2.3. Sea $f\colon G_1 \to G_2$ un epimorfismo. Entonces

$$G_1/\ker(f) \simeq G_2.$$

Lema 1.2.2. Sea H un subgrupo normal de G. Entonces

- Para cada subgrupo K de G que contiene a H, el conjunto $K/H = \{xH \colon x \in K\}$ es un subgrupo de G/H que es normal si y sólo si K es normal.
- Si $\mathcal{K}$ es un subgrupo de G/H, entonces la preimagen $K = \{x \in G \colon xH \in \mathcal{K}\}$ es un subgrupo de G que contiene a H, tal que $\mathcal{K} = K/H$.

Teorema 1.2.4. Sea $f \colon G_1 \to G_2$ un epimorfismo de grupos, entonces existe un biyección entre el conjunto de subgrupos de G_2 y el conjunto de subgrupos de G_1 que contienen a $\ker(f)$.

Teorema 1.2.5 (Segundo teorema de isomorfía de grupos). Sea H y K subgrupos de un grupo G y supóngase que K es normal. Entonces:

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

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

Teorema 1.2.6 (Tercer teorema de isomorfía de grupos). Sean $H \subset K$ subgrupos normales de un grupo G. Entonces:

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

1.2.2. Productos directos

Definición 1.2.11. Sean $H,\ K$ subgrupos de un grupo G. Se dice que G es el **producto directo interno** de H y K y se escribe $G = H \times K$ si se cumplen las siguientes condiciones:

- $G = HK$.
- $H \cap K = \{1\}$.
- $H \triangleleft G$ y $K \triangleleft G$.

La definición anterior se puede extender a familias arbitrarias de subgrupos normales, como se muestra en la siguiente definición.

Definición 1.2.12. Sea $\{H_i\}_{i \in I}$ un familia de subgrupos normales de un grupo G. Entonces G es llamado el **producto directo interno** de los subgrupos $\{H_i\}_{i \in I}$ si se cumplen las siguientes condiciones:

- $G = \langle H_i \colon i \in I \rangle$, es decir que cada elemento g de G se puede escribir como producto de un número finito de elementos de los subgrupos $\{H_i\}_{i \in I}$.
- $H_i \cap \langle H_j \colon j \in I,\ j \neq i \rangle = \{1\}$ para cada índice $i \in I$.

Definición 1.2.13. Dada una familia de grupos $G_1, \ldots, G_n$ considérese el producto cartesiano $G = G_1 \times \cdots \times G_n$. Considérese la operación entre elementos de G componente a componente usando la operación de cada $G_i, 1 \leq i \leq n$. Con la operación definida previamente es fácil demostrar que G es un grupo. A este se le llama **producto directo externo** de $G_1, \ldots, G_n$.

Si $G_1, \ldots, G_n$ es una familia de grupos y $G = G_1 \dot{\times} \cdots \dot{\times} G_n$ su **producto directo externo**, entonces los conjuntos

$$H_1 = \{(x, 1, \ldots, 1) \colon x \in G_1\}, \ldots, H_n = \{(1, 1, \ldots, x) \colon x \in G_n\}$$

son subgrupos normales de G tales que $G_i \simeq H_i, 1 \leq i \leq n$ y G es también el producto directo interno de los subgrupos $H_1, \ldots, H_n$. De manera similar, si G es el producto directo interno de una familia de subgrupos normales $H_1, \ldots, H_n$ y se construye el

producto directo externo $\bar{G} = H_1 \dot{\times} \cdots \dot{\times} H_n$, entonces se tiene que $\bar{G} \simeq G$. Debido a este hecho, no se hace distinción entre producto interno y externo.

1.2.3. Grupos abelianos

Los grupos abelianos resultan de mucho interés para el desarrollo del capítulo 5, así que se remarca sus importancia. Sea G un grupo abeliano. Un elemento de G es llamado un **elemento de torsión** si este es de orden finito. Si dos elementos $g, h \in G$ son de torsión, de órdenes m y n respectivamente, entonces es inmediato que $(g^{-1}h)^{mn} = 1$, lo cual demuestra que el conjunto de elementos de torsión de G es un subgrupo de G. Nótese que este hecho también demuestra que dado un número primo p, el conjunto de elementos de G cuyos órdenes son potencias de p también constituyen un subgrupo de G.

Definición 1.2.14. Sea G un grupo abeliano. Entonces, el subgrupo

$$T(G) = \{g \in G \colon \circ(g) < \infty\}$$

es llamado el **subgrupo de torsión** de G y el subgrupo

$$G(p) = \{g \in G \colon \circ(g) \text{ es una potencia de } p\}$$

es llamado la **componente p-primaria** de G.

Se dice que G es un grupo **libre de elementos de torsión** si $T(G) = (1)$. Un grupo abeliano que es producto directo de grupos cíclicos infinitos se llama **abeliano libre**. Al número de factores directos se le llama **rango** del grupo abeliano libre. Si dicho número no es finito, se dice que tiene **rango infinito**.

Teorema 1.2.7. Un grupo G que es abeliano, finitamente generado y libre de elementos de torsión debe ser libre.

Teorema 1.2.8. Sea G un grupo abeliano finitamente generado. Entonces $T(G)$ es finito, $G/T(G)$ es libre de rango finito y

$$G \simeq T(G) \times \frac{G}{T(G)}.$$

Lema 1.2.3. Sea g un elemento de orden $\circ(g) = p_1^{n_1} \cdots p_t^{n_t}$ de un grupo G. Entonces se puede escribir $g = g_1 \cdots g_t$ con $\circ(g_i) = p_i^{n_i}, i \leq i \leq t$. Más aún, los elementos $g_1, \ldots, g_t$ que están determinados de manera única son potencias de g y por lo tanto conmutan entre ellos.

Un elemento cuyo orden es potencia de un número primo p es llamado **p-elemento**. Por otro lado, si p no divide el orden del elemento, se dice que es un **p'-elemento**.

Lema 1.2.4. Sea G un grupo abeliano finito de orden $|G| = p_1^{n_1} \cdots p_t^{n_t}$. Entonces

$$G = G(p_1) \times \cdots \times G(p_t).$$

Definición 1.2.15. Sea p un primo. Un grupo finito G es llamado **p-grupo** si su orden es una potencia de p. Se dice que un grupo abeliano G es un **abeliano elemental** si existe un primo p tal que todos los elementos distintos al elemento identidad son de orden p.

Es interesante notar que los p-grupos abelianos elementales también pueden ser vistos como espacios vectoriales.

Lema 1.2.5. Sea G un p-grupo abeliano elemental. Entonces G es un espacio vectorial sobre $\mathbb{Z}_p$. Más aún, si G es finito entonces puede ser escrito como producto directo de un número finito de grupos cíclicos de orden p.

Para un grupo G se define su **exponente**, y se denota como $\exp(G)$, como el entero positivo más pequeño m, tal que $g^m = 1$ para cualquier $g \in G$. Nótese que G es un p-grupo abeliano elemental si y sólo $\exp(G) = p$ y que si G es un grupo abeliano con $\exp(G) = p^m$, entonces $\exp(G^p) = p^{m-1}$.

Teorema 1.2.9. Sea G un p-grupo abeliano finito. Entonces G se puede escribir como producto directo de p-subgrupos cíclicos. Esta descomposición es única, en el sentido que si

$$G = C_1 \times \cdots \times C_t = D_1 \times \cdots \times D_s$$

donde $C_i, D_j, 1 \leq i \leq t, 1 \leq j \leq s$, son p-grupos cíclicos de órdenes $p^{n_1} \geq \cdots \geq p^{n_t} > 1$ y $p^{m_1} \geq \cdots \geq p^{m_s} > 1$ respectivamente, entonces $t = s$ y $n_i = m_i, 1 \leq i \leq t$.

Proposición 1.2.2. Sea G un grupo abeliano finito de orden n. Entonces para cada divisor d de n, el número de subgrupos cíclicos de G de orden d es igual al número de factores cíclicos de G del mismo orden.

1.2.4. Grupos hamiltonianos

Se define el **grupo de cuaterniones** de orden 8 como:

$$K_8 = \langle a, b \colon a^4 = 1,\ a^2 = b^2,\ bab^{-1} = a^{-1} \rangle.$$

Los elementos de este grupo se enumeran de la siguiente manera:

$$K_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Definición 1.2.16. Dados dos elementos x, y en un grupo G, el **conmutador** de x con y es el elemento $[x, y] = x^{-1}y^{-1}xy \in G$. Dados dos subconjuntos H y K de un grupo G, se denota como $[H, K]$ el subgrupo de G generado por el conjunto:

$$\{[h, k] \colon h \in H, k \in K\}.$$

En particular, el grupo $G' = [G, G]$ es llamado **subgrupo conmutador** o **subgrupo derivado** de G.

Un cálculo directo demuestra que $K_8' = \mathcal{Z}(K_8) = \{1, a^2\}$. Además, a^2 es el único elemento de K_8 de orden 2, entonces si H es un subgrupo cualquiera de K_8, entonces se tiene que $K_8' = \{1, a^2\} \subset H$. Además cualquier subgrupo de K_8 es normal.

Definición 1.2.17. El 4-grupo de Klein está definido por

$$G = \langle a, b \colon a^2 = b^2 = (ab)^2 = 1 \rangle.$$

Ejercicio 1.2.1. Demostrar que K_8/K_8' es isomorfo al 4-grupo de Klein.

Solución 1.2.1. Se sabe que $K_8' = \{1, a^2\}$, entonces calculando las clases de equivalencia se tiene:

$$\begin{aligned}
\bar{1} &= K_8' \\
\bar{a} &= \{a, a^3\} \\
\bar{b} &= \{b, a^2b\} \\
\overline{ab} &= \{ab, a^3b\}
\end{aligned}$$

lo cual genera una partición, por lo tanto $K_8/K_8' = \{\bar{1}, \bar{a}, \bar{b}, \bar{ab}\}$. Ahora bien, $\bar{a} \cdot \bar{a} = \bar{a^2} = \bar{1}$, $\bar{b}\bar{b} = \bar{b^2} = \bar{a^2} = \bar{1}$ y finalmente $\overline{ab} \cdot \overline{ab} = \overline{(ab)^2} = \bar{1}$ con lo que concluye la demostración. □

Definición 1.2.18. Un grupo G es **hamiltoniano** si no es conmutativo y todos sus subgrupos son normales.

Lema 1.2.6. Todo grupo hamiltoniano contiene un subgrupo isomorfo a K_8.

Teorema 1.2.10. Un grupo G es hamiltoniano si y sólo si G es producto directo de un grupo cuaterniones de orden 8, un 2-grupo abeliano elemental E y un grupo abeliano A en el cual todos sus elementos son de orden impar.

La demostración de este importante teorema se puede consultar en (20:130).

1.3. Anillos, módulos y álgebras

En lo subsiguiente será de vital importancia conocer propiedades importantes de los anillos, módulos y álgebras, es por eso que se ha dedica esta sección para su estudio, la mayoría de veces, no se darán demostraciones.

1.3.1. Anillos

Definición 1.3.1. Un **anillo** es un conjunto no vacío R dotado con dos operaciones binarias llamadas suma y multiplicación y denotadas como $+$ y $\cdot$ respectivamente, tal que para cada $a, b \in R$ se cumplen las siguientes propiedades:

- $a + (b + c) = (a + b) + c$.
- Existe un único elemento $0 \in R$ tal que $a + 0 = 0 + a = a$.
- $a + b = b + a$.
- Para cada $a \in R$ existe un elemento $-a \in R$ tal que $a + (-a) = (-a) + a = 0$.
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- $a \cdot (b + c) = a \cdot b + a \cdot c$.
- $(a + b) \cdot c = a \cdot c + b \cdot c$.

Además, si se satisface

- $a \cdot b = b \cdot a$.

se dice que el anillo es **conmutativo**. Un anillo es llamado **dominio** si satisface:

- $a \cdot b = 0$ implica que $a = 0$ o $b = 0$.

Dos elementos a, b distintos de cero de un anillo R tales que $ab = 0$ son llamados **divisores de cero**. Así que un dominio es un anillo sin divisores de cero. Un anillo R que contiene un elemento $1 \neq 0$ tal que

$$1 \cdot a = a \cdot 1 = a, \text{ para todo } a \in R$$

es llamado **anillo con unidad**. A un anillo con unidad que es un dominio conmutativo se le llama **dominio entero**.

Definición 1.3.2. Un elemento a de un anillo R es **invertible** si existe un elemento $a^{-1} \in R$, conocido como su **inverso**, tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$. El conjunto

$$\mathcal{U}(R) = \{a \in R \colon a \text{ es invertible}\}$$

se llama el **grupo de unidades** de R.

A un anillo se le llama **de división** si todos los elementos distintos de cero son invertibles, dicho de otra manera, si $R\backslash\{0\} = \mathcal{U}(R)$. Un anillo de división conmutativo es un **campo**.

Ejemplo 1.3.1. El conjunto $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ de enteros módulo m es un anillo conmutativo. Más aún $\mathbb{Z}_m$ es un campo si y sólo si m es un número primo.

Ejemplo 1.3.2. Sea R un anillo. Entonces el conjunto $R[X]$ de todos los polinomios con coeficientes en R e indeterminada X con la operación usual de suma y multiplicación de polinomios es un anillo. El anillo de polinomios $R[X]$ es un dominio si y sólo si R lo es.

Ejemplo 1.3.3. Sea R un anillo. Entonces, el conjunto $M_n(R)$ de todas la matrices de $n \times n$ con entradas en R, con suma y producto usual de matrices es un anillo. Este anillo es llamado **anillo completo de matrices** de $n \times n$ sobre R.

Ejemplo 1.3.4. Sean $R_1, R_2, \ldots, R_n$ anillos. El anillo

$$R_1 \dot{\oplus} R_2 \dot{\oplus} \cdots \dot{\oplus} R_n = \{(a_1, a_2, \ldots, a_n),\ a_i \in R_i, 1 \leq i \leq n\},$$

con la suma y el producto definido componente a componente es llamado **suma directa** de los anillos $R_1, R_2, \ldots, R_n$.

El siguiente ejemplo es el primero de un anillo no conmutativo en la historia de las matemáticas.

Ejemplo 1.3.5. Sean i, j, k símbolos dados y considérese el conjunto $\mathcal{H}$ de todas las expresiones de la forma $x_0 + x_1 i + x_2 j + x_3 k$ donde los coeficientes x_0, x_1, x_2, x_3 son números reales. Se define la suma de dos elementos de este conjunto como

$$(x_0+x_1i+x_2j+x_3k)+(y_0+y_1i+y_2j+y_3k) = (x_0+y_0)+(x_1+y_1)i+(x_2+y_2)j+(x_3+y_3)k.$$

La multiplicación está definida de manera distributiva, con las siguientes reglas:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = k &= -ji \\ jk = i &= -kj \\ ki = j &= -ik. \end{aligned}$$

Por medio de un cálculo sencillo se demuestra que $\mathcal{H}$ es un anillo, llamado **anillo de cuaterniones reales**. Dado un cuaternión $\alpha = x_0 + x_1 i + x_2 j + x_3 k$, se define el

conjugado $\bar{\alpha}$ de α como

$$\bar{\alpha} = x_0 - x_1 i - x_2 j - x_3 k.$$

La norma de α se define como

$$\|\alpha\| = \alpha\bar{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

Al igual que en el caso de los números complejos, se cumple que:

- $\|\alpha\beta\| = \|\alpha\|\|\beta\| = \|\alpha\beta\|$.
- $\|\alpha\| \geq 0$ y $\|\alpha\| = 0$ si y sólo si $\alpha = 0$.

Si $\alpha \in \mathcal{H}$ es distinto de cero, se tiene que $\|\alpha\| \neq 0$, entonces se puede definir $\alpha' = \bar{\alpha}/\|\alpha\|$. Entonces

$$\alpha\alpha' = \alpha\frac{\bar{\alpha}}{\|\alpha\|} = 1$$

y de manera similar se demuestra que $\alpha'\alpha = 1$, de donde se sigue que $\alpha^{-1} = \alpha'$. Este argumento demuestra que $\mathcal{H}$ es un anillo de división. Se define $\mathcal{H}_{\mathbb{Q}}$ restringiendo $\mathcal{H}$ al campo de los números racionales. A este conjunto se le conoce como cuaterniones racionales. Finalmente se definen los **cuaterniones enteros** como

$$\mathcal{H}_{\mathbb{Z}} = \{x_0 + x_1 i + x_2 j + x_3 k \colon x_0, x_1, x_2, x_3 \in \mathbb{Z}\}.$$

Es evidente que $\mathcal{H}_{\mathbb{Z}}$ es un anillo de división. Sea $\alpha \in \mathcal{U}(\mathcal{H}_{\mathbb{Z}})$ entonces es inmediato, de la definición de norma, que $\|\alpha\|$ es un entero positivo, más aún, como $\alpha\alpha' = 1$ entonces $\|\alpha\|\|\alpha'\| = 1$ y consecuentemente $\|\alpha\| = 1$, es decir, $x_i = 1$ para algún

índice $0 \leq i \leq 3$ y $x_j = 0$ para $j \neq i$. De lo anterior se tiene

$$\mathcal{U}(\mathcal{H}_{\mathbb{Z}}) = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Definición 1.3.3. Un subconjunto no vacío S de un anillo R es un **subanillo** de R si es cerrado bajo las operaciones de R y es un anillo respecto a estas operaciones.

Definición 1.3.4. El **centro** de un anillo R es el subanillo

$$\mathcal{Z}(R) = \{a \in R \colon ax = xa, \text{ para todo } x \in R\}.$$

Definición 1.3.5. Un subconjunto no vacío L de un anillo R es un **ideal izquierdo** de R si cumple las siguientes propiedades:

- Si $x, y \in L$ entonces $x - y \in L$.
- Si $x \in L$ y $a \in R$ entonces $ax \in L$.

De manera similar se define un **ideal derecho** de un anillo R. Un subconjunto no vacío L de un anillo R se llama **ideal** de R si es un ideal derecho e izquierdo de R. Los subconjuntos $\{0\}$ y R de un anillo R siempre son ideales de R. Un ideal L de R distinto de estos se llama **ideal propio**. Nótese que si un ideal L de un anillo R contiene un elemento invertible a entonces $L = R$ no es ideal propio.

Definición 1.3.6. Sea R un anillo y $a \in R$. El conjunto

$$RA = \{xa \colon x \in R\}$$

es llamado el **ideal izquierdo generado por** a. Al elemento a se le conoce como **generador** de este ideal. Los ideales generados por un elemento $a \in R$ se llaman **ideales principales** y se denotan como (a).

Proposición 1.3.1. Sea D un anillo de división y n un entero positivo. Entonces el anillo completo de matrices $M_n(D)$ no contiene ideales propios.

Definición 1.3.7. Sean R, S anillos. Una aplicación $f\colon R \to S$ se llama **homomorfismo de anillos** si para cualesquiera $a, b \in R$ se cumple:

- $f(a+b) = f(a) + f(b)$.
- $f(ab) = f(a)f(b)$.

Definición 1.3.8. Sea $f\colon R \to S$ un homomorfismo de anillos. Entonces la **imágen** de f es el subanillo

$$\mathrm{Im}(f) = \{y \in S\colon \text{existe } x \in R, f(x) = y\}.$$

El **kernel** de f es el ideal

$$\ker(f) = \{x \in R\colon f(x) = 0\}.$$

Definición 1.3.9. Un homomorfismo de anillos $f\colon R \to S$ es un **epimorfismo** si es sobreyectivo. Se dice que f es un **monomorfismo** si es inyectivo. Finalmente, si f es inyectivo y sobreyectivo entonces se dice que f es un **isomorfismo**.

Un homomorfismo de un anillo R en sí mismo es un **endomorfismo** y si también es un isomorfismo entonces se llama **automorfismo** de R.

Definición 1.3.10. Sea I un ideal de R. El grupo cociente aditivo R/I con la multiplicación definida por $\bar{r}\bar{s} = \overline{rs}$ es un anillo llamado **cociente** de R por I.

1.3.2. Módulos y álgebras

Definición 1.3.11. Sea R un anillo. Un grupo aditivo abeliano M es llamado un R**-módulo izquierdo** si para todo $a \in R$ y $m \in M$ se cumple que $am \in M$ y

- $(a+b)m = am + bm$.
- $a(m_1 + m_2) = am_1 + am_2$.
- $a(b)m = (ab)m$.
- $1m = m$.

para cualesquiera $a, b \in R$ y $m, m_1, m_2 \in M$.

De manera similar, dado un anillo R, se define un R-módulo derecho considerando la multiplicación de elementos de M por elementos de R por la derecha. De acá en adelante, un R-módulo izquierdo será abreviado como R-módulo.

Ejemplo 1.3.6. Un ideal izquierdo L de un anillo R es un R-módulo, ya que el producto de elementos de R por elementos de L pertenece a L. Así mismo, los ideales derechos también son R-módulos derechos. En particular, un anillo siempre es un módulo sobre sí mismo. Cuando se considere un anillo como un R-módulo izquierdo o derecho sobre sí mismo se denotará como ${}_RR$ y R_R respectivamente.

Ejemplo 1.3.7. Sea L un ideal derecho de un anillo R y R/L el grupo cociente aditivo. Entonces R/L es un R-módulo con

$$r(a + L) = ra + L, \text{ para todo } r, a \in R$$

Definición 1.3.12. Sea R un anillo conmutativo. Un R-módulo A es un **R-álgebra** si existe una operación de multiplicación definida en A tal que con su adición y esta multiplicación A es un anillo que cumple:

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

para todo $r \in R$ y $a, b \in A$.

Definición 1.3.13. Sea M un módulo sobre un anillo R. Un conjunto no vacío $N \subset M$ es llamado un **R-submódulo** de M si se cumplen las siguientes condiciones:

- Para todos $x, y \in N$ se tiene $x + y \in N$
- Para cualquier $r \in R$ y todo $n \in N$, $rn \in N$

Si R es conmutativo y M es un R-álgebra, entonces se dice que N es un R-subálgebra de M si es un submódulo y un subanillo de M al mismo tiempo.

Todo módulo $M \neq \{0\}$ contiene al menos dos submódulos, a saber, M y $\{0\}$, que son llamados **triviales**. Un submódulo no trivial es llamado **submódulo propio**. Un módulo, distinto al módulo que sólo contiene al 0, que no contiene submódulos propios es un **módulo simple**. Sea N un submódulo de un R-módulo M. Al igual que en el caso de los anillos, el grupo cociente aditivo M/N es un R-módulo con $r\bar{m} = \overline{rm}, r \in R, m \in M$. Este es el módulo cociente entre M y N.

1.3.3. Módulos libres

Definición 1.3.14. Un conjunto $S = \{s_i\}_{i \in I}$, I un conjunto de índices, de elementos de un R-módulo M es un **conjunto de generadores** de M si $M = RS$, es decir, si todo elemento de M se puede escribir como un combinación lineal finita de elementos de S con coeficientes en R.

Definición 1.3.15. Un conjunto $S = \{s_i\}_{i \in I}$ de elementos de un R-módulo M es **linealmente independiente** o R-libre si toda combinación lineal de elementos de S con coeficientes en R de la forma

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

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

Definición 1.3.16. Un conjunto $S = \{s_i\}_{i\in I}$, I un conjunto de índices, de elementos de un R-módulo M es una **base** de M sobre R o una R-**base** si es linealmente independiente y un conjunto de generadores.

Definición 1.3.17. Un R-módulo M es **libre** si tiene una base.

Definición 1.3.18. Sea $\{M_i\}_{i\in I}$, I un conjunto de índices, un familia de submódulos de un R-módulo M. Se dice que M es la **suma directa** de submódulos de esta familia y se escribe $M = \oplus_{i\in I} M_i$ si se cumplen las siguientes condiciones:

- Para todo $i \in I$ se satisface que $M_i \cap \left(\sum_{j\neq i} M_j\right) = \emptyset$.
- $M = \sum_{i\in I} m_i$.

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

Definición 1.3.19. Un submódulo N de un R-módulo M es un **sumando directo** si existe otro módulo N' tal que $M = N \oplus N'$. Un módulo que no contiene sumandos directos, a excepción de los triviales, se llama **indescomponible**.

Caso contrario a los espacio vectoriales, no todo submódulo de un módulo dado es un sumando directo.

Lema 1.3.1. Sea N un submódulo de un R-módulo M. Entonces N es un sumando directo de M si y sólo si existe un endomorfismo $f\colon M \to M$ tal que $f \circ f = f$ e $\mathrm{Im}(f) = N$.

El homomorfismo $f\colon M \to M$ del lema anterior es la **proyección** de M en N.

Proposición 1.3.2. Sea R un anillo. Todo R-módulo M es una imagen epimórfica de un R-módulo libre.

1.3.4. Semisimplicidad

En álgebra lineal se demuestra que todo subespacio de espacio vectorial es un sumando directo. Esta aseveración no es válida en el caso de módulos sobre anillos arbitrarios, por ejemplo, $\mathbb{Z}$ no es un sumando directo de $\mathbb{Q}$ como $\mathbb{Z}$-módulo. Será de interés conocer los módulos que cumplen la propiedad de tener submódulos que sean sumandos directos.

Definición 1.3.20. Un R-módulo M es **semisimple** si todo submódulo de M es un sumando directo.

Proposición 1.3.3. Sea $N \neq (0)$ un submódulo de un módulo semisimple M. Entonces N es semisimple y contiene a un módulo simple.

Demostración. Sea S un submódulo arbitario de N. Entonces N es también submódulo de M, así que existe S' tal que $M = S \oplus S'$. Se asegura que $N = S \oplus (S' \cup N)$. En efecto, por definición $S \cap (S' \cup N) \subset S \cap S' = (0)$. Por otro lado, dado un elemento $n \in N$ se puede escribir $n = x + y$ con $x \in S, y \in S'$, pero $y = n - x \in N$, entonces $y \in N \cup S'$, con lo que se demuestra que N es semisimple.

Para demostrar que N contiene a un submódulo semisimple elíjase un elemento $x \in N, x \neq 0$. Considérese la familia de submódulos de N que tienen a x como elemento y nótese que dicha familia es no vacía, está parcialmente ordenada por inclusión y además toda cadena está acotada por N, por lo que, usando el lema de Zorn, existe un elemento maximal N_1. Como N es semisimple, existe N_2 submódulo de N tal que $N = N_1 \oplus N_2$. Se requiere demostrar que N_2 es simple. Si N_2 no fuera simple, entonces existe W submódulo propio de N_2 tal que $N_2 = W \oplus W'$, con W' submódulo de N_2. De esta manera, $N = N_1 \oplus W \oplus W'$ y $N_1 = (N_1 + W) \cup (N_1 + W')$. Como $x \notin N_1$ entonces $x \notin N_1 + W$ ni $x \in N_1 + W'$, lo cual contradice el hecho que N_1 es maximal. □

Teorema 1.3.1. Sea M un R-módulo. Entonces, las siguientes condiciones son equivalentes:

1. M es semisimple.
2. M es suma directa de submódulos simples.
3. M es suma (no necesariamente directa) de submódulos simples.

Demostración. (1) $\implies$ (2). Sea $\mathcal{F}$ la colección de todos los submódulos de M que se pueden escribir como suma directa de submódulos simples. La proposición anterior asegura la existencia de dichos submódulos. Se define un orden en $\mathcal{F}$ de la siguiente manera: dados dos elementos $\oplus_{i\in I} M_i$ y $\oplus_{i\in J} M_i$ de $\mathcal{F}$, se tiene que $\oplus_{i\in I} M_i \prec \oplus_{i\in J} M_i$ si y sólo si $I \subset J$. Ahora como $(\mathcal{F}, \prec)$ satisface las condiciones del lema de Zorn, existe un elemento maximal $M_0 \in \mathcal{F}$ que se puede escribir como $M_0 = \oplus_{i\in I} M_i$ con $M_i, i \in I$ simple. Ahora sólo falta demostrar que $M_0 = M$. En efecto, si $M_0 \neq M$, entonces existe un submódulo N de M tal que $M = M_0 \oplus N$, pero, por la proposición anterior, N contiene un submódulo simple S y por lo tanto $M_0 \oplus S = \oplus_{i\in I} M_i \oplus S \supset M_0$, lo cual contradice la maximalidad de M_0.

(2) $\implies$ (3) es trivial.

