



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
<b>1. CONCEPTOS PRELIMINARES</b>	<b>1</b>
1.1. Antecedentes . . . . .	1
1.2. Teoría de grupos . . . . .	1
1.3. Anillos, Módulos y Álgebras . . . . .	1
<b>2. GRUPO-ANILLOS</b>	<b>3</b>
2.1. Hechos Básicos De Los Grupo-Anillos . . . . .	3
2.2. Ideales de aumento . . . . .	11
2.3. Semisimplicidad . . . . .	17
2.4. Grupo-Algebras de grupos abelianos . . . . .	23
CONCLUSIONES	33
RECOMENDACIONES	35
BIBLIOGRAFÍA	37



# LISTA DE SÍMBOLOS

Símbolo	Significado
$x^n$	cancelación de $x$ al valor $n$
$E^c$	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
$\emptyset$	conjunto vacío
$\infty$	infinito
$\ln$	logaritmo natural
$(m, n)$	máximo común divisor entre $m$ y $n$
$\frac{d^n}{dx^n}$	$n$ -ésima derivada respecto de $x$
$\notin$	no pertenencia
$\forall$	para todo
$\in$	pertenencia
$\frac{d}{dx}$	primera derivada respecto de $x$
$\prod$	productoria
$\Leftrightarrow$	si y sólo si
$(a_n)_{n \in \mathbb{N}}$	sucesión de $a_n$
$\sum$	sumatoria
$ \cdot $	valor absoluto
$[\cdot] _{x=m}$	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 tesis.

## **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  $RG := \{\alpha | \alpha: G \rightarrow R, |\text{sop}(\alpha)| < \infty\}$  donde  $\text{sop}(\alpha) := \{g \in G : \alpha(g) \neq 0\}$ , a el conjunto  $\text{sop}(\alpha)$  se le llama el soporte de  $\alpha$ . 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  $+: RG \times RG \rightarrow R$  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  $\cdot: RG \times RG \rightarrow R$  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  $i: G \rightarrow RG$  tal que  $x \mapsto \alpha$  donde  $\alpha(x) = 1$  y  $\alpha(g) = 0$  si  $g \neq x$ . Con la identificación anterior es fácil notar que  $i$  es una función inyectiva. En efecto, si  $x, y \in G$  entonces  $i(x) = \alpha$ ,  $i(y) = \beta$ , pero  $\alpha \neq \beta$  si  $x \neq y$ , por definición. Ahora se probará que  $i$  es un homomorfismo de grupos. Nótese que  $i(xy) = \gamma$ , donde  $\gamma(xy) = 1$  y  $\gamma(g) = 0$  si  $g \neq xy$ . Por otro lado,  $i(x)i(y) = \alpha\beta$  donde  $(\alpha\beta)(u) = \sum_{gh=u} \alpha(g)\beta(h)$ , pero el producto  $\alpha(g)\beta(h)$  se anula a menos que  $g = x$  y  $h = y$ , en cuyo caso la función vale 1, con lo que se ha demostrado 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  $v: R \rightarrow RG$  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  $\gamma$  y  $\beta$  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 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  $\gamma$  y  $\alpha$  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. 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

$$\alpha = \sum_{g \in G} a_g g \quad (2.1)$$

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

*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:

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

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

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

La clausura de la operación  $+$  se sigue directamente de la definición. Vale la pena notar que para realizar esta prueba se usó 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:

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

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

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

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:

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

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

Y con esto concluye la prueba.  $\square$

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  $\text{rango}(RG) = |G|$

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

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ \downarrow i & \searrow f^* & \\ RG & & \end{array}$$

*Demostración.* Considérese la función  $f^*: RG \rightarrow A$  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.  $\square$

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  $f: G \rightarrow H$  un homomorfismo de grupos. Entonces, existe un único homomorfismo de anillos  $f^*: RG \rightarrow RH$  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 (monomorfismo)*

