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

TEORÍA DE LOS GRUPOS-ANILLOS Y SUS APLICACIONES

Hugo Allan García Monterrosa

Asesorado por el Lic. William Roberto Gutiérrez Herrera

Guatemala, FECHA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

TITULO DE TU TESIS (identi.tex)

TRABAJO DE GRADUACIÓN
PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

HUGO ALLAN GARCÍA MONTERROSA
ASESORADO POR EL Lic. WILLIAM ROBERTO GUTIERREZ HERRERA

AL CONFERÍRSELE EL TÍTULO
LICENCIADO EN MATEMÁTICA APLICADA

GUATEMALA, FECHA

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	Ing. Miguel Angel Dávila Calderón
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO
(Ver nomina.tex)

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADORA	Dra. Mayra Virginia Castillo Montes
EXAMINADOR	Lic. William Roberto Gutiérrez Herrera
EXAMINADOR	Lic. Francisco Bernardo Ral De La Rosa
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo 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 Coordinación de la Carrera de Licenciatura en Matemática Aplicada, el (Fecha).

Hugo Allan García Monterrosa

AGRADECIMIENTOS A:

Dios	Por permitirme culminar mis estudios de pregrado, brindando fortaleza y ayuda en todo momento.
Dedicatoria2	Ver agrade.tex.

ÍNDICE GENERAL

LISTA DE SÍMBOLOS **III**

RESUMEN **V**

OBJETIVOS **VII**

INTRODUCCIÓN **IX**

1. CONCEPTOS PRELIMINARES **1**
- 1.1. Antecedentes 1
- 1.2. Teoría de grupos 1
- 1.3. Anillos, Módulos y Álgebras 1

2. GRUPO-ANILLOS **3**
- 2.1. Hechos Básicos De Los Grupo-Anillos 3
- 2.2. Ideales de aumento 11
- 2.3. Semisimplicidad 16
- 2.4. Grupo-Algebras de grupos abelianos 22

3. TEORÍA DE REPRESENTACIÓN DE GRUPOS **33**
- 3.1. Definición y Ejemplos 33

CONCLUSIONES **45**

RECOMENDACIONES **47**

BIBLIOGRAFÍA **49**

LISTA DE SÍMBOLOS

Símbolo	Significado
$\boldsymbol{\not{x}^n}$	cancelación de x al valor n
$\boldsymbol{E^c}$	complemento de E
$\mathbb{C}$	conjunto de los números complejos
$\mathbb{Z}$	conjunto de los números enteros
$\mathbb{Z}^+$	conjunto de los números enteros positivos
$\mathbb{R}$	conjunto de los números reales
$\varnothing$	conjunto vacío
$\boldsymbol{\infty}$	infinito
$\mathbf{ln}$	logaritmo natural
$\boldsymbol{(m, n)}$	máximo común divisor entre m y n
$\frac{\boldsymbol{d^n}}{\boldsymbol{dx^n}}$	n-ésima derivada respecto de x
$\notin$	no pertenencia
$\forall$	para todo
$\in$	pertenencia
$\frac{\boldsymbol{d}}{\boldsymbol{dx}}$	primera derivada respecto de x
$\prod$	productoria
$\Leftrightarrow$	si y sólo si
$\boldsymbol{(a_n)_{n\in\mathbb{N}}}$	sucesión de a_n
$\sum$	sumatoria
$\lvert \cdot \rvert$	valor absoluto
$[\cdot]\big\rvert_{\boldsymbol{x=m}}$	valuación de expresión con $x = m$

RESUMEN

Resumen de tesis (obje.tex)

OBJETIVOS

General

- Solo un objetivo general (obje.tex)

Específicos

1. Al menos un objetivo específico (obje.tex)

INTRODUCCIÓN

Introducción de la tesis (intr.tex)

1. CONCEPTOS PRELIMINARES

1.1. Antecedentes

1.2. Teoría de grupos

aquí irá toda la teoría de grupos que se tenga que desarrollar previo a comenzar propiamente la tésis.

1.3. Anillos, Módulos y Álgebras

aquí también se tiene que escribir las definiciones, teoremas de morfías y todo lo de semisimplicidad.