(3) $\implies$ (1). Supóngase que $M = \sum_{i\in I} M_i$, donde cada componente $M_i, i \in I$ es simple. Sea N un submódulo propio cualquiera de M. Se demostrará que N es sumando directo. Considérese la familia

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

y nótese que si $N \cap M_i \neq (0)$ entonces $M_i \subset N$. Como $N \neq M$, se deduce que existe al menos un submódulo M_i tal que $N \cap M_i = (0)$ y $\mathcal{J} \neq \emptyset$. Por el lema de Zorn se puede encontrar un submódulo maximal en $\mathcal{J}$, a saber $M_0 = \sum_{i\in\mathcal{J}_0} M_i$. Como $\left(\sum_{i\in\mathcal{J}_0} M_i\right) \cap N = (0)$, sólo queda por demostrar que $M = M_0 + N$. Para ello se demostrará que $M_i \subset M_0 + N$, para todo $i \in I$. Supóngase por el absurdo que esto no es cierto, entonces existe un índice i_0 tal que $M_{i_0} \nsubseteq M_0 + N$. Ahora bien, M_{i_0} es simple, se tiene que $M_{i_0} \cap (M_0 + N) = (0)$. Entonces $(M_{i_0} + M_0) \cap N = (0)$, lo que implica que $M_{i_0} + M_0 \in \mathcal{J}$, lo cual contradice la maximalidad de M_0. □

Si se conoce la descomposición de un módulo semisimple como suma directa de módulos simples, entonces se puede determinar la estructura de todos sus submódulos.

Corolario 1.3.1. Sea $M = \oplus_{i\in I} M_i$ una descomposición de un módulo semisimple M como suma directa de submódulos y sea N un submódulo de M. Entonces, existe un subconjunto de índices $J \subset I$ tal que $N \simeq \oplus_{i\in J} M_i$.

Demostración. Como se vió en la demostración de la última implicación del teorema anterior, dado un submódulo N de M se puede encontrar un subconjunto de índices

$J_0 \subset I$ tal que $M = N \oplus N_0$, donde $N_0 = \oplus_{i \in J_0} M_i$. Entonces:

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

de donde se sigue el resultado, con $J = I \setminus J_0$. □

Corolario 1.3.2. Un módulo cociente L de un módulo semisimple M es isomorfo a un submódulo de M y por lo tanto es también semisimple.

Demostración. Sea L un módulo cociente de M, $\pi \colon M \to L$ el homomorfismo canónico y $N = \ker(\pi)$. Entonces, existe un submódulo N' de M tal que $M = N \oplus N'$ y por lo tanto $N' \simeq M/\ker(\pi) \simeq L$. Con esto, el resultado se sigue del corolario anterior. □

Definición 1.3.21. Un anillo R es **semisimple** si como módulo ${}_R R$ es semisimple.

Todo submódulo de ${}_R R$ es ideal izquierdo de un anillo R, así que R es semisimple si y sólo si todo ideal izquierdo es un sumando directo.

Teorema 1.3.2. Sea R un anillo. Entonces las siguientes proposicione son equivalentes:

1. Todo R-módulo es semisimple.
2. R es un anillo semisimple.
3. R es una suma directa de un número finito de ideales izquierdos minimales.

Demostración.
(1) $\implies$ (2) es evidente.

(2) $\implies$ (3). Como los submódulos de ${}_RR$ son precisamente los ideales izquierdos minimales de R, se sigue del teorema 1.3.1 que R se puede escribir como $R = \oplus_{i\in I} L_i$ donde cada $L_i, i \in I$ es un ideal izquierdo minimal. De esta manera sólo queda por demostrar que esta suma es finita. En particular, como $R = \langle 1\rangle$, el elemento $1 \in R$ se puede escribir como una suma finita; a saber: $1 = x_{i_1} + \cdots + x_{i_n}$, donde $x_{i_j} \in L_{i_j}$. Entonces para $r \in R$, se tiene que $r = r \cdot 1 = rx_{i_1} + \cdots + rx_{i_n}$, donde $rx_{i_j} \in L_{i_j}, 1 \leq j \leq n$. Esto demuestra que $R \subset L_{i_1} \oplus \cdots \oplus L_{i_n}$, de donde $R = L_{i_1} \oplus \cdots \oplus L_{i_n}$. Nótese que el teorema 1.3.1 demuestra inmediatamente que (3) $\implies$ (2), así que la demostración estará completa si se demuestra que (2) $\implies$ (1).

Supóngase que R es semisimple y sea M un R-módulo, entonces de la proposición 1.3.2 se sabe que M es una imagen epimórfica de un R-módulo libre F. Entonces F se puede escribir como $F = \oplus_i Ra_i$ donde $Ra_i \simeq R$ es semisimple. Por esto, F es semisimple y por lo tanto M lo es. □

Teorema 1.3.3. Sea R un anillo. Entonces R es semisimple si y sólo si todo ideal izquierdo L de R es de la forma $L = Re$, donde $e \in R$ es un idempotente.

Demostración. Supóngase que R es semisimple y sea L un ideal izquierdo de R. Entonces L es un sumando directo de R entonces existe un ideal izquierdo L' tal que $R = L \oplus L'$. De esa cuenta, se puede escribir $1 = x+y$ donde $x \in L$ y $y \in L'$. Entonces $x = x \cdot 1 = x^2 + xy$. De la igualdad anterior se deduce que $xy = x - x^2 \in L$ y como L' es un ideal izquierdo se tiene que $xy \in L'$. De la definición de suma directa se sabe que $L \cap L' = (0)$ por lo tanto $xy = x - x^2 = 0$, de donde $x = x^2$ es un idempotente. Es obvio que $Rx \subset L$. Además dado $a \in L$ se tiene que $a = a \cdot 1 = ax + ay$, de esto se obtiene $a - ax = ay \in L \cap L' = (0)$ y así $a = ax \in Rx$ demostrando que $L = Rx$.

Ahora bien, supóngase que los ideales izquierdos de R son de la forma propuesta en el enunciado. Dado esto, se requiere demostrar que todo ideal izquierdo de R

es sumando directo. Por hipótesis $L = Re$ donde $e \in R$ es idempotente. Sea $L' = R(1-e)$. Entonces es claro que L' es un ideal izquierdo y dado un elemento $x \in R$ se puede escribir $x = xe + x(1-e)$, así que $R = Re + R(1-e)$. Además si $x \in Re \cap R(1-e)$ se tiene que cumplir que $x = re = s(1-e)$, con $r, s \in R$. Entonces $xe = s(1-e)e = 0$, de donde $x = 0$. □

Teorema 1.3.4. Sea $R = \oplus_{i=1}^{t} L_i$ una descomposición de un anillo semisimple como suma directa de ideales izquierdos minimales. Entonces, existe una familia $\{e_1, \ldots, e_t\}$ de elementos de R tal que:

1. $e_i \neq 0, 1 \leq i \leq t$ es idempotente.
2. Si $i \neq j$ entonces $e_i e_j = 0$.
3. $1 = e_1 + \cdots + e_t$.
4. e_i no se puede escribir como $e_i = e_i' + e_i''$, donde e_i', e_i'' son idempotentes tales que $e_i, e_i'' \neq 0$ y $e_i' e_i'' = 0, 1 \leq i \leq t$.

Además, si existe una familia de idempotentes $\{e_1, \ldots, e_t\}$ que satisface las cuatro condiciones anteriores entonces la familia de ideales izquierdos minimales $L_i = Re_i$ es tal que $R = \oplus_{i=1}^{t} L_i$.

Demostración. Supóngase que $R = \oplus_{i=1}^{t} L_i$ es una descomposición del anillo R como suma directa de ideales izquierdos minimales. Con esta descomposición se puede escribir $1 = e_1 + \cdots + e_t$ donde $e_i \in L_i$. Entonces se deduce, como en el teorema anterior, que e_i es idempotente tal que $L_i = Re_i, 1 \leq i \leq t$. Si $i \neq j$ entonces $e_i e_j = 0$. Por último, si para algún índice i se puede escribir $e_i = e_i' + e_i''$, donde e_i', e_i'' son idempotentes tales que $e_i, e_i'' \neq 0$ y $e_i' e_i'' = 0$ entonces de nuevo, como en el teorema anterior, se obtiene que $L_i = Re_i' \oplus Re_i''$ con $Re_i', Re_i'' \neq 0$, lo cual contradice la minimalidad de L_i.

Para el converso, supóngase que existe una familia de idempotentes $\{e_1, \ldots, e_t\}$ que satisfacen las condiciones dadas. Se demostrará en primera instacia, que $L_i = Re_i$ es minimal. Para ello supóngase por el absurdo que no lo es, entonces existe un ideal izquierdo J tal que $J \subset L_i$, pero como ${}_RR$ es semisimple entonces L_i también lo es, por lo tanto existe J' tal que $L_i = J \oplus J'$. Esto implica que se puede escribir $e_i = e_i' + e_i''$, donde e_i', e_i'' son idempotentes tales que $e_i, e_i'' \neq 0$, lo cual es una contradicción. $R = L_1 + L_2 + \cdots + L_t$ se deduce fácilmente del hecho que $1 = e_1 + \cdots + e_t$. Ahora para demostrar que la suma es directa, tómese $x \in L_j \cap \left(\sum_{i \neq j} L_i\right)$. Entonces se puede escribir $x = r_j e_j = \sum_{i \neq j} r_i e_i$. Multiplicando por e_j por la derecha la ecuación anterior se obtiene $r_j e_j e_j = x = \sum_{i \neq j} r_i e_i e_j = 0$. $\square$

Definición 1.3.22. Sea R un anillo. Una familia de idempotentes $\{e_1, \ldots, e_t\}$ que satisfacen las condiciones 1, 2 y 3 del teorema anterior es llamada una **famlia completa de idempotentes ortogonales**. Un idempotente que satisface la condición 4 se llama **primitivo**.

Lema 1.3.2. Sea L un ideal izquierdo minimal de un anillo semisimple R y sea M un R-módulo. Entonces $LM \neq (0)$ si y sólo si $L \simeq M$ como R-módulos. En este caso $LM = M$.

1.3.5. El teorema de Wedderburn-Artin

Este teorema y los que sirven de base para su demostración son de mucha importancia, ya que revelan la estructura de los anillos semisimples.

Lema 1.3.3. Sea L un ideal izquierdo minimal de un anillo semisimple R. Entonces la suma de todos los ideales izquierdos de R isomorfos a L es un ideal bilateral de R.

Demostración. Sea $A = \sum_{J \simeq L} J$. Es evidente que A es un ideal izquierdo. Se desea demostrar que A es también un ideal derecho. Como R es semisimple se puede escribir $R = \oplus_{i=1}^{t} L_i$ como suma directa de ideales izquierdos minimales. Entonces $AR = \sum_{J \simeq L} JR = \sum_{J \sim L} \sum_{i=1}^{t} JL_i$, pero $JL_i = (0)$ o $JL_i = L_i$. Por el lema 1.3.2 se demuestra que la última alternativa sólo es posible cuando $J \simeq L_i$, lo que implica que $L_i \subset A$. De esta manera se demuestra que $AR \subset A$. □

Lema 1.3.4. Sea I un ideal que contiene a un ideal izquierdo minimal L de un anillo semisimple. Entonces I contiene a todos los ideales izquierdos isomorfos a L.

Demostración. Sea $L \subset I$ un anillo izquierdo minimal y sea J un ideal izquierdo isomorfo a L. Entonces, del lema 1.3.2, se tiene que $J = LJ \subset I$. □

Proposición 1.3.4. Sea L un ideal izquierdo minimal de un anillo simisimple R y B la suma de todos los ideales de R isomorfos a L. Entonces B es un ideal bilateral minimal de R.

Demostración. Sea B_1 un ideal de R contenido en B y L_1 un ideal izquierdo minimal de R contenido en B_1. Si $L_1 \not\simeq L$, entonces se tiene que $L_1 J = (0)$, para todo $J \simeq L$. Así, $L_1 B = (0)$ lo cual implica, en particular, que $L_1 L_1 = (0)$. Esto no es posible porque el teorema 1.3.3 implica que L_1 contiene a un elemento idempotente. Este argumento implica que $L_1 \simeq L$ y aplicando el lema anterior se obtiene que $B_1 = B$. □

Dada una descomposición de un anillo semisimple R como suma directa de ideales izquierdos minimales se puede agrupar los ideales izquierdos isomorfos de la siguiente manera:

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

Con la notación anterior, $L_{ij} \simeq L_{ik}$ y $L_{ij}L_{kh} = (0)$ si $i \neq k$, por el lema 1.3.2.

Teorema 1.3.5. Con la notación anterior, sea A_i la suma de todos los ideales izquierdos isomorfos a $L_{i1}, 1 \leq i \leq s$. Entonces:

1. Cada A_i es un ideal minimal de R.
2. $A_iA_j = (0)$ si $i \neq j$.
3. $R = \oplus_{i=1}^{s} A_i$ como anillos, donde s es el número de clases isomorficas de ideales minimales de R.

Demostración. (1) se sigue directamente de la proposición anterior. Para demostrar (2), se escribe

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

Entonces todo elemento $x \in R$ se puede escribir en la forma $x = x_{11} + \cdots + x_{rr_1} + \cdots + x_{s1} + \cdots + x_{xr_s}$, 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 $x = y_1 + \cdots + y_s$. Esto demuestra que $R = A_1 + \cdots + A_s$. Para terminar, se tiene que $A_i \cap A_j = (0)$ se sigue de la definición de A_i y del lema 1.3.2. □

Definición 1.3.23. Un anillo R es **simple** si sus únicos ideales son (0) y R.

Nótese que si D es un anillo y n un entero positivo, entonces $M_n(D)$ es un anillo simple.

Corolario 1.3.3. Los ideales $A_i, 1 \leq i \leq s$, definidos previamente son simples.

Proposición 1.3.5. Sea $R = \oplus_{i=1}^{s} A_i$ la descomposición de un anillo semisimple R como suma directa de ideales minimales. Entonces:

- Todo ideal I de R se puede escribir de la forma $I = A_{i_1} \oplus \cdots \oplus A_{i_t}$, donde $1 \leq i_{i_1} < \cdots < i_t \leq s$.
- Si $R = \oplus_{j=1}^{r} B_i$ es otra descomposición de R como suma suma directa de ideales minimales, entonces $s = r$ y (después de una posible ordenación de los índices) $A_i = B_i$ para todo i.

Demostración. Sea I un ideal de R. Entonces $I = \oplus_{i=1}^{s}(A_i \cap I)$. Como los A_i son minimales la primera propiedad queda probada. Por la misma razón cada B_j es igual a algún A_i y viceversa. □

Definición 1.3.24. Los únicos ideales minimales de un anillo semisimple R son llamados las **componentes simples de** R.

Teorema 1.3.6. Sea $R = \oplus_{i=1}^{s} A_i$ una descomposición de un anillo semisimple como suma directa de ideales minimales. Entonces existe una familia $\{e_1, \ldots, e_s\}$ de elementos de R tal que:

1. $e_i \neq 0, 1 \leq i \leq t$ es un idempotente central.
2. Si $i \neq j$ entonces $e_i e_j = 0$.
3. $1 = e_1 + \cdots + e_t$.
4. e_i no puede ser escrito como $e_i = e_i' + e_i''$ donde e_i', e_i'' son idempotentes centrales tales que $e_i', e_i'' \neq 0$ y $e_i' e_i'' = 0, 1 \leq i \leq t$.

Demostración. La demostración es análoga a la del teorema 1.3.4. La única diferencia es que $e_i, 1 \leq i \leq s$ son centrales. Entonces para $x \in R$ se tiene de la tercera condición que $x = \sum_{i=1}^{t} xe_i = \sum_{i=1}^{t} e_i x$. Como los A_i son ideales y la suma es directa se concluye que $xe_i = e_i x$. □

Definición 1.3.25. Los elementos $\{e_1, \ldots, e_s\}$ del teorema anterior son llamados los **idempotentes centrales primitivos de** R.

Lema 1.3.5. Sea R un anillo, $M = M_1 \oplus \cdots \oplus M_r$ y $N = N_1 \oplus \cdots \oplus \cdots \oplus N_s$ dos R-módulos escritos como sumas directas de submódulos. Sea $\epsilon_j \colon M_j \to M$ la inclusión de M_j en M y $\pi_i \colon N \to N_i$ el homomorfismo natural de N hacia sus componentes.

- Supóngase que para cualquier par de índices i, j existe un homomorfismo $\phi_{ij} \in \hom_R(M_j, N_i)$. Entonces, la aplicación $\phi \colon M \to N$ definida por:

$$\phi(m_1 + \cdots + m_r) = \begin{pmatrix} \phi_{11} & \cdots & \phi_{1r} \\ \vdots & \ddots & \vdots \\ \phi_{s1} & \cdots & \phi_{sr} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$$

$$= \underbrace{\phi_{11}(m_1) + \cdots + \phi_{1r}(m_r)}_{\in N_1} + \cdots + \underbrace{\phi_{s1}(m_1) + \cdots + \phi_{sr}(m_r)}_{\in N_s},$$

  es un homomorfismo. Para indicar que ϕ es de la forma previamente descrita se escribe $\phi = (\phi_{ij})$. El converso también es cierto, es decir, si ϕ es de la forma descrita en el inciso anterior, entonces $\phi_{ij} = \pi_i \circ \phi \circ \epsilon_j \in \hom_R(M_j, N_i)$ y $\phi = (\phi_{ij})$.
- Para $\phi = (\phi_{ij})$ y $\psi = (\psi_{ij})$ se tiene que $\phi + \psi = (\phi_{ij} + \psi_{ij})$.
- $\hom_R(M^{(n)}, M^{(n)}) \simeq M_n(\hom_R(M, M))$ como anillos.

Lema 1.3.6. Sea R un anillo, M un R-módulo semisimple y $B = \hom_R(M, M)$. Entonces M admite una estructura de B-módulo dada por $\phi \cdot m = \phi(m)$, para todo $\phi \in B, m \in M$. Más aún para cada $m \in M$ y $f \in \hom_B(M, M)$ existe un elemento $a \in R$ tal que $f(m) = am$.

Demostración. La primera aseveración es evidente. Para demostrar la segunda, sea $m \in M$ y considérese el submódulo Rm. Como M es semisimple, entonces existe un submódulo W tal que $M = RM \oplus W$. Si se denota la proyección hacia R_m como $\phi\colon M \to M$ se tiene que $\pi \in \hom_R(M, M) = B$. Dado un elemento $f \in \hom_B(M, M)$, se tiene:

$$f(m) = f(\pi(m)) = \pi(f(m)) \in Rm.$$

Así, existe un elemento $a \in R$ tal que $f(m) = am$. □

Teorema 1.3.7 (Teorema de densidad de Jacobson). Sea M un R-módulo semisimple, $B = \hom_R(M, M)$ y $f \in \hom_B(M, M)$. Si $\{m_1, \ldots, m_n\}$ es un conjunto arbitrario de elementos de M, entonces existe un elemento $a \in R$ tal que $f(m_i) = am_i$, para todo $1 \leq i \leq n$.

Demostración. Dada $f \in \hom_B(M, M)$ se define $f^{(n)}\colon M^{(n)} \to M^{(n)}$ por:

$$f^{(n)}(x_1 + \cdots + x_n) = f(x_1) + \cdots + f(x_n),\ x_1, \ldots, x_n \in M.$$

Sea $B' = \hom_R(M^{(n)}, M^{(n)})$. Se asegura que $f^{(n)} \in \hom_{B'}(M^{(n)}, M^{(n)})$. En efecto,

dado $\phi \in B'$, por lema 1.3.5 se puede escribir $\phi = (\phi_{ij}) \in \hom_R(M_j, M_i)$. Se tiene

$$\begin{aligned} f^{(n)} \circ \phi(m_1 + \cdots + m_n) &= f^{(n)}(\phi_{11}(m_1) + \cdots + \phi_{1n}(m_n) + \cdots \\ &\quad \cdots + \phi_{n1}(m_1) + \cdots + \phi_{nn}(m_n)) \\ &= \phi_{11}(f(m_1)) + \cdots + \phi_{1n}(f(m_n)) + \cdots \\ &\quad \cdots + \phi_{n1}(f(m_1)) + \cdots + \phi_{nn} f((m_n)) \\ &= \phi(f(m_1) + \cdots + f(m_n) \\ &= \phi \circ f^{(n)}(m_1 + \cdots + m_n). \end{aligned}$$

Además, debido al lema anterior, existe un elemento $a \in R$ tal que $f^{(n)}(m_1 + \cdots + m_n) = a(m_1 + \cdots + m_n)$, por lo tanto $f(m_i) = am_i, 1 \leq i \leq n$. □

Lema 1.3.7 (Lema de Schur). Sea R un anillo, M, N R-módulos simples y $f\colon M \to N$ un homomorfismo no nulo. Entonces f es un isomorfismo.

Demostración. Dado que $\mathrm{Im}(f)$ es un submódulo de un módulo simple N y no es igual a (0), entonces $\mathrm{Im}(f) = N$, así que f es epimorfismo. De manera similar $\ker(f)$ es un submódulo de un módulo simple N y no es igual a M entonces $\ker(f) = (0)$. De esto f es un monomorfismo y por lo tanto f es isomorfismo. □

Corolario 1.3.4. Sea R un anillo y M, N R-módulos simples. Entonces:

- Si $M \ncong N$ entonces $\hom_R(M, N) = (0)$.
- $\hom_R(M, M)$ es un anillo de división.

Teorema 1.3.8 (Wedderburn-Artin). Un anillo R es semisimple si y sólo si es una suma directa de álgebras de matrices sobre anillos de división:

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

Para la demostración de este importante resultado se sugiere ver (11:200).

Teorema 1.3.9. Sea R un anillo semisimple y supóngase que

$$R \simeq M_{n_1} \oplus \cdots \oplus M_{n_s} \simeq M_{m_1}(D_1') \oplus \cdots \oplus M_{m_r}(D_r'),$$

donde $D_i, D_j', 1 \leq i \leq s, 1 \leq j \leq r$ son anillos de división. Entonces $s = r$. Además bajo un posible reordenamiento de los índices, se tiene que $n_i = m_i, D_i \simeq D_i'$.

Demostración. Como los anillos de matrices sobre anillos de división son simples se tiene por la proposición 1.3.5 que $s = r$ y existe una biyección entre los dos conjuntos de ideales tal que los correspondientes ideales son iguales. Sólo falta demostrar que si $M_n(D) \simeq M_m(D')$, donde D y D' son anillos de división, entonces $n = m$ y $D \simeq D'$.

Sea $E = M_n(D)$, $E' = M_m(D')$ y

$$L = \begin{pmatrix} D & 0 & \cdots & 0 \\ D & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ D & 0 & \cdots & 0 \end{pmatrix}, L' = \begin{pmatrix} D' & 0 & \cdots & 0 \\ D' & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ D' & 0 & \cdots & 0 \end{pmatrix}.$$

Entonces $L = eE, L' = fE'$ donde e y f son las correspondientes matrices idempotentes con 1 en la posición $(1,1)$ y ceros en cualquier otra posición. Bajo

el isomorfismo $E \to E'$, e tiene imagen e' un idempotente tal que $e'L'$ es un ideal izquierdo minimal. Cambiando la base de E' se tiene el isomorfismo $E \to E'$ tal que $e \mapsto f$ y $L \to L$. Entonces

$$D \simeq eEe \to fE'f \simeq D'$$

y contando las dimensiones se llega a que $n = m$. □

2. GRUPO-ANILLOS

2.1. Hechos básicos de los grupo-anillos

En este capítulo se darán las definiciones que dan paso al estudio de los grupo-anillos y se relacionará la teoría de grupos y anillos con esta estructura matemática.

Considérese la siguiente construcción: Sea G un grupo cualquiera y R un anillo cualquiera. Entonces se define $RG := \{\alpha | \alpha \colon G \to R, |\operatorname{sop}(\alpha)| < \infty\}$ donde $\operatorname{sop}(\alpha) := \{g \in G : \alpha(g) \neq 0\}$. Al conjunto $\operatorname{sop}(\alpha)$ se le llama el **soporte de** α. Se puede observar que los elementos de RG son funciones con soporte finito.

Como RG es un conjunto de funciones, se puede considerar la suma usual de funciones para definir la operación suma en RG, a saber $+ \colon RG \times RG \to R$ de tal forma que si $\alpha, \beta \in RG$ entonces $(\alpha+\beta)(g) := \alpha(g)+\beta(g)$ para todo g elemento de G. Similarmente se puede definir la operación producto en RG como $\cdot \colon RG \times RG \to R$ de tal forma que si $u \in G$ $(\alpha \cdot \beta)(u) := \sum_{gh=u} \alpha(g)\beta(h)$. Con estas nociones se tiene:

Definición 2.1.1. El conjunto RG con las operaciones $+$ y $\cdot$ mencionadas anteriormente es llamado el **grupo-anillo de** G **sobre** R. En el caso de que R es conmutativo a RG se le llama también el **grupo-álgebra de** G **sobre** R.

Ahora se procede a mostrar dos teoremas que son básicos para el estudio posterior.

Teorema 2.1.1. Existe una copia de G en RG, es decir, se puede encontrar $G_1 \subset RG$ tal que existe un homomorfismo entre G y G_1.

Demostración. Considérese la función $i\colon G \to RG$ tal que $x \mapsto \alpha$ donde $\alpha(x) = 1$ y $\alpha(g) = 0$ si $g \neq x$. Con la identificación anterior es fácil notar que i es una función inyectiva. En efecto, si $x, y \in G$ entonces $i(x) = \alpha$, $i(y) = \beta$, pero $\alpha \neq \beta$ si $x \neq y$, por definición. Ahora se probará que i es un homomorfismo de grupos. Nótese que $i(xy) = \gamma$, donde $\gamma(xy) = 1$ y $\gamma(g) = 0$ si $g \neq xy$. Por otro lado, $i(x)i(y) = \alpha\beta$ donde $(\alpha\beta)(u) = \sum_{gh=u} \alpha(g)\beta(h)$, pero el producto $\alpha(g)\beta(h)$ se anula a menos que $g = x$ y $h = y$, en cuyo caso la función vale 1, con esto $i(x)i(y) = i(xy)$. □

A i se le llama la **función de inclusión** y de acá en adelante se usará dicho nombre para denotar a esta función.

Teorema 2.1.2. Existe una copia de R en RG.

Demostración. Considérese la función $v\colon R \to RG$ tal que $v(r) = \beta$ con $\beta(g) = r$ si $g = 1_G$ y $\beta(g) = 0$ si $g \neq 1_G$. Es claro que v es inyectiva y la demostración es análoga a la presentada en el teorema anterior. Ahora falta probar que v es un homomorfismo de anillos (que RG es un anillo se probará mas adelante). En efecto, $v(sr) = \theta$ donde $\theta(g) = sr$ si $g = 1_G$ y $\theta(g) = 0$ si $g \neq 1_G$. De manera similar se tiene que $v(s)v(r) = \gamma\beta$ donde $(\gamma\beta)(u) = \sum_{gh=u} \gamma(g)\beta(h)$ pero γ y β se anulan a menos que $g = h = 1_G$ y en ese caso $u = 1_G$, por lo que se ha probado que v es un homomorfismo de anillos. □

Con las identificaciones anteriores es fácil probar la siguiente:

Propiedad 2.1.1. Si $g \in G$ y $r \in R$ entonces $rg = gr$ en RG.

Demostración. Nótese que $r = \gamma$ y $x = \alpha$ y usando la definición del producto en RG se tiene que $rx = \gamma\alpha$ donde $(\gamma\alpha)(u) = \sum_{gh=u} \gamma(g)\alpha(h)$ pero por definición γ y α se anulan en todas partes excepto en $g = 1_G$ y $h = x$ respectivamente, por lo

tanto $(\gamma\alpha)(u) = r$ cuando $u = x$ y $(\gamma\alpha)(u) = 0$ para $u \neq x$. Por otro lado $xr = \alpha\gamma$ dada por $(\alpha\gamma)(u) = \sum_{gh=u} \alpha(g)\gamma(h)$ de nuevo la función sólo existe cuando $g = x$ y $h = 1_G$ de esa forma $(\alpha\gamma)(u) = r$ cuando $u = x$ y se anula en cualquier otro caso, con la cual concluye la demostración. □

La definición de grupo-anillo que se presentó anteriormente es bastante rigurosa y además es bien definida. Se construyó un espacio vectorial de funciones en el cual todas las operaciones tienen sentido, lo cual le brinda el soporte necesario para trabajar en álgebra.

En algunas ocasiones resulta un poco tedioso y complicado estar trabajando sobre un espacio vectorial de funciones, así que se replanteará los grupo-anillos como **R-combinaciones lineales**, es decir, a cada elemento de RG se le asigna una combinación lineal de elementos de G con coeficientes en R, de la siguiente manera

$$\alpha = \sum_{g \in G} a_g g, \tag{2.1}$$

donde $a_g \in R$ y $a_g \neq 0$ si $g \in \text{sop}(\alpha)$.

Nota 2.1.1. Con la identificación anterior se verifica que la suma de $\alpha, \beta \in RG$ es componente a componente, es decir $\alpha+\beta = \sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g+b_g)g$ y el producto está dado por $\alpha\beta = \sum_{g,h\in G} a_g b_h gh$.