*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.  $\square$

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  $\nu: G \rightarrow X$  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  $f: G \rightarrow A$  que satisface  $f(gh) = f(g)f(h)$  para todo  $g, h \in G$ , existe un único homomorfismo  $R$ -lineal  $f^*: X \rightarrow A$  tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} G & \xrightarrow{f} & A \\ \nu \downarrow & \nearrow f^* & \\ X & & \end{array}$$

Entonces  $X \simeq RG$

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

$$\begin{array}{ccccc} & & X & & \\ & \nearrow \nu & \vdots i^* & \searrow I_X & \\ & & RG & & \\ \nearrow i & & & & \searrow \nu^* \\ G & \xrightarrow{\nu} & X & & \end{array}$$

$\square$

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

**Definición 3.** El homomorfismo  $\epsilon: RG \rightarrow R$  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  $\alpha$  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 es 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  $*$ :  $RG \rightarrow RG$  definida por

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

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

## 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  $RG$ . Esta 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,

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

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

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

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

**Caso Base:** Nótese que el menor caso sucede en  $r = 2$ . Por lo tanto sea  $h \in H$  entonces  $h - 1 = s_1^{\epsilon_1} s_2^{\epsilon_2} - 1 = s_1^{\epsilon_1} (s_2^{\epsilon_2} - 1) + (s_1^{\epsilon_1} - 1) \in (S)$  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 una 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  $\Delta_R(G, H)$ .

**Independencia 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 describir como  $\sum_{i,j} r_{ij} q_i h_j = \sum_i \left( \sum_j r_{ij} q_i \right)$ . En la igualdad anterior se puede observar que como  $h_j \neq 1$  entonces necesariamente el lado izquierdo de la ecuación tienen distinto soporte que el lado derecho, por lo tanto ambos deben ser igual a cero, pero los elementos de  $G$  son linealmente independientes sobre  $R$  entonces  $r_{ij} = 0$  para todo  $i, j$ .

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

*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  $H \triangleleft G$  entonces el homomorfismo canónico  $\omega : G \rightarrow G/H$  puede ser extendido a un epimorfismo, a saber

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

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*

$$\text{Ker}(\omega^*) = \Delta(G, H)$$

*Demostración.* Considérese de nuevo  $\mathcal{T}$  el transversal de  $H$  en  $G$ . Entonces, cada elemento  $\alpha \in RG$  se puede escribir como  $\alpha = \sum_i i, j r_{ij} q_i h_j$ ,  $r_{ij} \in R$ ,  $q_i \in \mathcal{T}$ ,  $h_i \in H$ . Si se denota  $\bar{q}_i = \omega(q_i)$  entonces se tiene

$$\omega^*(\alpha) = \sum_i \left( \sum_j r_{ij} \right) \bar{q}_i$$

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

$$\alpha = \sum_i \left( \sum_j r_{ij} \right) \bar{q}_i \quad (2.5)$$

$$= \sum_{ij} r_{ij} q_i (h_j - 1) \in \Delta(G, H) \quad (2.6)$$

Con lo cual se tiene que  $\text{Ker}(\omega^*) \subset \Delta(G, H)$ . El hecho que  $\Delta(G, H) \subset \text{Ker}(\omega^*)$  es trivial, por lo tanto  $\text{Ker}(\omega^*) = \Delta(G, H)$   $\square$

**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  $\text{Ker}(\omega^*) = \Delta(G, H)$  entonces por el primer teorema de isomorfía  $\frac{RG}{\Delta(G, H)} \simeq \text{Im}(\omega^*)$  pero como  $\omega^*$  es sobreyectiva entonces  $\text{Im}(\omega^*) = R(G/H)$  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 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  $g^{-1} \in \nabla(I)$   $\square$

**Lema 3.** Si  $I$  es un ideal bilateral entonces  $\nabla(I) \triangleleft G$

*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  $(gi - 1) \in I$  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 allí, por lo tanto  $x = h_j$ . De lo anterior es inmediato que  $\nabla(\Delta(G, H)) \subset H$ . La otra contención es trivial.  $\square$