2. GRUPO-ANILLOS

2.1. Hechos Básicos De Los Grupo-Anillos

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

Considérese la siguiente construcción: Sea G un grupo cualquiera y R un anillo cualquiera. Entonces se define $RG := \{\alpha | \alpha \colon G \to R, |sop(\alpha)| < \infty\}$ donde $sop(\alpha) := \{g \in G : \alpha(g) \neq 0\}$, a el conjunto $sop(\alpha)$ se le llama el soporte de α. Se puede observar entonces 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 en mente se procede a definir a un grupo-anillo.

Definición 1. *El conjunto RG con las operaciones $+$ y $\cdot$ mencionadas anteriormente es llamado el* ***grupo-anillo de G sobre R****. En el caso en que R es conmutativo a RG se le llama también el* ***grupo-algebra de G sobre R***

Ahora se procede a mostrar dos teoremas que son básicos para el estudio de esta nueva estructura algebraica.

Teorema 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 $g \neq 0$. 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 lo que se ha demostrado que $i(x)i(y) = i(xy)$. □

Generalmente a i se le llama la función de inclusión, así que será la forma en que se nombrará de aquí en adelante.

Teorema 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 exactamente igual que en el teorema anterior. Ahora falta probar que v es un homomorfismo de anillos (con la aclaración que el hecho 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 en mente es fácil probar la siguiente propiedad.

Propiedad 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 ve 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, ya que se ha construido 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 $g \in sop(\alpha)$

Nota 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 $\alpha\beta = \sum_{g,h \in G} a_g b_h gh$

Ahora es práctico establecer los siguientes teoremas:

Teorema 3. *RG es un grupo aditivo*

Demostración. Se procede por incisos:

i) Sean $\alpha, \beta, \gamma \in RG$ entonces $\alpha + (\beta + \gamma) = \sum_{g \in G} a_g g + \left(\sum_{g \in G} b_g g + \sum_{g \in G} c_g g \right) = \sum_{g \in G} a_g g + \left(\sum_{g \in G} (b_g + c_g) g \right) = \sum_{g \in G} (a_g + b_g + c_g) g = \sum_{g \in G} ((a_g + b_g) + c_g) g = \left(\sum_{g \in G} (a_g + b_g) g \right) + \sum_{g \in G} c_g g = (\alpha + \beta) + \gamma$

ii) 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 en mente se procede a hacer los cálculos: $\alpha + 0 = \sum_{g \in G} (a_g + 0) g = \sum_{g \in G} (0 + a_g) = \sum_{g \in G} a_g g = \alpha$

iii) 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 $\alpha + (-\alpha) = \sum_{g \in G} (a_g + (-a_g)) g = \sum_{g \in G} ((-a_g) + a_g) g = \sum_{g \in G} 0 \cdot g = 0$

iv) $\alpha+\beta=\sum_{g\in G}a_g g+\sum_{g\in G}b_g g=\sum_{g\in G}(a_g+b_g)g=\sum_{g\in G}(b_g+a_g)g=\beta+\alpha$ $\square$

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 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:

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

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

vii) $(\alpha+\beta)\gamma=\left(\sum_{g\in G}(a_g+b_g)g\right)\left(\sum_{g\in G}c_g g\right)=\sum_{g,h\in G}(a_g+b_g)c_h gh=\sum_{g,h\in G}a_g c_h gh+$
$\sum_{g,h\in G}b_g c_h gh=\alpha\gamma+\beta\gamma$ $\square$

Es de interés estudiar la estructura algebraica de RG, así que se introduce una operación mas sobre RG

Definición 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 podemos proclamar el siguiente teorema