Teorema 2.1.3. RG es un grupo aditivo.

Demostración. Se procede por incisos:

- Sean $\alpha, \beta, \gamma \in RG$ entonces

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

- Existe $0 \in RG$ tal que $0 + \gamma = \gamma + 0 = \gamma$ para cualquier $\gamma \in RG$. A saber $0 = \sum_{g \in G} 0 \cdot g$. Con esta identificación se procede así:

$$\begin{aligned}
\alpha + 0 &= \sum_{g \in G} (a_g + 0) g \\
&= \sum_{g \in G} (0 + a_g) \\
&= \sum_{g \in G} a_g g = \alpha.
\end{aligned}$$

- Existe $-\alpha$ tal que $\alpha + (-\alpha) = (-\alpha) + \alpha = 0$ para cualquier $\alpha \in RG$. En efecto $-\alpha = \sum_{g \in G} -a_g g$ y por lo tanto

$$\begin{aligned}
\alpha + (-\alpha) &= \sum_{g \in G} (a_g + (-a_g)) g \\
&= \sum_{g \in G} ((-a_g) + a_g) g \\
&= \sum_{g \in G} 0 \cdot g = 0.
\end{aligned}$$

- $\alpha + \beta = \sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G}(a_g + b_g)g = \sum_{g\in G}(b_g + a_g)g = \beta + \alpha$. □

La clausura de la operación + se sigue directamente de la definición. Vale la pena notar que para realizar esta prueba se uso simplemente el hecho que G es grupo y R es un anillo y por lo tanto satisfacen propiedades algebraicas respecto de sus operaciones.

Nótese que se ha probado que $(RG, +)$ es un grupo abeliano, lo cual será de utilidad para el siguiente teorema:

Teorema 2.1.4. *RG es un anillo con las operaciones + y $\cdot$*

Demostración. Ya se ha probado que $(RG, +)$ es un grupo abeliano, por lo que a continuación se probará, de nuevo por incisos, que $(RG, \cdot)$ es asociativo y distributivo tanto por la derecha como por la izquierda:

- El producto es asociativo:

$$\begin{aligned}
\alpha(\beta\gamma) &= \left(\sum_{g\in G} a_g g\right)\left[\left(\sum_{g\in G} b_g g\right)\left(\sum_{g\in G} c_g g\right)\right] \\
&= \left(\sum_{g\in G} a_g g\right)\left(\sum_{g,h\in G} b_g c_h gh\right) \\
&= \sum_{f,g,h\in G} a_f(b_g c_h) f(gh) \\
&= \sum_{f,g,h\in G} (a_f b_g) c_h (fg) h \\
&= (\alpha\beta)\gamma.
\end{aligned}$$

- El producto es distributivo por la izquierda respecto de la suma:

$$\begin{aligned}\alpha(\beta+\gamma) &= \left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g + \sum_{g\in G} c_g g\right)\\ &= \sum_{g\in G} a_g g\left(\sum_{g\in G}(b_g + c_g)\right)\\ &= \sum_{g,h\in G} a_g(b_h + c_h)gh\\ &= \sum_{g,h\in G} a_g b_h gh + \sum_{g,h\in G} a_g c_h gh\\ &= \alpha\beta + \alpha\gamma.\end{aligned}$$

- El producto es distributivo por la izquierda respecto de la suma:

$$\begin{aligned}(\alpha+\beta)\gamma &= \left(\sum_{g\in G}(a_g + b_g)g\right)\left(\sum_{g\in G} c_g g\right)\\ &= \sum_{g,h\in G}(a_g + b_g)c_h gh\\ &= \sum_{g,h\in G} a_g c_h gh + \sum_{g,h\in G} b_g c_h gh\\ &= \alpha\gamma + \beta\gamma.\end{aligned}$$

□

Para enriquecer la estructura algebraica de RG, se introduce una operación mas sobre RG.

Definición 2.1.2. Sea $\lambda \in R$ entonces se define el producto por elementos del anillo como:

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} \lambda a_g g. \tag{2.2}$$

Con esta definición se estable el siguiente:

Teorema 2.1.5. RG es un R-módulo.

Demostración. Ya se estableció en el teorema 2.1.3 que $(RG, +)$ es un grupo aditivo. De la definición anterior se sigue que $\lambda\gamma \in RG$. Ahora se procede por incisos:

- $(\lambda_1 + \lambda_2)\alpha = \sum_{g\in G}(\lambda_1 + \lambda_2)a_g g = \sum_{g\in G}\lambda_1 a_g g + \sum_{g\in G}\lambda_2 a_g g = \lambda_1\alpha + \lambda_2\alpha.$
- $\lambda(\alpha + \beta) = \lambda\sum_{a_g+b_g} g = \sum g \in G\lambda(a_g + b_g)g = \sum_{g\in G}\lambda a_g g + \sum_{g\in G}\lambda b_g g = \lambda\alpha + \lambda\beta.$
- $\lambda_1(\lambda_2\alpha) = \lambda_1\sum_{g\in G}\lambda_2 a_g g = \sum_{g\in G}(\lambda_1(\lambda_2 a_g))g = \sum_{g\in G}((\lambda_1\lambda_2)a_g)g = \lambda_1\lambda_2\alpha.$
- $1_R\alpha = \sum g \in G 1_R a_g g = \sum_{g\in G} a_g g.$

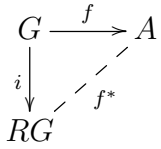
Y con esto concluye la prueba. □

Una extensión del resultado anterior es que si R es un anillo conmutativo entonces RG es un álgebra sobre R. Se puede resaltar que si R es conmutativo entonces el rango de RG como módulo libre sobre R está bien definido, de hecho si G es finito se tiene que rango$(RG) = |G|$.

Un resultado de mucha importancia en los grupo-anillos, es el que relaciona a estos con los homomorfismos, que es uno de los objetivos del álgebra.

Proposición 2.1.1. Sea G un grupo y R un anillo. Dado cualquier anillo A tal que $R \subset A$ y cualquier función $f\colon G \to A$ tal que $f(gh) = f(g)f(h)$ para cualquier $g, h \in G$, existe un único homomorfismo de anillos $f^*\colon RG \to A$, que es R-lineal, tal que $f^* \circ i = f$, donde i es la función de inclusión. Lo anterior se reduce a decir que el diagrama de la figura 2 es conmutativo.

Figura 2: Diagrama conmutativo para la proposición 2.1.1



Fuente: elaboración propia con paquete **xymatrix** para computadora.

Demostración. Considérese la función $f^*\colon RG \to A$ tal que $f^*(g) = \sum_{g\in G} a_g f(g)$. Ahora solo falta hacer los cálculos correspondiente para mostrar que f^* es un homomorfismo de anillos. En efecto

$$\begin{aligned} f^*(\alpha+\beta) &= \sum_{g\in G}(a_g+b_g)f(g) \\ &= \sum_{g\in G} a_g f(g) + \sum_{g\in G} b_g f(g) \\ &= f^*(\alpha) + f^*(\beta). \end{aligned}$$

De manera análoga se tiene

$$\begin{aligned} f^*(\alpha\beta) &= \sum_{g,h\in G} a_g b_h f(gh) \\ &= \sum_{g,h\in G} a_g b_h f(g) f(h) \\ &= f^*(\alpha) f^*(\beta). \end{aligned}$$

Ahora sea $r \in R$ entonces $f^*(r\alpha) = \sum_{g\in G} r a_g f(g) = r\sum_{g\in G} a_g f(g) = r f^*(\alpha)$. Sea $x \in G$ entonces $i(x) = \sum_{g\in G} a_g g$ donde $a_g = 1$ si $g = x$ y $a_g = 0$ en cualquier otro caso, por lo tanto $f^*(i(g)) = \sum_{g\in G} a_g f(g) = f(x)$. De los cálculos anteriores se sigue que $f^* \circ i = f$, con lo cual concluye la prueba. □

De la proposición anterior se deriva un corolario que será de utilidad en el desarrollo del trabajo.

Corolario 2.1.1. Sea $f\colon G \to H$ un homomorfismo de grupos. Entonces, existe un único homomorfismo de anillos $f^*\colon RG \to RH$ tal que $f^*(g) = f(g)$ para cualquier $g \in G$. Si R es conmutativo, entonces f^* es un homomorfismo de $R-$álgebra, mas aún si f es un epimorfismo (monomorfismo), entonces f^* es también un epimorfismo (monomorfismso).

Demostración. Usar el teorema anterior con $A = RH$ lo anterior se puede hacer porque RH es un anillo que contiene a R y hay una copia de H en RH, con lo cual se deriva que debe existir f^* homomorfismo $R-$ lineal de anillos tal que $f^*(g) = f(g)$ para cualquier elemento $g \in G$. □

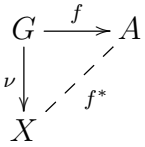
De hecho la proposición 2.1.1 se puede utilizar como una definición de RG, como se sigue de la siguiente proposición:

Proposición 2.1.2. Sea G un grupo y R un anillo. Sea X un anillo que contiene a R y $\nu\colon G \to X$ una función tal que $\nu(gh) = \nu(g)\nu(h)$ para todo $g, h \in G$ y tal que, para todo anillo A que contiene a R y cualquier función $f\colon G \to A$ que satisface $f(gh) = f(g)f(h)$ para todo $g, h \in G$, existe un único homomorfismo R-lineal $f^*\colon X \to A$ tal que el diagrama de la figura 3 es conmutativo: Entonces $X \simeq RG$

Demostración. La demostración es tan simple como notar que el diagrama de la figura 4 conmuta con I_X. □

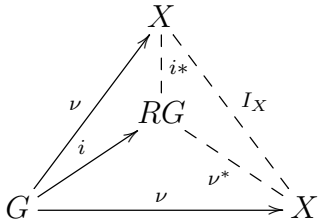
Nota 2.1.2. Si en el corolario 2.3.3 se hace $H = \{1\}$ y se considera la función $m\colon G \to \{1\}$ entonces esta función induce un homomorfismo de anillos $\epsilon\colon RG \to R$

Figura 3: Definición alternativa para RG



Fuente: elaboración propia con paquete **xymatrix** para computadora.

Figura 4: Diagrama conmutativo



Fuente: elaboración propia con paquete **xymatrix** para computadora.

tal que $\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a(g)$.

Definición 2.1.3. El homomorfismo $\epsilon\colon RG \to R$ dado por

$$\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

es llamado la **función de aumento de RG** y su núcleo, denotado por $\Delta(G)$, es llamado **el ideal de aumento** de RG.

Ahora se puede dar algunas propiedades importantes del ideal de aumento de RG. Nótese que si un elemento $\alpha = \sum_{g\in G} a_g g$ pertenece al ideal de aumento entonces

$\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0$ por lo tanto se puede escribir α de la siguiente forma:

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

Por lo tanto es claro que cualquier elemento de la forma $g-1, g \in G$ pertenece a $\Delta(G)$, mas aún se acaba de probar que el conjunto $\{g-1 : g \in G, g \neq 1\}$ es un conjunto de generadores del ideal de aumento de RG. Por otro lado, de la definición de RG se sigue que el conjunto anterior en linealmente independiente, con lo cual se ha probado la siguiente

Proposición 2.1.3. El conjunto $\{g-1 : g \in G, g \neq 1\}$ es base de $\Delta(G)$ sobre R. Es decir, se puede escribir

$$\Delta(G) = \left\{ \sum_{g\in G} a_g(g-1) : g \in G, g \neq 1, a_g \in R \right\}$$

donde, como es usual, se debe asumir que solo un número finito de los coeficientes a_g son distintos de cero.

Nótese que, en particular, si R es conmutativo y G es finito, entonces $\Delta(G)$ es un módulo libre sobre R con rango $|G|-1$.

Se concluye esta sección mostrando que el grupo-anillo RG donde R es conmutativo es un anillo con **involución**.

Proposición 2.1.4. Sea R un anillo conmutativo. La función $*\colon RG \to RG$ definida por:

$$\left(\sum_{g\in G} a(g)g\right)^* = \sum_{g\in G} a(g)g^{-1} \tag{2.3}$$

satisface:

- $(\alpha+\beta)^* = \alpha^* + \beta^*$.
- $(\alpha\beta)^* = \beta^*\alpha^*$.
- $\alpha^* = \alpha$.

Demostración. Se procede por incisos:

- $\left(\sum_{g\in G}(a_g+b_g)g\right)^* = \sum_{g\in G}(a_g+b_g)g^{-1} = \alpha^* + \beta^*$.
- $\left(\sum_{g,h\in G}(a_g b_h)gh\right)^* = \sum_{g,h\in G} a_g b_h h^{-1}g^{-1} = \sum_{g,h\in G} b_h a_g h^{-1}g^{-1} = \beta^*\alpha^*$.
- $\left(\left(\sum_{g\in G} a_g g\right)^*\right)^* = \left(\sum_{g\in G} a_g g^{-1}\right)^* = \sum_{g\in G} a_g g$. □

2.2. Ideales de aumento

En lo que sigue es de mucho interés encontrar condiciones de R y G que permitan descomponer a RG como sumas directas de ciertos subanillos. Será de especial interés conocer cuando RG es un anillo semisimple para así poder escribirlo como sumas directas de ideales minimales.

Con este fin se hará un estudio de la relación que hay entre los subgrupos de G y los ideales de RG. Está relación tendrá mucho utilidad cuando se trate con problemas concernientes a la estructura y propiedades de RG. Estas relaciones aparecieron por primera vez en un artículo publicado por A. Jennings, véase (12), y en la forma que se presentará en este trabajo, en el trabajo hecho por W. E. Deskins, véase (5). La idea de aplicarlo por primera vez en el estudio de la reducibilidad completa (como se hará en la siguiente sección) fue de I.G. Connell, véase (10).

Ya en materia, considérese el grupo G y el anillo R, se denotará con $\mathcal{S}(G)$ el conjunto de todos los subgrupos de G y con $\mathcal{I}(RG)$ el conjunto de los ideales por la izquierda de RG.

Definición 2.2.1. Para un subgrupo $H \in \mathcal{S}(G)$ se denota por $\Delta_R(G,H)$ el anillo por izquierda de RG generado por el conjunto $\{h-1 : h \in H\}$. Esto es,

$$\Delta_R(G,H) = \left\{ \sum_{h\in H} \alpha_h(h-1) : \alpha_h \in RG \right\}. \tag{2.4}$$

Cuando se esté trabajando con un anillo fijo R se omitirá el subíndice y por lo tanto al ideal anterior se le denotará simplemente como $\Delta(G,H)$. Nótese que el ideal $\Delta(G,G)$ coincide con $\Delta(G)$, del cual se habló en la sección anterior.

Lema 2.2.1. Sea H un subgrupo de un grupo G y sea S el conjunto de los generadores de H. Entonces, el conjunto $\{s-1 : s \in S\}$ es un conjunto de generadores de $\Delta(G,H)$ como ideal por izquierda de RG.

Demostración. Como S es un conjunto de generadores de H, cada elemento $1 \neq h \in H$ puede ser escrito en la forma $h = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_r^{\epsilon_r}$ donde $s_i \in S$ y $\epsilon_i = \pm 1$, $1 \leq i \leq r$. Por lo tanto es suficiente probar que todo elemento de la forma $h-1$ con $h \in H$ pertenece al ideal generado por $\{s-1 : s \in S\}$. Para hacer esto se procede por inducción matemática sobre r.

Caso Base: nótese que el menor caso sucede en $r = 2$. Por lo tanto sea $h \in H$ entonces $h-1 = s_1^{\epsilon_1} s_2^{\epsilon_2} = s_1^{\epsilon_1}(s_2^{\epsilon_2}-1) + (s_1^{\epsilon_1}-1) \in (S)$ donde (S) es el ideal generado por $\{s-1 : s \in S\}$.

Hipótesis de Inducción: supóngase que cualquier expresión de la forma

$$(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} - 1)$$

pertenece a (S).

Conclusión: considérese la expresión de la forma $(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} s_{k+1}^{\epsilon_{k+1}} - 1)$, hágase la sustitución $x = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k}$ entonces $(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} s_{k+1}^{\epsilon_{k+1}} - 1) = x s_{k+1}^{\epsilon_{k+1}} - 1 = x(s_{k+1}^{\epsilon_{k+1}} - 1) + (x - 1) \in (S)$ ya que $x - 1, x(s_{k+1}^{\epsilon_{k+1}} - 1) \in (S)$ por la hipótesis de inducción. La prueba está casi completa, sola falta decir que si apareciera algún $\epsilon_i = -1$ se aplica la factorización $y^{-1} - 1 = y^{-1}(1 - y)$ y el problema está resuelto. □

Para dar un mejor caracterización de $\Delta_R(G, H)$, denótese con $\mathcal{T} = \{q_i\}_{i \in I}$ un conjunto completo de representantes de clases izquierdas de H en G, un **transversal** de H en G. Se asumirá que siempre se elige como representante de la clase H en $\mathcal{T}$ a la unidad de G. De esa manera todo elemento $g \in G$ puede ser escrito de manera única en la forma $g = q_i h_j$ con $q_i \in \mathcal{T}$ y $h_j \in H$

Proposición 2.2.1. El conjunto $B_H = \{q(h - 1) : q \in \mathcal{T}, h \in H, h \neq 1\}$ es una base de $\Delta_R(G, H)$ sobre R.

Demostración. Se procede en dos partes, primero se debe probar que el conjunto dado es linealmente independiente y luego que también es un generador de $\Delta_R(G, H)$. Independecia lineal: supóngase que se tiene una combinación lineal de elementos de B_H que se anula, esto es $\sum_{i,j} r_{ij} q_i (h_j - 1) = 0$ con $r_{ij} \in R$. De lo anterior se sigue que $\sum_{i,j} r_{ij} q_i (h_j) - \sum_{i,j} r_{ij} q_i = 0$ por lo tanto $\sum_{i,j} r_{ij} q_i (h_j) = \sum_{i,j} r_{ij} q_i$ lo cual se puede escribir como $\sum_{i,j} r_{ij} q_i h_j = \sum_i \left(\sum_j r_{ij} q_i \right)$. En la igualdad anterior se puede observar que como $h_j \neq 1$ entonces necesariamente el lado izquierdo de la ecuación tienen distinto soporte que el lado derecho, por lo tanto ambos deben ser igual a cero,

pero los elementos de G son linealmente independientes sobre R entonces $r_{ij} = 0$ para todo i, j.

Generador: se debe probar que B_H es generador de $\Delta_R(G, H)$ para esto es suficiente demostrar que $g(h-1)$ se puede expresar como combinación lineal de elementos de B_H. Para esto basta recordar que $g = q_i h_j$ para algún $q_i \in \mathcal{T}$ y $h_j \in H$ entonces $g(h-1) = q_i h_j(h-1) = q_i(h_j h - 1) + (q_i - 1)$ con lo que se demuestra lo que se pedía. □

Nota 2.2.1. Si $G = H$ en la proposición anterior entonces $\mathcal{T} = \{1\}$ y por lo tanto $B_H = \{(h-1, h \in H, h \neq 1)\}$ y así esto se reduce a la proposición 2.1.3.

Ahora se explorará la opción usual cuando se está hablando de subgrupos, es decir, los subgrupos normales. De hecho, si $H \lhd G$ entonces el homomorfismo canónico $\omega : G \to G/H$ puede ser extendido a un epimorfismo de la siguiente manera:

$$\omega* : RG \to R(G/H)$$

tal que

$$\omega^* \left(\sum_{g \in G} a_g g \right) = \sum_{g \in G} a_g \omega(g).$$

Proposición 2.2.2. Con la notación anterior

$$\ker(\omega^*) = \Delta(G, H).$$

Demostración. Considérese de nuevo $\mathcal{T}$ el transversal de H en G. Entonces, cada elemento $\alpha \in RG$ se puede escribir como $\alpha = \sum i, j r_{ij} q_i h_j$, $r_{ij} \in R$, $q_i \in \mathcal{T}$, $h_i \in H$.

Si se denota $\overline{q_i} = \omega(q_i)$ entonces se tiene

$$\omega^*(\alpha) = \sum_i \left(\sum_j r_{ij} \right) \overline{q_i}.$$

Entonces, $\alpha \in \ker(\omega^*)$ si y sólo si $\sum_j r_{ij} = 0$ para cada calor de i. Entonces si se tiene un $\alpha \in \ker(w^*)$ se puede escribir

$$\begin{aligned} \alpha &= \sum_i \left(\sum_j r_{ij} \right) \overline{q_i} \\ &= \sum_{ij} r_{ij} q_i (h_j - 1) \in \Delta(G, H). \end{aligned}$$

Con lo cual se tiene que $\ker(\omega^*) \subset \Delta(G, H)$. El hecho que $\Delta(G, H) \subset \ker(\omega^*)$ es trivial, por lo tanto $\ker(\omega^*) = \Delta(G, H)$. □

Corolario 2.2.1. Sea H un subgrupo normal de G. Entonces $\Delta(G, H)$ es un ideal bilateral de RG y

$$\frac{RG}{\Delta(G, H)} \simeq R(G/H).$$

Demostración. Como $\ker(\omega^*) = \Delta(G, H)$ entonces por el primer teorema de isomorfía $\frac{RG}{\Delta(G,H)} \simeq Im(\omega^*)$ pero como ω^* es sobreyectiva entonces $Im(\omega^*) = R(G/H)$ con lo que concluye la prueba. □

Hasta este punto se ha visto que hay una relación entre subgrupos normales de G y los ideales bilaterales de RG, es decir, se pueden construir funciones de (S) a $\mathcal{I}(RG)$. La pregunta es entonces, ¿qué pasa con las funciones en la otra vía? Para

responder esa pregunta considérese

$$\nabla(I) = \{g \in G \colon g - 1 \in I\}.$$

Es fácil notar que $\nabla(I) = G \cap (1 + I)$.

Lema 2.2.2. $\nabla(I)$ es subgrupo de G.

Demostración. Se debe probar dos cosas:

- Sean $g_1, g_2 \in \nabla(I)$ entonces

$$g_1 g_2 - 1 = g_1(g_2 - 1) + (g_2 - 1) \in I,$$

  por lo tanto $g_1 g_2 \in \nabla(I)$.
- Si $g \in \nabla(I)$ entonces $g^{-1} - 1 = g^{-1}(1 - g) \in I$ de donde se sigue que $g^{-1} \in \nabla(I)$. □

Lema 2.2.3. Si I es un ideal bilateral entonces $\nabla(I) \lhd G$.

Demostración. Se quiere probar que $gig^{-1} \in \nabla(I)$ entonces todo se reduce a demostrar que $gig^{-1} - 1 \in I$. Nótese que $gig^{-1} - 1 = gi(g^{-1} - 1) + (gi - 1)$ como I es ideal bilateral, entonces $gi(g^{-1} - 1) \in I$ y $(g_i - 1) \in I$ por lo tanto $gig^{-1} \in I$. □

Proposición 2.2.3. Si $H \in (S)(G)$ entonces $\nabla(\Delta(G, H)) = H$.

Demostración. Sea $1 \neq x \in \nabla(\Delta(G, H))$ entonces $x - 1 \in \Delta(G, H)$ por lo tanto se puede escribir

$$x - 1 = \sum_{i,j} r_{ij} q_i (h_j - 1).$$

Como 1 aparece en el lado izquierdo de la ecuación también debe aparecer en el lado derecho, por lo tanto alguno de los q_i debe ser igual a uno y por lo tanto hay en término de la forma $r_{1j}(h_j - 1)$. Nótese que todos los elementos de G del lado derecho de la ecuación son distintos a pares pero x debe aparecer allí, por lo tanto $x = h_j$. De lo anterior es inmediato que $\nabla(\Delta(G, H)) \subset H$. La otra contención es trivial. $\square$

Según lo expuesto en la proposición anterior parece ser que ∇ y Δ son funciones inversas la una de la otra, pero esto no es cierto. Si se toma un ideal $I \in (I)(RG)$ entonces ¿qué pasa con $\Delta(G, \nabla(I))$? Pues bien, sea $x \in \Delta(G, \nabla(I))$ entonces $x = \sum_{i,j} r_{ij} q_i (m_j - 1)$, $m_j \in \nabla(I)$ por lo tanto $m_j - 1 \in I$ y de allí que $x \in I$. Con eso se ha probado que $\Delta(G, \nabla(I)) \subset I$, pero la igualdad no es necesariamente cierta. Considérese $I = RG$ entonces $\nabla(RG) = G$ de donde $\Delta(G, \nabla(RG)) = \Delta G \neq RG$.

2.3. Semisimplicidad

Con lo visto en la anterior sección ahora es accesible determinar condiciones necesarias y suficientes de R y G para que RG sea semisimple. Pero antes se probarán algunos resultados técnicos acerca de aniquiladores.

Definición 2.3.1. Sea X un subconjunto de RG. El aniquilador de X por la izquierda es el conjunto

$$Ann_i(X) = \{\alpha \in RG : \alpha x = 0, \text{ para cada } x \in X\},$$

y de manera análoga el aniquilador de X por la derecha es el conjunto

$$Ann_d(X) = \{\alpha \in RG : x\alpha = 0, \text{ para cada } x \in X\}.$$

Definición 2.3.2. Dado un grupo-anillo RG y un subconjunto finito X del grupo G, se denotará por $\hat{X}$ los siguientes elementos de RG

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

Lema 2.3.1. Sea H un subgrupo de G y sea R un anillo. Entonces $Ann_d(\Delta(G,H)) \neq \{0\}$ si y sólo si H es finito. En ese caso, se tiene

$$Ann_d(\Delta(G,H)) = \hat{H} \cdot RG$$

Mas aún, si $H \lhd G$ entonces $\hat{H}$ es central en RG y

$$Ann_d(\Delta(G,H)) = Ann_i(\Delta(G,H)) = RG \cdot \hat{H}.$$

Demostración. Supóngase que $Ann_d(\Delta(G,H)) = \{0\}$ y considérese $\alpha = \sum_{g \in G} a_g g \in RG$, $\alpha \in Ann_d(\Delta(G,H))$ entonces

$$\begin{aligned} (h-1)\alpha &= 0, \quad \text{para cada } h \in H \\ h\alpha - \alpha &= 0 \\ \sum_{g \in G} a_g ah &= \sum_{g \in G} a_g g. \end{aligned} \tag{2.5}$$

De la última ecuación se aprecia que $hg \in \text{sop}(\alpha)$ siempre y cuando $g \in \text{sop}(\alpha)$, pero $\text{sop}(\alpha)$ es finito, por tanto H es finito. De nuevo analizando la ecuación (2.5) se deduce que dado $g_0 \in \text{sop}(\alpha)$ entonces $hg_o \in \text{sop}(\alpha)$ para cualquier h elemento de H. De allí que se de la siguiente igualdad:

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

Lo anterior muestra que si H es finito entonces $Ann_d(\Delta(G,H)) \subset \hat{H}RG$. Por otro lado $h\hat{H} = \hat{H}$ ya que H es finito, entonces $h\hat{H} - \hat{H} = 0$ y por consiguiente $(h-1)\hat{H} = 0$ de donde $\hat{H}RG \subset Ann_d(\Delta(G,H))$.

Por último si $H \lhd G$ entonces para todo g elemento de G se cumple que $gHg^{-1} = H$ de donde $g\hat{H}g^{-1} = \hat{H}$ y se concluye que $\hat{H}g = g\hat{H}$ lo cual prueba que $\hat{H}$ es central en RG y de allí se sigue fácilmente la conclusión. □

Del lema anterior se sigue el siguiente:

Corolario 2.3.1. Sea G un grupo finito. Entonces

- $Ann_i(\Delta(G)) = Ann_d(\Delta(G)) = R \cdot \hat{H}$.
- $Ann_d(\Delta(G)) \cap \Delta(G) = \{a\hat{G} : a \in R, a|G| = 0\}$.

Demostración. Se procede por incisos:

- Ya se ha establecido que $\Delta(G,G) = G$, por lo tanto hágase $H = G$ en el teorema anterior y el resultado es inmediato.
- Sea $x \in Ann_d(\Delta G) \cap \Delta G$ entonces $x = a\sum_{g\in G} g$ y además $x \in \ker(\omega^*)$ por tanto $\ker(x) = a\omega^*\hat{G} = a|G| = 0$. □

Lema 2.3.2. Sea I un ideal bilateral de R. Supóngase que existe un ideal por la izquierda J tal que $R = I \oplus J$ (como R-módulos). Entonces $J \subset Ann_d(I)$.

Demostración. Sea $x \in J$ y $y \in I$ entonces $yx \in J$, $yx \in I$ entonces $yx \in J \cap I$ por lo tanto $yx = 0$ de donde $x \in Ann_d(I)$, por consiguiente $J \subset Ann_d(J)$. □

Lema 2.3.3. Si el ideal de aumento de RG es un sumando directo de RG como un RG-módulo entonces G es finito y $|G|$ es invertible en R.

