ANILLOS DE GRUPO LOCALES

JHAN CARLOS BARAJAS AVILA

UNIVERSIDAD INDUSTRIAL DE SANTANDER

FACULTAD DE CIENCIAS

ESCUELA DE MATEMÁTICAS

BUCARAMANGA

2024

ANILLOS DE GRUPO LOCALES

JHAN CARLOS BARAJAS AVILA

Trabajo de Grado para optar al título de
Matemático

Director
Alexander Holguín Villa
Doctor en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2024

DEDICATORIA

Dedicado a mis padres, Margarita Avila y Carlos Barajas. Este logro no habría sido posible sin su apoyo incondicional, ustedes son mi más grande inspiración.

AGRADECIMIENTOS

Quisiera agradecer en primer lugar a Dios, por brindarme su amor, fuerza y sabiduría para no desfallecer y poder llegar hasta aquí.

Agradecer a mis padres, Margarita y Carlos por creer en mí, incluso cuando yo lo dejé de hacer, con su amor y sacrificio he podido culminar uno de mis sueños, por brindarme todo lo necesario y darme el ejemplo de ser una buena persona, siempre mostrándome el verdadero camino, el camino de Dios, los amo con todo mi corazón.

Quisiera expresar mi más profundo agradecimiento al profesor Alexander Holguín Villa, por su paciencia y dedicación por este trabajo, sumando su experiencia y conocimiento. Su disposición y su fe en mí han sido vitales para culminar esta tesis.

Quiero agradecer a mis familiares, en especial a mis hermanos Diana, Gerson y Laura, por apoyarme en las buenas y en las malas, así mismo, agradecer a mis amigos que me acompañaron y me apoyaron en este largo camino, a todos, mil gracias.

CONTENIDO

RESUMEN

TÍTULO: ANILLOS DE GRUPO LOCALES [*]

AUTOR: JHAN CARLOS BARAJAS AVILA [**]

PALABRAS CLAVE: ANILLOS DE GRUPO, ANILLOS LOCALES.

DESCRIPCIÓN:

Un anillo es llamado local si tiene exactamente un ideal maximal y en este caso coincide con el radical de Jacobson del anillo. Muchos problemas del álgebra conmutativa y la geometría algebraica pueden reducirse al caso cuando el anillo es local, como por ejemplo a menudo un anillo local surge de la localización de un anillo en un ideal primo. Se busca llevar esta noción de anillo local a la estructura algebraica de interés *anillo de grupo*, donde se observarán las caracterizaciones del anillo y del grupo y así determinar cuándo es un anillo local.

El trabajo consta de cuatro capítulos. En el primer capítulo se abarcan los conceptos preliminares para el desarrollo del tema principal, en el segundo capítulo, se estudian la propiedades y resultados de la estructura algebraica de interés, los anillos de grupo, en el tercer capítulo se introduce el concepto de localización y el concepto de localidad en el contexto anillo teórico, por último en el cuarto capítulo, se presentan las condiciones necesarias y suficientes tanto del anillo como del grupo, que garantizan cuándo un anillo de grupo es local, asumiendo en todo momento que los anillos son no nulos y asociativos con identidad o unidad.

---

[*] Trabajo de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Alexander Holguín Villa, Doctor en Matemáticas

ABSTRACT

TITLE: LOCAL GROUP RINGS [*]

AUTHOR: JHAN CARLOS BARAJAS AVILA [**]

KEYWORDS: GROUP RINGS, LOCAL RINGS.

DESCRIPTION:

A ring is called local if it has exactly one maximal ideal and in this case coincides with the Jacobson radical of the ring. Many problems in commutative algebra and algebraic geometry can be reduced to the case when the ring is local, for instance a local ring often arises from the localization of a ring in a prime ideal. The aim is to bring the notion of a local ring to the algebraic structure *group ring* where will observe the characterizations of the ring and the group and thus determine when it is a local ring.

The monograph consists of four chapters. The first covers the preliminary concepts for the development of the main theme, in the second chapter, the properties and results of the algebraic structure of interest, group rings, are studied, in the third chapter the concept of localization and the concept of locality in the theoretical ring context are introduced, finally, in the last chapter, the necessary and sufficient conditions of both the ring and the group are presented, which guarantee when a group ring is local, assuming at all times that the rings are non-zero and associative with identity or unity.

---

[*] Bachelor Thesis

[**] Facultad de Ciencias. Escuela de Matemáticas. Director: Alexander Holguín Villa, Doctor en Matemáticas.

INTRODUCCIÓN

En la práctica, un anillo local conmutativo a menudo surge como resultado de la localización de un anillo en un ideal primo. El concepto de anillos locales fue introducido por W. Krull en 1938 bajo el nombre "*Stellenringe*" , aquí él definió *Stellenringe* como un anillo Noetheriano con un solo ideal maximal [*] , se eligió el nombre *Stellenring* porque estos anillos a menudo se asocian con puntos en variedades algebraicas y analíticas, C. Chevalley los renombró como anillos locales "*local rings*", dado que un anillo asociado con un punto en una variedad proporciona propiedades locales de la variedad, [1].

En Teoría de Anillos, los anillos locales son aquellos que son comparativamente simples y sirven para describir lo que se llama "comportamiento local". El álgebra local es la rama del álgebra conmutativa que estudia los anillos locales conmutativos y sus módulos.

El concepto de anillo de grupo es relativamente antiguo, aparece implícitamente en un artículo de A. Caley en 1854, que es considerado el primer trabajo en teoría abstracta de grupos. Los anillos de grupo ganaron importancia por derecho propio luego de la inclusión de preguntas en anillos de grupo en la famosa lista de problemas de I. Kaplansky, otros hechos importantes para estimular el área fueron, el artículo de I. G. Connell considerando cuestiones de teoría de anillos en el contexto de los anillos de grupo, la inclusión de capítulos sobre anillos de grupo en los libros sobre teoría de anillos de J. Lambek y P. Ribenboim así como la publicación completa del primer libro dedicado al tema, por

---

[*] Un anillo Noetheriano es un anillo conmutativo con unidad donde todo ideal es finitamente generado

[1] Masayoshi NAGATA. "Local rings". En: *Interscience Tracts in Pure and Appl. Math.* (1962).

D. S. Passman, para más detalles ver [[2], Chap. 3, pág. 129] y las referencias indicadas allí.

En 1970 T. Gulliksen, P. Ribenboim y T. M. Viswanathan publicaron el artículo "*An elementary note on group rings*", [3], en esta nota se derivan algunos resultados elementales en anillos de grupo sobre anillos conmutativos, asumiendo también en la mayoría de los casos que el grupo es abeliano, siendo uno de ellos de cuándo el anillo de grupo es local.

El presente trabajo está enfocado en el estudio de los anillos de grupo locales, teniendo como principal referencia el artículo de W. K. Nicholson [4] "*LOCAL GROUP RINGS*", en el cual el autor se propuso generalizar algunos resultados de Gulliksen, Ribenboim y Viswanathan, donde el anillo de coeficientes fue tomado conmutativo.

---

[2] César POLCINO MILIES y Sudarshan K SEHGAL. *An introduction to group rings*. 1st Edition. Vol. 1. Springer Science & Business Media, 2002.

[3] Tor GULLIKSEN, Paulo RIBENBOIM y T.M VISWANATHAN. "An elementary note on group-rings." En: (1970).

[4] W. K. NICHOLSON. "Local group rings". En: *CMB* 15.1 (1972), 137 bibrangedash 138.

1. PRELIMINARES

En este capítulo se presentan algunos conceptos de la teoría de grupos, la teoría de anillos y las nociones básicas sobre módulos, que se usarán a lo largo de este trabajo. Para detalles adicionales y demostraciones de algunos resultados, que sólo serán enunciados, consultar [5], [6], [7], [2].

1.1. GRUPOS

En álgebra abstracta, un grupo es una estructura algebraica con una operación binaria, con muchas propiedades y resultados vitales para este trabajo.

Definición 1.1.1. *Un* **grupo** G *es un conjunto no vacío con una operación binaria (denotada por* $\cdot$*), tal que para todo* $a, b, c \in G$ *se cumplen las siguientes condiciones:*

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
2. *Existe en* G *un elemento "neutro", el cual se denotará por* e*, tal que para todo* $a \in G$ *se cumple que* $a \cdot e = e \cdot a = a$.
3. *Para todo* $a \in G$*, existe un elemento "inverso"*$a^{-1} \in G$ *tal que* $a \cdot a^{-1} = a^{-1} \cdot a = e$.

En adelante, por simplicidad $a \cdot b$ se denotará por ab. Si además para todo $a, b \in G$ se cumple que $ab = ba$, entonces se dirá que G es un grupo abeliano. Si el conjunto G es finito, entonces el número de elementos de G es llamado su **orden** y es denotado por $|G|$.

---

[5] Michael ATIYAH. *Introduction to commutative algebra*. 1st Edition. CRC Press, 2018.

[6] Phani Bhushan BHATTACHARYA, Surender Kumar JAIN y SR NAGPAUL. *Basic abstract algebra*. 2nd Edition. Cambridge University Press, 1994.

[7] J. GALLIAN. *Contemporary abstract algebra*. 8th Edition. North-Holland Publishing Company, 2021.

El orden de un elemento $a \in G$ es el menor entero positivo n tal que $a^n = e$, si no existe tal entero n, se dice que a tiene orden infinito, el orden de un elemento a se denota por $ord(a)$.

Ejemplo 1.1.2. *Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$, son grupos abelianos con la operación de suma usual.*

El conjunto de los enteros $\mathbb{Z}$ con la multiplicación usual no es grupo ya que no satisface la propiedad 3 en la definición anterior. Por ejemplo, 2 no tiene inverso multiplicativo, pues no existe $a \in \mathbb{Z}$ tal que $2a = 1$.

Un subconjunto no vacío H de un grupo G es llamado **subgrupo** de G, si H mismo es un grupo bajo la operación de G. Se usa la notación $H \preceq G$ para indicar que H es un subgrupo de G y $S(G)$ para denotar el conjunto de subgrupos de G. Además H es un **subgrupo normal** de G si para todo $x \in G$, $x^{-1}Hx = H$, que como es usual se denota por $H \lhd G$.

Sea H un subgrupo de un grupo G, dado un elemento $a \in G$, a los subconjuntos

$$aH = \{ah : h \in H\} \quad \text{y} \quad Ha = \{ha : h \in H\},$$

son llamados **clase lateral a izquierda y derecha** (respectivamente) del subgrupo H, determinadas por el elemento a, donde a es el **representante** de la clase.

Ejemplo 1.1.3. *En este trabajo es de interés, el grupo de los cuaternios de orden 8, el cual tiene la siguiente presentación:*

$$\mathcal{Q}_8 = \langle a, b : a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} \rangle,$$

y por extensión es,

$$\mathcal{Q}_8 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\},$$

que además de ser finito y no abeliano, tiene la característica de que todos sus subgrupos son ***normales****, es decir, si H es subgrupo de $\mathcal{Q}_8$, entonces para todo $x \in \mathcal{Q}_8$, $x^{-1}Hx = H$.*

Cabe recordar que si G es un grupo, entonces se define el centro de G por,

$$\mathcal{Z}(G) = \{x \in G : xg = gx, \text{ para todo } g \in G\};$$

se tiene que $\mathcal{Z}(G)$ es subgrupo de G, más aún, $\mathcal{Z}(G)$ es subgrupo normal de G.