Según lo expuesto en la proposición anterior pareciera ser cierto que  $\nabla$  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 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  $H \triangleleft G$  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

$$(h - 1)\alpha = 0 \quad \text{para cada } h \in H \quad (2.7)$$

$$h\alpha - \alpha = 0 \quad (2.8)$$

$$\sum_{g \in G} a_g ah = \sum_{g \in G} a_g g \quad (2.9)$$

De la última ecuación se aprecia que  $hg \in \text{sop}(\alpha)$  siempre y cuando  $g \in \text{sop}(\alpha)$ , pero  $\text{sop}(\alpha)$  es finito, por tanto  $H$  es finito. De nuevo analizando la ecuación 2.9 se deduce que dado  $g_0 \in \text{sop}(\alpha)$  entonces  $hg_0 \in \text{sop}(\alpha)$  para cualquier  $h$  elemento de  $H$ . De allí que se de la siguiente igualdad:

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

Lo anterior muestra que si  $H$  es finito entonces  $\text{Ann}_d(\Delta(G, H)) \subset \hat{H}RG$ . 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  $\hat{H}RG \subset \text{Ann}_d(\Delta(G, H))$

Por último si  $H \triangleleft G$  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 allí se sigue fácilmente la conclusión.  $\square$

Del lema anterior se sigue el siguiente corolario.

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

- (i)  $\text{Ann}_i(\Delta(G)) = \text{Ann}_d(\Delta(G)) = R \cdot \hat{H}$
- (ii)  $\text{Ann}_d(\Delta(G)) \cap \Delta(G) = \{a\hat{G} : a \in R, a|G| = 0\}$

*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  $x \in \text{Ann}_d(\Delta G) \cap \Delta G$  entonces  $x = a \sum_{g \in G} g$  y además  $x \in \text{Ker}(\omega^*)$  por tanto  $\text{Ker}(x) = a\omega^*\hat{G} = a|G| = 0$   $\square$

**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  $J \subset \text{Ann}_d(I)$*

*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  $x \in \text{Ann}_d(I)$  y por consiguiente  $J \subset \text{Ann}_d(I)$   $\square$

**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  $\Delta G$  el núcleo de  $\epsilon$  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  $R$

*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  $R$ -módulo.<sup>1</sup> Considérese  $M$  como  $RG$ -módulo, tal que  $M \in RG$ , entonces existe  $N$  como  $R$ -módulo tal que

$$RG = M \oplus N$$

Sea  $\pi: RG \rightarrow M$  la proyección canónica asociada con la suma directa. Se define  $\pi^*: RG \rightarrow M$  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  $\pi^*$  es un  $RG$ -homomorfismo tal que  $(\pi^*)^2 = \pi^*$  y  $M = \text{Im}(\pi^*)$ , lo cual se muestra en dos partes a continuación:

#### Homomorfismo:

Basta demostrar que  $\pi^*(ax) = a\pi^*(x)$  para cada  $a, g \in G$ , ya que  $\pi^*$  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  $RG$ -módulo, así que  $\pi(gm) = gm$  y por lo tanto

---

<sup>1</sup>Recordar que esto es por una propiedad de anillos que debo poner en el capítulo 1



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

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  $RG = M \oplus ker(\pi^*)$   $\square$

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 un 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  $I_i$ ,  $1 \leq i \leq r$

Se ha hecho énfasis en este resultado, ya que en el siguiente capítulo 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  $\text{car}(K) \nmid |G|$ . Entonces:

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

$$\text{ss y } n_1^2 + n_2^2 + \dots + n_r^2 = |G|$$

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

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

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

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

de donde se sigue 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  $kd_i a_i = 0$  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.  $\square$

## 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  $\text{car}(K) \nmid |G|$ . 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  $G = \langle a : a^n = 1 \rangle$  y que  $K$  es un campo tal que  $\text{car}(K) \nmid |G|$ . Considérese la función  $\phi: K[X] \rightarrow KG$  dada por

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

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

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

donde  $\text{ker}(\phi) = \{f \in K[X] : f(a) = 0\}$ . Como  $K[X]$  es un dominio<sup>2</sup> de ideales principales se deduce que  $\text{Ker}(\phi)$  es un ideal generado por el polinomio mónico  $f_0$ , de menor grado posible, tal que  $f_0(a) = 0$ .