Demostración. Las condiciones anteriores aseguran que existe J como en el lema anterior tal que $RG = \Delta G \oplus J$, de donde $J \subset \Delta G$ y por tanto $\Delta G \neq \{0\}$, con lo cual G es necesariamente finito. Por otra parte $1 \in RG$ entonces $1 = e_1 + e_2$ donde $e_1 \in \Delta G$ y $e_2 = a\hat{G}$, de lo cual se sigue que $\epsilon(1) = 1 = \epsilon(e_1) + \epsilon(e_2)$ pero $\epsilon(e_1) = 0$ por ser ΔG el núcleo de ϵ por ende se tiene $a|G| = 1$ con lo que se ha mostrado lo pedido. □

Ahora se está en disposición de determinar condiciones necesarias y suficientes en R y G para que el grupo-anillo RG sea semisimple. Los primeros resultados que apuntaron en esta dirección fueron dados por Maschke, logros que están plasmados en el siguiente teorema:

Teorema 2.3.1 (Maschke). Sea G un grupo. Entonces, el grupo-anillo RG es semisimple si y sólo si las siguientes condiciones son verdaderas:

- R es un anillo semisimple.
- G es finito.
- $|G|$ es invertible en R.

Demostración. Se procederá a probar las implicaciones en ambos sentidos:

- En esta parte se asume que RG es semisimple, por lo tanto se puede utilizar el hecho que $\frac{RG}{\Delta(G)} = R$. De lo anterior se deduce que R es un cociente y ya se ha demostrado que los cocientes son simples. Por otro lado se sabe que $\Delta(G)$ es un ideal y de la semisimplicidad de RG se sabe que $\Delta(G)$ es sumando directo y del lema 2.3.3 se asegura que la segunda y tercera condición se satisfacen.

- Para mostrar la segunda implicación, supóngase que todas las condiciones de los incisos son verdaderas. De la primera condición se sigue que RG es semisimple como R-módulo. Considérese M como RG-módulo, tal que $M \in RG$, entonces existe N como R-módulo tal que

$$RG = M \oplus N.$$

Sea $\pi\colon RG \to M$ la proyección canónica asociada con la suma directa. Se define $\pi^*\colon RG \to M$ tal que:

$$x \mapsto \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx), \text{ para cada } x \in RG.$$

Es claro que dicha función existe, ya que G es finito por la segunda condición y se cumple que $\frac{1}{|G|} < \infty$ por la tercera. Se desea probar que π^* es un RG -homomorfismo tal que $(\pi^*)^2 = \pi^*$ y $M = Im(\pi^*)$, lo cual se muestra en dos partes a continuación:
Homomorfismo: basta demostrar que $\pi^*(ax) = a\pi^*(x)$, para cada $a, g \in G$, ya que π^* ya es un R-homomorfismo. En efecto

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

Ahora se tiene que $ga \in G$, por ser G un grupo, por lo tanto cuando g recorre todo G el producto ga también lo hará, ya que a es un elemento dado fijo. Por lo tanto la última expresión se puede volver a escribir como:

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

Sobreyectividad y composición: nótese que $gm \in M$ ya que M es un RG-módulo, así que $\pi(gm) = gm$ y por lo tanto

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

De lo anterior se sigue que $Im(\pi^*) \subset M$ y además $(\pi^*)^2 = \pi$. Por otro lado sea $m \in M$, entonces $\pi^*(m) = m \in Im(\pi^*)$, de donde $M \in Im(\pi^*)$.
De esta manera se tiene que $\ker(\pi^*)$ es un RG-submódulo tal que $RG = M \oplus ker(\pi^*)$. □

Como es usual en ciencias, se explorará un caso particular del teorema anterior con la interrogante natural ¿qué pasa si en lugar de un anillo se considera un campo? La pregunta anterior se reduce a contemplar el caso $R = K$, donde K es un campo. Un campo siempre es semisimple, además se sabe que $|G|$ es invertible siempre y cuando $|G| \neq 0$, es decir, $\text{car}(K) \nmid |G|$, de donde se sigue el siguiente

Corolario 2.3.2. Sea G un grupo finito y K un campo. Entonces KG es semisimple si y solo si $\text{car}(K) \nmid |G|$.

Aunque no es el objetivo de este trabajo dar una descripción de los grupo-álgebra, resulta tentador replantear el teorema de Wedderburn-Artin en este contexto, con lo cual se brinda mas información acerca de la estructura algebraica de un grupo-álgebra.

Teorema 2.3.2. Sea G un grupo finito y sea K un campo tal que $car(K) \nmid |G|$. Entonces:

- KG es suma directa de un numero finito de ideales bilaterales $\{B_i\}_{1\leq i\leq r}$, los componentes simples de KG. Cada B_i es una anillo simple.

- Todo ideal bilateral de KG es suma directa de algunos de los miembros de la familia $\{B_i\}_{1\leq i\leq r}$.
- Cada componente simple B_i es isomorfo a un anillo completo de matrices de la forma $M_{n_i}(D_i)$, donde D_i es un anillo de división conteniendo una copia isomorfa de K en su centro. Además el isomorfismo

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

  es un isomorfismo de álgebras.
- En cada anillo de matrices $M_{n_i}(D_i)$, el conjunto

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

  es un ideal minimal izquierdo. Dado $x \in KG$, se considera

$$\phi(x) = (\alpha_1, \dots, \alpha_r) \in \oplus_{i=1}^{r} M_{n_i}(D_i)$$

  y se define el producto de x por un elemento $m_i \in I_i$ como $xm_i = \alpha_i m_i$. Con esta definición, I_i se convierte en un KG-módulo simple.
- $I_i \not\simeq I_j$, si $i \neq j$.
- Cualquier KG-módulo simple es isomorfo a algún I_i, $\quad 1 \leq i \leq r$.

Se ha hecho énfasis en este resultado, ya que en el siguiente capitulo, se explorará la conexión entre este y la teoría de representación de grupos.

Corolario 2.3.3. Sea G un grupo finito y K un campo algebraicamente cerrado

tal que $\text{car}(K) \nmid |G|$. Entonces:

$$Kg \simeq \oplus_{i=1}^{r} M_{n_i}(K)$$

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

Demostración. Como $\text{car}(K) \nmid |G|$ es inmediato que

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

donde D_i es un anillo de división conteniendo una copia de K en su centro. Calculando la dimensión sobre K en ambos lados de la ecuación se tiene:

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

de donde se sique que cada anillo de división D_i es de dimensión finita. Sea $0 \neq d_i \in D_i$ entonces $kd_i = 0$ implica que $k = 0$. Similarmente, dado $a_i \in D_i$ tal que $kd_i 0 a_i$ se tiene que $k = a_i d_i^{-1} \in K$ por ser K algebraicamente cerrado y por lo tanto $[D_i : K = 1]$ y $D_i = K$ para $1 \leq i \leq r$, con lo cual concluye la demostración. □

2.4. Grupo-álgebras de grupos abelianos finitos

En esta sección se dará una descripción completa de grupo-anillo cuando el grupo es finito y además abeliano.

Como en la parte final de la sección anterior, se supone que K es un campo tal que $\text{car}(K) \nmid |G|$. Esta caracterización fue dada por primera vez por S. Perlis y G Walker, véase (16).

Se comenzará con el caso donde G es un grupo cíclico, así que se asume que $G = \langle a \colon a^n = 1 \rangle$ y que K es un campo tal que $\text{car}(K) \nmid |G|$. Considérese la función $\phi \colon K[X] \to KG$ dada por

$$K[X] \ni f \mapsto f(a) \in KG$$

Debido a que la función ϕ consiste en tomar un polinomio de $K[G]$ y evaluarlo en a, es obvio que ϕ es un epimorfismo de anillos y por lo tanto:

$$KG \simeq \frac{K[X]}{\ker(\phi)}$$

donde $ker(\phi) = \{f \in K[X] : f(a) = 0\}$. Como $K[X]$ es un dominio de ideales principales se deduce que $\ker(\phi)$ es un ideal generado por el polinomio mónico f_0, de menor grado posible, tal que $f_0(a) = 0$.

Nótese que bajo el isomorfismo anterior, es claro que el elemento $a \in RG$ se mapea en $X + (f_0) \in \frac{K[X]}{(f_0)}$. Además de $a^n = 1$ se sigue que $X^n - 1 \in \ker(\phi)$, ya que si existiera un polinomio $f = \sum_{i=0}^{r} k_i x^i$ con $r < n$ entonces $f(a) \neq 0$ debido a que los elementos de $\{1, a, a^2, \ldots, a^r\}$ son linealmente independientes sobre K. De esa manera se puede asegurar que $\ker(\phi) = (X^n - 1)$ por lo que se satisface

$$KG \simeq \frac{K[X]}{(X^n - 1)}.$$

Sea $X^n - 1 = f_1 f_2 \cdots f_t$, la descomposición de $X^n - 1$ como producto de polinomios irreducibles en $K[X]$. Como se está asumiendo que $\text{car}(K) \nmid n$, este polinomio debe ser separable y por lo tanto $f_i \neq f_j$ si $i \neq j$. Utilizando el teorema

chino del residuo se puede escribir:

$$KG \simeq \frac{K[X]}{f_1} \oplus \frac{K[X]}{f_2} \oplus \cdots \oplus \frac{K[X]}{f_t}.$$

Utilizando este isomorfismo es fácil notar que el generador a tiene imagen $(X + (f_1), \ldots, X + (f_t))$. Considérese ζ_i una raíz de f_i, $1 \leq i \leq t$. Entonces, se tiene $\frac{K[X]}{(f_i)} \simeq K(\zeta_i)$. Por lo tanto

$$KG \simeq K(\zeta_1) \oplus K(\zeta_2) \oplus \cdots \oplus K(\zeta_t).$$

Como todos los elementos $\zeta_i, \quad 1 \leq i \leq t$ son raíces de $X^n - 1$, se ha probado que KG es isomorfo a la suma directa de extensiones ciclotómicas de K. Finalmente bajo este ultimo isomorfismo el elemento a tiene imagen $(\zeta_1, \zeta_2, \ldots, \zeta_t)$.

Antes de continuar, se presentan algunos ejemplos para estudiar y comprender de mejor manera como trabajan las conclusiones anteriores.

Ejemplo 2.4.1. Sea $G = \langle a \colon a^7 = 1 \rangle$ y $K = \mathbb{Q}$. En este caso la descomposición de $X^7 - 1$ en $\mathbb{Q}$ es

$$X^7 - 1 = (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1),$$

de esta forma si ζ es una raíz de la unidad de orden 7 distinta de 1, se puede escribir lo siguiente

$$\mathbb{Q}G = \mathbb{Q}(1) \oplus \mathbb{Q}(\zeta) = \mathbb{Q} \oplus \mathbb{Q}(\zeta).$$

Ejemplo 2.4.2. Sea $G = \langle a : a^6 = 1 \rangle$ y $K = \mathbb{Q}$. La descomposición de $X^6 - 1$ en $\mathbb{Q}[X]$ es

$$X^6 - 1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1),$$

entonces se obtiene

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

donde $\frac{-1+\sqrt{3}}{2}$ es raíz de X^2+X+1 y $\frac{1+i\sqrt{3}}{2}$ es raíz de X^2-X+1, pero $\mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right) \simeq \mathbb{Q}\left(\frac{-1-i\sqrt{3}}{2}\right) \simeq \mathbb{Q}\left(\frac{-(1+i\sqrt{3})}{2}\right) \simeq \mathbb{Q}\left(\frac{1+i\sqrt{3}}{2}\right)$ por lo que en realidad los últimos dos sumandos son iguales, dejando la expresión de la siguiente manera:

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

Los resultados anteriores dan una muy buena descripción de los grupos anillos cuando el anillo es un campo y el grupo es abeliano, por lo cual ahora se trabajará en un caso más general.

Para poder hacer esto, se tratará de calcular todos los sumando directos en la descomposición de KG.

El lector debe recordar que para un d entero positivo dado, el polinomio ciclotómico de orden d, denotado por Φ_d, es el producto $\Phi_d = \prod_j (x - \zeta_j)$, donde ζ_j hace el recorrido por todas las raíces primitivas de la unidad de orden d. También es conocido que $X^n - 1 = \prod_{d|n} \Phi_d$, es decir que $X^n - 1$ se puede expresar como el producto de todos los polinomios ciclotómicos Φ_d en $K[X]$, donde d es un 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 $K[X]$.

Entonces la descomposición de KG puede ser escrita en la forma:

$$KG \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} \frac{K[X]}{(f_{d_i})} \simeq \oplus_{d|n} \oplus_{i=1}^{a_d} K(\zeta_{d_i})$$

donde ζ_{d_i} denota una raíz de f_{d_i}, $1 \leq i \leq a_d$. Para un d fijo, todos los elementos ζ_{d_i} son raíces primitivas de la unidad de orden d, por lo tanto, todos los campos de la forma $K(\zeta_{d_i}), \quad 1 \leq i \leq a_d$ son iguales y se puede escribir simplemente

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

donde ζ_d es una raíz primitiva de orden d y $a_d K[\zeta_d]$ denota la suma directa de a_d campos diferentes, todos ellos isomorfos a $K(\zeta_d)$.

Por otro lado, como $\deg(f_{d_i}) = [K(\zeta_d) : K]$, se deduce que todos los polinomios tienen el mismo grado para $1 \leq i \leq a_d$. De esta forma, calculando el grado en la descomposición de Φ_d, se tiene

$$\phi(d) = a_d[K(\zeta_d) : K],$$

donde ϕ es la función totiente de Euler. Como G es un grupo cíclico de orden n, para cada divisor de n, el número de elementos de orden d en G, que se denota con n_d, es precisamente $\phi(d)$, entonces:

$$a_d = \frac{n_d}{|K(\zeta_d) : K|}$$

Dado n, un entero positivo, se cumple que si la factorización de n en producto de números primos es $n = p_1^{n_1} \cdots p_t^{n_t}$, entonces

$$\phi(n) = p_1^{n_1-1}(p_1 - 1) \cdots p_t^{n_t-1}(p_t - 1).$$

Una propiedad de mucha importancia es el famoso teorema de Euler: Si m y n son primos relativos entonces $m^{\phi(n)} \equiv 1 \pmod{n}$.

Ejemplo 2.4.3. Sea $G = \langle a : a^n = 1 \rangle$ un grupo cíclico de orden n y $K = \mathbb{Q}$. Es conocido que el polinomio $X^n - 1$ se descompone en $\mathbb{Q}[X]$ como un producto de polinomios ciclotómicos, a saber:

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

y los polinomios Φ_d son irreducibles en $\mathbb{Q}[Q]$. Por lo tanto, en este caso en particular, la descomposición de $\mathbb{Q}G$ es:

$$\mathbb{Q}G \simeq \oplus_{d|n} \mathbb{Q}(\zeta_d).$$

Bajo este isomorfismo al generador a le corresponde a la tupla cuyas entradas son raíces primitivas de la unidad de orden d, donde d es cualquier divisor positivo de n.

Para cerrar esta sección se demostrará que la caracterización anteriormente dada también es válida en los grupo-anillos con grupos abelianos finitos.

Lema 2.4.1. Sea R un anillo conmutativo y G, H grupos, entonces $R(G \times H) \simeq (RG)H$ (el grupo-anillo de H sobre el anillo RG).

Demostración. Considérese el conjunto $M_{n,\gamma} = \{g : (g,h) \in \text{sop}(\gamma)\}$ y la función $f \colon R(G \times H) \to (RG)H$ tal que $\gamma \mapsto \beta$ donde $\beta = \sum_{h \in H} \alpha_h h$ con $\alpha_h = \sum_{g \in M_{h,\gamma}} a_{gh} g$. Se debe demostrar que f es una función biyectiva y además es un homomorfismo de anillos. Para demostrar que f es un homomorfismo primero se prueba que dicha

función conserva sumas. Sea $\gamma_1, \gamma_2 \in R(G \times H), \quad \gamma_1 = \sum_{g \in G, h \in H} a_{gh}(g,h), \quad \gamma_2 = \sum_{g \in G, h \in H} b_{gh}(g,h)$. De esta forma se tiene $f(\gamma_1) = \sum_{h \in H} \beta_h h, \quad \beta_h = \sum_{g \in M_{h,\gamma_1}} a_{gh} h$ y $f(\gamma_2) = \sum_{h \in H} \xi_h h, \quad \xi_h = \sum_{g \in M_{h,\gamma_2}} b_{gh} h$.

Haciendo la operatoria se tiene:

$$f(\gamma_1) + f(\gamma_2) = \sum_{h \in H} (\beta_h + \xi_h) h = \sum_{h \in H} \alpha_h h,$$

en donde $\alpha_h = \beta_h + \xi_h$. Por otro lado:

$$f(\gamma_1) + f(\gamma_2) = f\left(\sum_{g \in G, h \in H} (a_{gh} + b_{gh}) g \right) = \sum_{h \in H} \alpha_h h, \quad \alpha_h = \sum_{g \in M_h, \gamma_1 + \gamma_2} (a_{gh} + b_{gh}) g.$$

De lo anterior se deduce fácilmente que $\alpha_h = \sum_{g \in M_h, \gamma_1} a_{gh} g + \sum_{g \in M_h, \gamma_2} b_{gh} g = \beta_h + \xi_h$.

La aplicación f conserva productos. En efecto, sean $\gamma_1, \gamma_2 \in R(G \times H)$, entonces haciendo la operatoria:

$$\gamma_1 \gamma_2 = \sum_{g,m \in G, h,n \in H} a_{gh} b_{mn} (g,h)(m,n).$$

Como ya se ha probado que f conserva sumas, ahora es suficiente demostrar que dados $(g,h), (m,n) \in (G \times H)$ se cumple que $f((g,h)(m,n)) = f((g,h)) f((m,n))$ y que además f es R-lineal. En efecto, se tiene:

$$f((g,h)) f((m,n)) = (gh)(nm) = gnhm$$

y además:

$$f((g,h)(n,m)) = f((gn,hm)) = gnhm.$$

El hecho de que f es R-lineal se sigue directamente de la definición de f.

Para demostrar que f es inyectiva se debe probar que el único elemento que anula a f es el neutro de $R(G \times H)$. En efecto, considérese $\gamma \in R(G \times H), \quad \gamma = \sum_{g \in G, h \in H} a_{gh}(g,h)$ tal que $f(\gamma) = \sum_{h \in H} \alpha_h h = 0, \quad \alpha_h = \sum_{g \in M_{h,\gamma} = a_{gh}} h$, lo cual implica que $a_{gh} = 0$ para cada $g \in G, h \in H$, de donde $\gamma = 0$.

Dado $\sum_{h \in h} \alpha_h h \in (RG)H$ se construye $\gamma = \sum_{g \in G, h \in H} a_{gh}(g,h)$, donde a_{gh}, es decir, el coeficiente de (g,h) es el mismo que el de g en α_h, con esto se demuestra que f es sobreyectiva, con lo que concluye la prueba. □

Lema 2.4.2. Sea $\{R_i\}_{i \in I}$ una familia de anillos y sea $R = \oplus_{i \in I} R_i$. Entonces para cualquier grupo G se tiene $RG \simeq \oplus_{i \in I} R_i G$.

Demostración. Considérese la función $f\colon \oplus_{i \in I} R_i G \to RG$ dado por $(\alpha_1, \ldots, \alpha_n) \mapsto \sum_{g \in G} a_g g, \quad a_g = (a_g^{(1)}, \ldots, a_g^{(n)})$, donde $a_g^{(i)}$ es el coeficiente de g en $\alpha_i = \sum_{g \in G} a_g^{(i)} g$. Se debe comprobar que f es un homomorfismo de anillos. Sean $\alpha = (\alpha_1, \ldots, \alpha_n), \ \beta = (\beta_1, \ldots, \beta_n) \in \oplus_{i \in I} R_i G$, entonces su suma viene dada por $\gamma = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$, y con ello la imagen de la suma es $f(\gamma) = \sum_{g \in G} c_g g, \quad c_g = (a_g^{(1)} + b_g^{(1)}, \ldots, a_g^{(n)} + b_g^{(n)})$.

Por otro lado, se tiene:

$$\begin{aligned} f(\alpha)+f(\beta) &= \sum_{g\in G} a_g g + \sum_{g\in G} b_g g \\ &= \sum_{g\in G} (a_g + b_g) g \\ &= \sum_{g\in G} d_g g, \quad d_g = (a_g^{(1)} + b_g^{(1)}, \ldots, a_g^{(n)} + b_g^{(n)}) \end{aligned}$$

por lo tanto $f(\alpha+\beta) = f(\alpha) + f(\beta)$ y con esto se demuestra que f conserva sumas.

Para demostrar que f conserva producto, se procede de manera similar que en la parte anterior, con lo que se tiene $\gamma = \alpha\beta = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n)$, y por lo tanto, su imagen bajo f, es $f(\gamma) = \sum_{u\in G} c_u u$ donde $c_u = (c_u^{(1)}, \ldots, c_u^{(n)}), \quad c_u^{(i)} = \sum_{gh=u} a_g^{(i)} b_h^{(i)}$.

Por otro lado, $f(\alpha) = \sum_{g\in G} a_g g, \quad f(\beta) = \sum_{g\in G} b_g g$, multiplicando, se obtiene $f(\alpha)f(\beta) = \sum_{u\in G} d_u u, \quad d_u = \sum_{gh=u} a_g b_h = \left(\sum_{gh=u} a_g^{(1)} b_h^{(1)}, \ldots, \sum_{gh=u} a_g^{(n)} b_h^{(n)}\right) = c_u$

Se procede a demostrar que f es inyectiva. Para ello supóngase que $f(\alpha) = \sum_{g\in G} a_g g = 0$ entonces $a_g = (0, \ldots, 0)$, de donde $\alpha = (0, \ldots, 0)$.

Dado $\sum_{g\in G} a_g g, \quad a_g = (a_g^{(1)}, \ldots, a_g^{(n)})$. Entonces se construye

$$\alpha = \left(\sum_{g\in G} a_g^{(1)} g, \ldots, \sum_{g\in G} a_g^{(n)} g \right).$$

De esto, se puede verificar que $f(\alpha) = \sum_{g\in G} a_g g$, con lo que se prueba que f es sobreyectiva. □

Teorema 2.4.1 (Perlis-Walker). Sea G un grupo finito abeliano de orden n y

sea K un campo tal que $\text{car}(K) \nmid n$. Entonces

$$KG \simeq \oplus_{d|n} a_d K(\zeta),$$

donde ζ_d es una raíz primitiva de la unidad de orden d y $a_d = \frac{n_d}{[K(\zeta_d):K]}$. En esta expresión n_d denota el número de elementos de orden d en G.

Demostración. Para demostrar el teorema se procede por inducción sobre el orden de G. Supóngase que el resultado es válido para cualquier grupo abeliano de orden menor que n.

Sea G tal que $|G| = n$. Si G es generado no hay algo que demostrar. Si G no fuera un grupo generado se puede utilizar el teorema 1.2.9 de estructura de los grupos finitos abelianos para escribir $G = G_1 \times H$ donde H es generado y $|G_1| = n_1 < n$. Por hipótesis de inducción se puede escribir

$$RG_1 \simeq \oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1}),$$

donde $a_{d_1} = \frac{n_{d_1}}{[K(\zeta_{d_1}):K]}$ y n_{d_1} denota el numero de elementos de orden d_1 en G_1. Aplicando el lema 2.4.1 se cumple

$$RG = R(G_1 \times H) \simeq (RG_1)H \simeq \left(\oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})\right) H$$

y utilizando el lema 2.4.2

$$RG = \left(\oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1})\right) H \simeq \oplus_{d_1|n_1} a_{d_1} K(\zeta_{d_1}) H.$$

Como H es cíclico se puede escribir

$$\oplus_{d_1|n_1} \oplus_{d_2||H|} a_{d_1} a_{d_2} K(\zeta_{d_1}, \zeta_{d_2}),$$

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

Sea $d = [d_1, d_2]$ entonces por el teorema del elemento primitivo, se tiene $K(\zeta_d) = K(d_1, d_2)$ por tanto

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

donde $a_d = \sum_{d1,d2} a_{d_1} a_{d_2}$ y donde la suma recorre todos los d_1, d_2 son números naturales tales que $[d_1, d_2] = d$. Por otro lado, del hecho que

$$[K(\zeta_d) : K] = [K(\zeta_{d_1, \zeta_{d_2}}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K]$$

se tiene que:

$$a_d[K(\zeta_d : K)] = \sum_{d_1,d_2} a_{d_1} a_{d_2} [K(\zeta_{d_1,\zeta_{d_2}}) : K(\zeta_{d_1})][K(\zeta_{d_1}) : K] = \sum_{d_1,d_2} n_{d_1} n_{d_2}. \qquad \square$$

3. TEORÍA DE REPRESENTACIÓN DE GRUPOS

3.1. Definición y ejemplos

Como se mencionó en el capítulo 1 el concepto de **grupo de permutaciones** fue dado explícitamente por primera vez en las memorias de Galois en 1830, aunque la primera definición de grupo abstracto fue dado hasta en 1854 por Cayley, aunque pasó inadvertidamente por un tiempo, hasta que dicha definición fue dada nuevamente en repetidas ocasiones por varios matemáticos, a saber: Leopold Kronecker en 1870, Heinrich Martin Weber en 1882 y Ferdinand Georg Frobenius en 1887. De esa forma los grupos fueron considerados por mucho tiempo como objetos concretos antes de llegar a ser estudiados como estructuras algebraicas abstractas.

En este contexto histórico es natural hacer la pregunta: Dado un grupo abstracto ¿cómo se puede saber qué grupo es? Es decir, ¿se puede decir cuándo es un grupo de permutaciones, un grupo lineal o un grupo de transformaciones proyectivas? En la última interrogante es importante aclarar que se listó sólo algunos ejemplos de las clases de grupos que existen.

En 1879, durante las lecturas de un coloquio matemático realizado en Evanston, Illinois, Felix Klein planteó la posibilidad de representar un grupo abstracto dado como un grupo de transformaciones lineales (véase (8)).

Siguiendo estas ideas, Theodor Molien, Georg Frobenius, Issai Schur, William Burnside y Heinrich Maschke desarrollaron la teoría básica de la representación de grupos al inicio del siglo XX y Burnside presentó la primera exposición sistemática

de este tema en su libro (3), que actualmente es considerado un libro clásico en este tema.

La teoría de la representación se volvió mas importante a medida que se fueron obteniendo nuevos resultados. Uno de los resultados mas importantes es el famoso teorema que establece que si p y q son números enteros primos y a, b enteros positivos, entonces cualquier grupo de orden $p^a q^b$ es soluble. Este teorema fue demostrado en 1904 por William Burnside usando la teoría de representación de grupos y, como dato curioso, la primera demostración que no utiliza dicha teoría fue proporcionada por John Griggs Thompson más de 60 años después (ver (7)).

William Burnside también conjeturó que todo grupo de orden impar es soluble. Esta conjetura fue un problema abierto hasta que Walter Feit y John Thompson dieron una demostración de esta conjetura en 1963 (ver (6)), usando para ello teoría de la representación. Luego de hacer énfasis en la importancia histórica que tiene la teoría de representación de grupos, se presentan algunas definiciones de la misma.

Definición 3.1.1. Sean G un grupo, R un anillo conmutativo y V un R-módulo libre de rango finito. Una **representación** de G sobre R, con espacio de representación V, es un homomorfismo de grupos $T\colon G \to GL(V)$, donde $GL(V)$ es el grupo de automorfismo de V. El rango de V es llamado **grado** de la representación T y se denotará como $\deg(T)$.

Para $g \in G$ se denotará con $T_g\colon V \to V$ al automorfismo correspondiente bajo T. Así, si $g, h \in G$, se tiene que $T_{gh} = T_g \circ T_h$ y $T_1 = I$.

El caso en el que R es un campo es de particular importancia. Históricamente, este fue el primer caso que se estudió y es en ese contexto donde se obtuvieron la mayor parte de resultados.

Si se escoge una R-base de V, se puede definir un isomorfismo ϕ de $GL(V)$ al grupo $GL(n, R)$ de matrices invertibles $n \times n$ con coeficientes en R, asignándole a cada automorfismo $T \in GL(V)$ su matriz respecto a la base dada. Esto da paso a la siguiente

Definición 3.1.2. Sea G un grupo y R un anillo conmutativo. Una representación matricial de G sobre R de grado n es un homomorfismo de grupos $T\colon G \to GL(n, R)$.

Si $T\colon G \to GL(V)$ es una representación de G sobre R con espacio de representación V y se considera el isomorfismo $\phi\colon GL(V) \to GL(n, R)$ asociada a alguna R-base, entonces $\phi \circ T\colon G \to GL(n, R)$ es una representación matricial de G. De manera similar, dada una representación matricial $T\colon G \to GL(n, R)$, entonces $\phi^{-1} \circ T\colon G \to GL(V)$ es una representación de G sobre R. Debido a este hecho, no se hará distinción entre representación y representación matricial.