Sea H un subgrupo normal de un grupo G, entonces toda clase lateral a izquierda de H en G, también es clase lateral a derecha y viceversa, se denota por G/H al conjunto de todas las clases laterales de H en G, es decir,

$$G/H = \{gH : g \in G\};$$

es claro que el conjunto G/H es grupo bajo la siguiente operación,

$$(aH)(bH) = (ab)H; \quad a, b \in G$$

y es llamado el **grupo cociente** de G por H

Definición 1.1.4. *Un grupo G es llamado* **localmente finito** *si todo subgrupo* **finitamente generado** *de G es finito, además, si p es un número primo, al grupo finito G se le llama p***-grupo** *si su orden es una potencia de p. Finalmente, si todo elemento de G tiene orden p, G es llamado p***-grupo abeliano elemental***.*

Es claro ver que para todo $x \in \mathcal{Q}_8$, $x^{2^k} = 1$, por lo tanto $\mathcal{Q}_8$ es un 2*-grupo*.

Definición 1.1.5. *Un* **homomorfismo** *f de un grupo G en un grupo H es una función de G en H, que preserva las operaciones, es decir, $f(ab) = f(a)f(b)$, para todo $a, b \in G$. Si además f es inyectiva (resp. sobreyectiva), se le llama* **monomorfismo** *(resp.* **epimorfismo***). En el caso de f ser un epimorfismo, suele denotarse por $f : G \twoheadrightarrow H$. Finalmente, si*

f es a la vez monomorfismo y epimorfismo, se le denomina a f ***isomorfismo****, y en este caso se dirá que G y H son grupos isomorfos, denotándolo por $G \cong H$.*

Sea $f : G \to H$ un homomorfimo de grupos, se definen los conjuntos *kernel* e *imagen* de f respectivamente por,

$$ker_f = \{g \in G : f(g) = e_h\} \quad \text{y} \quad Im_f = \{f(g) : g \in G\}.$$

Algunas propiedades de los homomorfismos de grupos serán enunciados a continuación.

Proposición 1.1.6. *Sean $f : G \to H$ un homomorfismo de grupos, e_G y e_H los neutros en H y G respectivamente. Entonces;*

1. $f(e_G) = e_H$
2. $f(g^{-1}) = f(g)^{-1}$
3. *Si $n \in \mathbb{Z}$, entonces $f(g^n) = f(g)^n$*
4. $ker_f \lhd G$
5. *f es inyectiva si y sólo si $ker_f = \{e_G\}$*
6. $Im_f \preceq H$

Teorema 1.1.7. *Sea $f : G \to H$ un homomorfismo de grupos, entonces*

$$G/ker_f \cong Im_f.$$

En particular si f es un homomorfismo sobreyectivo (epimorfismo), entonces

$$G/ker_f \cong H.$$

1.2. ANILLOS

Muchos conjuntos están naturalmente dotados de dos operaciones binarias (suma y producto), como es el caso de los anillos, que es un concepto importante para el desarrollo de este trabajo. A continuación se presenta formalmente dicha noción y algunos resultados fundamentales en su estudio y de interés en este trabajo.

Definición 1.2.1. *Un* **anillo** R *es un conjunto con dos operaciones binarias (suma y producto) tales que:*

1. R *es un grupo abeliano con la suma.*

2. *El producto es asociativo y distributivo respecto a la suma, es decir,*

$$a(bc) = (ab)c \quad \textit{y} \quad a(b+c) = ab + ac, \;\; (a+b)c = ac + bc \;\; \forall\, a, b, c \in R.$$

Si además, $ab = ba$*, para todo* $a, b \in R$*,* R *es llamado un* **anillo conmutativo***. Por otro lado, si en* R *existe un elemento identidad* $1 = 1_R$*, tal que* $1x = x1 = x$*, para todo* $x \in R$*, se llama a* R **anillo con unidad o identidad.**

Ejemplo 1.2.2.

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *y* $\mathbb{C}$ *son anillos conmutativos con unidad con las operaciones suma y producto usuales.*

2. *Dado un anillo* R*, el conjunto de matrices cuadradas de tamaño* $n \times n$ *con* $n > 1$ *y coeficientes en* R*, denotado por* $M_n(R)$*, es un anillo (no conmutativo) con la suma y producto usuales. Si* R *tiene unidad* 1*, la unidad de* $M_n(R)$ *es* $1_{M_n(R)} = I_n$*, la matriz identidad de orden* n*.*

3. *Dado* $n \in \mathbb{N}$*, el conjunto* $\mathbb{Z}_n$ *de los enteros módulo* n*, es un anillo conmutativo con unidad, con la suma y el producto módulo* n*.*

4. *Sean $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ símbolos y el conjunto $\mathcal{H}_{\mathbb{R}}$ de todas las expresiones de la forma,*

$$x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k},$$

donde los coeficientes x_0, x_1, x_2, x_3 son números reales. Se define la suma componente a componente, es decir,

$$(x_0+x_1\boldsymbol{i}+x_2\boldsymbol{j}+x_3\boldsymbol{k})+(y_0+y_1\boldsymbol{i}+y_2\boldsymbol{j}+y_3\boldsymbol{k}) = (x_0+y_0)+(x_1+y_1)\boldsymbol{i}+(x_2+y_2)\boldsymbol{j}+(x_3+y_3)\boldsymbol{k}.$$

El producto está definido distributivamente, teniendo en cuenta las siguientes reglas para el producto entre los símbolos $\boldsymbol{i}, \boldsymbol{j}$ y $\boldsymbol{k}$:

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

Cálculos directos muestran que $\mathcal{H}_{\mathbb{R}}$, con las operaciones anteriores, es un anillo, llamado **anillo de cuaternios reales**, *además*

$$\mathcal{Q}_8 \cong \{1, -1, \boldsymbol{i}, -\boldsymbol{i}, \boldsymbol{j}, -\boldsymbol{j}, \boldsymbol{k}, -\boldsymbol{k}\}.$$

es un isomorfismo de grupos multiplicativos.

Algunos conceptos importantes en teoría de anillos y que serán de uso recurrente en este trabajo son los siguientes:

Definición 1.2.3.

1. *Sea R un anillo, al conjunto $\mathcal{U}(R)$ de elementos invertibles, como es usual se le llama conjunto de* **unidades** *de R. En el caso que R sea conmutativo, es claro que $\mathcal{U}(R)$ es un grupo multiplicativo.*

2. *Sea R un anillo conmutativo, $a \in R$ con $a \neq 0$ es llamado* **divisor cero***, si existe $b \in R$ con $b \neq 0$, tal que $ab = 0$. A un anillo conmutativo sin divisores cero, se le llama* **dominio entero***. En el caso que todo elemento no-cero de R sea invertible, se denomina a R* **anillo de división***, y si además, R es conmutativo, se le llama* **cuerpo***.*

3. *La* ***característica*** *de un anillo R es el menor entero positivo n tal que $na = 0$, para todo $a \in R$. Caso tal entero positivo no exista, se dice que R tiene característica cero. La característica de R se denotará por $car(R)$. Sea R un anillo con 1_R, es evidente que $car(R) = n$ si y sólo si $n \cdot 1_R = 0$, $n \in \mathbb{N}$, más aún, en el caso de R ser dominio entero o un cuerpo, la $car(R) = 0$ ó $car(R) = p$, donde p es un entero primo.*

4. *Un elemento a de un anillo R es llamado* **nilpotente** *si existe un entero $n > 0$ tal que $a^n = 0$, al conjunto de elementos nilpotentes se denota por η_R, es decir,*

$$\eta_R = \{a \in R : \text{ para algún } n > 0,\ a^n = 0, \}.$$

5. *Un elemento $x \in R$ es* **cuasi-regular***, si existe $y \in R$, tal que $x+y = xy$. Se Denotará al conjunto de elementos cuasi-regulares por $\mathcal{Q}_{reg}(R)$.*

En el Ejemplo 1.2.2, dado un cuaternio $\alpha = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$, se define su conjugado $\bar{\alpha}$ como $\bar{\alpha} = x_0 - x_1\boldsymbol{i} - x_2\boldsymbol{j} - x_3\boldsymbol{k}$ y su norma como $\|\alpha\| = \alpha\bar{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2$, se sigue que,

$$\|\alpha\beta\| = \|\alpha\|\|\beta\| = \|\beta\alpha\| \text{ y}$$

$$\|\alpha\| \geq 0, \|\alpha\| = 0 \text{ si y sólo si } \alpha = 0.$$

Ahora, para $\alpha \in \mathcal{H}_{\mathbb{R}}$ diferente de cero, se puede definir $\alpha^{-1} = \dfrac{\bar{\alpha}}{\|\alpha\|}$, y así,

$$\alpha^{-1}\alpha = \frac{\bar{\alpha}}{\|\alpha\|}\alpha = \frac{\|\alpha\|}{\|\alpha\|} = 1 = \frac{\|\alpha\|}{\|\alpha\|} = \alpha\frac{\bar{\alpha}}{\|\alpha\|} = \alpha\alpha^{-1},$$

es decir, todo elemento α diferente de cero en $\mathcal{H}_{\mathbb{R}}$ es invertible, y así $\mathcal{H}_{\mathbb{R}}$ es un anillo de división. Si tomamos los coeficientes en el cuerpo de los numero racionales $\mathbb{Q}$, se obtiene el anillo $\mathcal{H}_{\mathbb{Q}}$ de cuaternios racionales, el cual también es un anillo de division. De igual manera si se toma los coeficientes en el cuerpo de los complejos $\mathbb{C}$, se obtiene el anillo $\mathcal{H}_{\mathbb{C}}$, pero en este caso, $\mathcal{H}_{\mathbb{C}}$ no es un anillo de división, dado que, $\alpha = 1 + i\boldsymbol{k} \in \mathcal{H}_{\mathbb{C}}$, es no-cero, pero su norma $\|\alpha\| = 1 + i^2 = 0$.

Un subconjunto no vacío S de un anillo R es un **subanillo** de R, si S mismo es un anillo con las operaciones de R restrictas a S.

Existen algunos ejemplos de subanillos; por ejemplo, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ que, a su vez, es un subanillo de $\mathbb{C}$, además, ambos $\mathbb{Q}$ y $\mathbb{C}$ pueden considerarse subanillos de $\mathcal{H}_{\mathbb{R}}$.

El siguiente lema permite verificar cuándo un subconjunto no vacío S de R es un subanillo.

Lema 1.2.4. *Un subconjunto no vacío S de un anillo R es un subanillo de R si, y sólo si, se cumplen las siguientes condiciones:*

- *Dados $x, y \in S$, entonces $x - y \in S$,*
- *Dados $x, y \in S$, entonces $xy \in S$.*

El concepto de homomorfismo de anillos es en esencia el mismo que en el caso de grupos, excepto que ahora se involucran las dos operaciones del anillo.

Sean R y S anillos. Una aplicación $\phi : R \to S$ que preserva las operaciones, es decir, para todo $x, y \in R$:

1. $\phi(x + y) = \phi(x) + \phi(y)$,
2. $\phi(xy) = \phi(x)\phi(y)$;

es llamada un **homomorfismo de anillos**.

Si R y S son anillos con unidad 1_R y 1_S respectivamente, no es necesariamente cierto que $\phi(1_R) = 1_S$. En efecto, la aplicación $\phi : M_2(\mathbb{Q}) \to M_3(\mathbb{Q})$ dada por,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}, \tag{1}$$

es un homomorfismo de anillos y $\phi(I_2) \neq I_3$. Se puede demostrar que $\phi(1_R) = 1_S$, si S es un dominio entero o si ϕ es un **epimorfismo**, es decir, un homomorfismo sobreyectivo, el cual se denotará por, $\phi : R \twoheadrightarrow S$, [2, Pág. 75].
En caso de que ϕ sea inyectivo, se le llama a ϕ un **monomorfimo**, finalmente, ϕ es llamado un **isomorfismo**, si ϕ es a la vez un monomorfismo y un epimorfismo.