Teorema 5. *RG es un R -módulo*

Demostración. Ya se estableció en el teorema 3 que $(RG, +)$ es un grupo aditivo. De la definición anterior se sigue que $\lambda\gamma \in RG$. Ahora se procede por incisos:

i) $(\lambda_1 + \lambda_2)\alpha = \sum_{g\in G}(\lambda_1 + \lambda_2)a_g g = \sum_{g\in G} \lambda_1 a_g g + \sum_{g\in G} \lambda_2 a_g g = \lambda_1\alpha + \lambda_2\alpha$

ii) $\lambda(\alpha + \beta) = \lambda \sum_{a_g+b_g} g = \sum g \in G\lambda(a_g + b_g)g = \sum_{g\in G} \lambda a_g g + \sum_{g\in G} \lambda b_g g = \lambda\alpha + \lambda\beta$

iii) $\lambda_1(\lambda_2\alpha) = \lambda_1 \sum_{g\in G} \lambda_2 a_g g = \sum_{g\in G}(\lambda_1(\lambda_2 a_g))g = \sum_{g\in G}((\lambda_1\lambda_2)a_g)g = \lambda_1\lambda_2\alpha$

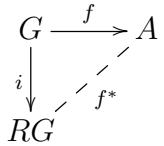
iv) $1_R\alpha = \sum g \in G1_R a_g g = \sum_{g\in G} a_g g$

Y con esto concluye la prueba. □

Una extensión del resultado anteriormente presentado 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 $rango(RG) = |G|$

Ahora se establecerá un resultado de mucha importancia en los grupo-anillos, ya que relaciona a estos con los homomorfismos, que es uno de los objetivos del álgebra.

Proposición 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 siguiente diagrama es conmutativo:*



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, $f^*(\alpha+\beta) = \sum_{g\in G}(a_g+b_g)f(g) = \sum_{g\in G} a_g f(g) + \sum_{g\in G} b_g f(g) = f^*(\alpha) + f^*(\beta)$.
Similarmente $f^*(\alpha\beta) = \sum_{g,h\in G} a_g b_h f(gh) = \sum_{g,h\in G} a_g b_h f(g)f(h) = f^*(\alpha)f^*(\beta)$. 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 no es mas que un caso especial de la misma, pero se establecerá por aparte porque será de utilidad en el desarrollo de este trabajo de graduación.

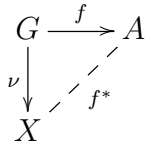
Corolario 1. *Sea $f\colon G \to H$ un homomorfismo de grupos. Entonces, existe un único homomorfismo de anillos $f^*\colon RG \to RH$ tal que $f^*(g) = f(g)$ para cualquier $g \in G$. Si R es conmutativo, entonces f^* es un homomorfismo de $R-$ álgebras, mas aún si f es un epimorfismo (monomorfismo), 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 $g \in G$. Con lo cual concluye la prueba. □

De hecho la proposición 1 se puede utilizar como una definición de RG, como se sigue de la siguiente proposición:

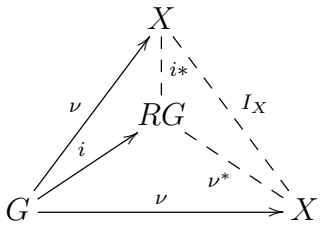
Proposición 2. *Sea G un grupo y R un anillo. Sea X un anillo conteniendo R y $\nu\colon G \to X$ una función tal que $\nu(gh) = \nu(g)\nu(h)$ para todo $g, h \in G$ y tal que, para todo anillo A que contiene a R y cualquier función $f\colon G \to A$ que satisface $f(gh) = f(g)f(h)$ para todo $g, h \in G$, existe un único homomorfismo R-lineal $f^*\colon X \to A$ tal*

que el siguiente diagrama es conmutativo:



Entonces $X \simeq RG$

Demostración. La demostración es tan simple como notar que el siguiente diagrama conmuta con I_X



□

Nota 2. Si en el corolario 6 se hace $H = \{1\}$ y se considera la función $m\colon G \to \{1\}$ entonces esta función induce un homomorfismo de anillos $\epsilon\colon RG \to R$ tal que $\epsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a(g)$.

Definición 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* ***el ideal de aumento*** *de* RG

Ahora se puede decir 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:

Proposición 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 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:

(i) $(\alpha + \beta)^* = \alpha^* + \beta^*$

(ii) $(\alpha\beta)^* = \beta^*\alpha^*$

(iii) $\alpha^* = \alpha$

Demostración. Se procede por incisos:

(i) $\left(\sum_{g\in G}(a_g+b_g)g\right)^* = \sum_{g\in G}(a_g+b_g)g^{-1} = \alpha^* + \beta^*$

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

(iii) $\left(\left(\sum_{g\in G} a_g g\right)^*\right)^* = \left(\sum_{g\in G} a_g g^{-1}\right)^* = \sum_{g\in G} a_g g$ □

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 (dar cita) y, en la forma que se presentará en este trabajo, en el trabajo hecho por W. E. Deskins (dar cita). 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 (dar cita).