Ejemplo 3.1.1. Dado un grupo G y un anillo conmutativo R, la función $T\colon G \to GL(n, R)$ tal que a cada elemento G le asocia la matriz identidad de $GL(n, R)$ es una representación matricial de G. A esta función se le llama **representación trivial** de G sobre R de grado n.

Ejemplo 3.1.2. Sea G el grupo de Klein de cuatro elementos, es decir, $G = \{1, a, b, ab\}$. Este grupo tiene tres elementos de orden dos. Entonces $T\colon G \to GL(2, \mathbb{Z})$ es la función tal que:

$$T(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad T(a) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$T(b) = \begin{pmatrix} -1 & 0 \\ 0 & 2 \end{pmatrix}, \quad T(ab) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Ejemplo 3.1.3. Sea S_n el grupo de simetrías de n símbolos y R un anillo conmutativo. Sea V un R-módulo libre de rango n con base $\{v_1, v_2, \ldots, v_n\}$. Para facilitar la comprensión de este ejemplo, se sugiere al lector imaginar que $V = \underbrace{\mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{n}$ con su base canónica.

Por otra parte, considérese la función $f\colon S_n \to GL(V)$ de la siguiente manera: a cada elemento $\sigma \in S_n$, se le asigna la función $T_\sigma \in GL(V)$, que actúa, de manera natural, como:

$$T_\sigma(v_i) = v_{\sigma(i)}.$$

Como T_σ deja a la base intacta (salvo permutaciones), es claro que T_σ es un isomorfismo. Es claro que T es un isomorfismo, por su definición, y por lo tanto una representación de S_n.

Como se puede apreciar una representación por si sóla puede ser poca descriptiva, por lo tanto se considera de más utilidad conocer la representación matricial. Para este caso en particular, considérese $A(\sigma)$, la matriz asociada a T_σ, que se obtiene al calcular $T_\sigma(v_j)$ como combinación lineal de la base. Como $T_\sigma(v_j) = v_{\sigma(j)}$, entonces los coeficientes de la matriz anterior son cero en todas sus entradas excepto en $(\sigma(j), j)$, en la cual la entrada vale uno. De esta manera es fácil notar que $A(\sigma)$ es una matriz que tiene exactamente una entrada igual a uno en cada fila y columna y las demás iguales a cero. Dicha matriz se conoce como la **matriz de permutación**.

Ejemplo 3.1.4 (La representación Regular). Sea G un grupo finito de orden n y R un anillo conmutativo. Se requiere definir una representación de G sobre R, para

ello se considerará como espacio de representación a RG, es decir, a el grupo-anillo de G sobre R.

Considérese la función $T\colon G \to GL(RG)$ de la siguiente manera: a cada elemento $g \in G$ se le asigna la función lineal T_g que transforma a los elementos de la base por medio de multiplicación por la izquierda, esto es, $T_g(g_i) = gg_i$. Es claro que T es una representación de G, debido a que:

$$T_{gh}(y) = (gh)y = g(h(y)) = T_g T_h(y).$$

En este caso hay que recordar que G es una base de RG sobre R y se pueden enumerar, en algún orden, los elementos de G como sigue:

$$G = \{1 = g_1, g_2, \ldots, g_n\},$$

por lo tanto es fácil notar que en la correspondiente representación matricial con respecto a la base G de RG, la imagen de cualquier elemento $g \in G$ es una matriz de permutación, debido a la cerradura del producto en G.

La representación anterior usualmente es llamada la **representación regular de G sobre R por la izquierda**. Para ilustrar de mejor manera a continuación se muestra un ejemplo concreto:

Ejemplo 3.1.5. Sea $G = \{1, a, a^2\}$ un grupo cíclico de orden tres. Enumérese los elementos de G como $g_1 = 1$, $g_2 = a$, $g_3 = a^2$. Para encontrar la representación regular de a, basta con multiplicar por a los elementos de G por la izquierda:

$$ag_1 = g_2, \quad ag_2 = g_3, \quad ag_3 = g_1$$

entonces se tiene:

$$T_a(g_1) = g_2, \quad T_a(g_2) = g_3, \quad T_a(g_3) = g_1,$$

por lo tanto la matriz asociada con a en la base dada es:

$$\rho(a) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

que no es más que una matriz de permutación.

Ejemplo 3.1.6. Considérese, de nuevo, el grupo de Klein de cuatro elementos, $G = \{1, a, b, ab\}$ con la numeración: $g_1 = 1$, $g_2 = a$, $g_3 = b$, $g_4 = ab$.

Para conocer la representación regular de a, se procede a multiplicar por la izquierda por a a los elementos de G:

$$ag_1 = g_2, \quad ag_2 = g_1, \quad ag_3 = g_4, \quad ag_4 = g_3,$$

entonces

$$T_a(g_1) = g_2, \quad T_a(g_2) = g_1, \quad T_a(g_3) = g_4, \quad T_a(g_4) = g_3$$

y como en el ejemplo anterior, se puede obtener la representación matricial de a:

$$\rho(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

De manera similar se obtiene la representación matricial de los elementos restantes de G:

$$\rho(b) = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \rho(ab) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \rho(1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Nota 3.1.1. Ya se mencionó que $\rho(g)$ con $g \in G$ es una matriz de permutación, pero es importante hacer notar que si se toma $1 \neq g \in G$, entonces para cualquier $g_i \in G$ se tiene que $gg_i \neq g_i$. Esto implica que para cualquier elemento g_i de la base se cumple que $T_g(g_i) \neq g_i$ y por ende los elementos de la diagonal de $\rho(g)$ son todos iguales a cero. Más aún, de lo anteriormente expuesto, se deduce que si $g \neq 1$ entonces $\mathrm{tr}(\rho(g)) = 0$ si $g \neq 1$ y $tr(\rho(g)) = |G|$ si $g = 1$. Este resultado elemental es de mucha importancia cuando se está trabajando con la representación regular.

Ejemplo 3.1.7. (Algunas representaciones de grupos cíclicos) Considérese el grupo cíclico $G = \{1, a, \ldots, a^{m-1}\}$ y sea K un campo. Si se desea construir una representación matricial $A\colon G \to GL(n, K)$ es necesario escoger la matriz $A(a)$, ya que por ser A un homomorfismo, las matrices de representación de los restantes elementos del grupo están determinadas por $A(a^r) = (A(a))^r$. Además para demostrar que A es un homomorfismo de grupos, basta con probar que $(A(a))^r = I$, para algún $r \in \mathbb{Z}$.

Supóngase que $\text{car}(K) \nmid m$ y que K contiene una raíz primitiva de la unidad de orden m, ξ. Entonces

$$A\colon G \to GL(1, K)$$

tal que, $A(a) = \xi$ es una representación, ya que $(A(a))^r = \xi^r = 1$ para algún r. Además, si $\{\xi_1, \cdots, \xi_m\}$ es un conjunto de todas las raíces de la unidad unidad de orden m que son distintas a pares entonces la función $B\colon G \to GL(m, K)$ dada por

$$B(a) = \begin{pmatrix} \xi_1 & & \dots & 0 \\ 0 & \xi_2 & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & \xi_m \end{pmatrix}$$

es una representación de G sobre K de grado m, ya que $\xi_i^r = 1$ para algún $r \in \mathbb{Z}$, entonces

$$(B(a))^r = \begin{pmatrix} \xi_1^r & & \dots & 0 \\ 0 & \xi_2^r & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & \xi_m^r \end{pmatrix} = I.$$

Nótese que esta representación es distinta a la representación regular, que en el caso de a, está dada por

$$\Gamma(a) = \begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Además si $\text{car}(K) \mid m$ entonces se propone la representación $C\colon G \to GL(2, K)$, dada por

$$C(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

ya que $(C(a))^r = \begin{pmatrix} 1 & r \cdot 1 \\ 0 & 1 \end{pmatrix} = I$ para $r \in \mathbb{Z}$, dado que $\text{car}(K) < \infty$.

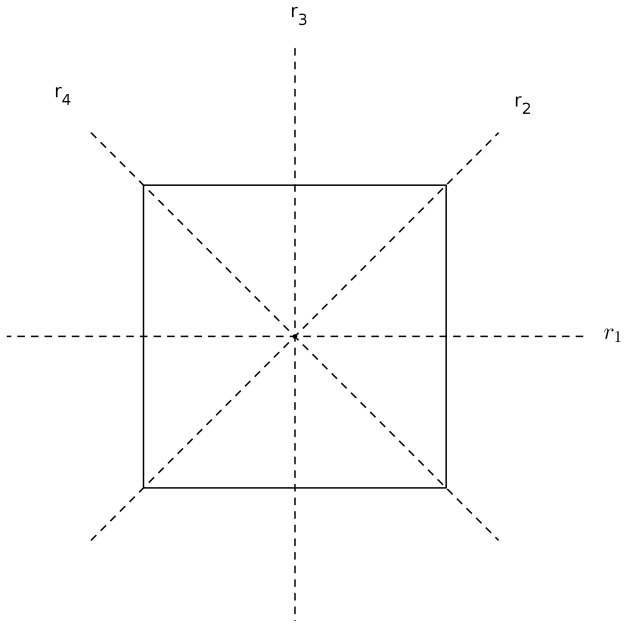
Ejemplo 3.1.8 (Representación de D_4). Considérese el grupo de simetrías de un cuadrado. Este grupo de 8 elementos, a saber, las reflexiones a través de los ejes r_1, r_2, r_3, r_4 (véase la Figura 5) y las rotaciones con ángulos $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ y 2π alrededor del centro.

Sea a la rotación de ángulo $\frac{\pi}{2}$ y b la reflexión a través del eje r_2. Es fácil ver, bajo consideraciones geométricas, que cualquier otro elemento de este grupo se puede obtener por medio de a y b.

De manera mas abstracta, este grupo, que es llamado grupo diédrico de orden ocho y usualmente denotado por D_4, puede ser definido con dos generadores que satisfacen las relaciones

$$a^4 = 1, \quad b^2 = 1, \quad baba = 1.$$

Figura 5: Forma gráfica del grupo D_4



Fuente: elaboración propia con programa para computadora geogebra.

Por lo tanto este grupo puede ser descrito como

$$D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Como todas los elementos de este grupo están en terminos de a y b, entonces para encontrar una representación matricial $A\colon D_4 \to GL(n, K)$ sobre el campo K, será suficiente encontrar matrices $A(a)$, $B(b)$ tales que $A(a)^4 = I$, $A(b)^2 = I$, $A(b)A(a)A(b)A(a) = I$.

Es fácil determinar representaciones de grado uno para D_4 en un campo K de

característica diferente a dos, de la siguiente manera:

$$\begin{aligned} A(a) &= 1 \qquad & A(b) &= 1 \\ B(a) &= 1 \qquad & B(b) &= -1 \\ C(a) &= -1 \qquad & C(b) &= 1 \\ D(a) &= -1 \qquad & D(b) &= -1. \end{aligned}$$

Pensando en el significado geométrico de a y b, como dos funciones del plano al plano, se puede calcular sus matrices con respecto a la base canónica para obtener otra representación matricial de D_4:

$$W(a) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad , \quad W(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

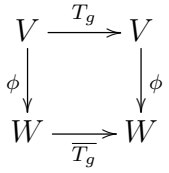
Ejemplo 3.1.9 (Suma directa de representaciones). Sean $T\colon G \to GL(V)$ y $S\colon G \to GL(W)$ dos representaciones de un grupo G sobre un anillo conmutativo R. Se puede definir una nueva representación $V \oplus W$, que es llamada la **suma directa** de dos representaciones dadas y se denota como $T \oplus S$, de la siguiente manera:

$$(T \oplus S)_g = T_g \oplus S_g, \quad \text{para cada } g \in G.$$

Si se eligen bases $\{v_1, \ldots, v_n\}$ y $\{w_1, \ldots, w_m\}$ de V y W respectivamente y se denota por $g \mapsto A(g)$ y $g \mapsto B(g)$ las correspondientes representaciones matriciales en las bases dadas, entonces la representación matricial asociada a $T \oplus S$ con respecto a la base $\{(v_1, 0), \ldots, (v_n), (0, w_1), \ldots, (0, w_n)\}$ de $V \oplus W$, viene dada por

$$g \mapsto \begin{pmatrix} A(g) & 0 \\ 0 & B(g) \end{pmatrix}.$$

Figura 6: Diagrama conmutativo para representaciones equivalentes



Fuente: elaboración propia con programa para computadora **xymatrix**.

Los ejemplos anteriormente expuestos sirven de motivación para introducir algunos conceptos de teoría de la representación. En este trabajo se restringirán las representaciones al caso en el cual R es un campo, debido a que con este caso se logra ilustrar la relación de teoría de representación con los problemas de grupo-anillos.

Primero considérese $T\colon G \to GL(V)$ una representación de un grupo G sobre un campo K y asúmase que $\phi\colon V \to W$ es un isomorfismo de espacios vectoriales sobre K. Entonces se puede definir una nueva representación $\overline{T}\colon G \to GL(W)$ por medio de $\overline{T_g}\colon \phi \circ T_g \circ \phi^{-1}$ para todo $g \in G$. Esto es, esencialmente, una copia de T. La relación entre estas dos representaciones está ilustrada en el diagrama de la figura 6, lo cual sugiere la siguiente:

Definición 3.1.3. Dos representaciones $T\colon G \to GL(V)$ y $\overline{T}\colon G \to GL(W)$ de un grupo G sobre el mismo campo K se dicen que son **equivalentes** si existe un isomorfismo $\phi\colon V \to W$ tal que $\overline{T_g} = \phi T_g \phi^{-1}$ para cualquier $g \in G$.

Definición 3.1.4. Dos representaciones matriciales $A\colon G \to GL(n, K)$ y $B\colon G \to GL(n, K)$ de un grupo G sobre un campo K se dicen **equivalentes** si existe una matriz invertible $U \in GL(n, K)$ tal que $A(g) = UB(g)U^{-1}$ para cualquier $g \in G$.

Ejemplo 3.1.10. Sea G un grupo cíclico de orden m y K un campo que contiene a $\{\xi_1, \xi_2, \ldots, \xi_m\}$, el conjunto de todas las raíces distintas de la unidad de orden m. Entonces, si se consideran las representaciones B y Γ dadas en el ejemplo 3.1.7 con

$$\mathsf{U} = \begin{pmatrix} \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\ \xi_2 & \xi_2^2 & \cdots & \xi_2^m \\ & & \cdots & \\ \xi_m & \xi_m^2 & \cdots & \xi_m^m \end{pmatrix}.$$

Es claro que $\mathsf{U} \in GL(n, K)$, ya que U es una matriz de Vandermonde con $det(\mathsf{U}) = \prod_{1 \leq i < j \leq m}(\xi_i - \xi_j) \neq 0$. Entonces, calculando, por un lado se tiene

$$B(a)\mathsf{U} = \begin{pmatrix} \xi_1 & 0 & \cdots & 0 \\ 0 & \xi_2 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & \xi_m \end{pmatrix} \begin{pmatrix} \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\ \xi_2 & \xi_2^2 & \cdots & \xi_2^m \\ & & \cdots & \\ \xi_m & \xi_m^2 & \cdots & \xi_m^m \end{pmatrix} = \begin{pmatrix} \xi_1^2 & \xi_1^3 & \cdots & \xi_1 \\ \xi_2^2 & \xi_2^3 & \cdots & \xi_2 \\ & & \cdots & \\ \xi_m^2 & \xi_m^2 & \cdots & \xi_m \end{pmatrix},$$

similarmente

$$\mathsf{U}\Gamma(a) = \begin{pmatrix} \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\ \xi_2 & \xi_2^2 & \cdots & \xi_2^m \\ & & \cdots & \\ \xi_m & \xi_m^2 & \cdots & \xi_m^m \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & 0 & \cdots & 0 \\ & & \cdots & \\ 0 & 0 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} \xi_1^2 & \xi_1^3 & \cdots & \xi_1 \\ \xi_2^2 & \xi_2^3 & \cdots & \xi_2 \\ & & \cdots & \\ \xi_m^2 & \xi_m^2 & \cdots & \xi_m \end{pmatrix}$$

con lo que se ha demostrado que $A(g) = \mathsf{U}B(g)\mathsf{U}^{-1}$, para cualquier $g \in G$ y concluye que B y Γ son equivalentes.

Considérese $T\colon G \to GL(V)$ una representación de un grupo G sobre el campo K, con espacio de representación V y supóngase que V contiene un subespacio W que es invariable bajo T, esto es, un subespacio tal que $T_g(W) \subset W$, para cualquier

$g \in G$. Entonces se puede considerar el homomorfismo de grupos que asigna a cada elemento $g \in G$ la restricción de T_g al subespacio W. Por ser T_g la restricción, es claro que el homomorfismo anterior es una representación de G sobre K, con espacio de representación W.

Con el afán de dar una representación matricial de este hecho, considérese una base $\{w_1, w_2, \ldots, w_t\}$ de W y extiéndase a una base $\{w_1, \cdots, w_t, v_{t+1}, \cdots, v_n\}$ de V. Entonces la matriz asociada a cada función T_g, $g \in G$ con respecto a esa base es de la forma

$$\begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix}$$

donde $A(g) \in GL(t, K), C(g) \in GL(n-t, K)$ y $B(g)$ es una matriz de $t \times (n-t)$. Estas consideraciones sugieren la siguiente:

Definición 3.1.5. Una representación $T\colon G \to GL(V)$ de un grupo G sobre un campo K es llamada **irreducible** si los únicos subespacios propios de V que son invariantes bajo T son los triviales, es decir, V y $\{0\}$.

La representación es llamada **reducible** si V contiene subespacios no triviales que son invariantes bajo T.

Definición 3.1.6. Una representación matricial $M\colon G \to GL(n, K)$ es llamada **reducible** si existe una matriz $\mathsf{U} \in GL(n, K)$ tal que para cualquier $g \in G$, se tiene que la matriz $\mathsf{U}M(g)U^{-1}$ es de la forma

$$\mathsf{U}M(g)U^{-1} = \begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix}.$$

El ejemplo 3.1.10 muestra que la representación regular de un grupo cíclico de orden m, sobre un campo K que contiene raíces de la unidad de orden m es reducible. De hecho, cualquier representación regular de un grupo finito $G \neq \{1\}$ sobre cualquier campo es reducible. En efecto, nótese que si en el espacio de representación RG se toma el elemento $\hat{G} = \sum_{g \in G} g$ entonces $T_g(\hat{G}) = \hat{G}$ por lo tanto el subespacio generado por $\hat{G}$ es invariante bajo T y $(\hat{G}) \neq RG$.

Definición 3.1.7. Una representación $T\colon G \to GL(V)$ de un grupo G sobre un campo K es llamada **completamente reducible** si para todo subespacio W que es invariante bajo T existe un subespacio invariante W' tal que $V = W \oplus W'$.

Para entender de mejor manera esta definición se dará una interpretación en términos de matrices.

Sea $\{w_1, w_2, \ldots, w_t\}$ y $\{w_{t+1}, \ldots, w_n\}$ bases dadas para W y W' respectivamente, entonces $\{w_1, w_t, w_{t+1}, \ldots, w_n\}$ es una base de V y para cualquier $g \in G$ la matriz de T_g con respecto a esta base es de la forma

$$\begin{pmatrix} A(g) & 0 \\ 0 & B(g) \end{pmatrix}$$

donde $A(g)$ y $B(g)$ son las matrices de representación de T_g en W y W' con respecto a las bases dadas.

Definición 3.1.8. Una representación matricial $M\colon G \to GL(n, K)$ es llamada completamente reducible si cualquier representación matricial M de la forma

$$\begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix}$$

es equivalente a una representación matricial de la forma

$$\begin{pmatrix} A(g) & 0 \\ 0 & D(g) \end{pmatrix}.$$

3.2. Representación y módulos.

En este sección se estudiará la conexión que hay entre módulos y representaciones. Dicha conexión se establece usando el concepto de grupo-anillo.

Proposición 3.2.1. Sea G un grupo y R un anillo conmutativo con unidad. Entonces, existe una biyección entre representaciones de G sobre R y RG-módulos libres y de rango finito.

Demostración. Dada una representación $T\colon G \to GL(V)$ de G sobre R, se asocia a ella el RG-módulo construido a partir de V manteniendo la misma estructura aditiva y definiendo el producto de un elemento $v \in V$ por un escalar $\alpha = \sum_{g\in G} a_g g \in RG$ como

$$\alpha v = \left(\sum_{g\in G} a_g g\right) v = \sum_{g\in G} a(g) T_g(v). \tag{3.1}$$

Usando está definición de producto se verifica:

- Distributividad de la suma de escalares respecto al producto por escalar

$$\begin{aligned}(\alpha+\beta)v &= \left(\sum_{g\in G}(a_g+b_g)g\right)v \\ &= \sum_{g\in G}(a_g+b_g)T_g(v) \\ &= \sum_{g\in G}a_gT_g(v)+\sum_{g\in G}b_gT_g(v) \\ &= \alpha v+\beta v.\end{aligned}$$

- Distributividad de la suma de elementos del módulo respecto al producto por escalar

$$\begin{aligned}\alpha(v+w) &= \left(\sum_{g\in G}a_gg(v+w)\right) \\ &= \sum_{g\in G}a_gT_g(v+w) \\ &= \sum_{g\in G}a_gT_g(v)+\sum_{g\in G}a_gT_g(w) \\ &= \alpha v+\alpha w.\end{aligned}$$

- Para la asociatividad, por un lado se tiene

$$\begin{aligned}\alpha(\beta v) &= \left(\sum_{h\in G}a(g)h\right)\left(\sum_{g\in G}b(g)T_g(v)\right) \\ &= \sum_{h\in G}a(h)T_h\left(\sum_{g\in G}b(g)T_g(v)\right) \\ &= \sum_{h,g\in G}a(h)b(g)T_{hg}(v).\end{aligned}$$

Por otro lado se tiene

$$\begin{aligned}(\alpha\beta)v &= \left(\sum_{h,g\in G} a(h)b(g)hg\right)(v)\\ &= \sum_{h,g\in G} a(h)b(g)T_{hg}(v)\end{aligned}$$

con lo que se comprueba que $\alpha(\beta v) = (\alpha\beta)v$.

- Considérese $\alpha = 1_G$, entonces

$$\begin{aligned}\alpha v &= T_{1_G}(v)\\ &= I(v)\\ &= v.\end{aligned}$$

Por lo expuesto anteriormente es fácil notar que la multiplicación por escalar definida en la ecuación (3.1) induce un RG-módulo.

Al converso, si M es un RG-módulo de rango finito sobre R, se define la representación de G sobre R asignando a cada elemento $g \in G$ el R-automorfismo $T_g\colon M \to M$ dado por $T_g(m) = gm$.

Nótese que dado $T\colon G \to GL(V)$ una representación de G sobre R y M su RG-módulo inducido, se tiene que S, la representación inducida por M, es tal que $S_g(m) = gm = \alpha m \simeq T_g(m)$, donde α es la imagen de la inmersión de G en RG dada en el teorema 2.1.1.

De manera similar, dado M un RG-módulo y $S\colon G \to GL(M)$ su representación inducida, entonces su RG-módulo inducido por la ecuación (3.1) deja invariante a M. Por lo tanto se ha demostrado que las aplicaciones construidas anteriormente son inversas la una de la otra. □

Como ejemplo considérese un grupo finito G y RG como un módulo sobre sí mismo, de esta forma RG es de rango finito $|G|$ sobre R. Entonces, dado un elemento $x \in G$, la representación $T_x \colon RG \to RG$ viene dada por:

$$T_x\left(\sum_{g\in G} a(g)g\right) = x\left(\sum_{g\in G} a(g)g\right) = \left(\sum_{g\in G} a(g)gxg\right).$$

Esto significa que $x \in G$ actúa en los elementos de la base $G = \{g_1, \ldots, g_n\}$ multiplicándolos por la izquierda. En otras palabras, la representación asociada al RG-módulo RG es precisamente la representación regular de G.

Lema 3.2.1. Sea $T \colon G \to GL(V)$ una representación de un grupo G sobre un campo K, con espacio de representación V, entonces un subespacio $W \subset V$ es invariante bajo T si y sólo si W es un KG-módulo de V.

Demostración. Se procede a demostrar este hecho en dos partes:

- Sea $W \subset V$ invariante bajo T, entonces $T_g(W) = W$ para cualquier $g \in G$. Sean $w_1, w_2 \in W$ se tiene que $T_g(w_1 + w_2) = T_g(w_1) + T_g(w_2) \in W$, así $T_g^{-1}(T_g(w_1 + w_2)) \in W$. Por otra parte, si se considera $\alpha = \sum_{g\in G} a(g)g$ entonces $\alpha w = \sum_{g\in G} a(g)T_g(w) \in W$ y por lo tanto W es un KG-módulo de V.
- Sea W subespacio de V, $W \subset V$ y W un KG-módulo de V, entonces para $w \in W$ y $g \in RG$ se tiene $gw = 1 \cdot T_g(w) \in W$. □

Teorema 3.2.1. Sea G un grupo y K un campo. Entonces:

- Dos representaciones T y T' de G sobre R son equivalentes si y sólo si los correspondientes RG-módulos son isomorfos.

- Una representación es irreducible (o completamente reducible) si y sólo si el correspondiente RG-módulo es irreducible (o completamente reducible).

Demostración. Se procede a demostrar este lema por incisos:

- Supóngase que T y T' son representaciones de G sobre K equivalentes, entonces existe $\phi\colon V \to W$ isomorfismo, donde V y W son los espacios de representación de T y T' respectivamente, tal que $T'_g = \phi T_g \phi^{-1}$ para cualquier $g \in G$. Entonces se probará que ϕ es isomorfismo de RG-módulos también. En efecto

$$\begin{aligned}
\phi(\alpha v) &= \phi\left(\sum_{g\in G} a(g)T_g(v)\right) \\
&= \sum_{g\in G} a(g)\phi(T_g(v)) \\
&= \sum_{g\in G} a(g)T'_g(\phi(v)) \\
&= \alpha\phi(v).
\end{aligned}$$

- Supóngase que M y N son RG-módulos isomorfos, entonces existe $f\colon M \to N$ isomorfismo de RG-módulos. Sean T y T' las representaciones inducidas por M y N respectivamente, entonces:

$$\begin{aligned}
(fT_g f^{-1})(n) &= f\left(T_g\left(f^{-1}(n)\right)\right) \\
&= f\left(gf^{-1}(n)\right) \\
&= gf\left(f^{-1}(n)\right) \\
&= gn \\
&= T'_g(n)
\end{aligned}$$

con lo que se comprueba que T y T' son equivalentes.

- Si una representación T es irreducible, entonces los únicos subespacios de V que son invariantes bajo T son los triviales y, por el lema anterior, los únicos submódulos de M, el módulo inducido por T, son los los triviales. De manera análoga se puede demostrar el converso. $\square$

También es posible notar que si un RG-módulo M admite una descomposición como suma directa de submódulos $M = \oplus_{i=1}^{t} M_i$ y si T y T_i denota las representaciones correspondientes a estos módulos, entonces $T = \oplus_{i=1}^{t} T_i$.

En lo que sigue, se mostrará como la información que ya se conoce acerca de los grupo-anillos se puede trasladar a términos de representaciones de grupos.

El lector deberá recordar que en el corolario 2.3.2, como consecuencia directa del teorema de Maschke, se demostró que si K es un campo tal que $\text{car}(K) \nmid |G|$, entonces KG es un anillo semisimple. Además, se demostró en el teorema 2.3.2 que en este caso todo KG-módulo es simple. Por lo tanto, en particular, se sigue inmediatamente que todo KG-módulo finito dimensional sobre K se puede escribir como suma directa de módulos irreducibles.

En términos de representaciones, esto significa que bajo estas condiciones, toda representación de G sobre K es la suma directa de representaciones irreducibles. Así, para determinar todas las representaciones de G sobre K, mediante equivalencia, es suficiente determinar todos los KG-módulos irreducibles, salvo isomorfismos.

Ahora, es necesario hacer uso del teorema de Wedderburn-Artin aplicado a grupo-anillos (teorema 2.3.2), el cual establece que el número de KG-módulos irreducibles que no son isomorfos entre sí, es precisamente el número de componentes simples de KG y estas están determinadas exclusivamente por la estructura de KG.