El concepto de ideal se debe a R. Dedekind, quién fue alumno de K. F. Gauss, quién lo introdujo mientras estudiaba la teoría de números algebraicos. L. Kronecker (1823-1891), alumno de E. Kummer, definió los ideales de polinomios como una herramienta importante para el estudio de la geometría algebraica, ésto motivo a que este concepto tuviera aplicaciones en otra ramas matemáticas.

Definición 1.2.5. *Un subanillo I de un anillo R, es llamado* **ideal izquierdo** *(resp. derecho), si $RI \subset I$ (resp. $IR \subset I$) y se denota por $I \preceq_l R$ (resp. $I \preceq_r R$).*

Finalmente, si I es la vez un ideal izquierdo y derecho, como es usual, será denominado **ideal bilateral** *de R y se denotará por $I \preceq R$. Los subconjuntos $\{0\}$ y R son siempre ideales de R, llamados ideales triviales, y los diferentes a éstos, se llaman ideales propios.*

Si R es un anillo **conmutativo**, el *ideal principal* generado por $a \in R$, es el conjunto, $\langle a \rangle = \{ra : r \in R\}$. Además, se tiene que si $a \in \mathcal{U}(R)$, entonces $\langle a \rangle = R$. Así mismo, si $I \preceq R$ contiene un elemento invertible u, sigue que $I = \langle u \rangle = R$. En particular, $\langle 1 \rangle = R$.

Teorema 1.2.6. *Sean R un anillo e I un subanillo de R. El conjunto de las clases laterales de I en R,*

$$R/I = \{r + I : r \in R\},$$

con las operaciones suma y producto dada respectivamente por,

$$+ : \big(s + I, t + I\big) \mapsto (s + t) + I \quad \textbf{y} \quad \cdot : \big(s + I, t + I\big) \mapsto st + I,$$

es un anillo si, y sólo si I es un ideal de R. R/I es llamado anillo factor o cociente de R por I.

Ejemplo 1.2.7.

1. *Sea a un elemento de un anillo R, entonces $Ra = \{xa : x \in R\}$ es ideal izquierdo de R, en este caso Ra es llamado el ideal izquierdo generado por a.*

2. *Si R es un anillo con unidad, entonces todo ideal del anillo de matrices $M_n(R)$ es de la forma $M_n(I)$, donde I es ideal de R.*

3. *Sean I, J ideales de un anillo R, entonces el conjunto*

$$I + J = \{x + y : x \in I, y \in J\}$$

es un ideal de R, llamado el ***ideal suma*** *de I y J.*

Sea D un anillo de división. Por el ejemplo anterior, los ideales de $M_n(D)$ son de la forma $M_n(I)$, donde I es ideal de D. Dado que los elementos no-cero en D son unidades, sigue que los únicos ideales son los triviales $\{0\}$ y D, en realidad se se ha demostrado la siguiente proposición.

Proposición 1.2.8. *Si D es un anillo de división, entonces $M_n(D)$ no tiene ideales no triviales.*

En el presente trabajo se hace uso del **Lema de Zorn**, por ello se presentarán algunos conceptos asociados.

Definición 1.2.9.

1. *Un* **orden parcial** *sobre un conjunto X es una relación "$\preceq$" en X, que es* **reflexiva, antisimétrica, y transitiva**. *Además, un conjunto con un orden parcial $(X, \preceq)$ es llamado* **conjunto parcialmente ordenado**.

2. *Una* **cadena** *$\mathcal{C}$ es un subconjunto del conjunto parcialmente ordenado $(X, \preceq)$, tal que para todo $a, b \in \mathcal{C}$, $a \preceq b$ o $b \preceq a$, es decir, en $\mathcal{C}$ todo par de elementos son comparables.*

3. *Un elemento $s \in X$ es una* **cota superior** *de $\mathcal{C}$, si $a \preceq s$ para todo $a \in \mathcal{C}$.*

4. *Un elemento $m \in X$ es* **maximal** *respecto a $\preceq$, si $m \preceq a$, $a \in X$, implica que $m = a$. En otras palabras, $m \in X$ es maximal respecto a $\preceq$, si no existe $a \in X$ tal que $m \preceq a$.*

El siguiente axioma de la teoría de conjuntos parcialmente ordenados es de uso habitual en matemáticas, y es conocido como **Lema de Zorn**, el cual es equivalente al *Axioma de Elección*, [[6], Pág. 211].

Lema 1.2.10. *Si toda cadena $\mathcal{C}$ en un conjunto parcialmente ordenado $(X, \preceq)$ tiene una cota superior en X, entonces $(X, \preceq)$ tiene un elemento maximal.*

El siguiente resultado es de uso frecuente en el estudio de anillos e ideales.

Teorema 1.2.11. *Sean $\phi : R \twoheadrightarrow T$ un epimorfismo de anillos y $N := K_\phi$ el kernel de ϕ, entonces $\Phi : I \mapsto \phi(I)$ define una correspondencia (1-1) del conjunto de ideales izquierdos (derechos o bilaterales) de R que contienen a N sobre el conjunto de los ideales izquierdos (derechos o bilaterales) de T respectivamente, correspondencia que preserva el orden, es decir, $I \subset J$ si y sólo si $\phi(I) \subset \phi(J)$.*

Note que si I es un ideal, se tiene asociado el epimorfismo canónico $\pi_I : R \twoheadrightarrow R/I$ y así, como consecuencia del teorema anterior, existe una correspondencia (1-1), preservando el orden, entre los conjuntos de ideales izquierdos (derechos o bilaterales) de R que contienen al $\ker_{\pi_I}$ y los de R/I. Más aún,

$$\ker_{\pi_I} = I \qquad \text{y} \qquad \pi_I(J) = \{\pi_I(a) : a \in J\} = \{a + I : a \in J\} = J/I.$$

Se ha probado el siguiente resultado, la cual es la versión más usada del **Teorema de Correspondencia**.

Corolario 1.2.12. *Si I es un ideal del anillo R, entonces todo ideal de R/I es de la forma $\bar{J} = J/I$, donde $J \supseteq I$ es un ideal de R.*

Note que, en particular, el Corolario 1.2.12 demuestra que si $\mathfrak{m}$ es un ideal propio del anillo R y ningún ideal (diferente a R) de R lo contiene propiamente, entonces el anillo cociente $R/\mathfrak{m}$ no tiene ideales no triviales, esto motiva los siguientes conceptos.

Definición 1.2.13. *Un ideal $\mathfrak{m}$ es un **ideal maximal** de un anillo R, si $\mathfrak{m} \neq \langle 1 \rangle$ y no existe un ideal I tal que $\mathfrak{m} \subset I \subset \langle 1 \rangle$. Un ideal propio $\mathfrak{p}$ es llamado **ideal primo**, si dados $a, b \in R$ y $ab \in \mathfrak{p}$, entonces $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.*

Se tiene la siguiente caracterización de ideales primos y maximales en el contexto conmutativo.

Proposición 1.2.14. *Sean R un anillo conmutativo con unidad 1_R y $\mathfrak{p}, \mathfrak{m}$ ideales de R,*

1. *$\mathfrak{p}$ es un ideal primo si y sólo si $R/\mathfrak{p}$ es un dominio entero,*

2. *$\mathfrak{m}$ es un ideal maximal si y sólo si $R/\mathfrak{m}$ es un cuerpo.*

Demostración.

1. Suponga que $R/\mathfrak{p}$ es un dominio entero y $ab \in \mathfrak{p}$. Entonces $(a+\mathfrak{p})(b+\mathfrak{p}) = ab+\mathfrak{p} = \mathfrak{p}$, es decir, el elemento cero de $R/\mathfrak{p}$, por lo tanto como $R/\mathfrak{p}$ es un dominio entero, $a + \mathfrak{p} = \mathfrak{p}$ o $b + \mathfrak{p} = \mathfrak{p}$, lo que quiere decir que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Así, $\mathfrak{p}$ es un ideal primo. Para probar la recíproca, observe que $R/\mathfrak{p}$ también es un anillo conmutativo con unidad, si se tiene que $\mathfrak{p}$ es un ideal primo, $(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p} = \mathfrak{p}$, entonces, $ab \in \mathfrak{p}$ y así, $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$, por lo cual $(a + \mathfrak{p})$ o $(b + \mathfrak{p})$ es cero en $R/\mathfrak{p}$.

2. Suponga que $R/\mathfrak{m}$ es un cuerpo y J es un ideal de R, tal que $\mathfrak{m} \subset J$. Sea $b \in J$ con $b \notin \mathfrak{m}$, entonces $b + \mathfrak{m}$ es un elemento distinto de cero de $R/\mathfrak{m}$ y, por lo tanto, existe un elemento $c + \mathfrak{m}$ en $R/\mathfrak{m}$ tal que $(b + \mathfrak{m})(c + \mathfrak{m}) = 1 + \mathfrak{m}$, la unidad de $R/\mathfrak{m}$. Dado que $b \in J$, se tiene que $bc \in J$. Dado que

$$1 + \mathfrak{m} = (b + \mathfrak{m})(c + \mathfrak{m}) = bc + \mathfrak{m},$$

se tiene que $1 - bc \in \mathfrak{m} \subset J$ y como $bc \in J$, entonces $1 \in J$, luego $R = J$ y se sigue que $\mathfrak{m}$ es un ideal maximal. Ahora suponga que $\mathfrak{m}$ es un ideal maximal y sea $b \in R \setminus \mathfrak{m}$. Es suficiente mostrar que $b + \mathfrak{m}$ es unidad en $R/\mathfrak{m}$. Considere el conjunto $J = \{br + m : r \in R, m \in \mathfrak{m}\}$. Note que si $x = br_1 + m_1$ y $y = br_2 + m_2$, entonces $x-y = b(r_1-r_2)+(m_1-m_2) \in J$ y además, si $s \in R$, entonces $sx = xs \in J$. Por otro lado, con $r = 0$, se tiene que $J \supseteq \mathfrak{m}$. Como $\mathfrak{m}$ es maximal, entonces $J = R$. Luego $1 \in J$ y así $1 = br' + m'$ para $r' \in R$ y $m' \in \mathfrak{m}$, por lo tanto,

$$1 + \mathfrak{m} = br' + m' + \mathfrak{m} = br' + \mathfrak{m} = (b + \mathfrak{m})(r' + \mathfrak{m}),$$

es decir, $b + \mathfrak{m} \in \mathcal{U}\big(R/\mathfrak{m}\big)$ y así $R/\mathfrak{m}$ es un cuerpo.

□

Observación 1.2.15.

1. *Si R es un anillo conmutativo con 1_R, sigue de la proposición anterior que todo ideal maximal $\mathfrak{m}$ es un ideal primo.*

2. *En $R = \mathbb{Z}[x]$, $\mathfrak{p} = \langle x \rangle$ es ideal primo, dado que $R/\mathfrak{p} \cong \mathbb{Z}$, que es dominio entero. Ahora bien, $\langle x \rangle \subset \langle x, 2 \rangle$, el ideal de todos los polinomios con coeficientes enteros con término constante par. En otras palabras, en general un ideal primo $\mathfrak{p}$ no necesariamente es un ideal maximal.*

Los ideales primos son fundamentales en el Álgebra Conmutativa, el siguiente teorema y sus corolarios aseguran que siempre se tiene un número suficiente de éstos.

