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

Símbolo	**Significado**
$\boldsymbol{\cancelto{n}{x}}$	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
$\boldsymbol{\frac{d^n}{dx^n}}$	n-ésima derivada respecto de x
$\notin$	no pertenencia
$\forall$	para todo
$\in$	pertenencia
$\boldsymbol{\frac{d}{dx}}$	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
$[\cdot]\rvert_{\boldsymbol{x=m}}$	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 $RG := \{\alpha : \alpha : G \to R, |sop(\alpha)| < \infty\}$ 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 GR son funciones de tal forma que su soporte es 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 $+ : RG \times RG \to R$ de tal forma que si $\alpha, \beta \in RG$ entonces $(\alpha+\beta)(g) := \alpha(g)+\beta(g)$ para todo g elemento de G . Similarmente podemos definir la operación producto en RG como $\cdot : RG \times RG \to R$ 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 puede definir a un grupo-anillo.

Definición 1. *El conjunto RG con las operaciones + y · 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* $grupo - algebradeGsobreR$

Ahora se procede a hacer 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 homomorfis entre G y* G_1.

Demostración. Considérese la función $i : G \to RG$ 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 $\alpha \neq beta$ por definición si $x \neq y$ Ahora se probará que i es un homomorfismo de grupos, nótese que $i(xy) = \gamma$, donde $\gamma(xy) = 1$ y $\gamma(g) = 0$ si $g \neq xy$, pero $i(x)i(y) = \alpha\beta$ 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 $h = y$ y en $u = xy$ la función vale 1 así que $i(x)i(y) = i(xy)$. $\square$

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 $v : R \to RG$ tal que $v(r) = \beta$ donde $\beta(g) = r$ 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. $\square$

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 defición 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. $\square$

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

La clausura de la operación + se sigue directamente de la definición vale la pena notar que para realizar esta prueba se uso simplemente 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, a hora 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) $(\alpha+\beta)\gamma=\left(\sum_{g\in G}(a_g+b_g)g\right)\left(\sum_{g\in G} c_g g\right)=\sum_{g,h\in G}(a_g+b_g)c_h gh=\sum_{g,h\in G} a_g c_h gh+\sum_{g,h\in G} b_g c_h gh=\alpha\gamma+\beta\gamma$

□

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

Y con esto conluye 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 homomorfismo, 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 $f : G \to A$ tal que $f(gh) = f(g)f(h)$ para cualquier $g, h \in G$, existe un único homomorfismo de anillos $f^* : RG \to A$, 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:*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "i"'] & A \\ RG \arrow[ur, dashed, "f^*"'] & \end{tikzcd}$$

De hecho la proposición anterior se puede utilizar como una defición 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 $\nu : G \to X$ 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 $f : G \to A$ que satisface $f(gh) = f(g)f(h)$ para todo $g, h \in G$, existe un único homomorfismo $R-lineal$ $f^* : X \to A$ tal que el siguiente diagrama es conmutativo:*

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\nu"'] & A \\ X \arrow[ur, dashed, "f^*"'] & \end{tikzcd}$$

Entonces $X \simeq RG$

Demostración. Considérese la función $f^* : RG \to A$ 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 $f^*(r\alpha) = \sum_{g\in G} ra_g f(g) = r\sum_{g\in G} a_g f(g) = rf^*(\alpha)$ 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. $\square$

De la proposción 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 $f : G \to H$ un homomorfismo de grupos. Entonces, existe un unico homomorfismo de anillos $f^* : RG \to RH$ 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. $\square$

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

Definición 3. *El homomorfismo $\epsilon : RG \to R$ 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 $*: RG \to RG$ 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 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. *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.

$\square$

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 $\sum_{i,j} r_{ij} q_i h_j = \sum_i \left(\sum_j r_{ij} q_i\right)$. En la igualdad anterior se puede observar que como $h_j \neq 1$ entonces necesariamente el lado izquierdo de la ecuación tienen distinto 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 $g = q_i h_j$ 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.

$\square$

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 $Ker(\omega^*) = \Delta(G,H)$ $\square$

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.

$\square$

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

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

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

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

Demostración: Se debe probar dos cosas:

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

$$g_1g_2 - 1 = g_1(g_2 - 1) + (g_2 - 1) \in I$$

por lo tanto $g_1g_2 \in \nabla(I)$

(ii) Si $g\$in\nabla(I)$ entonces $g^{-1} - 1 = g^{-1}(1 - g) \in I$ de donde se sigue que $g^{-1} \in \nabla(I)$

$\square$

Lema. *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 $gig^{-1} \in I$.

$\square$

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 alli, 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 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 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 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. *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 $Ann_d(\Delta(G,H)) = \{0\}$ entonces sea $\alpha = \sum_{g\in G} a_g g \in RG$, $\alpha \in Ann_d(\Delta(G,H))$ entonces

$$\begin{aligned}
(h-1)\alpha &= 0 \forall h \in H && (2.7)\\
h\alpha - \alpha &= 0 && (2.8)\\
\sum_{g\in G} a_g a h &= \sum_{g\in G} a_g g && (2.9)
\end{aligned}$$

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 alli que se de la siguiente igualdad:

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

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.

$\square$Del

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 $Ker(x) = a\omega^*\hat{G} = a|G| = 0$

$\square$

Lema. *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 $J \subset Ann_d(J)$ $\square$

Lema. *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. $\square$

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

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)