En particular, es importante recordar que si se escribe KG en la forma

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

donde $D_i, 1 \leq i \leq r$, son anillos de división que contienen a K en sus centros, y si se calcula la dimensión en ambos lados de la ecuación, se tiene

$$|G| = \sum_{i=1}^{r} n_i^2 [D_i : K].$$

Por otro lado, se sabe que el módulo irreducible I_i correspondiente a la componente simple $M_{n_i}(D_i)$ es isomorfo a $D_i^{n_i}$. Como el grado de la correspondiente representación T_i viene dado por la dimensión de este módulo sobre K, se obtiene que

$$\deg(T_i) = [D_i^{n_i} : K] = n_i [D_i : K]$$

así, se puede escribir

$$|G| = \sum_{i=1}^{r} n_i \deg(T_i).$$

Ejemplo 3.2.1. Se mostró en el ejemplo 2.4.1 que si $G = \langle a \rangle$ denota al grupo cíclico de orden siete, entonces

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

donde ζ denota una raíz primitiva de la unidad de orden siete. De lo anterior, las componentes simples de $\mathbb{Q}G$ son anillos de matrices de 1×1 sobre los anillos $\mathbb{Q}$ y

$\mathbb{Q}(\zeta)$ respectivamente y por ende existen solamente dos representaciones irreducibles que no son equivalentes, S y T de G sobre $\mathbb{Q}$, con grados

$$\deg(S) = [\mathbb{Q} : \mathbb{Q}] = 1, \quad \deg(T) = [\mathbb{Q} : \mathbb{Q}] = 6.$$

Como las representaciones 1-dimensionales son equivalentes si y sólo si son iguales y como cualquier grupo admite la representación trivial $S\colon G \to GL(1, \mathbb{Q})$ dada por $S_g = 1$, para cada $g \in G$, entonces la representación 1-dimensional de G sobre $\mathbb{Q}$ es la trivial.

Para determinar T_a, de acuerdo a las consideraciones anteriores, se debe considerar el $\mathbb{Q}G$-módulo irreducible $I_2 = D_2^{n_2}$ correspondiente a la segunda componente simple de $\mathbb{Q}$. Entonces, la representación $T\colon G \to GL(I_2)$ está dada por $T_a(v) = av$, para cada $v \in I_2$. En este caso, $n_2 = 1$ y $D_2 = \mathbb{Q}(\zeta)$, así que $I_2 = \mathbb{Q}(\zeta)$, donde la multiplicación por un elemento $\alpha = (\alpha_1, \alpha_2) \in \mathbb{Q}G$ está dada por $\alpha v = \alpha_2 v$, para todo $v \in \mathbb{Q}(\zeta)$. Recordando que el elemento $a \in \mathbb{Q}(\zeta)$ le corresponde, vía isomorfismo, el elemento $(1, \zeta) \in \mathbb{Q} \oplus \mathbb{Q}(\zeta)$ se tiene

$$T_a(v) = av = \zeta v, \quad v \in \mathbb{Q}(\zeta).$$

Por lo tanto, si se toma $\{1, \zeta, \zeta^2, \ldots, \zeta^5\}$ como una base de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$, entonces

la correspondiente matriz está dada por

$$A(a) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}.$$

Ejemplo 3.2.2 (Representaciones del grupo diédrico de orden ocho.). Se ha probado en ele ejemplo 3.1.8 que el grupo D_4 admite cuatro representaciones distintas de grado uno y una representación W de grado dos sobre $\mathbb{Q}$, por lo tanto existen cuatro componentes simples isomorfas a $\mathbb{Q}$. Sean $M_n(D)$ la componente simple correspondiente a la representación de grado dos. Como $2 = \deg(W) = n[D : \mathbb{Q}]$, entonces $n = 1$ y $[D : \mathbb{Q}]$ o $n = 2$ y $[D : \mathbb{Q}] = 1$.

Para el primer caso, se puede observar que $\mathbb{Q}D_4$ debe ser de la forma

$$\mathbb{Q}D_4 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus D \oplus D',$$

donde D' es una anillo de división con $[D' : \mathbb{Q}] = 2$. Es fácil notar que un anillo de división de dimensión dos sobre un campo tiene que ser conmutativo, entonces $\mathbb{Q}D_4$ es conmutativo, lo cual es una contradicción, ya que D_4 no es abeliano.

En consecuencia, se debe tener que $n = 2$ y $D = \mathbb{Q}$. De esta forma

$$\mathbb{Q}D_4 \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}).$$

4. ELEMENTOS ALGEBRAICOS

4.1. Generalidades y definiciones

En este capítulo será de especial interés estudiar algunos elementos algebraicos en grupo-álgebras usando la representación regular que puede ser definida para un álgebra finito dimensional con unidad sobre un campo K de la siguiente manera.

Definición 4.1.1. Sea $T\colon A \to \hom_K(A,A)$ tal que $a \mapsto T_a \in \hom_K(A,A)$, definida mediante multiplicación por la izquierda por a. Esto es, T_a es una aplicación tal que $T_a(x) = ax$, para cualquier $x \in A$.

Se puede observar a partir de la definición que

$$\begin{aligned} T_{a+b} &= T_a + T_b \\ T_{ab} &= T_a T_b \\ T_{ka} &= kT_a \end{aligned}$$

para todo $a, b \in A$, $k \in K$. Mas aún, la aplicación $a \mapsto T_a$ es inyectiva debido a que $T_a(1) = a$. Eligiendo una base $\{a_1, \ldots, a_n\}$ de A sobre K se puede representar a T_a con una matriz $\rho(a)$, con lo que se obtiene la representación matricial:

$$a \mapsto \rho(a) \in M_n(K).$$

Si a es un elemento algebraico de A, esto es, si existe un polinomio no nulo $f(X) \in K[X]$ tal que $f(a) = 0$, entonces los valores propios de la matriz $\rho(a)$ también anulan a $f(X)$, debido al teorema de Cayley-Hamilton (véase (13:241)).

De esta manera, por ejemplo, si a es un elemento nilpotente entonces los valores propios de $\rho(a)$ son todos cero. Si a es de orden multiplicativo finito, es decir, si $a^m = 1$ para algún m entero positivo, entonces los valores propios de $\rho(a)$ son raíces de la unidad de orden m.

Lema 4.1.1. Sea G un grupo finito y K un campo. Sea p la representación regular de KG y $\gamma = \sum_{g\in G} \gamma(g)g \in KG$. Entonces la traza de $\rho(\gamma)$ viene dada por

$$\operatorname{tr} \rho(\gamma) = |G|\gamma(1).$$

Demostración. Se sabe que $\operatorname{tr} \rho(\gamma)$ es independiente de la base elegida, así que se elige $G = \{g_1, \ldots, g_n\}$ como K-base para KG y se asume que $g_1 = 1$. Entonces

$$\rho(\gamma) = \rho\left(\sum_{g\in G} \gamma(g)g\right) = \sum_{g\in G} \gamma(g)\rho(g).$$

Para un elemento $1 \neq g \in G$, se tiene $gg_i \neq g_i$, para $1 \leq i \leq n$, de donde se sigue que los elementos de la diagonal de la matriz $\rho(g)$ son todos nulos si $g \neq 1$. Así $\operatorname{tr} \rho(g) = 0$ si $g \neq 1$. Más aún, como $\rho(1)$ es la matriz identidad, se tiene que $\operatorname{tr} \rho(1) = n$. Entonces

$$\operatorname{tr} \rho(\gamma) = \sum_{g\in G} \gamma(g) \operatorname{tr}(g) = \gamma(1) \operatorname{tr} \rho(1) = \gamma(1)|G|. \qquad \square$$

Lema 4.1.2. Sea $\gamma = \sum_{g\in G} \gamma(g)g$ una unidad de orden finito en el grupo-anillo entero $\mathbb{Z}G$ con G un grupo finito y asúmase que $\gamma(1) \neq 0$. Entonces $\gamma = \gamma(1) = \pm 1$.

Demostración. Sea $|G| = n$ y supóngase que $\gamma^m = 1$ para algún entero positivo m. Si se considera la representación regular ρ del grupo-álgebra $\mathbb{C}G$ y a $\mathbb{Z}G$ como un subanillo de la misma, se tiene que $\operatorname{tr} \rho(\gamma) = n\gamma(1)$. Como $\gamma^m = 1$, entonces

$(\rho(\gamma))^m = \rho(\gamma^m) = I$, de esto se sigue que $\rho(\gamma)$ es raíz del polinomio $X^m - 1$, cuyas raíces son todas distintas. Esto implica, por el teorema espectral (véase (13:214)), que existe una base de $\mathbb{C}G$ donde la matriz de $\rho(\gamma)$ es diagonal de la forma

$$\mathbb{A} = \begin{pmatrix} \xi_1 & & & \\ & \xi_2 & & \\ & & \ddots & \\ & & & \xi_n \end{pmatrix}, \quad \xi_i^m = 1.$$

Entonces $\operatorname{tr} \rho(\gamma) = \sum_{i=1}^{n} \xi_i$ y así

$$n\gamma(1) = \sum_{i=1}^{n} \xi_i.$$

Por lo tanto, aplicando valor absoluto,

$$|n\gamma(1)| = \left| \sum_{i=1}^{n} \xi_i \right| \leq \sum_{i=1}^{n} |\xi| = n.$$

Como $|n\gamma(1)| = n|\gamma(1)| \leq n$, entonces $|\gamma(1)| = 1$ y $|\sum_{i=1}^{n} \xi_i| = \sum_{i=1}^{n} |\xi_i|$, lo cual sucede si y sólo si $\xi_1 = \xi_2 = \cdots = \xi_n$.

Así $n\gamma(1) = n\xi_1$ y $\gamma(1) = \xi_1 = \pm 1$. Se concluye que $\rho(\gamma) = \pm I$, de donde, $\gamma = \pm 1$. □

Corolario 4.1.1. Supóngase que $\gamma = \sum_{g \in G} \gamma(g)g$ es una unidad central en el grupo-anillo entero $\mathbb{Z}G$ con G un grupo finito de orden finito. Entonces γ es de la forma $\gamma = \pm g$ con $g \in \mathcal{Z}(G)$.

Demostración. Sea $\gamma = \sum_{g \in G} \gamma(g)g$ una unidad central de orden m. Supóngase que $\gamma(g_0) \neq 0$, para algún $g_0 \in G$. Entonces γg_0^{-1} es también una unidad de orden finito en $\mathbb{Z}G$. Mas aún, el coeficiente de 1 en la expresión de γg_0^{-1} es $\gamma(g_0) \neq 0$, de donde $\gamma g_0^{-1} = \pm 1$ y por lo tanto $\gamma = \pm g_0$. □

Una consecuencia inmediata del corolario anterior es el siguiente

Teorema 4.1.1. Sea A un grupo abeliano finito. Entonces, el grupo de torsión de las unidades del grupo-anillo entero $\mathbb{Z}A$ es igual $\pm A$.

Ahora se desea hacer un estudio de los elementos idempotentes. Es evidente que en cualquier anillo con unidad el 0 y el 1 son elementos idempotentes, estos elementos son llamados **idempotentes triviales** de un anillo. Se verá a continuación que los elementos idempotentes e en un grupo-álgebra están fuertemente influenciados por su primer coeficiente $e(1)$.

Teorema 4.1.2. Sea G un grupo finito y K un campo de característica cero. Supóngase que $e \in KG$ y e es idempotente. Entonces:

- $e(1) \in \mathbb{Q}$.
- $0 \leq e(1) \leq 1$.
- $e(1) = 0 \Leftrightarrow e = 0$ y $e(1) = 1 \Leftrightarrow e = 1$.

Demostración. Considérese la representación regular de KG escrita con respecto a la base G de KG. Entonces, por el lema 4.1.1, se tiene que $\operatorname{tr} \rho = |G|e(1)$. Más aún, como $e^2 = e$, $\rho(e)$ satisface el polinomio $X^2 - X = X(X-1)$ y por lo tanto $\rho(e)$ puede ser diagonalizada. Los valores propios de $\rho(e)$ son 0 o 1 ya que $\rho(e)$ es idempotente. Debido a que la traza es la suma de los donde valores propios, se tiene que $\operatorname{tr} \rho(e) = r$, donde r es el número de valores propios iguales a 1 y por lo tanto

también es el rango de $\rho(e)$. Por lo expuesto anteriormente se puede afirmar que $0 \leq e(1) \leq 1$.

Nótese que $e(1) = 0$ si y sólo si el rango de $\rho(e)$ es 0 y eso pasa sólo si $e = 0$. Similarmente $e(1) = 1$ si y sólo si el rango de $\rho(e)$ es $\mid G \mid$, lo cual pasa sólo si $\rho(e)$ es la matriz identidad, es decir, si $e = 1$. □

4.2. Elementos idempotentes

Se ha demostrado en el teorema 4.1.2 que si K es un campo de característica cero y G es un grupo finito, entonces cualquier elemento idempotente $e \in KG$ cumple que $e(1) \in \mathbb{Q}$. Se dará, en esta sección, un resultado análogo a este resultado, donde K tiene característica $p > 0$.

Teorema 4.2.1. Sea K un campo de característica $p > 0$ y sea G cualquier grupo. Supóngase que $e \in KG$ es un idempotente. Entonces $e(1) \in F_p$, donde F_p es el subcampo primo de K.

La demostración de este resultado está fuera del alcance de este trabajo, pero se recomienda al lector consultar (15).

En el teorema 4.1.2 se demostró el teorema anterior cuando la característica del campo es cero con la condición de que el grupo sea finito, pero dicho resultado es válido aún cuando el grupo es infinito, pero su demostración requiere el uso de resultados previos de teoría de números. Para la demostración del siguiente resultado, se sugiere al lector consultar (15).

Teorema 4.2.2. Sea G un grupo cualquiera y K un campo de característica cero. Supóngase que $e = e^2 = \sum e(g)g \in KG$. Entonces:

- $e(1) \in \mathbb{Q}$.
- $0 \leq e(1) \leq 1$.
- $e(1) = 0 \Leftrightarrow e = 0$ y $e(1) = 1 \Leftrightarrow e = 1$.

Supóngase que $e = e^2 \in \mathbb{Z}G$, como $e(1)$ es un entero, se sigue del teorema anterior que $e = 0$ o $e = 1$. Así, se obtiene el siguiente

Corolario 4.2.1. El grupo-anillo entero $\mathbb{Z}G$ sólo contiene idempotentes triviales, para cualquier grupo G.

4.3. Unidades de torsión

Se demostró en el lema 4.1.2 que si G es un grupo finito, $\gamma \in \mathbb{Z}G$ es una unidad de orden finito y $\gamma(1) \neq 0$ entonces $\gamma = \pm 1$. Dicho resultado es válido también cuando G es un grupo infinito.

Teorema 4.3.1. Sea $\gamma = \sum \gamma(g)g \in \mathbb{Z}G$ que satisface $\gamma^n = 1$, para algún entero positivo n. Si $\gamma(1) \neq 0$ entonces $\gamma = \pm 1$.

Demostración. Sea $\mathbb{C}[X]$ el anillo de polinomios con coeficientes en $\mathbb{C}$. Considérese el homomorfismo $\phi\colon \mathbb{C}[X] \to \mathbb{C}[\gamma]$ dada por $X \mapsto \gamma$. El kernel de este homomorfismo es el ideal $\langle f(X) \rangle$ generado por el polinomio minimal $f(X)$ de γ. Entonces $f(X)$ divide a $X^n - 1$ y por lo tanto tiene sus raíces distintas. Así, se tiene

$$\mathbb{C}[\gamma] \simeq \frac{\mathbb{C}[X]}{\langle (X) \rangle} \simeq \mathbb{C} \oplus \mathbb{C} \oplus \cdots \oplus \mathbb{C} \simeq \oplus_i \mathbb{C}e_i,$$

donde los e_i son idempotentes ortogonales primitivos de $\mathbb{C}[\gamma]$. De lo anterior, se puede escribir $\gamma = \sum_i \xi_i e_i$ donde $\xi_i \in \mathbb{C}$, $\xi_i^n = 1$ y $e_i e_j = \delta_{ij} e_j$, con δ_{ij} la función delta de Kronecker.

Calculando el primer coeficiente en ambos lados de la ecuación y usando el teorema 4.2.2 se obtiene

$$\gamma(1) = \sum \xi_i e_i(1) = \sum \xi_i \frac{r_i}{s}, \quad \text{con } r_i, s \in \mathbb{Z}, \quad r_i, s \geq 0.$$

Entonces, $s\gamma(1) = \sum \xi_i r_i$. De igual manera; como $\sum e_i = 1$ se tiene que $1 = \sum \frac{r_i}{s}$, así $\sum r_i = s$. De donde

$$|s\gamma(1)| = \left|\sum \xi_i r_i\right| \leq \sum |\xi||r_i| = \sum |r_i| = s.$$

Como $|s\gamma(1)| \leq s$, se tiene $|\gamma(1)| = 1$ y también $|\sum \xi_i r_i| = \sum |\xi_i||r_i|$. Se sigue que todos los ξ_i son iguales y $\gamma = \sum \xi_1 e_1 = \xi_1 = \gamma(1) \in \mathbb{Z}$. □

Este último resultado tiene bastantes consecuencias útiles. El lector deberá recordar que, como se mostró en la proposición 2.1.4, hay una involución estándar en $\mathbb{Z}G$ dada por

$$\gamma = \sum \gamma(g)g \mapsto \gamma* = \sum \gamma(g)g^{-1},$$

tal que

$$\begin{aligned}
(\gamma^*)^* &= \gamma \\
(\gamma + \mu)^* &= \gamma^* + \mu^* \\
(\gamma\mu)^* &= \mu^*\gamma^* \\
(c\gamma)^* &= c\gamma^*,
\end{aligned}$$

para todo $\gamma, \mu \in \mathbb{Z}G$ y $c \in \mathbb{Z}$. Más aún,

$$(\gamma\gamma^*)(1) = \sum(\gamma(g))^2$$

lo cual implica que $\gamma\gamma^* = 0$ si y sólo si $\gamma = 0$.

Corolario 4.3.1. Supóngase que $\gamma \in \mathbb{Z}G$ tiene la propiedad de conmutar con γ^*. Si γ es una unidad central de orden finito, entonces $\gamma = \pm g_0$ para algún $g_0 \in G$.

Demostración. Por hipótesis $\gamma^n = 1$ para algún entero positivo n y $\gamma\gamma^* = \gamma^*\gamma$, por lo tanto $(\gamma\gamma^*) = 1$. Más aún, $(\gamma\gamma^*)(1) = \sum \gamma(g)^2 \neq 0$. Entonces, por el teorema anterior, $\gamma\gamma^* = 1$. De esta manera, existe un único coeficiente $\gamma(g_0)$ que es distinto de cero. Se concluye entonces que $\gamma = \pm g_0$. □

Corolario 4.3.2. Todas las unidades centrales de orden finito en $\mathbb{Z}G$ son triviales.

Corolario 4.3.3. Si A es un grupo abeliano cualquiera, entonces todas las unidades de torsión de $\mathbb{Z}A$ son triviales.

4.4. Elementos nilpotentes

Ahora se desea clasificar los grupo-álgebras KG de un grupo finito G sobre un anillo K tal que KG no tiene elementos nilpotentes no triviales. Es posible observar que si $\text{car}(K) = p > 0$ y G contiene un elemento g tal que $g^{p^n} = 1$ para algún entero positivo n, entonces $(g-1)^{p^n} = g^{p^n} - 1 = 0$. De esto se sigue el resultado

Proposición 4.4.1. Si K es un campo de característica $p > 0$ y G contiene p-elementos, entonces KG contiene elementos nilpotentes.

A partir de este punto se asumirá que G es finito, $p \geq 0$ y que si $p > 0$ entonces G no tiene p-elementos. Supóngase que KG no contiene elementos nilpotentes a excepción de los triviales y sea $e \in KG$ un idempotente. Entonces, para cada $x \in KG$, el idempotente $\eta = ex(1-e)$ satisface $\eta^2 = 0$ y por lo tanto $ex = exe$. Similarmente si $\eta = (1-e)xe$ entonces $\eta^2 = 0$ y $xe = exe$, con lo que se comprueba que e es central. Ahora para cualquier $g \in G$, el elemento $e = \frac{\hat{g}}{\circ(g)} = \frac{\sum_{i=1}^{\circ(g)} g^i}{\circ(g)}$ es idempotente y por lo tanto es central. Esto significa que el subgrupo $\langle g \rangle$ es normal para cualquier $g \in G$. Se sigue del teorema 1.2.10 que G es abeliano o hamiltoneano.

En el caso que G sea hamiltoniano, $G = K_8 \times E \times A$, donde K_8 es el grupo de cuaterniones de orden ocho, $E^2 = 1$ y A es un grupo abeliano de orden impar. Para obtener más información de este caso es necesario hacer un estudio mas profundo del grupo-álgebra FK_8, donde F es un campo.

Proposición 4.4.2. Sea K un campo de característica $p \geq 0$ y sea G un grupo finito. Si KG no tiene elementos nilpotentes entonces todos los idempotentes de KG son centrales y G es abeliano o hamiltoniano.

En lo que sigue el lector deberá recordar el concepto de números cuaterniones. Los números cuaterniones, con coeficientes racionales, se escriben como sumas directas de espacios vectoriales:

$$H_{\mathbb{Q}} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

con su ya conocida multiplicación, véase (9: 31). Se puede definir formalmente una estructura similar sobre cualquier campo F. Considérese el espacio vectorial

$$H(F) = F \oplus Fi \oplus Fj \oplus Fk$$

y defínase la multiplicación distributivamente con $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$ y $ki = j = -ik$. De esta forma $H(F)$ es un anillo no conmutativo.

Para un elemento $\alpha = a + bi + cj + dk \in H(F)$ se define:

$$\overline{\alpha} = a - bi - cj - dk \ , \ \alpha' = a - bi + cj + dk.$$

Luego de hacer algunos cálculos sencillos se obtiene

Lema 4.4.1. Sea $\alpha \in H(F)$. Entonces:

- $\alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2$.
- $\alpha'\alpha = (a^2 + b^2 - c^2 - d^2) + (2ac + 2bd)j + (2ad - 2bc)k$.

Al escalar $N(\alpha) := \alpha\overline{\alpha}$ se le llama la norma de α.

Proposición 4.4.3. El álgebra de los cuaterniones $H(F)$ tiene divisores de cero si y sólo si la ecuación $X^2 + Y^2 = -1$ tiene solución en F.

Demostración. Supóngase que existen elementos $a, b \in F$ tal que $a^2 + b^2 = -1$. Entonces, para $\alpha = a + bi + j$ se tiene $N(\alpha) = \alpha\overline{\gamma} = 0$; α es divisor de cero en $H(F)$.

Falta demostrar que si $H(F)$ tiene divisores de cero, entonces la ecuación $X^2 + Y^2 = -1$ tiene soluciones en F. Cuando F es de característica dos se tiene $1 + 0 = -1$ entonces se asumirá que $\text{car}(F) \neq 2$. Supóngase que existen elementos $\alpha = a+bi+cj+dk \neq 0$ y $\beta \neq 0 \in H(F)$ tal que $\alpha\beta = 0$. Entonces, $\overline{\alpha}\alpha\beta = N(\alpha)\beta = 0$ de donde $N(\alpha) = a^2 + b^2 + c^2 + d^2 = 0$. Si alguno de los coeficientes de α es cero, se tiene que la ecuación $X^2 + Y^2 = -1$ tiene solución en F. Si, por el contrario, todos los coeficientes de α son distintos de cero se puede considerar $\alpha'\alpha\beta = 0$ y

del lema 4.4.1 se sabe que $\gamma = \alpha'\alpha$ a lo sumo tiene tres coeficientes no nulos y por lo tanto $N(\gamma)\beta = 0$ implica que $X^2 + Y^2 = -1$ tiene solución en F. Por último falta considerar el caso en que $\gamma = 0$, en cuyo caso se tiene, por el lema 4.4.1, que $a^2 + b^2 - c^2 - d^2 = 0$ y de $N(\alpha) = 0$ se sigue que $a^2 + b^2 + c^2 + d^2 = 0$ entonces $a^2 + b^2 = 0$, de donde $\left(\frac{a}{b}\right)^2 + 0 = -1$. □

Este resultado se puede ampliar de la siguiente manera.

Proposición 4.4.4. Las siguientes proposiciones son equivalentes:

- El álgebra de los cuaterniones $H(F)$ no tiene divisores de cero.
- La ecuación $X^2 + Y^2 = -1$ no tiene solución en F.
- $H(F)$ es un anillo de división.

Demostración. Para la demostración de esta proposición solo falta probar que si $H(F)$ no tiene divisores de cero entonces es un anillo de división. Sea $0 \neq \alpha \in H(F)$ entonces $\overline{\alpha}\alpha = N(\alpha) \neq 0$ y por lo tanto $\alpha\left(\frac{\overline{\alpha}}{N(\alpha)}\right) = 1$. □

Teorema 4.4.1. Supóngase que $\text{car}(F) \neq 2$. Entonces el álgebra de los cuaterniones $H(F)$ es un anillo de división o isomorfo a $M_2(F)$, el anillo de matrices de 2×2 sobre el campo F. La última opción sucede únicamente si $X^2 + Y^2 = -1$ tiene solución en F.

Demostración. Se debe demostrar que si $H(F)$ no es un anillo de división entonces es isomorfo a $M_2(F)$. En efecto, supóngase que existen $x, y \in F$ tal que $x^2 + y^2 = -1$.

Considérese la aplicación $\theta\colon H(F) \to M_2(F)$ dada por:

$$\begin{aligned}
\theta(i) &= \begin{pmatrix} x & y \\ y & -x \end{pmatrix} \\
\theta(j) &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
\theta(k) &= \begin{pmatrix} -y & x \\ x & y \end{pmatrix} \\
\theta(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}
\end{aligned}$$

y por extensión lineal en F. Para demostrar que θ es biyectiva, basta demostrar que las cuatro matrices dadas anteriormente son linealmente independientes en F, es decir, si existen $a, b, c, d \in F$ tal que

$$a \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} + b \begin{pmatrix} x & y \\ y & -x \end{pmatrix} + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} -y & x \\ x & y \end{pmatrix} = 0$$

entonces $a = b = c = d = 0$. En efecto, de la ecuación anterior se obtiene

$$\begin{aligned}
a + bx - dy &= 0 \\
by + c + dx &= 0 \\
by - c + dx &= 0 \\
a - bx + dy &= 0
\end{aligned}$$

un sistema de ecuaciones homogéneo en a, b, c, d con determinante $4(x^2 + y^2) \neq 0$, entonces la única solución de dicho sistema es la trivial, de donde $H(F) \simeq M_2(F)$. $\square$

Por lo expuesto en esta sección, el lector podrá intuir que es esencial poder trabajar con álgebras de cuaterniones sobre campos ciclótomicos de la forma $F = \mathbb{Q}(\xi)$, donde ξ es una raíz primitiva de la unidad.

Teorema 4.4.2. Sea $F = \mathbb{Q}(\xi_m)$ un campo ciclotómico, con ξ_m una raíz primitiva de la unidad de orden m, donde m es un entero impar mayor que 1. Entonces, la ecuación $X^2 + Y^2 = -1$ tiene solución en F si y sólo si el orden multiplicativo de 2 módulo m es par.

Para la demostración de dicho teorema y una lectura más profunda de este tema el lector puede consultar (14). Como consecuencia de este teorema se tiene

Lema 4.4.2. Sea $F = \mathbb{Q}(\xi_m)$ como en el teorema anterior. Entonces $H(F)$ tiene divisores de cero si y sólo si el orden multiplicativo de 2 módulo m es par.

Ahora se describe la estructura algebraica del grupo-álgebra $F(K_8)$.

Lema 4.4.3. Sea F un campo de característica distinta de 2. Entonces,

$$FK_8 \simeq 4F \oplus H(F).$$

Demostración. Se escribe K_8 como

$$K_8 = \langle a, b \colon a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} \rangle$$

y como se demostró en el ejercicio 1.2.1, $\overline{K_8} = \frac{K_8}{K_8'}$ es el grupo de Klein de cuatro elementos, se tiene

$$F\overline{K_8} \simeq F \oplus F \oplus F \oplus F.$$

Por otro lado, como existe $\phi\colon FK_8 \to H(F)$ endomorfismo dada por $a \mapsto i$, $b \mapsto j$, se sigue que $H(F)$ es isomorfo a algún sumando simple de FK_8 y contando las dimensiones se obtiene el resultado. □

Ahora se tiene la capacidad de clasificar las grupo-álgebras FG con la propiedad que FG no contenga elementos nilpotentes.

Teorema 4.4.3. Sea F un campo de característica $p > 0$ y sea G un grupo finito. Entonces FG no tiene elementos nilpotentes si y sólo si G es un p'-grupo abeliano.