Ya en materia de hecho, 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 izquierda de RG.

Definición 4. *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 subindíce 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 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 $h = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdot s_r^{\epsilon_r}$ 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 $(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_k^{\epsilon_k} - 1) \in (S)$

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 5. *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 rescribir como $\sum_{i,j} r_{ij}q_ih_j = \sum_i \left(\sum_j r_{ij}q_i\right)$. En la igualdad anterior se puede observar que como $h_j \neq 1$ entonces necesariamente el lado izquierdo de la ecuación tienen distinto soporto 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 elemtos de B_H. Para esto basta recordar que $g = q_ih_j$ para algún $q_i \in \mathcal{T}$ y $h_j \in H$ entonces $g(h-1) = q_ih_j(h-1) = q_i(h_jh-1) + (q_i-1)$ con lo que se demuestra lo que se pedía. □

Nota 3. Es claro que 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 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, a saber

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

tal que

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

Proposición 6. *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

$$\begin{aligned} \alpha &= \sum_i \left(\sum_j r_{ij}\right) \overline{q_i} && (2.5)\\ &= \sum_{ij} r_{ij} q_i (h_j - 1) \in \Delta(G,H) && (2.6) \end{aligned}$$

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. *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 ismorfia $\frac{RG}{\Delta(G,H)} \simeq Im(\omega^*)$ 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 e 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. *$\nabla(I)$ es subgrupo de G*

Demostración. Se debe probar dos cosas:

(i) 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 $g_1 g_2 \in \nabla(I)$

(ii) 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 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 7. *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 $q_1 = 1$ 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. □

Según lo expuesto en la proposición anterior pareciera ser cierto que ∇ y $\Delta/$ 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 alli 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 5. *Sea X un subconjunto de RG. El aniquilador de X por la izquierda es el conjunto*

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

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

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

Definición 6. *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 4. *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

$$\begin{aligned} (h-1)\alpha &= 0 \quad \text{para cada } h \in H && (2.7)\\ h\alpha - \alpha &= 0 && (2.8)\\ \sum_{g\in G} a_g ah &= \sum_{g\in G} a_g g && (2.9) \end{aligned}$$

De la última ecuación se aprecia que $hg \in sop(\alpha)$ siempre y cuando $g \in sop(\alpha)$, pero $sop(\alpha)$ es finito, por tanto H es finito. De nuevo analizando la ecuación 2.9 se deduce que dado $g_0 \in sop(\alpha)$ entonces $hg_o \in sop(\alpha)$ 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 $g\hat{H}g^{-1} = \hat{H}$ de donde se concluye inmediatamente que $\hat{H}g = g\hat{H}$ lo cual prueba que $\hat{H}$ es central en RG y de alli se sigue fácilmente la conclusión. □

Del lema anterior se sigue el siguiente corolario.

Corolario 3. *Sea G un grupo finito. Entonces*

(i) $Ann_i(\Delta(G)) = Ann_d(\Delta(G)) = R \cdot \hat{H}$

(ii) $Ann_d(\Delta(G)) \cap \Delta(G) = \{a\hat{G} : a \in R, a|G| = 0\}$

Demostración. Se procede por incisos

(i) Ya se ha establecido que $\Delta(G, G) = G$, por lo tanto hágase $H = G$ en el teorema anterior y el resultado es inmediato.

(ii) 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 5. *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 $x \in Ann_d(I)$ y por consiguiente $J \subset Ann_d(J)$ □

Lema 6. *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 Maschkes, logros que están plasmados en el siguiente teorema:

Teorema 6 (Maschke)**.** *Sea G un grupo. Entonces, el grupo-anillo RG es semisimple si y sólo si las siguientes condiciones son verdaderas:*

(i) *R es un anillo semisimple*

(ii) *G es finito*

(iii) *$|G|$ 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 6 se asegura que las condiciones (ii) y (iii) se satisfacen.