Teorema 1.2.16. *Cada anillo $R \neq 0$ tiene al menos un ideal maximal.*

Demostración. Sea $(X, \subseteq)$ el conjunto parcialmente ordenado de todos los ideales propios de R; dado que $\{0\} \in X$, se tiene que X es diferente de vacío. Considere $\mathcal{C} = \{I_i\}_{i \in \Delta}$ una cadena de ideales en X y sea $I = \bigcup_{i \in \Delta} I_i$, entonces si $a, b \in I$, sigue que $a \in I_i$ y $b \in I_j$ para algunos $i, j \in \Delta$. Luego, suponiendo sin perdida de generalidad que $I_i \subseteq I_j$, sigue que $a - b \in I_j$ y así, $a - b \in I$. Es claro que $ra = ar \in I$, para todo $r \in R$ y por tanto I es ideal propio de R y así, $I \in X$ es una cota superior de $\mathcal{C}$, luego por el Lema de Zorn, X tiene un elemento maximal.

□

Proposición 1.2.17.

1. *Para todo ideal propio I de R existe un ideal maximal $\mathfrak{m}$ de R que lo contiene.*

2. *Todo elemento $a \in R \setminus \mathcal{U}(R)$ pertenece a un ideal maximal $\mathfrak{m}$.*

Demostración.

1. Dado que $I \neq R$, entonces $R/I \neq \{0\}$ y por el *Teorema* 1.2.16, R/I tiene al menos un ideal maximal $\bar{\mathfrak{m}}$ y se sigue del Corolario 1.2.12 que $\bar{\mathfrak{m}} = \mathfrak{m}/I$ con $I \subseteq \mathfrak{m} \preceq R$.

2. Como a no es unidad en R, entonces $\langle a \rangle \neq R$, sigue del ítem anterior, que existe un ideal maximal $\mathfrak{m}$, tal que $\langle a \rangle \subseteq \mathfrak{m}$.

□

En lo que sigue, se denotará por $Specm(R)$ al conjunto de ideales maximales del anillo R.

Definición 1.2.18. *El* **radical de Jacobson** *denotado por $J(R)$ está definido como la intersección de todos los ideales maximales izquierdos de R,*

$$J(R) = \bigcap_{\mathfrak{m} \in Specm(R)} \mathfrak{m}.$$

De la definición, es claro ver que el radical de Jacobson es un ideal izquierdo de R. Más aún, es un ideal bilateral.

Ejemplo 1.2.19. *Sea $\mathbb{Z}$ el anillo de los enteros. Los ideales maximales son de la forma $\langle p \rangle$, donde p es un número primo, por lo tanto*

$$J(\mathbb{Z}) = \bigcap \langle p \rangle = \{0\},$$

ya que el 0 es el único entero divisible por todos los números primos.

La siguiente proposición es una caracterización de los elementos en el radical de Jacobson.

Proposición 1.2.20. *Sean R un anillo y $x \in R$, entonces $x \in J(R)$ si y sólo si $1 - xy \in \mathcal{U}(R)$, para todo $y \in R$.*

Demostración. Sea $x \in J(R)$ y suponga que $1 - xy \notin \mathcal{U}(R)$. Se sigue de la Proposición 1.2.17 que $1 - xy \in \mathfrak{m} \in Specm(R)$. Por la definición del radical de Jacobson, se tiene que $x \in J(R) \subset \mathfrak{m}$, por lo tanto $xy \in \mathfrak{m}$ y así, $1 \in \mathfrak{m}$, lo cual es imposible.

Recíprocamente, suponga que $x \notin \mathfrak{m}$ para algún $\mathfrak{m} \in Specm(R)$, entonces x y $\mathfrak{m}$ generan el ideal $\langle 1 \rangle$, por lo tanto $1 = u + xy$, para $u \in \mathfrak{m}$ y para algún $y \in R$. Así, $1 - xy \in \mathfrak{m}$, por lo cual $1 - xy$ no es unidad.

□

Modificando "ligeramente" la demostración de la proposición anterior, es posible establecer la conexión de **invertibilidad de elementos** evidente en dicho resultado vía ideales. Más exactamente, suponga que el ideal I de R es tal que $I \subseteq J(R)$ y que existe algún elemento $a \in I$ tal que $(1 + a) \notin \mathcal{U}(R)$. Sigue del ítem dos de la Proposición 1.2.17 que existe al menos un ideal $\mathfrak{m} \in Specm(R)$ que contiene a $(1 + a)$. Como $I \subseteq J(R)$ y $a \in I$, entonces $a \in \mathfrak{m}$ y así $1 = (1 + a) - a$ es elemento de $\mathfrak{m}$, que es una contradicción.

Recíprocamente, si todo elemento de $1 + I$ tiene inverso en R, pero $I \nsubseteq J(R)$, sigue de la definición de radical de Jacobson que existe $\mathfrak{m} \in Specm(R)$ tal que $I \nsubseteq \mathfrak{m}$. Si $a \in I \setminus \mathfrak{m}$, se tiene de la maximalidad de $\mathfrak{m}$ que el ideal generado por a y $\mathfrak{m}$ coincide con R, es decir, $\langle a, \mathfrak{m} \rangle = R$. Así, $m + ra = 1 \in R$, para algunos $m \in \mathfrak{m}$ y $r \in R$. Por lo tanto, $m = (1 - ra) \in 1 + I \subseteq \mathcal{U}(R)$ con $m \in \mathfrak{m}$, que es absurdo, dado que $\mathfrak{m}$ es un ideal propio.

Exactamente, se ha establecido el siguiente resultado.

Proposición 1.2.21. *Sea I un ideal del anillo R. Entonces $I \subseteq J(R)$ si y sólo si cada elemento de la clase lateral $1 + I$ tiene un inverso en R.*

Definición 1.2.22. *Un elemento a de un anillo R, se llama **cuasi-regular izquierdo** (resp.*

***cuasi-regular derecho**) si $1-a$ tiene un inverso izquierdo (resp. si tiene un inverso derecho).*

Anteriormente se mencionó el concepto de cuasi-regular y otra forma de definirlo es diciendo que un elemento a es **cuasi-regular** si $1-a$ es invertible.

Sea R un anillo. Si $a \in R$ es cuasi-regular izquierdo y derecho, entonces existen $x, y \in R$, tales que $x(1-a) = (1-a)y = 1$, luego,

$$x = x1 = x((1-a)y) = (x(1-a))y = 1y = y,$$

entonces $x = y$ y $1-a$ es invertible, específicamente se ha demostrado el siguiente lema.

Lema 1.2.23. *Sea R un anillo. Si un elemento $a \in R$ es cuasi-regular izquierdo y derecho, entonces a es cuasi-regular.*

Lema 1.2.24. *Sean R un anillo y $I \preceq_l R$. Si cada elemento $a \in I$ es cuasi-regular izquierdo, entonces todo elemento de I es cuasi-regular.*

Demostración. Sea $a \in I$ un elemento arbitrario y x el inverso izquierdo de $1-a$, por conveniencia, tome $1-x = b$, entonces $(1-b)(1-a) = 1$, así $1-a-b+ba = 1$. Luego $b = ba - a = (b-1)a \in I$, por lo tanto, b tiene un inverso izquierdo x_b y además tiene inverso derecho $1-a$, sigue del Lema 1.2.23, $x_b = 1-a$ es el inverso de $1-b$. Esto implica que x es el inverso de $1-a$, luego a es cuasi-regular.

□

Sea R un anillo. I es llamado un **ideal cuasi-regular izquierdo**, si $I \preceq_l R$ y además sus elementos son cuasi-regulares.

Proposición 1.2.25. *Sea R un anillo. Entonces $J(R)$ es el único ideal maximal cuasi-regular izquierdo de R.*

Demostración. Es necesario demostrar que todos los elementos de $J(R)$ son cuasi-regulares y que todo ideal cuasi-regular izquierdo de R está contenido en $J(R)$. Sea $a \in J(R)$ y suponga que no es cuasi-regular, entonces $1 \notin R(1-a)$, y así, $R(1-a) \neq R$, por lo tanto, la familia,

$$\mathcal{F} = \{I \neq \langle 1 \rangle : I \preceq_l R, R(1-a) \subset I\},$$

es no vacía y cumple las condiciones del Lema de Zorn; así, existe un ideal maximal I_0 que contiene a $R(1-a)$, en particular $1-a \in I_0$ y de la Definición 1.2.18 se tiene que $J(R) \subset I_0$, lo que implica que $1 = (1-a) + a \in I_0$, que es una contradicción, el argumento anterior muestra que todo elemento de $J(R)$ es cuasi-regular izquierdo, así, sigue del Lema 1.2.24, que $J(R)$ es cuasi-regular, como se afirma.

Por otro lado, para demostrar que $J(R)$ contiene todos los ideales cuasi-regulares izquierdos, suponga que I es un ideal cuasi-regular izquierdo, no contenido en $J(R)$, por lo tanto, existe un ideal maximal izquierdo I_0 tal que $I \not\subset I_0$, luego $I + I_0 = R$ y así, $1 = x + y$ con $x \in I$, $y \in I_0$, por lo cual $y = 1 - x \in I_0$ tiene un inverso, (ya que $x \in I$ es cuasi-regular) lo cual es imposible.

□

Observe que, hasta ahora, se ha demostrado que el radical de Jacobson de un anillo R es la intersección de todos los ideales maximales izquierdos de R, o también es el único ideal maximal cuasi-regular izquierdo. Se podría haber hecho definiciones similares trabajando a la derecha, pero se mostrará que ambas definiciones posibles del radical de Jacobson coinciden. Sean $J_l(R)$ y $J_r(R)$ los radicales Jacobson izquierdo y derecho de R, respectivamente. Dado que $J_r(R)$ también es un ideal izquierdo y todos sus elementos son cuasi-regulares, la Proposición 1.2.25 muestra que $J_r(R) \subset J_l(R)$. De manera analoga, tomando las afirmaciones correspondientes a la derecha, se puede demostrar que

$J_l(R) \subset J_r(R)$, por lo tanto, $J_l(R) = J_r(R)$.

Definición 1.2.26. *Un ideal I de un anillo R es llamado **nil**, si para cada $x \in I$, existe un entero positivo n_x tal que $x^{n_x} = 0$. Además, I es **nil de exponente acotado**, si existe un entero positivo n tal que $x^n = 0$, para todo $x \in I$. Por otro lado I es **nilpotente** si existe un entero positivo n tal que $I^n = \{0\}$.*

El **nilradical** η_R, es el conjunto de los elementos nilpotentes, es un ejemplo de un ideal nil, de hecho, es un nil ideal maximal.

Suponga que I es un ideal nilpotente, entonces existe $n \in \mathbb{Z}^+$ tal que $x_{i_1}x_{i_2}\cdots x_{i_n} = 0$, para cualesquiera $x_{i_1}, x_{i_2}, \cdots, x_{i_n} \in I$. En particular, si $x_{i_j} = x$, para $1 \leq j \leq n$, entonces $x^n = 0$, para todo $x \in I$. Por tanto, se demuestra que todo ideal nilpotente es nil. La recíproca no siempre es cierta.

Ejemplo 1.2.27. *Sea $\mathbb{F}$ un cuerpo, un ejemplo de un ideal nilpotente en el anillo de matrices triangulares superiores (2×2), $R = \left\{ \begin{bmatrix} r & r \\ 0 & r \end{bmatrix} : r \in \mathbb{F} \right\}$, es el ideal $I = \left\{ \begin{bmatrix} 0 & r \\ 0 & 0 \end{bmatrix} : r \in \mathbb{F} \right\}$, ya que $I^2 = 0$.*

Con base a lo anterior, se presenta la siguiente proposición, que es otra caracterización del radical de Jacoson, pero en terminos de los ideales nil.