Demostración. Supóngase que FG no tiene elementos nilpotentes. Entonces de las proposiciones 4.4.1 y 4.4.2 se tiene que G es un p'-grupo y que G es abeliano o hamiltoniano. Supóngase que G es hamiltoneano. Entonces $p \neq 2$. Más aún, siempre se puede resolver $X^2 + Y^2 = -1$ en un campo con p elementos (y por lo tanto también en F). Entonces FK_8 tiene elementos nilpotentes por el teorema 4.4.1 y el lema 4.4.3. Así, G debe ser abeliano. Para el converso basta notar que FG, siendo semisimple y conmutativo, es suma directa de campos. □

Existe una caracterización cuando el campo tiene característica cero, a continuación se presentan los resultados sin su demostración, pero se recomienda al lector consultar (19).

Teorema 4.4.4. Sea G un grupo finito de orden $2^k m$ con $(2, m) = 1$. Entonces $\mathbb{Q}G$ no tiene elementos nilpotentes si y sólo si G es abeliano o hamiltoniano con la propiedad de que el orden de 2 módulo m sea impar.

Teorema 4.4.5. Sea G un grupo nilpotente finitamente generado. El grupo-anillo $\mathbb{Z}G$ no tiene elementos nilpotentes si y sólo si cada subgrupo finito de G es normal y sucede alguna de las siguientes condiciones:

- $T(G)$, el conjunto de los elementos de torsión de G, es un subgrupo abeliano.
- $T(G) = K_8 \times E \times A$, donde E es un 2-grupo elemental abeliano y A es un grupo abeliano de orden impar m tal que el orden multiplicativo de 2 módulo m es impar.

5. UNIDADES DE LOS GRUPO-ANILLOS

5.1. Algunas formas de construir unidades

Sea R un anillo. El conjunto $\mathcal{U}(R) = \{x \in R : \text{ existe } y \in R : xy = yx = 1\}$ es el grupo de unidades de un anillo. En particular, dado un grupo G y un anillo R, $\mathcal{U}(RG)$ denota al grupo de unidades del grupo-anillo RG. Como la función de aumento $\mathcal{E}\colon RG \to R$, dada por $\mathcal{E}\left(\sum a(g)g\right) = \sum a(g)$, es un homomorfismo de anillos, se tiene que $\mathcal{E}(u) \in \mathcal{U}(R)$, para todo $u \in \mathcal{U}(RG)$. Se denotará como $\mathcal{U}_1(RG)$ el subgrupo de unidades de aumento 1 en $\mathcal{U}(RG)$, a saber

$$\mathcal{U}_1(RG) = \{u \in \mathcal{U}(RG) : \mathcal{E}(u) = 1\}.$$

Para una unidad u del grupo-anillo integral $\mathbb{Z}G$ se tiene que $\mathcal{E}(u) = \pm 1$, entonces es claro que

$$\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G).$$

De la misma manera, para un anillo R arbitrario se tiene que

$$\mathcal{U}(RG) = \mathcal{U}(R) \times \mathcal{U}_1(RG).$$

No se conocen muchas formas para construir unidades. La mayoría de las construcciones conocidas son antiguas y elementales. A lo largo de este capítulo, se mostrará y describirá algunas de estas construcciones, donde se trabajará principalmente con grupo-álgebras KG sobre un campo K y con el grupo-anillo entero $\mathbb{Z}G$.

Ejemplo 5.1.1 (Unidades Triviales). Un elemento de la forma rg, donde $r \in \mathcal{U}(R)$ y $g \in G$, tiene inverso $r^{-1}g^{-1}$. Los elementos de esta forma son llamados **unidades triviales** de RG. De esta manera, por ejemplo, los elementos $\pm g$, $g \in G$ son las unidades triviales del grupo-anillo entero $\mathbb{Z}G$. Si K es un campo, entonces las unidades triviales de KG son los elementos de la forma $kg, k \in K, k \neq 0, g \in G$. Hablando de manera general, los grupo-anillos contienen unidades no triviales.

Ejemplo 5.1.2. Sea $\eta \in R$ tal que $\eta^2 = 0$, entonces se tiene $(1+\eta)(1-\eta) = 1$. De este hecho, tanto $1+\eta$ como $1-\eta$ son unidades de R. De la misma manera, si $\eta \in R$ es tal que $\eta^k = 0$ para algún entero positivo k, entonces se tiene que

$$(1-\eta)(1+\eta+\eta^2+\cdots+\eta^{k-1}) = 1-\eta^k = 1,$$

$$(1+\eta)(1-\eta+\eta^2+\cdots\pm\eta^{k-1}) = 1\pm\eta^k = 1.$$

Así, $1 \pm \eta$ son unidades de R. Estas unidades son llamadas **unidades unipotentes** de R. En un grupo-álgebra KG sobre un campo de característica $p > 0$ se puede iniciar la búsqueda de unidades unipotentes investigando a los elementos nilpotentes. Si $g \in G$ es de orden p^n, entonces $(1-g)^{p^n} = 0$, de esta forma se demuestra que $\mu = 1 - g$ es nilpotente.

En este caso $1 - \eta = g$ es trivial, pero $1 + \eta = 2 - g$ es no trivial, a menos que $\mathrm{car}(K) = 2$. Nótese que $g - g^2 = g(1-g)$ también es nilpotente, entonces $1 + g - g^2$ es una unidad no trivial si $g^2 \neq 1$.

En el teorema 4.4.4 y 4.4.3 se clasificaron todos los grupos finitos tal que el grupo-álgebra KG no tiene elementos nilpotentes. Se vera entonces que las grupo-álgebras de grupos finitos casi siempre tienen unidades no triviales.

Proposición 5.1.1. Sea G un grupo tal que no es libre de elementos de torsión y K un campo de característica $p \geq 0$. Entonces KG sólo tiene unidades triviales si y sólo si se cumple alguna de las siguientes condiciones

- $K = F_2$ y $G = C_2$ o C_3.
- $K = F_3$ y $G = C_2$.

Demostración. Supóngase que todas las unidades de KG son triviales. Considérese $N = \langle a \rangle$ subgrupo finito de G de orden n. Si no existe $b \in G$ que normalize a N, entonces $\eta = (a-1)(1 + a + \cdots + a^{n-1})$ es no nulo, pero $\eta^2 = (a-1)b(1 + a + \cdots + a^{n-1})(a-1)b(1 + a + \cdots + a^{n-1}) = 0$, de esa cuenta, $\eta + 1$ es unidad no trivial de KG, proposición que contradice la hipótesis, de donde se concluye que todo subgrupo finito de G es normal.

Sea H un subgrupo finito propio de G y considérese $\hat{H} = \sum_{h \in H} h$. Es fácil notar que $\hat{H}$ es central y $\hat{H}^2 = |H|\hat{H}$. Tómese $g \in G - H$ fijo. Si $|H| = 0$ en K entonces $\hat{H}^2 = 0$ y $g + \hat{H}$ es una unidad no trivial de KG con inverso $g^{-}1(1 - g^{-}1\hat{H})$. Si $|H| \neq 0$ en K, entonces $e = \frac{1}{H}\hat{H}$ es idempotente central y $e + g(1-e)$ es una unidad no trivial con inverso $e + g^{-}1(1-e)$. En ambos casos se llega a una contradicción, por lo que se concluye que $G = \langle a \rangle$ es de orden primo.

Si $\text{car}(K) = p$ entonces $1 + c\hat{G}, c \in K$ es una unidad no trivial, a menos que $p = 2$ y $K = F_2$.

Por otro lado, si $\text{car}(K) \neq p$ entonces, del hecho que $K\langle a \rangle$ es semisimple y conmutativo, $K\langle a \rangle$ es suma directa de campos, a saber

$$K\langle a \rangle \simeq K \oplus K(\zeta) \oplus K(\theta) \oplus + \cdots$$

donde $\zeta, \theta, \dots$ son raíces de la unidad de orden p. Bajo este isomorfismo, se tiene $a \mapsto (1, \zeta, \theta, \dots)$, por lo que una unidad trivial $ka^i, 0 \neq k \in K$ tiene imagen $(k, k\zeta^i, k\theta^i, \dots)$. Nótese que si la descomposición de $K\langle a \rangle$ tuviera más de dos componentes se tendrían unidades de la forma $(1, \zeta, 1, \dots)$ que no corresponden a unidades triviales de $K\langle a \rangle$. Entonces se debe tener

$$K\langle a \rangle \simeq K \oplus E,\ E = K(\zeta),\ |K| = q,\ |E| = q^r,\ \circ(a) = p.$$

Al contar el número de unidades y de elementos se tiene

$$p(q-1) = (q-1)(q^r - 1), p^q = q \cdot q^r.$$

De la condición anterior, se tiene que $q^p = q(p-1)$ y $q^{p-1} = p + 1$, lo cual sólo es posible para $q = 2$ y $p = 3$ o $q = 3$ y $p = 2$. Con lo que se demuestra que $K = F_2$ y $G = C_3$ o $K = F_3$ y $G = C_2$.

Para el converso, una simple inspección demuestra que $F_2C_2, F_3C_3 \simeq F_2 \oplus F_4$ y $F_3C_2 \simeq F_3 \oplus F_3$ tiene dos, tres y cuatro unidades triviales, lo cual coincide con el número de unidades triviales en cada caso. □

Se ha llegado al punto en el que se desea clasificar los grupos de torsión G de tal forma que el grupo-anillo entero $\mathbb{Z}G$ tenga solo unidades triviales.

Ejemplo 5.1.3. En el ejemplo anterior se dio la construcción de unidades unipotentes a partir de elementos nilpotentes. Ahora se verán elementos nilpotentes en particular que también poseen esa característica.

Supóngase que R tiene divisores de cero, es decir, se pueden encontrar elementos $x, y \in R$ no nulos tales que $xy = 0$. Si t es algún otro elemento de R entonces $\eta = ytx$

es no nulo tal que $\eta^2 = (ytx)(ytx) = ytxytx = 0$, así $1+\eta$ es una unidad. En el caso especial cuando $R = \mathbb{Z}G$ es un grupo-anillo entero, una manera sencilla de obtener un divisor de cero es considerar un elemento $a \in G$ de orden finito $n > 1$, entonces $a-1$ es divisor de cero, ya que $(a-1)(1+a+\cdot+a^{n-1}) = 0$. De esa manera, tomando cualquier elemento $b \in G$, se puede construir una unidad de la forma

$$\mu_{a,b} = 1 + (a-1)b\hat{a}, \text{ con } \hat{a} = 1 + a + \cdots + a^{n-1}. \tag{5.1}$$

Definición 5.1.1. Sean $a \in G$ un elemento de orden finito n y b cualquier otro elemento de G. La unidad $\mu_{a,b}$ dada por la ecuación (5.1) es llamada unidad bicíclica del grupo-anillo $\mathbb{Z}G$. Se denotará por $\mathcal{B}_2$ el subgrupo de $\mathcal{U}(\mathbb{Z}G)$ generado por todas las unidades bicíclicas de $\mathbb{Z}G$.

Es claro que si $a, b \in G$ conmutan, entonces $\mu_{a,b} = 1$. Se desea saber para que casos $\mu_{a,b}$ es una unidad trivial de $\mathbb{Z}G$.

Proposición 5.1.2. Sean g, h elementos de un grupo G con $\circ(g) = n < \infty$. Entonces, la unidad bicíclica $\mu_{g,h}$ es trivial si y sólo si h normaliza a $\langle g \rangle$, en cuyo caso $\mu_{g,h} = 1$.

Demostración. Supóngase que h normaliza a $\langle g \rangle$, entonces $h^{-1}gh = g^j$, para algún entero positivo j. De esto se tiene $gh = g^j h$ y como $g^j\hat{g} = \hat{g}$, se tiene $gh\hat{g} = h\hat{g}$. Haciendo los cálculos $\mu_{g,h} = 1 + (g-1)h\hat{g} = 1 + gh\hat{g} - h\hat{g} = 1$.

Para el converso, supóngase que $\mu_{g,h}$ es trivial, entonces, del hecho que $\mathcal{E}(\mu_{g,h}) = 1$, existe $x \in G$ tal que $\mu_{g,h} = x$. De esta cuenta, se tiene

$$1 + (1-g)h\hat{g} = x$$

y de esta ecuación se infiere que

$$1 + h(1 + g + g^2 + \cdots + g^{n-1}) = x + gh(1 + g + g^2 + \cdots + g^{n-1}).$$

Si $x = 1$ se tiene que $h = ghg^i$ para algún entero positivo i. Si $x \neq 1$ entonces $h \notin \langle g \rangle$, pero 1 aparece en el lado izquierdo de la ecuación, por lo que también debe aparecer en el lado derecho, esto es, existe k entero positivo tal que $ghg^k = 1$ entonces $h = g^{-1}g^{-k} = g^{-(k+1)}$ y por lo tanto $h \in \langle g \rangle$, lo cual es una contradicción. □

Como consecuencia inmediata se tiene el resultado:

Proposición 5.1.3. Sea G un grupo finito. El grupo $\mathcal{B}_2$ es trivial si y sólo si todo subgrupo de G es normal.

Proposición 5.1.4. Toda unidad bicíclica $\mu_{g,h} \neq 1$ de $\mathbb{Z}G$ es orden infinito.

Demostración. Dado $\mu_{g,h} = 1 + (g-1)h\hat{g}$ se tiene

$$\mu_{g,h}^s = (1 + (g-1)h\hat{g}^s = 1 + s(g-1)h\hat{g})$$

entonces $\mu_{g,h}^s = 1$ si y sólo si $(g-1)h\hat{g} = 0$, lo cual sucede solo si $\mu_{g,h} = 1$. □

Se desea explorar que pasa cuando se trabaja con grupos conmutativos finitos. El lector deberá recordar la definición de la función totiente de Euler ϕ.

Definición 5.1.2. Sea g un elemento de orden n en un grupo G. Una unidad cíclica de Bass[1] es un elemento del grupo-anillo $\mathbb{Z}G$ de la forma:

$$\mu_i = (1 + g + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi n}}{n}\hat{g}$$

donde i es un entero tal que $1 < i < n - 1$ y $(i, n) = 1$.

Como es natural, se debe mostrar que μ_i es una unidad. Es claro que, para $g \in G, \mu_i$ pertenece al grupo-anillo $\mathbb{Q}\langle g\rangle$. Se vió en el ejemplo 2.4.3 que $\mathbb{Q}\langle g\rangle \simeq \oplus_{d|n}\mathbb{Q}(\zeta_d)$ donde ζ_d es una raíz primitiva de la unidad de orden d. Más aún, bajo este isomorfismo, la proyección de g en cada componente es la respectiva raíz de la unidad, así que un elemento de la forma $(1 + g + \cdots + g^{i-1})$ proyecta, en cada componente, un elemento de la forma:

$$1 + \zeta_d + \cdots + \zeta_d^{i-1} \in \mathbb{Z}[\zeta_n].$$

Si $\zeta_d \neq 1$, entonces el elemento ζ_d es invertible en $\mathbb{Z}[\zeta_d]$ y es llamada unidad ciclotómica. De lo anterior, el inverso de α_d es

$$\alpha_d^{-1} = \frac{\zeta_d - 1}{\zeta_d^i - 1} = \frac{\zeta_d^{ik}}{\zeta_d^i - 1} = 1 + \zeta_d^i + \cdots + \zeta_d^{i(k-1)},$$

donde k es cualquier entero tal que $ik \equiv 1 \pmod{n}$. Es claro que $\alpha_d^{-1} \in \mathbb{Z}[\zeta_d] \in \mathbb{Z}[\zeta_n]$.

Para la primer componente las cosas cambian, ya que la proyección es precisamente el valor i, que no es invertible. Ahora bien, como $(i, n) = 1$ y aplicando el teorema de Euler, se tiene que $i^{\phi(n)} = 1 + tn$ para algún $t \in \mathbb{Z}$. Considérese el elemento

$$(1 + g + \cdots + g^{i-1})^{\phi(n)} - t\hat{g}$$

[1]Hyman Bass (5 de octubre, 1932) es un matemático estadounidense conocido por sus trabajos en álgebra y en matemática educativa.

y nótese que $\hat{g}$ es cero en cualquier componente $\mathbb{Q}(\zeta_d)$, con $\zeta_d \neq 1$, por lo que la proyección de μ_i e cada una de estas componentes es una unidad. Ahora, analizando el caso de la primera componente de nuevo, se puede observar que dicha proyección es $i^{\phi(n)} - tn = 1$, con lo cual se prueba que la proyección sobre dicha componente también es unidad. Más aún, se obtuvo que $-t = \frac{1-i^{\phi(n)}}{n}$, por lo que el elemento $(1 + g + \cdots + g^{i-1})^{\phi(n)} - t\hat{g})$ considerado anteriormente es precisamente μ_i.

De esta forma se ha demostrado que la proyección de μ_i en todas las componente de $\oplus_{d|n}\mathbb{Z}[\zeta_d]$ es una unidad. Si se denota por R la preimagen de este anillo bajo el isomorfismo, se tiene que μ_i es unidad en R.

Proposición 5.1.5. Sea g un elemento de orden finito en un grupo G. Entonces, el elemento

$$\mu_i = (1 + g + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\hat{g},$$

donde i es un entero tal que $1 < i < n - 1$ y $(i, n) = 1$, es invertible y su inversa es

$$\mu_i^{-1} = (1 + g^i + \cdots + g^{i(k-1)})^{\phi(n)} + \frac{1 - k^{\phi(n)}}{n}\hat{g},$$

donde k es cualquier entero tal que $ik \equiv 1 \pmod{n}$.

Proposición 5.1.6. Sea g un elemento de orden finito n en un grupo G y sea l un entero tal que $1 < l < n - 1$ y $(l, n) = 1$. Entonces, la unidad cíclica de Bass

$$\mu_l = (1 + g + \cdots + g^{l-1})^{\phi(n)} + \frac{1 - l^{\phi(n)}}{n}\hat{g}$$

es de orden infinito.

Demostración. Se sabe que

$$\mathbb{Q}\langle g\rangle \simeq \mathbb{Q} \oplus \cdot \oplus \mathbb{Q}(\zeta^d) \oplus \cdots \oplus \mathbb{Q}(\zeta),$$

donde ζ es una raíz primitiva de la unidad de orden n y d representa a los divisores de n. Más aún, en el isomorfismo se tiene

$$g \mapsto (1, \ldots, \zeta^d, \ldots, \zeta).$$

Sea μ_l como en la proposición. Se requieren demostrar que la proyección $\mu_l(\zeta)$ en la última componente es de orden infinito. Primero nótese que dicha proyección es de la forma $\mu_l(\zeta) = (1 + \zeta + \cdots + \zeta^{l-1})^{\phi(n)}$, de esa cuenta, si $(1 + \cdots + \zeta^{l-1})^{\phi(n)}$ fuera de orden finito, entonces se tendría que $(1 + \cdots + \zeta^{l-1})$ sería de orden finito. Como $\{\pm\zeta^t \colon 0 \leq t \leq n-1\}$ son todas raíces de la unidad de $\mathbb{Q}(\zeta)$, se tendría que $(1+\cdots+\zeta^{l-1}) = \pm\zeta^s$ para algún entero positivo s. Multiplicando la última ecuación por $(1-\zeta)$ se observa que $1-\zeta^l = \pm\zeta^s(1-\zeta)$. Así, tomando valores absolutos, se obtiene $\mid 1-\zeta^l \mid = \mid 1-\zeta \mid$. Escribiendo $\zeta = \cos\theta + i\sin\theta$, por el teorema de DeMoivre, se tiene $\zeta^l = \cos(l\theta) + i\sin(l\theta)$, de donde se deduce que $\mid 1-\zeta \mid^2 = \mid 1-(\cos\theta+i\sin\theta) \mid^2 = 2(1-\cos\theta)$ y $\mid 1-\zeta^l \mid^2 = \mid 1-(\cos(l\theta)+i\sin(l\theta) \mid^2 = 2(1-\cos(l\theta))$, de esa cuenta, $\cos\theta = \cos(l\theta)$, lo cual implica que $l\theta = \theta$ o $l\theta = 2\pi - \theta$, por lo tanto $\zeta^l = \zeta$ o $\zeta^l = \zeta^{-1}$. En cualquiera de los dos casos se obtiene una contradicción, lo cual demuestra que μ_l tiene orden infinito. □

Nota 5.1.1. En la definición de unidad cíclica de Bass μ_l, l está en el rango $1 < l < n-1$. Si se toma $l = n-1$ se tiene

$$\mu_l = (1 + g + \cdots + g^{n-2})^{\phi(n)} + \frac{1 - l\phi(n)}{n}\hat{g}.$$

La proyección de μ_l sobre cualquier componente es $(-g^{-1})^{\phi(n)}$ y $\mu_l = (-g^{-1})^{\phi(n)}$ es

trivial. Así mismo, de la restricción $1 < l < n-1$, se tiene que $n \geq 5$ para que μ_l esté definida.

Nota 5.1.2. Lo proposición anterior demuestra que μ_l es una unidad no trivial.

Ejemplo 5.1.4. Ahora considérese $g \in G$ un elemento de orden impar, $n \neq 1$ y el elemento

$$\mu = 1 - g + g^2 - \cdots + g^{c-1},$$

donde $(c, 2n) = 1$. Entonces la proyección en cada componente de $\mathbb{Q}\langle g \rangle$ es una unidad ciclótomica y como la proyección en la primera componente es 1, se tiene que μ es una unidad en $\mathbb{Z}\langle g \rangle$. Esta unidad es llamada una **unidad alternante**.

5.2. Unidades triviales

En el capítulo anterior se demostró que si G es un grupo abeliano, entonces todas las unidades de torsión de $\mathbb{Z}G$ son triviales. Ahora en esta sección se hará un breve estudio de los grupos G que hacen que todas las unidades de $\mathbb{Z}G$ sean triviales.

El lector deberá recordar que una unidad trivial de $\mathbb{Z}G$ es un elemento de la forma $\pm g$, $g \in G$. Así, si todas las unidades de $\mathbb{Z}G$ son triviales, entonces se tiene que $\mathcal{U}(\mathbb{Z}\mathbb{G}) = \pm G$. Esta condición se traduce, en términos de unidades normalizadas, como $\mathcal{U}_1(\mathbb{Z}G) = G$.

Lema 5.2.1. Sea G un grupo de torsión tal que $\mathcal{U}_1(\mathbb{Z}G) = G$. Entonces todo subgrupo de G es normal.

Demostración. Para demostrar este lema, es suficiente demostrar que todo subgrupo cíclico de G es normal. De esta forma, supóngase que existe un subgrupo cíclico $\langle g \rangle$ de G que no es normal, es decir, existe $h \in G$, tal que $h^{-1}gh \notin \langle g \rangle$ y se sigue de la proposición 5.1.2 que la unidad bicíclica $u = 1 + (1 - g)h\hat{g}$ es no trivial. □

Es sabido que si G es un grupo abeliano, entonces sus subgrupos son normales. Además, se recuerda al lector que todo grupo de torsión no abeliano G tal que todos sus subgrupos son normales es llamado un grupo hamiltoniano, este grupo tiene la forma

$$G = K_8 \times E \times A,$$

donde E es un 2-grupo abeliano elemental, es decir, todo elemento $a \neq 1$ en E es de orden 2, A es un grupo abeliano donde todos sus elementos son de orden impar y K_8 es el grupo de los cuaterniones de orden ocho:

$$K_8 = \langle a, b \colon a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} \rangle.$$

Proposición 5.2.1. Sea G un grupo de torsión tal que $\mathcal{U}_1(\mathbb{Z}G) = G$. Entonces G es abeliano de exponente igual a $1, 2, 3, 4$ o 6, o bien, G es un 2-grupo hamiltoniano.

Demostración. Del lema anterior se sigue que G es abeliano o bien G es hamiltoniano. Primero supóngase que G es abeliano. Si su exponente es diferente de $1, 2, 3, 4$ ó 6 entonces G contiene un elemento de orden n, con $n = 5$ o $n > 6$. En ambos casos, se tiene que $\phi(n) > 2$ (ya que $\phi(n) \equiv \quad (\text{mód } 2)$) y la proposición 5.1.6 demuestra que G contiene una unidad cíclica de Bass que es no trivial.

De manera análoga, si G es hamiltoniano pero no es un 2-grupo, entonces G contiene un elemento $x \in A$ de orden $p > 2$. Entonces, el elemento $g = ax$ tiene

orden $n = 4p$ y, de nuevo, $\phi(n) > 2$, por lo que G contiene una unidad cíclica de Bass. $\square$

La condición dada en la proposición anterior también es suficiente, pero su demostración no es tan trivial. Se demostrará este hecho a través de una serie de lemas.

Lema 5.2.2. Sea G un grupo tal que las unidades de $\mathbb{Z}G$ son triviales y C_2 un grupo cíclico de orden 2. Entonces las unidades de $\mathbb{Z}(G \times C_2)$ también son triviales.

Demostración. Sea $C_2 = \langle a : a^2 = 1 \rangle$. Como $\mathbb{Z}(G \times C_2) \simeq (\mathbb{Z}G)C_2$, un elemento $u \in \mathbb{Z}(G \times C_2)$ puede ser escrito de la forma $u = \alpha + \beta a$ donde $\alpha, \beta \in \mathbb{Z}G$. Debido a que u es unidad, tiene que existir otro elemento $u^{-1} = \gamma + \delta a$ tal que

$$(\alpha + \beta a)(\gamma + \delta a) = (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)a = 1.$$

Entonces

$$\begin{aligned} \alpha\gamma + \beta\delta &= 1 \\ \alpha\delta + \beta\gamma &= 0. \end{aligned}$$

Así, se tiene

$$(\alpha + \beta)(\gamma + \delta) = \alpha\gamma + \beta\delta + \alpha\delta + \beta\gamma = 1$$

$$(\alpha - \beta)(\gamma - \delta) = \alpha\gamma + \beta\delta - (\alpha\delta + \beta\gamma) = 1$$

lo cual demuestra que $(\alpha + \beta)$ y $(\alpha - \beta)$ son unidades en $\mathbb{Z}G$ y por lo tanto son

unidades triviales. Entonces, existen $g_1, g_2 \in G$ tales que

$$\alpha + \beta = \pm g_1, \quad \alpha - \beta = \pm g_2.$$

De estas últimas igualdades, se sigue que $\alpha = \frac{1}{2}(\pm g_1 \pm g_2)$, pero como los coeficientes de α deben ser enteros, tiene que ser cierto que $g_1 = \pm g_2$. De esta manera, se tienen dos opciones:

$$\alpha + \beta = \alpha - \beta = \pm g_1 \quad \text{o} \quad \alpha + \beta = -(\alpha - \beta) = \pm g_1.$$

Para el primer caso, se obtiene $\alpha = \pm g_1$ y $\beta = 0$, mientras que para el segundo caso $\alpha = 0$ y $\beta = \pm g_1$. En ambos casos se obtiene que u es trivial. □

Lema 5.2.3. Las unidades del grupo-anillo $\mathbb{Z}K_8$ son triviales.

Demostración. En este punto, vale la pena recordar que

$$K_8 = \{1, a, b, ab, a^2, a^3, a^2b, ab^3\}.$$

Entonces, todo elemento $\alpha \in \mathbb{Z}K_8$ es de la forma

$$\alpha = x_0 + x_1a + x_2b + x_3ab + y_0a^2 + y_1a^3 + y_2a^2b + y_3ab^3.$$

Ahora, téngase en consideración al anillo de cuaterniones enteros, esto es, el anillo

$$H = \{m_0 + m_1i + m_2j + m_3k \colon m_0, m_1, m_2, m_3 \in \mathbb{Z}\}.$$

Es fácil ver que las únicas unidades de H son $\pm 1, \pm i, \pm j, \pm k$. Ahora considérese el

epimorfismo $\phi\colon \mathbb{Z}K_8 \to H$ dado por

$$\alpha \mapsto (x_0 - y_0) + (x_1 - y_1)i + (x_2 - y_2)j + (x_3 - y_3)k.$$

Por ser un morfismo, si α es unidad en $\mathbb{Z}K_8$ entonces $\phi(\alpha)$ es unidad de H; por lo tanto, para algún índice r, $\quad 0 \leq r \leq 3$, se debe cumplir que

$$\begin{aligned} x_r - y_r &= 1 \\ x_s - y_s &= 0 \text{ si } s \neq r. \end{aligned}$$

Por otro lado, es fácil notar que a^2 es central y que $\frac{K_8}{\langle a^2 \rangle} \simeq C_2 \times C_2$. Si se denota como $\bar{g}$ la clase de un elemento $g \in K_8$ bajo el cociente y como $\psi\colon \mathbb{Z}K_8 \to \mathbb{Z}\left(\dfrac{K_8}{\langle a^2 \rangle}\right)$, la extensión de la proyección canónica $K_8 \to \left(\dfrac{K_8}{\langle a^2 \rangle}\right)$ hacia $\mathbb{Z}K_8$, se tiene que

$$\psi(\alpha) = (x_0 + y_0) + (x_1 + y_1)\bar{a} + (x_2 + y_2)\bar{b} + (x_3 + y_3)\bar{a}\bar{b}.$$

Se sigue del lema anterior que las unidades de $\mathbb{Z}(C_2 \times C_2)$ son triviales. Así, para algún índice h, $0 \leq h \leq 3$, se tiene

$$\begin{aligned} x_h + y_h &= \pm 1 \\ x_k + y_k &= 0, \text{ si } h \neq k. \end{aligned}$$

Es fácil notar que $r = h$ y

$$x_r = \mp 1, y_r = 0, x_s = y_s = 0, \text{ si } s \neq r,$$

o

$$x_r = 0, y_r = \pm 1, x_s = y_s = 0 \text{ si } s \neq r.$$

En ambos casos se llega a que α es unidad trivial de $\mathbb{Z}K_8$. □

Lema 5.2.4. Sea ζ una raíz primitiva de la unida de orden 3 ó 4. Entonces, las unidades del anillo ciclotómico $\mathbb{Z}[\zeta]$ son simplemente $\{\pm\zeta^i\}$.