- Para mostrar la segunda implicación, asúmase que (i), (ii) y (iii) son verdaderas. De (i) se sigue que RG es semisimple como $R-modulo$. [1] Considérese M como $RG-modulo$, tal que $M \in RG$, entonces existe N como R-modulo tal que

$$RG = M \oplus N$$

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

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

  Es claro que dicha función existe, ya que G es finito por (ii) y es $\frac{1}{|G|} < \infty$ por (iii). 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:

[1] Recordar que esto es por una propiedad de anillos que debo poner en el capitulo 1

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:

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

Sobreyectiva y Composición:

Nótese que $gm \in M$ ya que M es un RG - modulo, 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 $M \in Im(\pi^*)$.

Por lo anteriormente expuesto se sigue directamente que $Ker(\pi^*)$ es un RG - submodulo 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, $car(K) \nmid |G|$, de donde se sigue el siguiente corolario:

Corolario 4. *Sea G un grupo finito y K un campo. Entonces KG es semisimple si y solo si $car(K) \nmid |G|$*

Aunque no es el objetivo de este trabajo de graduación 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 7. *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 de este trabajo, se explorará la conexión entre este resultado y la teoría de representación de grupos.

Corolario 5. *Sea G un grupo finito y K un campo algebraicamente cerrado tal que $car(K) \nmid |G|$. Entonces:*

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

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

Demostración. Como $car(K) \nmid |G|$ 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 finito dimensional. 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-Algebras de grupos abelianos

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 $car(K) \nmid |G|$. Esta caracterización fue dada por primera vez por S. Perlis y G Walker (dar la referencia).

Se comenzará con el caso donde G es un grupo cíclico, así que se asume que $G =< a : a^n = 1 >$ y que K 4s un campo tal que $car(K) \nmid |G|$. Considérese la función $\phi : K[X] \to KG$ 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[2] 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 $char(K) \nmid n$, este polinomio debe ser separable y por lo tanto $f_i \neq f_j$ si $i \neq j$. Utilizando el teorema chino del residuo [3] 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

[2] poner esto en el capitulo uno y hacer referencia

[3] tambien en la parte inicial y luego referencia a el

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

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 baja 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 1. *Sea* $G =< a \colon a^7 = 1 >$ *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. *Sea* $G =< a \colon a^6 = 1 >$ *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 mas 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. Tambień 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}, $\quad 1 \leq i \leq a_d$. 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 $grad(f_{d_i}) = [K(\zeta_d) : K]$, 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:

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

Ejemplo 3. *Sea* $G =< a : a^n = 1 >$ *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:*

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

Hay que notar, que como en casos anteriores, bajo este isomorfismo el generador a *corresponde a la tupla cuyas entradas son raíces primitivas de la unidad de orden* d, *donde* d *es cualquier divisor positivo de* n.

Finalmente se cerrará esta sección demostrando un hecho muy importante, a saber, que la caracterización anteriormente dada también es válida en los grupo-anillos con grupos abelianos finitos.

Teorema 8. *Perlis-Walker Sea G un grupo finito abeliano de orden n y sea K un campo tal que $char(K) \nmid n$. 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 este fórmula n_d denota el número de elementos de orden d en G.

Demostración. Para proceder con la demostración es necesario enunciar y demostrar los siguientes lemas:

Lema 7. *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 $M_{n,\gamma} = \{g : (g,h) \in sop(\gamma)\}$. 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.

Homomorfismo:

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

   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 $\alpha_h = \sum_{g\in M_h,\gamma_1} a_{gh}g + \sum_{g\in M_h,\gamma_2} b_{gh}g = \beta_h + \xi_h$

2. **Conserva productos:** Sean $\gamma_1, \quad \gamma_2 \in R(G\times H)$, 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 $(g,h), \quad (m,n) \in (G\times H)$ se cumple que $f((g,h)(m,n)) = f((g,h))f((m,n))$ y que además f es $R-$lineal. En efecto, por un lado

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

y por el otro lado se tiene:

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

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

3. f **es inyectiva:** Para demostrar que f es inyectiva se debe demostrar que el único elemento que anula a f es elemento neutro de $R(G\times H)$. Para el 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 $\gamma = 0$

4. f **es sobreyectiva:** 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 lo que concluye la prueba. □

Lema 8. *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 $(\alpha_1, \cdots, \alpha_n) \mapsto \sum_{g\in G} a_g g, \quad a_g = (a_g^{(1)}, \cdots, a_g^{(n)})$, 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.