Proposición 1.2.28. *Todo ideal nil de un anillo R está contenido en el radical de Jacobson $J(R)$.*

Demostración. Sea I un ideal nil de R y tome cualquier elemento $a \in I$. Entonces $a^n = 0$ para algún entero positivo n y $1 - a$ es invertible, con inverso $1 + a + \cdots + a^{n-1}$. Por tanto, I es un ideal cuasi-regular izquierdo y de la Proposición 1.2.25 se deduce que $I \subset J(R)$. □

1.3. MÓDULOS

La noción de módulo, apareció implícitamente en los trabajos de Dedekind sobre teoría de números. Su estudio sistemático comenzó en un artículo clásico de E. Noether (Nichtkommutative Algebra) de 1929, que también fue muy importante para el desarrollo de la teoría de los anillos de grupo y contenía todos los hechos básicos de esta teoría.

Definición 1.3.1. *Sea R un anillo y M un grupo abeliano con la suma. M es llamado R-**módulo a izquierda**, si existe una aplicación $\mu : R \times M \to M$, dada por $(r, m) \mapsto rm$, tal que para todo $a, b \in R$ y $m, m_1, m_2 \in M$, verifica las siguientes condiciones:*

1. $(a + b)m = am + bm$,
2. $a(m_1 + m_2) = am_1 + am_2$,
3. $a(bm) = (ab)m$,
4. $1m = m$.

De manera similar se pueden definir los módulos-R o **módulos a derecha** sobre el anillo R, es decir, se tiene una aplicación $\hat{\mu} : M \times R \to M$, donde ahora el anillo R actúa por derecha sobre los elementos de M. En lo que sigue, a menos que se indique explícitamente, se utilizará la expresión R-módulo como abreviatura de R-módulo a izquierda.

De la definición se deduce que si $\mathbb{F}$ es un cuerpo, entonces el concepto de $\mathbb{F}$-módulos coincide con la noción familiar de espacios vectoriales sobre el cuerpo $\mathbb{F}$.

Ejemplo 1.3.2.

1. *Sean G un grupo abeliano con la suma y $\mathbb{Z}$ el anillo de los enteros, entonces G es un $\mathbb{Z}$-módulo.*

2. *Sea I un ideal izquierdo de un anillo R. Dado que el producto de elementos de R por elementos de I está en I, se deduce que I puede considerarse como un R-módulo. De manera similar, los ideales derechos pueden considerarse módulos-R. En particular, un anillo es siempre un módulo sobre sí mismo.*

   Cuando se considera un anillo R, como un módulo izquierdo (resp. derecho) sobre sí mismo, para hacer explícito este hecho, se usan las notaciones ${}_RR$ y (resp. R_R).

3. *Sea I un ideal izquierdo de un anillo R y sea R/I el grupo cociente con la suma. Entonces R/I es un R-módulo, definiendo,*

$$r(a+I) = ra + I,$$

   para todo $r, a \in R$.

En un anillo conmutativo R, Un R-módulo A es una **R-álgebra** si existe una operación de multiplicación definida en A, donde con su adición, A es un anillo tal que:

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

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

Observe que, si A es un anillo con unidad 1 y dado que $R \cdot 1 \cong R$, entonces $R \subset \mathcal{Z}(A)$. En efecto, dados $r \in R$ y $a \in A$ arbitrarios, entonces

$$ra = r(a1) = (ra)1 = a(r1) = ar.$$

Tenga en cuenta que si R es un anillo conmutativo, el anillo de matrices $M_n(R)$ es un ejemplo de R-álgebra. Además el anillo de cuaternios reales introducido en el Ejemplo 1.2.2 es un ejemplo de $\mathbb{R}$-álgebra.

Definición 1.3.3. *Sea M un módulo sobre un anillo R. Un conjunto no vacío $N \subset M$ es llamado un R-submódul**o de M, si se cumplen,***

1. *Para todos $x, y \in N$ se tiene $x + y \in N$,*
2. *Para cualquier $r \in R$ y todo $n \in N$, $rn \in N$.*

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

De la definición anterior, se deduce directamente que si V es un espacio vectorial sobre un cuerpo $\mathbb{F}$, entonces los $\mathbb{F}$-submódulos de V son precisamente sus subespacios. De manera similar, los $\mathbb{Z}$-submódulos de un grupo abeliano G son sus subgrupos. Si se considera el anillo R como un módulo izquierdo (resp. derecho) sobre sí mismo, entonces los submódulos de ${}_RR$ son sus ideales izquierdos (resp. derechos).

Todo módulo $M \neq \{0\}$ contiene al menos dos submódulos, M y $\{0\}$, que son llamados triviales, un submódulo no trivial es llamado submódulo propio, un módulo distinto de cero que no contiene ningún submódulo propio, es llamado **simple**.

2. ANILLOS DE GRUPO

A continuación se presenta a RG, la estructura de interés en este trabajo, la cual presenta propiedades tanto del grupo G como del anillo de coeficientes R. Dicha estructura algebraica es un punto de encuentro entre la teoría de grupos y la teoría de anillos y por tal motivo, ha sido abordada desde diferentes puntos de vista, en particular, el teórico de anillos indaga sobre propiedades anillo-teóricas en este contexto.

Sean G un grupo (multiplicativo) no necesariamente finito con elemento neutro e y R un anillo con unidad $1_R = 1$. Se desea construir un R-módulo, que tenga los elementos de G como una base, usando al tiempo las operaciones de G y R que le den estructura de anillo. Para ello, se denota por RG al conjunto de todas las combinaciones lineales de la forma,

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

donde $a_g \in R$ y $a_g = 0$ casi siempre, es decir, el número de coeficientes diferentes de 0 es finito.

Dado un elemento $\alpha = \sum_{g \in G} a_g g \in RG$, se define su soporte, como el subconjunto de elementos de G que aparecen en α, es decir,

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

Note que, si dados dos elementos α y $\beta \in RG$, donde $\alpha = \sum_{g \in G} a_g g$ y $\beta = \sum_{g \in G} b_g g$. Se tiene que, si $\alpha = \beta$, entonces $\sum_{g \in G} (a_g - b_g)\, g = 0$, debido a que $supp(\alpha) = supp(\beta) \subset G$ es base de RG. Así, $a_g - b_g = 0$ y por lo tanto $a_g = b_g$. Recíprocamente, si $a_g = b_g$ para

todo $g \in G$, entonces

$$\alpha = \sum_{g \in G} a_g g = \sum_{g \in G} b_g g = \beta.$$

Se define la suma de elementos en RG componente a componente, es decir,

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

Además, su producto está dado por:

$$\alpha\beta = \sum_{g,h \in G} a_g b_h gh = \sum_{u \in G} c_u u, \quad c_u = \sum_{gh=u} a_g b_h.$$

Como R es un anillo, entonces, R es un grupo abeliano con la suma y así de la suma definida para RG, es claro que RG también es un grupo abeliano con "$+$".

Ahora bien, sean $\alpha, \beta, \gamma \in RG$, note que,

$$\begin{aligned}
\alpha(\beta\gamma) &= \sum_{g \in G} a_g g \left[\sum_{h \in G} b_h h \sum_{k \in G} c_k k \right] \\
&= \sum_{g \in G} a_g g \left[\sum_{h,k \in G} b_h c_k hk \right] \\
&= \sum_{g,h,k \in G} a_g \left(b_h c_k\right) g \left(hk\right) \\
&= \sum_{g,h,k \in G} \left(a_g b_h\right) c_k \left(gh\right) k \\
&= \sum_{g,h \in G} a_g b_h gh \left[\sum_{k \in G} c_k k \right] \\
&= \left(\alpha\beta\right) \gamma,
\end{aligned}$$

es decir, el producto en RG es asociativo.

Usando la propiedad distributiva en R y la definición de producto en RG, es claro que son validas las leyes distributivas (a izquierda y derecha) del producto respecto a la suma,

$$\alpha(\beta+\gamma)=\alpha\beta+\alpha\gamma \quad \text{y} \quad (\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma.$$

Además, la unidad en RG viene dada por $1_{RG}=\sum_{g\in G}u_g g$, donde $u_e=1_R$ y $u_g=0$ para todo $g\neq e$. Por tanto RG es un anillo con unidad 1_{RG}.

Finalmente, RG tiene estructura de R-módulo al considerar el producto,

$$\mu : R\times RG\to RG,$$

dado por:

$$\Big(\lambda,\sum_{g\in G}a_g g\Big)\mapsto \lambda\Big(\sum_{g\in G}a_g g\Big)=\sum_{g\in G}(\lambda a_g)g.$$

En particular si $R=\mathbb{F}$ es un cuerpo, $\mathbb{F}G$ es un $\mathbb{F}$-espacio vectorial.

Ahora se presentará la definición transversal a esta monografía.

Definición 2.0.1. *El conjunto RG, con las operaciones definidas anteriormente, es llamado el* **anillo de grupo** *de G sobre R. En el caso que R sea un anillo conmutativo, RG también es llamado el* **álgebra de grupo** *de G sobre R.*

Ejemplo 2.0.2.

1. *Sean $\mathbb{F}_2$ y $C_2=\langle x : x^2=1\rangle$, luego*

$$\mathbb{F}_2C_2=\left\{\sum_{g\in C_2}a_g g : a_g\in\{0,1\}\right\},$$

por lo tanto,

$$\mathbb{F}_2C_2=\{0,1,x,1+x\}.$$

2. *Considere el grupo de los cuaternios*

$$\mathcal{Q}_8 = \langle x, y : x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$$

y sea R *un anillo arbitrario, entonces*

$$R\mathcal{Q}_8 = \left\{ \sum_{g \in \mathcal{Q}_8} a_g g : \ a_g \in R \right\} = \left\{ \sum_{i=0}^{3} a_i x^i + \left(\sum_{j=4}^{7} a_j x^{j-4} \right) y : \ a_i, a_j \in R \right\}.$$

Las siguientes aplicaciones son de interés en este trabajo, dado que caracterizan el grupo y el anillo respecto a los anillos de grupo.

1. El encaje $i : G \hookrightarrow RG$, le asigna a cada $x \in G$ el elemento $i(x) = \sum_{g \in G} a_g g$, donde $a_x = 1$ y $a_g = 0$ para todo $g \neq x$.

   Por tanto, se puede considerar a G como un subconjunto de RG, y así, G es una base de RG sobre R.

2. La aplicación $v : R \longrightarrow RG$, dada por $v(r) = \sum_{g \in G} a_g g$ con $a_{1_g} = r$ y $a_g = 0$ si $g \neq 1_g$.

   Se tiene que la anterior aplicación es un monomorfismo de anillos, por lo cual, se considera a R como un subanillo de RG.

Note que Re es subanillo de RG, dado que $Re \cong R$ por la siguiente aplicacion:

$$r \mapsto re.$$

De lo anterior se deduce que $rg = gr$ en RG, dado que

$$gr = (1g)(re) = (1r)(ge) = rg.$$

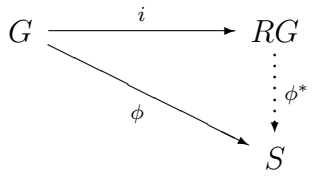
Por lo tanto, si R es conmutativo, entonces $R \subset \mathcal{Z}(RG)$. En efecto, si $r \in R$ y $\alpha \in RG$,

entonces,

$$r\alpha = r \cdot \sum_{g\in G} a_g g = \sum_{g\in G} (ra_g)g = \sum_{g\in G} a_g(rg) = \sum_{g\in G} a_g(gr) = \sum_{g\in G} a_g g \cdot r = \alpha r.$$

Ahora se presentará una "propiedad universal" de los anillos de grupo.