Demostración. Se considerará primero el caso en que ζ es una raíz cúbica de la unidad. Recordemos que el polinomio minimal de ζ es $X^2 + X + 1$, así que todo elemento $\alpha \in \mathbb{Z}[\zeta]$ es de la forma $\alpha = a + b\zeta$, con $a, b \in \mathbb{Z}$. Supóngase que α es una unidad de $\mathbb{Z}[\zeta]$. Dado que la aplicación $f\colon \mathbb{Z}[\zeta] \to \mathbb{Z}[\zeta]$ dada por $f(x + y) = x + y\zeta^2$ es un automorfismo, se sigue que $\alpha' = a + b\zeta^2$ es también una unidad y así

$$\alpha\alpha' = (a + b\zeta)(a + b\zeta^2) = a^2 + b^2 + ab(\zeta + \zeta^2) = a^2 + b^2 - ab$$

es también una unidad, pero $\alpha\alpha' \in \mathbb{Z}$, así que $a^2 + b^2 - ab = \pm 1$. Supóngase, sin pérdida de generalidad, que $\mid a \mid \geq \mid b \mid$. Si $b \neq 0$, se sigue $a^2 + b^2 > ab \pm 1$, lo cual es una contradicción.

Si $b = 0$, entonces $\alpha = a \in \mathbb{Z}$ es una unidad y $\alpha = \pm 1$. Si $b = 1$, se tiene que $a^2 + 1 = a \pm 1$ lo cual implica que $a^2 = a$ o $a^2 - a + 2 = 0$. Para el primer caso se tiene $a = 0$ o $a = 1$ y para el segundo caso no se tiene solución en los enteros. Si $a = 0$ se tiene $\alpha = b\zeta$ y como $\mid \alpha \mid = 1$, se sigue que $\alpha = \pm\zeta$. Finalmente, si $a = b = 1$ se tiene que $\alpha = 1 + \zeta = -\zeta^2$. El caso en que ζ es raíz primitiva de la unidad de orden cuatro es aún más fácil, ya que $\zeta = i$ y los elementos en $\mathbb{Z}[i]$ son de la forma $\alpha = a + bi, a, b \in \mathbb{Z}$, es decir que $\alpha \in \mathbb{C}$ y por lo tanto $a = \pm 1$ y $b = 0$ o $a = 0$ y $b = \pm 1$ □

Teorema 5.2.1 (Higman). Sea G un grupo de torsión. Entonces, todas las unidades de $\mathbb{Z}G$ son triviales si y sólo si G es un grupo abeliano de exponente igual a $1, 2, 3, 4$ o 6 o G es un 2-grupo hamiltoniano.

Demostración. La condición necesaria ya se ha demostrado. Para probar la condición suficiente, considérese el caso en que G es un grupo abeliano de exponente igual a $1, 2, 3, 4$ o 6 y supóngase que G es finito. En este caso, el teorema 2.4.1 asegura que

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

donde ζ_d denota a las raíces primitivas de la unidad de orden d y $a_d = \dfrac{\eta_d}{\mid K(\zeta_d : K \mid)}$. En esta fórmula, η_d denota el número de elementos de orden d en G. En otra palabras, solamente las raíces de la unidad cuyos órdenes son iguales a los órdenes de los elementos en G aparecen en la descomposición. Sea R la preimagen, bajo el isomorfismo, del orden

$$M = \oplus_{d|n} a_d \mathbb{Z}[\zeta_d].$$

Nótese que si G es como se propuso al inicio, entonces G es de la forma

$$\begin{aligned}
G &\simeq C_2 \times \cdots \times C_2, \\
G &\simeq C_3 \times \cdots \times C_3, \\
G &\simeq C_4 \times \cdots \times C_4, \\
G &\simeq C_2 \times \cdots \times C_2 \times C_3 \times \cdots \times C_3, \\
G &\simeq C_2 \times \cdots \times C_2 \times C_4 \times \cdots \times C_4.
\end{aligned}$$

Sin embargo, por el lema 5.2.2, se puede asumir que G es del segundo o del tercer tipo. En ambos casos, se sigue del lema 5.2.4 que todas las unidades de R son triviales y

por lo tanto de orden finito. Como $\mathcal{U}(\mathbb{Z}G)$ está contenido en R, también sus unidades son de orden finito, como G es abeliano, se sigue que estas deben ser triviales. En el caso en que G es un 2-grupo hamiltoniano la conclusión se sigue directamente de los lemas 5.2.2 y 5.2.4 $\square$

6. APLICACIONES

En este capítulo se darán los conceptos básicos de teoría de códigos. Se empezará dando una descripción del sistema de comunicación como lo propuso Claude E. Shannon[1] en 1948. En esta parte también se introducirán todos los conceptos básicos del sistema de comunicación como canal, codificador, decodificador y código. Una vez la teoría básica está dada se hace un breve estudio de los códigos lineales, para terminar este capítulo con una clase de códigos en particular, los cíclicos.

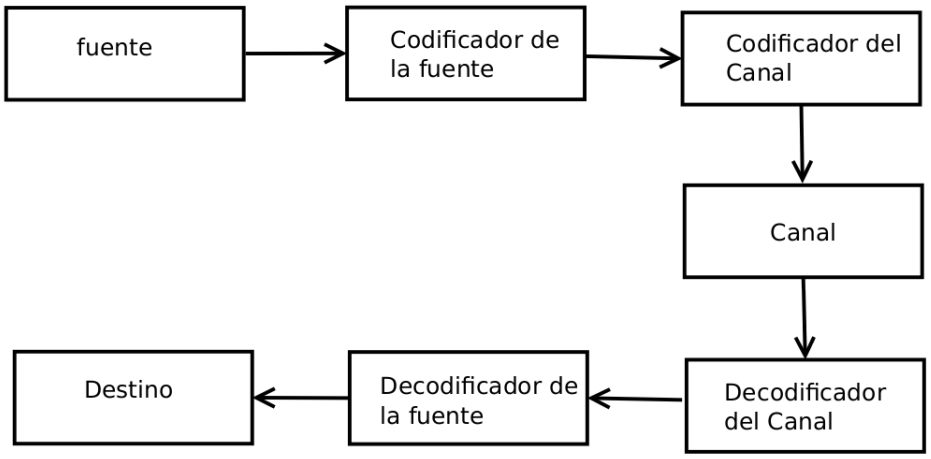
6.1. Sistema de comunicación

La figura 7 muestra un sistema de comunicación de una **fuente** a un **destino** mediante un **canal**. La comunicación puede ser en el dominio del espacio (es decir, de un punto a otro) o en el dominio del tiempo (al guardar información en algún punto en el tiempo para ser recuperada posteriormente). La codificación de la fuente tiene doble propósito. Primero, servir como traductor entre la salida de la fuente y la entrada al canal. Por ejemplo, si la información transmitida de la fuente al destino está en señal análoga y el canal espera recibir señal digital, se necesitará una conversión de análoga a digital en la fase de codificación y un convertidor de señal digital a análoga en la fase de decodificación.

Como segunda función se podría requerir que el codificador de la fuente comprima la salida de la fuente para economizar en la longitud de la transmisión, eso significa que en el otro extremo, el decodificador de la fuente necesitará descomprimir

[1]Claude Elwood Shannon (Míchigan, 30 de abril de 1916 – 24 de febrero de 2001) fue un ingeniero electrónico y matemático estadounidense, recordado como el padre de la teoría de la información.

Figura 7: Sistema de comunicación propuesto por Shannon



Fuente: Elaboración propia con software Dia.

la señal.

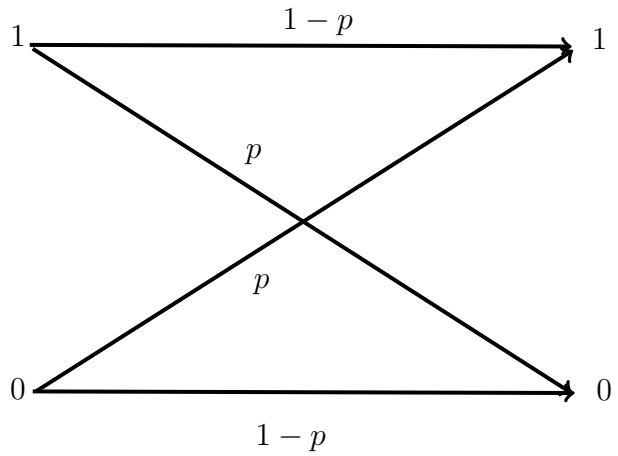
Algunas aplicaciones necesitan que el decodificador restaure la información para que sea idéntica a la original, en cuyo caso se dice que la compresión es **sin pérdidas**.

Otras aplicaciones, como la mayoría de transmisiones de audio e imágenes, permiten una diferencia controlada o distorsión entre la información original y la restaurada, así que esta posibilidad es usada para lograr mayor compresión. En este caso se dice que la compresión es **con pérdidas.**

Los canales no son perfectos debido a limitaciones físicas y de ingeniería, es decir, su salida puede diferir de su entrada debido al ruido o a defectos de fabricación.

Más aún, en algunos casos el diseño requiere que el formato de la información de salida del canal difiera del formato de entrada. Además hay aplicaciones tales como

Figura 8: Canal binario simétrico

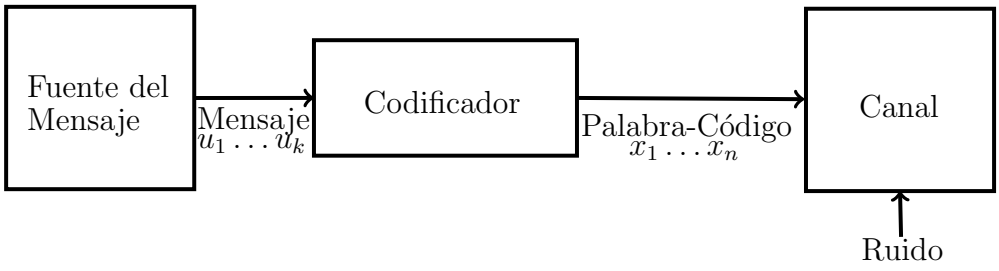


Fuente: Elaboración propia con software Dia.

los medios de almacenamiento masivo magnético y óptico, donde no se permiten ciertos patrones en el flujo de bits a transmitir. Dado esto, el rol principal del codificador del canal, es superar estas limitaciones y hacer el canal tan transparente como sea posible, tanto desde el punto de vista de la fuente como del destino.

Es así como entran a participar los códigos. Los códigos fueron inventados para corregir errores en los canales de comunicación debido al ruido. Por ejemplo, supóngase que hay un cable telegráfico desde Ciudad de Guatemala hasta Ciudad de Panamá, mediante el cual se pueden transmitir unos y ceros. Usualmente cuando un cero es enviado se recibe un cero, pero ocasionalmente un cero puede ser recibido como un uno o un uno como un cero. Supóngase que en promedio, 1 de cada 100 símbolos se recibe de forma errónea, es decir, por cada símbolo hay una probabilidad $p = 1/100$ de que ocurra un error en el canal. A esto se le llama un canal binario simétrico y se denota como BSC por sus siglas en inglés. Además supóngase que se enviarán muchos mensajes importantes por ese cable y se necesita enviarlos de

Figura 9: Proceso de codificación



Fuente: Elaboración propia con software Dia y exportado a TEX

manera rápida y segura. Los mensajes ya se encuentran escritos como cadenas de ceros y unos, producidos, quizás, por alguna computadora.

Se van a **codificar** estos mensajes para darles una protección en contra del ruido del canal. Un bloque de k símbolos del mensaje $u = u_1 \dots u_k,\ u_i = 0$ o 1, será codificado como una **palabra-código** $x = x_1 \dots x_n, x_i = 0$ o 1 donde $n \geq k$ (véase la figura 9). Estas palabra-códigos forman un código. La primera parte de la palabra-código consiste en el mensaje mismo:

$$x_1 = u_1,\ x_2 = u_2,\ \dots,\ x_k = u_k,$$

seguido de $n-k$ símbolos de comparación $x_{k+1}, \dots, x_n$. Los símbolos de comparación son elegidos de tal forma que las palabra-códigos satisfagan

$$H \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = Hx^t = 0,$$

donde la matriz H de $(n-k)\times k$ es la matriz de comparación de paridad del código, dada por

$$H = [A \mid I_{n-k}], \tag{6.1}$$

donde A es una matriz fija de $(n-k)\times k$ de ceros y unos e

$$I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

es la matriz identidad de $(n-k)\times(n-k)$. La aritmética en la ecuación (6.1) se hace en módulo 2, es decir que se está trabajando con el campo $\mathbb{Z}_2$.

Ejemplo 6.1.1. La matriz de comparación de paridad

$$H = \left(\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right)$$

define un código con $k = 3$ y $n = 6$. Para este código

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

El mensaje $u_1u_2u_3$ es codificado en la palabra-código $x = x_1x_2x_3x_4x_5x_6$ que empieza

con el propio mensaje:

$$x_1 = u_1, x_2 = u_2, x_3 = u_3,$$

seguido de tres símbolos de comparación $x_4x_5x_6$ tales que $Hx^t = 0$, es decir, se cumple

$$\begin{aligned} x_2 + x_3 + x_4 &= 0, \\ x_1 + x_3 + x_5 &= 0, \\ x_1 + x_2 + x_6 &= 0. \end{aligned} \tag{6.2}$$

Si el mensaje es $u = 011$, entonces $x_1 = 0,\ x_2 = 1,\ x_3 = 1$ y los símbolos de comparación son

$$\begin{aligned} x_4 &= 0 \\ x_5 &= 1 \\ x_6 &= 1 \end{aligned}$$

por lo que la palabra-código es $x = 011011$.

Las ecuaciones dadas por (6.2) son llamadas de **comparación de paridad del código**. Las ecuaciones de paridad dicen que el cuarto, quinto y sexto símbolo siempre deben sumar cero módulo 2, es decir, su suma siempre es par.

Es fácil notar que el número de palabra-códigos posibles para esta matriz es

$2^3 = 8$. Estas son:

$$\begin{array}{lll} 000000 & 011011 & 110110 \\ 001110 & 100011 & 111000 \\ 010101 & 101101 & \end{array} .$$

En general en un código hay 2^k palabra-códigos, si el alfabeto es $\{0, 1\}$.

Luego de haber visto de manera intuitiva un código lineal, se da la definición formal:

Definición 6.1.1. Un código de bloques lineal sobre GF(q) de longitud n y dimensión k, es un subespacio de $V_n(q)$ de dimensión k, donde $V_n(q)$ es un espacio vectorial de dimensión n sobre GF(q). Se denota a este como **código lineal** (n, k).

El término código de bloques se refiere al hecho que toda palabra-código tiene la misma longitud, es decir, es una n-upla. La palabra lineal se deriva del simple hecho que las palabra-códigos forman un subespacio. También existen los códigos de árbol, de los cuales los códigos de convolución son un caso especial. Dichos códigos no dividen el mensaje en bloques. En la práctica de la ingeniería estos códigos son bastante importantes, pero no se hablará de estos en este trabajo.

Definición 6.1.2. La distancia de Hamming $d(u, v)$ entre dos n-uplas u y v de $V_n(q)$ está definida como el número de coordenadas en el cual difieren. El peso de Hamming $\omega(u)$ de una n-upla $u \in V_n(q)$ es el número de coordenadas no nulas de u.

La mayor parte del trabajo en teoría de códigos se desarrolla en base a la distancia de Hamming. Otra métrica con la que también se trabaja es la de Lee.

Como se dijo anteriormente, en la transmisión de una palabra-código en algún canal se puede producir errores debido al ruido. Por error, se entiende que puede ocurrir un cambio en cualquiera de las coordenadas de la n-upla trasmitida. Justamente el punto de codificar es que, bajo ciertas circunstancias, estos errores se pueden corregir.

6.2. Códigos cíclicos

Ya que se ha hecho la presentación de los códigos lineales, se procede a estudiar una clase muy particular e importante de ellos; los códigos cíclicos.

Definición 6.2.1. Un código es cíclico si es lineal y además todo desplazamiento cíclico de las coordenadas de una palabra-código es también una palabra-código.

Los códigos cíclicos figuran entre los primeros que aparecieron para el uso práctico, estos eran implementados usando registros de desplazamientos. Para poder hacer un buen diseño de códigos es necesario conocer la estructura algebraica de los mismos. En esta sección se abordará la estructura algebraica de los códigos cíclicos. El lector deberá notar que los códigos cíclicos no dependen de la linealidad de los mismos, de hecho, también existen los códigos cíclicos no lineales.

Resulta muy conveniente identificar a los códigos cíclicos con polinomios, esto es, a cada palabra-código

$$a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}^n$$

se le asocia el polinomio

$$a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in \mathbb{F}[x]_n.$$

Si c es una palabra-código del código $\mathcal{C}$, entonces $c(x)$ es su polinomio-código asociado. Con esta identificación, la palabra-código con corrimiento $\tilde{c}$ tiene el polinomio-código asociado

$$\tilde{c}(x) = c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-2}.$$

Así, es tentador pensar que $\tilde{c}(x)$ es casi igual al producto $xc(x)$. Más aún,

$$\tilde{c}(x) = xc(x) - c_{n-1}(x^n - 1)$$

de donde se deduce que

$$\tilde{c}(x) = xc(x)(\text{mód } x^n - 1).$$

Dicho de otra manera $\tilde{c}(x)$y $xc(x)$ son iguales en el anillo de polinomios $\mathbb{F}[x]$ con multiplicación módulo $x^n - 1$. Como se esta trabajando con códigos, según la definición $\mathbb{F} = GF(q)$ y $GF(q)[x]$ es el anillo de polinomios sobre $GF(q)$ en la variable x. Entonces, por lo dicho en el párrafo anterior, resulta claro que hay un isomorfismo natural entre $GF(q)[x]/(x^n - 1)$ y los polinomios de grado menor que n con multiplicación definida módulo $x^n - 1$. Se denota al anillo $GF(q)[x]/(x^n - 1)$ como A_n. Es claro que A_n es también un álgebra sobre $GF(q)$. Más aún, si $C_n = \langle x \rangle,\ x^n = 1$, es un grupo cíclico de orden n, es evidente que existe un isomorfismo entre $GF(q)C_n$ y $GF(q)[x]/(x^n - 1) = A_n$, donde se ha utilizado el símbolo x para ambas álgebras con el único propósito de hacer énfasis en esta identificación.

Lo anterior quiere decir que $A_n \simeq GF(q)C_n$, pero $GF(q)C_n$ es un grupo-álgebra, con lo cual se ha demostrado que los códigos cíclicos son un grupo-álgebra y

por lo tanto su estructura algebraica está plenamente identificada. Además se tiene el siguiente:

Teorema 6.2.1. Un código lineal (n, k) $\mathcal{C}$ sobre $GF(q)$ es cíclico si y sólo si dicho código es un ideal de A_n.

Demostración. Sea $\mathcal{C}$ un ideal de A_n. Es claro que $\mathcal{C}$ es un subespacio de A_n como espacio vectorial, por lo que solamente falta verificar que es un subespacio cíclico, lo cual se sigue del hecho que $\mathcal{C}$ es ideal y por lo tanto cerrado bajo multiplicación por x. Para el converso, supóngase que $\mathcal{C}$ es un subespacio cíclico, eso quiere decir que es cerrado bajo la suma y el producto por x y por lo tanto es cerrado bajo el producto de cualquier elemento de A_n, entonces $\mathcal{C}$ es un ideal. □

Como el lector podrá notar, el estudio de códigos cíclicos, se reduce a estudiar los ideales de A_n, que es un grupo-álgebra. Para ello será provechoso conocer cuando A_n es semisimple o no, tarea que se realizó en el capítulo 3. Así por el corolario 2.3.2 se sabe que A_n es semisimple si y sólo si $\text{car}(K) \nmid |G|$. En el caso de tener un campo binario esta condición se reduce a exigir que $|G|$ sea un número impar. Supóngase que $\text{car}(K) \nmid |G|$ entonces aplicando el teorema 1.3.3 se deduce que todo ideal de A_n es de la forma $L = A_n e$, donde $e \in A_n$ es un elemento idempotente. De esto se obtiene el siguiente:

Teorema 6.2.2. Si $\text{car}(K) \nmid |G|$ entonces el estudio de los grupos cíclicos es equivalente al estudio de ideales en grupo-álgebras generadas por elementos idempotentes.

Para el estudio de los ideales de A_n es importante conocer la factorización de $x^n - 1$. En general se desea que los factores de $x^n - 1$ no sean de multiplicidad mayor a 1. Recordando que $GF(q)$ es el campo extensión de Galois con p^n elementos

entonces se puede verificar que $x^n - 1$ no posee factores aparte de los lineales si y sólo si $(n, q) = 1$.

Teorema 6.2.3. El único polinomio mónico $g(x)$ de grado mínimo en un ideal A de A_n es un generador de A y divide a $x^n - 1$. La dimensión de A es $n - \deg(g)$. Más aún, si $g(x)$ es un divisor de $x^n - 1$ entonces también es un generador de un ideal A en A_n.

Para la demostración del teorema anterior se sugiere consultar (2:52). De la misma fuente se puede consultar la demostración del siguiente:

Teorema 6.2.4. Sean A_1 y A_2 dos ideales del grupo-álgebra $GF(q)C_n$ con polinomios generadores $g_1(x)$ y $g_2(x)$ respectivamente. Entonces

- $A_1 \cup A_2$ es generado por $(g_1(x), g_2(x)$.
- $A_1 \cap A_2$ es generado por $[g_1(x), g_2(x)]$.
- $A_1 A_2$ es generado por $(g_1(x)g_2(x), x^n - 1)$.

Un código (n, k) cíclico sobre $GF(q)$ corresponde a un ideal A_n que es generado por $g(x)$, un divisor de $x^n - 1$. De esta forma, siendo σ_q la función definida como $\sigma_{q^n-1} \equiv iq \pmod{q^n - 1}$, se tiene según (2: 31), que el número de factores de $x^n - 1$ es $\sigma_q(n)$ y de esta cuenta el número de códigos cíclicos de longitud n sobre $GF(q)$, $(n, q) = 1$ es $2^{\sigma_q(n)}$, lo cual incluye los códigos triviales, a saber: el código (0) y el grupo-álgebra. Esto complementa la teoría desarrollada en la sección 2.4 en la cual se demuestra que el grupo-álgebra $GF(q)C_n$ es suma directa de extensiones ciclotómicas de $GF(q)$. Ahora bien, algunos de estos códigos podrían ser equivalentes, así que es de interés saber cuando los ideales del grupo-álgebra son equivalentes para lo cual se sugiere consultar (2:43-45)

Ejemplo 6.2.1. Considérese el grupo-álgebra del grupo cíclico C_3 sobre $GF(2)$ cuyos elementos son:

$$GF(2)C_3 = \{O, l, g, g^2, 1+g, 1+g^2, g+g^2, 1+g+g^2\}$$

y como C_3 es abeliano, de la sección 2.4, se tiene que los ideales del grupo-álgebra deben ser bilaterales. Esto implica que los ideales no pueden ser isomorfos a pares y además cada ideal contiene un idempotente central que los genera (véase teorema 1.3.3). Para esta álgebra en particular existen dos ideales no triviales, que son:

$$A_1 = \{O, 1+g+g2\},$$
$$A_2 = \{O, g+g^2, 1+g^2, 1+g\}$$

con idempotentes generadores

$$e_1 = 1+g+g^2$$
$$e_2 = g+g^2$$

respectivamente. Además se sigue que:

$$GF(2)C_3 = A_1 \oplus A_2.$$

CONCLUSIONES

1. Para el estudio de los grupo-anillos es importante conocer la estructura de los grupos abelianos y hamiltonianos así como la teoría de módulos y el teorema de Wedderburn-Artin.
2. Las condiciones necesarias y suficientes para que un grupo-anillo sea semisimple vienen dadas por el teorema de Maschke.
3. Toda representación de un anillo conmutativo sobre un grupo dado corresponde a un módulo del grupo-anillo correspondiente.
4. En general no es fácil encontrar unidades no triviales en grupo-anillos, pero es posible construir algunas usando elementos idempotentes.
5. Las grupo-álgebras dan estructura matemática a los códigos correctores conocidos como cíclicos.
6. Cuando la característica del campo no divide al orden del grupo el estudio de los códigos cíclicos se reduce a estudiar los ideales de grupo-álgebras generadas por elementos idempotentes.

RECOMENDACIONES

1. Usar el primer capítulo como guía de temas para el desarrollo de un curso de álgebra moderna de pregrado.
2. Para el estudio de los códigos cíclicos se puede utilizar los resultados del capítulo 2, en especial los de las secciones 2.3 y 2.4.
3. Estudiar la teoría de códigos correctores desde el punto de vista algebraico, permitiendo así dictaminar la capacidad correctora de los mismos.
4. Para la lectura de los capítulos 2 y 3 es importante tener conocimientos previos de teoría de grupos y anillos.
5. Implementar el estudio de teoría de módulos en el curso de álgebra 2 de la licenciatura en matemática aplicada de la USAC.

BIBLIOGRAFÍA

[1] BELL, Eric. *Los grandes matemáticos.* Argentina: Editorial Losada, 1948.

[2] BLAKE, Ian. *The mathematical theory of coding.* Estados Unidos: Academic Press Inc, 1975.

[3] BURNSIDE, William. *The theory of Groups of Finite Order.* 2da ed. Cambridge: Cambridge University Press, 1911.

[4] CAUCHY, Augustin-Louis. Oeuvres complètes. 1era ed. Cambridge: Cambridge University Press, 2009.

[5] DESKINS, Eugene. "Finite abelian groups with isomorphic group algebras". *Duke Mathematical Journal.* 1956, vol 23, núm. 1, p. 35-40.

[6] FEIT, Walter, et al. "The solvability of groups of odd order". *Pacific J. Math.* 1963, vol 13, núm 3, p. 775-1029.

[7] GOLDSHMIDT, David. "A group theoretic proof of the $p^a q^b$ theorem for odd primes". *Mathematische Zeitschrift.* 1970, vol 113, núm. 5, p. 373-375.

[8] HAWKINS, Thomas. "The origins of the Theory of Group Characters". *Archive for History of Exact Sciences.* 1971, vol 7, núm. 2, p. 142-170.

[9] HERSTEIN, Nathain. *Topics in Algebra.* 2da ed. New York: Macmillah, 1986 . 381 p.

[10] IAN, Connell. “On the group ring”. *Canad. J. Math.* 1963, vol 15, núm 1, p. 650-685.

[11] ISAACS, Martin. *Algebra: a graduate course*. Estados Unidos: Editorial Pacific Grove, 1940.

[12] JENNINGS, Arthur. “The structure of the group ring of a p-group over a modular field”. *Transactions of The American Mathematical Society*. 1941, vol. 50, núm 1, p. 175-185.

[13] LANG, Serge. *Linear Algebra*. 3ra ed. Nueva York: Springer-Verlag, 2004. 308 p.

[14] MOSER, Claude. “Representation de -1 comme somme de carres dans un corps cyclotomique quelconque”. *Journal of Number Theory*. 1973, vol 5, núm. 2, p. 138-141.

[15] PASSMAN, Donald. *The algebraic structure of group rings*. New York: Wiley-Interscience, 1977. 550 p.

[16] PERLIS, Sam; WALKER, Gordon. “Abelian group algebras of finite order”. *Transactions of The American Mathematical Society*. 1950, vol 68, núm 3, p. 420-426.

[17] POLCINO, César; SEHGAL, Sudarshan. *An introduction to group rings*. Dordrecht: Kluwer Academic Publishers, 2002. 371 p.

[18] STEWART, Ian. *De aquí al infinito – Las matemáticas de hoy.* España: Editorial Crítica, 1998.

[19] SUDARSHAN, Sehgal. *Topics in Group Rings*.New York: Marcel Dekker, 1978. 233 p.

[20] ZASSENHAUS, Hans. *The theory of groups*. Estados Unidos: Chelsea publishing company, 1937.