1. **Conserva sumas:** Sean $\alpha = (\alpha_1, \cdots, \alpha_n), \quad \beta = (\beta_1, \cdots, \beta_n) \in \oplus_{i\in I} R_i G$, entonces su suma viene dada por $\gamma = (\alpha_1 + \beta_1, \cdots, \alpha_n + \alpha_n)$, y con ello la imagen de la suma seria $f(\gamma) = \sum_{g\in G} c_g g, \quad c_g = (a_g^{(1)}, \cdots, a_g^{(n)})$.

   Por otro lado, se tiene:

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

   por lo tanto $f(\alpha + \beta) = f(\alpha) + f(\beta)$

2. **Conserva productos:** Como en el caso anterior, se tiene $\gamma = \alpha\beta = (\alpha_1\beta_1, \cdots, \alpha_n\beta_n)$, y por lo tanto, su imagen bajo f, es $f(\gamma) = \sum_{u\in G} c_u u, \quad c_u = (c_u^{(1)}, \cdots, c_u^{(n)}), \quad c_u^{(i)} = \sum_{gh=u} a_g^{(i)} b_h^{(i)}$.

   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 $f(\alpha)f(\beta) = \sum_{u\in G} d_u u, \quad d_u = \sum_{gh=u} a_g b_h = \left(\sum_{gh=u} a_g^{(1)} b_g^{(1)}, \cdots, \sum_{gh=u} a_g^{(n)} b_g^{(n)}\right) = c_u$

3. f **es inyectiva:** Supóngase que $f(\alpha) = \sum_{g\in G} a_g g = 0$ entonces $a_g = (0, \cdots, 0)$, de donde $\alpha = (0, \cdots, 0)$

4. f **es sobreyectiva:** Dado $\sum_{g\in G} a_g g, \quad a_g = (a_g^{(1)}, \cdots, a_g^{(n)})$. Entonces se construye $\alpha = \left(\sum_{g\in G} a_g^{(1)} g, \cdots, \sum_{g\in G} a_g^{(n)} g\right)$ y es fácil verificar que $f(\alpha) = \sum_{g\in G} a_g g$

□

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 de estructura [4] de los grupos finitos abelianos para escribir $G = G_1 x H$ donde H 4s 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 7 se cumple

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

utilizando el lema 8 se obtiene

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

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

[4] poner en capitulo 1

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

con $a_d = \sum_{d1,d2} a_{d_1} a_{d_2}$ 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:

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

□

3. TEORÍA DE REPRESENTACIÓN DE GRUPOS

3.1. Definición y Ejemplos

Como se mencionó en el capítulo 1 [1] el concepto de **grupo de permutaciones** fue dado explícitamente por primera vez en [2] 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 que grupo es -en particular - ? Es decir, ¿ Se puede decir cuando es un grupo de permutaciones, un grupo lineal o un grupo de transformaciones proyectivas - sólo por citar algunos ejemplos- ?

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 [3].

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 [4], que actualmente es considerado un libro clásico en este

[1] ponerlo ejemplos en esta parte de la definición de grupos

[2] poner el libro: Memorias de Galois

[3] hacer referencia al libro T Hawkins, Hypercomplex number Lie groups and the creation of group representation theory, Archive Hist. Exact Sci. 8 (1972), pagina 269

[4] referencia al libro

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. [5] 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 mas de 60 años después (ver [6])

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 [7], usando para ello teoría de la representación.

Luego de hacer énfasis en la importancia histórica que tiene la teoría de representación de grupos, se entra a estudiar algunas definiciones de la misma.