Proposición 2.0.3. *Sean G un grupo y R un anillo.*



Dado un anillo S tal que $R \subset S$ y una aplicación $\phi : G \to S$ tal que $\phi(gh) = \phi(g)\phi(h)$, entonces existe un único homomorfismo $\phi^* : RG \to S$, tal que $\phi^* \circ i = \phi$. Es decir, el diagrama es conmutativo.

Además, si $R \subset \mathcal{Z}(S)$ (y así S puede verse como R-álgebra), entonces ϕ^* es un homomorfismo de R-álgebras.

La proposición anterior con algunas adecuaciones sirve como definición del concepto de anillo de grupo, [[2], Pág. 133]. El siguiente resultado, el cual es una consecuecia de la Proposición 2.0.3, permite extender homomorfismos de grupos a homomorfismos de anillos de grupo, más exactamente se tiene.

Corolario 2.0.4. *Sea $f : G \to H$ un homomorfismo de grupos, entonces existe un único homomorfismo $f^* : RG \to RH$ tal que $f^*(g) = f(g)$.*

Note que si en el corolario anterior $H = \{1\}$, la aplicación $G \to \{1\}$, induce un homomorfismo $\varepsilon : RG \to R$ dado por $\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$. Este último homomorfismo y su kernel son definidos a continuación.

Definición 2.0.5. *El homomorfismo $\varepsilon : RG \to R$ definido anteriormente, es llamado* **aplicación de aumento** *de RG y su kernel es llamado el* **ideal de aumento** *de RG y se denota por $\Delta(G)$.*

Note que si $\alpha = \sum_{g\in G} a_g g \in RG$ pertenece a $\Delta(G)$, entonces,

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g = 0,$$

por lo tanto, se obtiene que:

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

Además, claramente todos los elementos de la forma $g-1$ con $g \in G$, pertenecen a $\Delta(G)$. De la anterior observación se deduce que $\{g-1 : g \in G, g \neq 1\}$ es un conjunto de generadores de $\Delta(G)$ sobre R. Note que la expresión $\sum_{g\in G} a_g(g-1) = 0_{RG}$ se cumple si todos los coeficientos a_g son iguales a 0_R y así, el conjunto $\{g-1 : g \in G, g \neq 1\}$ es linealmente independiente, más exactamente, se ha probado el siguiente resultado.

Proposición 2.0.6. *El conjunto* $\{g-1 : g \in G, g \neq 1\}$ *es una base de* $\Delta(G)$ *sobre* R *y así,*

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

Dado $H \in S(G)$, se denota por $\Delta(G,H)$ al ideal izquierdo de RG generado por $\{h-1 : h \in H\}$, es decir,

$$\Delta(G,H) = \left\{\sum_{h\in H} a_h(h-1) : a_h \in RG\right\}.$$

Un **transversal de H en G** $T = \{q_i\}_{i\in I}$ es un conjunto completo de *representantes de clases laterales izquierdas* de H en G, de manera que $g \in G$, $g = q_i h_j$ con $q_i \in T$ y $h_j \in H$. El siguiente resultado da una mejor descripción de $\Delta(G,H)$, usando la noción de transversal.

Proposición 2.0.7. $B_H = \{q(h-1) : q \in T, h \in H, h \neq 1\}$ *es base de* $\Delta(G,H)$ *sobre R.*

Demostración. Primero se mostrará que B_H es linealmente independiente respecto a R.

Suponga que tiene una combinación lineal $\sum_{ij} r_{ij}q_i(h_j - 1) = 0$, $r_{ij} \in R$, por lo tanto,

$$\sum_{ij} r_{ij}q_i h_j = \sum_i \left(\sum_j r_{ij} \right) q_i,$$

dado $h_j \neq 1$, para todo los valores de j. Se deduce que los elementos de la ecuación anterior tienen soporte disjunto. Como los elementos en G son linealmente independientes respecto a R, entonces todos los coeficientes deben ser 0, en particular, $rij = 0$, para todo i, j. Ahora para mostrar que B_H genera a $\Delta(G, H)$, es suficiente mostrar que cada elemento de la forma $g(h - 1)$, $g \in G$, $h \in H$ se puede escribir como una combinación de elementos de B_H. Como $g = q_i h_j$ para algún $q_i \in T$ y algún $h_j \in H$, se tiene que

$$g(h - 1) = q_i h_j(h - 1) = q_i(h_j h - 1) - q_i(h_j - 1),$$

que era lo se quería mostrar.

□

Ahora se dará una interpretación para $\Delta(G, H)$ cuando H es subgrupo normal de G. En efecto si $H \lhd G$, el epimorfismo $\phi : G \twoheadrightarrow G/H$ puede extenderse al epimorfismo $\Phi : RG \twoheadrightarrow R(G/H)$ dado por,

$$\sum_{g \in G} a_g g \longmapsto \sum_{g \in G} a_g \phi(g) = \sum_{g \in G} a_g \bar{g},$$

donde $\bar{g}$ es la imagen de g en G/H. Note que $Ker_\Phi = \Delta(G, H)$, por tanto, se ha demostrado la siguiente proposición.

Proposición 2.0.8. *Si $H \lhd G$, entonces $ker_\Phi = \Delta(G, H) \preceq RG$ y además,*

$$RG/\Delta(G, H) \cong R(G/H).$$

Como caso especial, al tomar $H = G$, $G \to \{1\}$, induce $RG \to R$, la aplicación de aumen-

to y su kernel es $\Delta(G)$. En particular $RG/\Delta(G) \cong R$.

El siguiente resultado del artículo “On the group rings ” [8, Proposition 9, pág. 665], será vital para la obtención de los teoremas principales de este trabajo.

Proposición 2.0.9. *Sean R un anillo y H un subgrupo de G, entonces $J(RG) \cap RH \subset J(RH)$, en particular $J(RG) \cap R \subset J(R)$, además, si R es artiniano o G es localmente finito, entonces $J(RG) \cap R = J(R)$.*

Demostración. Si $r' \in RH \cap J(RG)$, entonces $1 - r'x$ tiene inverso en RG para todo $x \in RH$ (de hecho para todo $x \in RG$); pero $1 - r'x \in RH$ y así $1 - r'x$ también tiene inverso en RH, por lo tanto $r' \in J(RH)$.

Además, si R es artiniano, $J(R) = \eta_R = R \cap \eta_{RG} \subset R \cap J(RG)$, [8, Pág. 666]. Ahora suponiendo que G es localmente finito y $a \in J(R)$, se probará que $a \in J(RG)$, es decir, que para cualquier $r \in RG$ se debe encontrar un $x \in RG$ tal que $(1 + ar)x = 1$. Sea $H = supp(r) = \{1, g_2, \ldots, g_n\}$ (que es finito por como asumimos a G). Si

$$r = a_1 + a_2 g_2 + \cdots + a_n g_n,$$

$$x = x_1 + x_2 g_2 + \cdots + x_n g_n,$$

entonces,

$$((1 + (aa_1) + aa_2 g_2 + \cdots + aa_n g_n)(x_1 + \cdots + x_n g_n) = 1,$$

---

8 Ian G CONNELL. “On the group ring”. En: *CJM* 15 (1963), págs. 650-685.

luego,

$$\begin{aligned}(1+aa_1)x_1 + aa_{12}x_2 + \cdots + aa_{1n}x_n &= 1,\\ aa_{21}x_1 + (1+aa_1)x_2 + \cdots + aa_{2n}x_n &= 0,\\ \vdots \qquad\qquad &\qquad \vdots\\ aa_{n1}x_1 + aa_{n2}x_2 + \cdots + (1+aa_1)x_n &= 0,\end{aligned}$$

donde en la i-ésima, $a_{i1}, \ldots, a_{i,i-1}, a_{i,i+1}, \ldots a_{in}$ son una permutación de $a_2, a_3, \ldots, a_n$. Si R es conmutativo, el determinante de este sistema es claramente de la forma $1 + aa'$, donde $a' \in R$, dado que $a \in J(R)$, entonces $1 + aa'$, así, el sistema tiene solución, luego $(1 + ar)x = 1$.

□

Los siguientes resultados serán útiles para la demostración del teorema principal.

Proposición 2.0.10. *Sean R un anillo y G un grupo.*

1. *Si $\Delta(G) \subset J(RG)$, entonces G es un p-grupo y $p \in J(R)$.*

2. *$\Delta(G)$ es nilpotente si y sólo si G es un p-grupo finito y p es nilpotente en R.*

Demostración.

1. Suponga que $g \in G$ es de orden infinito, por lo tanto,

$$(1-g) + (1-g^2) = 2 - g - g^2 \in \Delta(G) \subset J(RG),$$

luego $1 - (2 - g - g^2)$ tiene inverso por derecha, es decir,

$$(-1 + g + g^2)x = 1 \text{ para algún } x \in RG.$$

Por [8, Proposition 4, pág 656], suponga que el $supp(x)$ está contenido en el subgrupo cíclico generado por g, y así,

$$(-1 + g + g^2)(a_0 + a_1 g + \cdots + a_n g^n) = g^k,$$

para algunos $n > 0$ y k, donde a_0 y a_n son distintos de cero. El lado izquierdo contiene los términos distintos, $-a_0$ y $a_n g^{n+2}$, lo que contradice la igualdad, por lo cual, $g \in G$ tiene orden finito, escogiendo cualquier orden n y cualquier número primo p que divida a n, existe $g \in G$ con orden p, Luego, para cualquier $a \in R$,

$$1 + (1 - g)[p + (p - 1)g + (p - 2)g^2 + \cdots + g^{p-1}]a$$

tiene un inverso por derecha, es decir, se puede considerar a x un polinomio en g, tal que,

$$[1 + (1 - g)(p + \cdots + g^{p-1})a]x = 1$$

puede considerarse una ecuación en RG_p, donde G_p es el grupo cíclico de orden p. Si I es un ideal en RG_p generado por el elemento $1 + g + g^2 + \cdots + g^{p-1}$, RG_p/I es equivalente a reemplazar g^{p-1} por $-1 - g - \cdots - g^{p-2}$, entonces la anterior ecuación se convierte en,

$$(1 + pa)\bar{x} = 1,$$

donde $\bar{x} = a_0 + a_1 g + \cdots + a_{p-2} g^{p-2}$, por lo tanto,

$$(1 + pa)a_0 = 1.$$

Dado que a es arbitrario, implica que $p \in J(R)$. No existe otro primo $q \in J(R)$, debido a que $lp + mq = 1 \in J(R)$ con l, m enteros apropiados, contradiciendo el hecho de que $J(R)$ es un ideal propio, por lo tanto, p es el único primo que divide cualquier orden de los elementos del grupo G, así G es $p - grupo$.

2. (Ver, [8], Theorem 9, pág. 681).

□

3. ANILLOS LOCALES & LOCALIZACIÓN

En este capítulo se estudiará el concepto de "localidad" en un anillo y se introducirá algunas caracterizaciones y propiedades básicas de este anillo. Así mismo la localización es una manera formal de introducir los "denominadores" a un anillo o módulo dado, es decir, la localización introduce un nuevo anillo (módulo resp.) a partir de un anillo o módulo inicial R (M resp.), [5]. A menudo un anillo local surge de la localización de un anillo conmutativo en un ideal primo. Existen anillos con exactamente un ideal maximal, como es en el caso de los cuerpos, esto motiva la definición central del presente trabajo.