---

<sup>2</sup>poner esto en el capítulo uno y hacer referencia

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  $\{1, a, a^2, \dots, a^r\}$  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 <sup>3</sup> 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  $(X + (f_1), \dots, X + (f_t))$ .

Considérese  $\zeta_i$  una raíz de  $f_i$ ,  $1 \leq i \leq t$ . Entonces, se tiene  $\frac{K[X]}{(f_i)} \simeq K(\zeta_i)$ . Por lo tanto

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

Como todos los elementos  $\zeta_i$ ,  $1 \leq i \leq t$  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  $(\zeta_1, \zeta_2, \dots, \zeta_t)$

---

<sup>3</sup>tambien en la parte inicial y luego referencia a el

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

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

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

de esta forma si  $\zeta$  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  $G = \langle a: a^6 = 1 \rangle$  y  $K = \mathbb{Q}$ . La descomposición de  $X^6 - 1$  en  $\mathbb{Q}[X]$  es

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

entonces se obtiene

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

donde  $\frac{-1+i\sqrt{3}}{2}$  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  $\Phi_d$ , es el producto  $\Phi_d = \prod_j (x - \zeta_j)$ , donde  $\zeta_j$  hace el recorrido por todas las raíces primitivas de la unidad de orden  $d$ . También es conocido que  $X^n - 1 = \prod_{d|n} \Phi_d$ , es decir que  $X^n - 1$  se puede expresar como el producto de todos los polinomios ciclotómicos  $\Phi_d$  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  $\Phi_d$  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  $\zeta_{d_i}$  denota una raíz de  $f_{d_i}$ ,  $1 \leq i \leq a_d$ . Para un  $d$  fijo, todos los elementos  $\zeta_{d_i}$  son raíces primitivas de la unidad de orden  $d$ , por lo tanto, todos los campos de la forma  $K(\zeta_{d_i})$ ,  $1 \leq i \leq a_d$  son iguales y se puede escribir simplemente

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

donde  $\zeta_d$  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  $\text{grad}(f_{d_i}) = [K(\zeta_d) : K]$ , 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  $\Phi_d$ , se tiene

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

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

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

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

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

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  $\text{char}(K) \nmid n$ . Entonces*

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

donde  $\zeta_d$  es una raíz primitiva de la unidad de orden  $d$  y  $a_d = \frac{n_d}{[K(\zeta_d):K]}$ . En esta 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  $M_{n,\gamma} = \{g : (g, h) \in \text{sop}(\gamma)\}$ . y la función  $f: R(G \times H) \rightarrow (RG)H$  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  $\gamma_1, \gamma_2 \in R(G \times H)$ , entonces haciendo la operat

toria:

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

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

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

y por el otro lado se tiene:

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

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  $\gamma \in R(G \times H)$ ,  $\gamma = \sum_{g \in G, h \in H} a_{gh}(g, h)$  tal que  $f(\gamma) = \sum_{h \in H} \alpha_h h = 0$ ,  $\alpha_h = \sum_{g \in M_h, \gamma = a_{gh}h}$ , 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  $\alpha_h$ . Con lo que concluye la prueba.  $\square$

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

Por otro lado, se tiene:

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

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

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

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

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

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

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 <sup>4</sup> de los grupos finitos abelianos para escribir  $G = G_1 x H$  donde  $H$  es generado y  $|G_1| = n_1 < n$ . Por hipótesis de inducción se puede escribir

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

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

---

<sup>4</sup>poner en capitulo 1

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

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

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

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

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

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

□

# 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)** 3<sup>a</sup> ed. (International Series in Pure and Applied Mathematics)
  
- [2] Apellido, Nombre. **Titulo**  $n$ -sima ed. (Editorial)