Definición 7. *Sea 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 automorfismos de V. El rango de V es llamado* ***grado*** *de la representación T y se denotará como $grad(T)$.*

Para $g \in G$ se denotará como $T_g\colon V \to V$ 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,

[5] poner esto en el glosario o en donde corresponde: Un grupo G es soluble si hay una cadena de subgrupos $e = H_0 \subset H_1 \subset \cdots \subset H_n \subset H_n = G$ tal que para cada i, el subgrupo H_i es normal en H_{i+1} y el grupo cociente H_{i+1}/H_i es abeliano.

[6] poner la bibliografia 48

[7] ver 39

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:

Definición 8. *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.

Para ilustrar lo que se expuso anteriormente, se ha considerado necesario, exponer algunos ejemplos sencillos.

Ejemplo 4. *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 5. *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:*

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

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

Ejemplo 6. *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 $\{v_1, v_2, \cdots, v_n\}$. 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 mas 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 7 (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:*

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

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. Es importante notar que esta representación se construyó a partir de la multiplicación por la izquierda, así que sería mas apropiado llamarla representación regular por la izquierda de G sobre R.

Para ilustrar de mejor manera a continuación se muestra un ejemplo:

Ejemplo 8. *Sea* $G = \{1, a, a^2\}$ *un grupo cíclico de orden tres. Enúmerese 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:*

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

que no es más que una matriz de permutación.

Ejemplo 9. *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:

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

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

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

Nota 4. 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 $tr(\rho(g)) = 0$ 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 10. *[Algunas representaciones de grupos cíclicos] Considérese el grupo cíclico $G = \{1, a, \cdots, a^{m-1}\}$ 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 $r \in \mathbb{Z}$.*

Súpongase que $car(K) \nmid m$ 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 ordem m que son distintas a pares entonces la función $B\colon G \to GL(m, K)$ dada por

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

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

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

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

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

Finalmente si $car(K) \mid m$ *entonces se propone la representación* $C\colon G \to GL(2,K)$, *dada por*

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

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

Ejemplo 11 (Representación de D_4)**.** *Considérese el grupo de simetrías de un cuadrado. Este grupo de 8 elementos, a saber, las reflecciones a través de los ejes* r_1, r_2, r_3, r_4 *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 dihédrico de orden ocho y usualmente denotado por D_4 *– puede ser definido con dos generadores que satisfacen las relaciones*

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

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:

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

Ejemplo 12 (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:*

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

Si se eligen bases $\{v_1, \ldots, v_n\}$ y $\{w_1, \ldots, w_m\}$ de V y N 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

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

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, escensialmente, una copia de T. La relación entre estas dos representaciones está ilustrada en el siguiente diagrama:

$$\begin{array}{ccc} V & \xrightarrow{T_g} & V \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ W & \xrightarrow[\overline{T_g}]{} & W \end{array} .$$

Lo cual sugiere lo siguiente:

Definición 9. *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 10. *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 13. *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 10 con*

$$\mathsf{U} = \begin{pmatrix} \xi_1 & \xi_1^2 & \cdots & \xi_1^m \\ \xi_2 & \xi_2^2 & \cdots & \xi_2^m \\ & & \cdots & \\ \xi_m & \xi_m^2 & \cdots & \xi_m^m \end{pmatrix}, \quad \mathsf{U} \in GL(n,K)^8$$

entonces, calculando por un lado se tiene

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

similarmente

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

[8] Esto es evidente, ya que U es una matriz de Vandermonde con $det(\mathsf{U}) = \prod_{1 \le i < j \le m} (\xi_i - \xi_j) \neq 0$.

con lo que se ha demostrado que $\mathsf{A(g)} = \mathsf{UB(g)U^{-1}}$*, para cualquier* $g \in G$ *y concluye que* B *y* $\mathsf{\Gamma}$ *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 asúmase 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 se tiene entonces 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

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

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

Definición 11. *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 12. *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*

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

CONCLUSIONES

1. Conclusiones (c_y_r.tex)

RECOMENDACIONES

1. Recomendaciones (c_y_r.tex)

BIBLIOGRAFÍA

[1] Ahlfors, Lars V. **Complex Analysis (An Introduction to the Theory of Analytic Functions of One Complex Variable)** 3ª ed. (International Series in Pure and Applied Mathematics)

[2] Apellido, Nombre. **Titulo** n-sima ed. (Editorial)