Definición 3.0.1. *Un anillo R es llamado* **local***, si tiene exactamente un único ideal maximal $\mathfrak{m}$.*

Los siguientes resultados son de uso frecuente, no solo en los textos de álgebra, sino también en los artículos de investigación, permiten determinar si un anillo es local en términos de los elementos de un ideal propio y si un ideal $\mathfrak{m} \in Specm(R)$ es el único. En resumen el resultado permite establecer cuando un anillo R es local.

Proposición 3.0.2. *Sea R un anillo,*

1. *Sea $\mathfrak{m}$ un ideal propio de R tal que $x \in R \setminus \mathfrak{m}$ es unidad de R, entonces R es local y $\mathfrak{m}$ es su único ideal maximal.*

2. *Si $\mathfrak{m} \in Specm(R)$ tal que cada elemento de $1 + \mathfrak{m}$ es unidad de R, entonces R es local.*

Demostración.

1. Sea $I \neq \langle 1 \rangle$ un ideal arbitrario de R, es claro que I no contiene unidades, por lo tanto $I \subset \mathfrak{m}$, es decir, $\mathfrak{m}$ es el único ideal máximal, entonces R es un anillo local.

2. Sea $x \in R \setminus \mathfrak{m}$. Dado $\mathfrak{m}$ es un ideal maximal, entonces el ideal generado por x y $\mathfrak{m}$ generan a $\langle 1 \rangle$. Por lo tanto, existen $y \in R$ y $n \in \mathfrak{m}$, tales que $xy + n = 1$ y así, $xy = 1 - n \in 1 + \mathfrak{m}$ y es unidad. Así $x \in R \setminus \mathfrak{m}$ es unidad y se sigue del ítem anterior R es local.

□

Usando el ítem dos de la proposición anterior y el segundo resultado de la Proposición 1.2.14, note que, un anillo R no-conmutaivo es **local** si y sólo si $R/J(R)$ es un anillo de división. Como consecuencia, se establece el siguiente resultado.

Proposición 3.0.3. *Sea R un anillo. R es local si y sólo si todo elemento en $R \setminus J(R)$ es unidad.*

La prueba de la anterior proposición se deriva de las Proposiciones 3.0.2 & 1.2.17.

Ejemplo 3.0.4.

1. *Considere $\mathbb{F}[x]$ el anillo de polinomios con coeficientes en el cuerpo $\mathbb{F}$. La aplicación $\phi : \mathbb{F}[x] \to \mathbb{F}$, dada por $\phi(f) = f(0)$ es un homomorfismo, llamado homomorfismo de evaluación en 0. Ahora bien, si $\mathbb{F}[x] \ni f$, entonces $\phi(f) = f(0) = 0$ si y sólo si $a_0 = 0$ y así, $ker_\phi = \langle x \rangle$. Como $\mathbb{F}[x]/\langle x \rangle \cong \mathbb{F}$, entonces $\mathbb{F}[x]/\langle x \rangle$ es un anillo local.*

2. *El anillo de series formales sobre el cuerpo $\mathbb{F}$,*

$$\mathbb{F}[\![x]\!] = \Big\{ \sum_{k \geq 0} \alpha_k x^k : \alpha \in \mathbb{F} \Big\}$$

   es un anillo local y su ideal máximal consiste de las series con termino constante cero.

3. *Sea $\mathbb{R}\big(x\big) = \{p(x)/q(x) : p(x), q(x) \in \mathbb{R}[x], q(0) \neq 0\}$ el anillo de funciones racionales sobre $\mathbb{R}$. Es claro ver que $\mathfrak{m} = \{p(x)/q(x) : p(x), q(x) \in \mathbb{R}[x], q(0) \neq 0$ y $p(0) = 0\}$ es*

un ideal propio, además si $p(x)/q(x) \in \mathbb{R}\big(x\big) \setminus \mathfrak{m}$*, entonces* $p(x)/q(x)$ *es unidad, así por el ítem uno de la Proposición 3.0.2, se tiene que* $\mathbb{R}\big(x\big)$ *es local.*

4. *Sean* $\mathbb{F}$ *un cuerpo y* n *un entero positivo. Entonces el anillo*

$$R = \mathbb{F}[x]/\langle x^n \rangle$$

es un anillo local y su ideal maximal es

$$\mathfrak{m} = \Big\{ \overline{p(x)} = \sum_{i=1}^{n-1} \alpha_i x^i + \langle x^n \rangle : \alpha_i \in \mathbb{F} \Big\}.$$

En efecto:

a) *Note que si* R *es un anillo conmutativo y* $r \in \eta_R$*, entonces* $r^m = 0$*, para algún* $m > 1$*, así,* $1 + r \in \mathcal{U}(R)$ *dado que,*

$$\big(1+r\big)\big(1-r+r^2-\cdots(-1)^{m-1}r^{m-1}\big) = 1 = \big(1-r+r^2-\cdots(-1)^{m-1}r^{m-1}\big)\big(1+r\big).$$

b) *Ahora, si* $\mathfrak{m} \ni \overline{p(x)}$*, entonces* $\overline{p(x)}^n = \langle x^n \rangle$ *y así, todo elemento* $\overline{p(x)} \in \mathfrak{m}$ *es nilpotente. Más aún,* $1 + \overline{p(x)} = \overline{1 + p(x)}$ *es invertible, por el ítem dos de la Proposición 3.0.2, se sigue lo requerido.*

El siguiente lema, permite transferir el concepto de localidad a través de epimorfismos.

Lema 3.0.5. *Sea* $\phi : R \twoheadrightarrow S$ *un epimorfismo no-cero de anillos, entonces* R *es local si y sólo si* S *es local y* $ker_\phi \subset J(R)$.

Demostración. Suponga que S es local y $ker_\phi \subset J(R)$, por el Teorema 1.2.11, existe una correspondencia $1-1$ entre los ideales izquierdos maximales de S y los ideales izquierdos maximales de R que contienen al $\ker_\phi$, se sigue que si S es anillo local, entonces R tiene exactamente un ideal izquierdo maximal y así, $J(R)$ es ideal maximal como ideal

izquierdo, es decir, R es anillo local.

Recíprocamente, si R es local, entonces $J(R)$ es el único ideal maximal de R y además, $ker_\phi \subset J(R)$, caso contrario, $\phi(R) = \{0\}$ que es una contradicción. De nuevo por el Teorema 1.2.11 (correspondencia), que preserva el orden, se tiene que S tiene un único ideal izquierdo maximal.

□

Observación 3.0.6. *Note que por el lema anterior, el anillo cociente de un anillo local es local, es decir, si R es un anillo local, entonces R/I es local.*

El término **localización** se originó en la geometría algebraica, si R es un anillo de funciones definidas sobre algún objeto geométrico (variedad algebraica) V, y se quiere estudiar esta variedad "localmente" cerca de un punto p, entonces se considera el conjunto S de todas las funciones que no son cero en p y se localiza R con respecto a S. El anillo resultante $S^{-1}R$ contiene información sobre el comportamiento de V entorno a p y excluye información que no es "local", como **los ceros** de funciones que están fuera de V. Lo cual se puede asociar por lo propuesto por C. Chevalley cuando definio "Local Ring".

El procedimiento mediante el cual se construye el cuerpo de los racionales $\mathbb{Q}$ a partir del anillo de números enteros $\mathbb{Z}$ ("encaja" $\mathbb{Z}$ en $\mathbb{Q}$) se puede extender fácilmente a cualquier dominio entero D y produce el cuerpo de fracciones $Q(D)$.

La construcción consiste en tomar parejas ordenadas, (a, s) donde a y s pertenecen a un dominio entero D y $s \neq 0$. Estableciendo una relación de equivalencia entre dichos pares:

$$(a, s) \equiv (b, t) \iff at - sb = 0.$$

Esto funciona sólo si D es un dominio entero, ya que para verificar la transitividad involu-

cra cancelar, por el hecho de que D no tiene divisores cero.

Sin embargo esto puede ser generalizado de la siguiente manera, sean R un anillo y S un **subconjunto multiplicativo** (es decir, $1 \in S$ y S es cerrado bajo la multiplicación). Entonces se define en $R \times S$ la relación de equivalencia

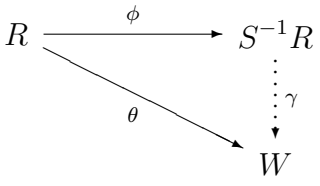
$$(a, s) \equiv (b, t) \iff (at - sb)u = 0, \text{ Para algún } u \in S.$$

Claramente es reflexiva y simétrica, para ver que es transitiva se usa el hecho de que S es un conjunto multiplicativo.

Definición 3.0.7. *El conjunto de clases de equivalencia de la relación anterior será denotado por $S^{-1}R$. Se le da estructura de anillo con la suma y el producto de fracciones de la misma manera que en álgebra elemental [5, Chap. 3, pág. 36]. Tal anillo es llamado* **anillo de fracciones**.

Existe un homomorfismo $\phi : R \to S^{-1}R$, entre el anillo inicial R y el anillo de fracciones, definido por $\phi(x) = x/1$. El anillo $S^{-1}R$ tiene la siguiente propiedad universal.

Proposición 3.0.8. *Sean R un anillo conmutativo con unidad y S un conjunto multiplicativo.*



Sea $\theta : R \to W$ un homomorfismo de anillos, tal que $\theta(s)$ es una unidad en W para todo $s \in S$. Entonces existe un único homomorfismo de anillos $\gamma : S^{-1}R \to W$, tal que $\theta = \gamma \circ \phi$.

Demostración. Si γ satisface las condiciones, entonces $\gamma(a/1) = \gamma(\phi(a)) = \theta(a)$, para todo $a \in R$, por lo tanto, si $s \in S$,

$$\gamma(1/s) = \gamma((s/1)^{-1}) = \gamma(s/1)^{-1} = \theta(s)^{-1},$$

así, γ es única, determinada por θ y su existencia se debe a que

$$\gamma(a/s) = \theta(a)\theta(s)^{-1}.$$

Luego γ es claramente un homomorfismo de anillo siempre que esté bien definido. Suponga que $a/s = a'/s'$; entonces existe $t \in S$ tal que $(as' - a's)t = 0$, por lo tanto,

$$(\theta(a)\theta(s') - \theta(a')\theta(s))\theta(t) = 0,$$

como $t \in S$, $\theta(t)$ es unidad en W, por lo tanto,

$$\theta(a)\theta(s)^{-1} = \theta(a')\theta(s')^{-1}.$$

□

El anillo de fracciones $S^{-1}R$ y el homomorfismo ϕ tienen las siguientes propiedades.

1. $s \in S$, entonces $\phi(s)$ es unidad en W;
2. $\phi(a) = 0$, entonces $as = 0$, para algún $s \in S$;
3. Cada elemento de $S^{-1}R$ es de la forma $\phi(a)\phi(s)^{-1}$, para $a \in R$ y $s \in S$.

Estas tres condiciones permiten extender el anillo de fracciones $S^{-1}R$ a un isomorfismo. Específicamente se tiene el siguiente corolario:

Corolario 3.0.9. *Si $\theta : R \to W$ es un homomorfismo de anillos tal que,*

1. *$s \in S$, entonces $\theta(s)$ es unidad en W;*
2. *$\theta(a) = 0$, entonces $as = 0$, para algún $s \in S$;*
3. *Cada elemento de W es de la forma $\theta(a)\theta(s)^{-1}$; entonces hay un único isomorfismo $\gamma : S^{-1}R \to W$, tal que $\theta = \gamma \circ \phi$.*

Demostración. Dada la Proposición 3.0.8, se tiene que demostrar que $\gamma(a/s) = \theta(a)\theta(s)^{-1}$ es un isomorfismo. Por el tercer ítem todo elemento en W es de la forma $\theta(a)\theta(s)^{-1}$, por lo tanto γ es sobreyectiva. Para mostrar su inyectividad, note que si $\gamma(a/s) = 0$, entonces $\theta(a) = 0$, por el ítem dos se tiene que, $at = 0$ para algún $t \in S$, luego $(a, s) = (0, 1)$, esto es, $a/s = 0$ en $S^{-1}R$, y así $ker_\gamma = 0$, entonces γ es inyectiva.

□

Ejemplo 3.0.10.

1. *Sean R un anillo y $\mathfrak{p}$ un ideal primo. Entonces $S = R \setminus \mathfrak{p}$ es un conjunto multiplicativo. Se escribirá $S^{-1}R = R_\mathfrak{p}$, donde $R_\mathfrak{p}$ es local. Este proceso es llamado "localización de un anillo" en un ideal primo. Este tipo de localización es fundamental en álgebra conmutativa, porque muchas propiedades de un anillo conmutativo se pueden ver en sus anillos locales. Por ejemplo, un anillo es regular si y sólo si todos sus anillos locales son regulares.*

2. *Sea $R = \mathbb{F}[t_1, \cdots, t_n]$, donde $\mathbb{F}$ es un cuerpo, t_i son independientes y $\mathfrak{p}$ un ideal primo. Entonces $R_\mathfrak{p}$ es el anillo de todas las funciones racionales f/g, donde $g \notin \mathfrak{p}$. Si V es la variedad definida por el ideal $\mathfrak{p}$, es decir, el conjunto de todos los elementos $x = (x_1, \cdots, x_n) \in \mathbb{F}^n$ tal que $f(x) = 0$ siempre que $f \in \mathfrak{p}$, entonces (siempre que $\mathbb{F}$ sea infinito) todo puede identificarse con el anillo de todas las funciones racionales en $\mathbb{F}^n$ que están definidas en casi todos los puntos de V; es el anillo local de $\mathbb{F}^n$ a lo largo de la variedad V. Este es el prototipo de los anillos locales que surgen en geometría algebraica.*

3. *Si x es un elemento de un anillo conmutativo R, entonces podemos considerar un conjunto multiplicativo con las potencias de x, es decir, $S = \{1, x, x^2, \dots\}$, luego $S^{-1}R$ puede ser identificado por $R[x^{-1}] = R[s]/(xs - 1)$. (La prueba consiste en demostrar que este anillo satisface la Proposición 3.0.8.)*

Algunas propiedades del anillo de fracciones, son las siguientes.

Observación 3.0.11. *Sea R un anillo conmutativo.*

1. $S^{-1}R = 0$ *si y sólo si* S *contiene al* 0*.*
2. *El homomorfismo de anillos* $R \longrightarrow S^{-1}R$ *es inyectivo si y sólo si* S *no contiene divisores de cero.*

4. ANILLOS DE GRUPO LOCALES

El concepto de *anillo local* fue introcido en el capítulo 3, la idea principal de este trabajo es llevar la noción de localidad a la estructura de interés, los anillos de grupo. Así mismo, examinar las propiedades y características tanto del anillo como del grupo, y así, identificar cuándo esta estructura es local.

Uno de los objetivos principales de esta monografía es generalizar los siguientes resultados del articulo "*An elementary note on group rings*", [3, (h) & (i), pág. 153], en el que Gulliksen, Ribenboim y Viswanathan tomaron el anillo de coeficientes conmutativo y el grupo abeliano.

Proposición 4.0.1. *Si R es un anillo tiene sólo un ideal maximal, $\mathfrak{m}$, tal que $R/\mathfrak{m}$ tiene característica p y G es un p-grupo abeliano, entonces RG tiene sólo un ideal maximal. Además, si R es un anillo local (noetheriano) y G es finito, entonces RG es local.*

Demostración. Sea $\bar{\mathfrak{m}}$ cualquier ideal maximal en RG. Dado que G es un grupo abeliano de *torsión* [*], de [3, (a), pág. 149], se deduce que $\bar{\mathfrak{m}} \cap R$ es un ideal maximal, por lo que $\bar{\mathfrak{m}} \cap R = \mathfrak{m}$ y por lo tanto $R/(\bar{\mathfrak{m}} \cap R)$ tiene característica p. Luego, de [3, (f), pág 152], se tiene que $\bar{\mathfrak{m}} = \varepsilon^{-1}(\bar{\mathfrak{m}} \cap R) = \varepsilon^{-1}(\mathfrak{m})$, donde ε es la aplicación de aumento. Mostrando así que RG tiene un único ideal maximal. La segunda afirmación es obvia. Note que si R es noetheriano y G finito, entonces RG es noetheriano.

□

Ahora, se probará la recíproca de la anterior proposición.

---

[*] Un grupo G es llamado grupo de torsión si todos sus elementos son elementos de torsión, es decir, todo $g \in G$ tiene orden finito.

Proposición 4.0.2. *Sea G un grupo abeliano, $G \neq e$. Si RG tiene un único ideal maximal, entonces,*

1. *R tiene un único ideal maximal, $\mathfrak{m}$;*
2. *$R/\mathfrak{m}$ tiene característica $p \neq 0$;*
3. *G es p-grupo.*

Demostración. Dado que $R \cong RG/ker_{\varepsilon}$, entonces R tiene un único ideal maximal, denotado por $\mathfrak{m}$. Sea c el exponente característico del cuerpo $\mathbb{F} = R/\mathfrak{m}$, es decir, $c = 1$ cuando $car(\mathbb{F}) = 0$, o $c = car(\mathbb{F})$ en caso contrario. Suponga que existe un elemento $g \in G$ tal que su orden no es una potencia de c. Se deriva una contradicción, entonces c debe ser un primo p y cada elemento de G tiene orden una potencia de p. Si g tiene orden finito, no potencia de c, entonces alguna potencia de g tiene orden un primo $q \neq c$. Si g tiene orden infinito, sea $q \neq c$ cualquier primo. Denotaremos por C el subgrupo cíclico de G generado por g y sea T el grupo multiplicativo de todas las raíces de unidad en alguna clausura algebraica en $\mathbb{F}$. Considere el homomorfismo $\omega_0 : C \to T$ definido por $\omega_0(g) = \alpha$, donde α es la raíz q^{th} de unidad (note que $\alpha \neq 1$). Dado que T es un grupo divisible, se puede extender el homomorfismo ω_0 al homomorfimso $\omega : G \to T$. Sea $D = \omega(G)$ y considere el cuerpo $\mathbb{F}[D]$. Ahora, sea el homomorfismo canónico $\pi_{\mathfrak{m}} : R \to R/\mathfrak{m} = \mathbb{F}$, por lo tanto,

$$\mathfrak{m}' = ker_{\theta \circ \varepsilon} = \varepsilon^{-1}(\mathfrak{m})$$

es un ideal maximal de RG. De igual manera, considere la aplicación $v : RG \to \mathbb{F}[D]$ definida por:

$$v\left(\sum_{h \in G} a_h h\right) = \sum_{h \in G} \theta(a_h) \cdot \omega(h),$$

así, v es un homomorfismo en $\mathbb{F}[D]$ y $N = ker_v$ es un ideal maximal de RG. Además, se tiene que $N \neq \mathfrak{m}'$ dado que $e - g \in \mathfrak{m}'$ mientras que $e - g \notin N$, ya que $1 \neq \alpha$. Lo que contradice la hipótesis de que RG es local, probando así lo enunciado.

□

Ahora se presentarán los resultados del artículo “Local Group Rings”, con el fin de tener las condiciones necesarias para demostrar el resultado principal de esta monografía.

Teniendo en cuenta la Proposición 3.0.5, ésta se puede extender a anillos de grupo, tomando el epimorfismo $\Phi : RG \twoheadrightarrow R(G/H)$ de la Proposición 2.0.8. Entonces, se tiene el siguiente corolario.

Corolario 4.0.3. *Sean R un anillo, G un grupo y $H \lhd G$. Entonces RG es local si y sólo si $R(G/H)$ es local y $\Delta(G, H) \subset J(RG)$. En particular, RG es local si y sólo si R es local y $\Delta(G) \subset J(RG)$.*

Los anteriores resultados involucran los conceptos de epimorfismo y subgrupo normal. Sin embargo, en el siguiente resultado se presentará la localidad en anillos de grupo teniendo en cuenta tanto el radical de Jacobson del anillo como el del anillo de grupo.

Proposición 4.0.4. *Suponga que RG es local y $H \in S(G)$. Entonces RH es local y $J(RH) = J(RG) \cap RH$. En particular, $J(R) = J(RG) \cap R$.*

Demostración. Suponga que $r \in \Delta(G, H)$, entonces $\sum_{h \in H} r_h = 0$. Por lo tanto, $r \in \Delta(G) \subset J(RG)$ ya que RG es local. Por la Proposición 2.0.9, siempre se tiene que $J(RG) \cap RH \subset J(RH)$, luego $r \in J(RH)$ y así $\Delta(G, H) \subset J(RH)$. Como R es local, sigue del Corolario 4.0.3 que RH es local.
Sea $r \in RH \setminus J(RG)$, luego, r es unidad en RG por la Proposición 3.0.3. Dado que $r \in RH$, por [1,Pág 252] r es unidad en RH, entonces $r \notin J(RH)$. Por consecuencia $J(RH) \subset J(RG) \cap RH$.

□

---

1 S.A AMITSUR. “On the semi-simplicity of group algebras”. En: 6 (1959), págs. 251-253.

El siguiente corolario busca garantizar la recíproca de la anterior proposición.

Corolario 4.0.5. *RG es local si y sólo si RH es local para todo $H \in S(G)$ finitamente generado.*

Demostración. Sea RG local, sigue de la proposición anterior, que RH es local. Recíprocamente, sea $r \in \Delta(G)$. Si H es un subgrupo finitamente generado por el soporte de r, entonces $r \in \Delta(G, H) \subset J(RH)$. Luego r es cuasi-regular, y así, $\Delta(G)$ es un ideal cuasi-regular por la Proposición 1.2.25. Por lo tanto, $\Delta(G) \subset J(RG)$. Más aún, RG es local por el Corolario 4.0.3.

□

Se necesita conocer las condiciones necesarias en términos del grupo y el anillo, para determinar cuándo un anillo de grupo es local, queriendo generalizar los resultados de las Proposiciones 4.0.1 y 4.0.2. Por lo tanto ya se tienen las herramientas tanto anillo teóricas como propias de los anillos de grupo, que permiten enunciar el resultado principal de esta monografía, el cual será demostrado en detalle y hace parte del articulo de Nicholson, [[4], Pág 138].

Teorema 4.0.6. *Sean R un anillo y G un grupo.*

1. *Si RG es local, entonces R es local, G es un p-grupo y $p \in J(R)$.*
2. *Si R es local, G es un p-grupo localmente finito y $p \in J(R)$, entonces RG es local.*
3. *Si G es abeliano, entonces RG es local si y sólo si R es local, G es un p-grupo y $p \in J(R)$.*

Demostración.

1. Por el Corolario 4.0.3, si RG es local, entonces R es local. Además, se sigue del ítem uno de la Proposición 2.0.10 que si $\Delta(G) \subset J(RG)$, entonces G es un p-grupo y $p \in J(R)$.

2. Dado el Corolario 4.0.5 asuma que G es finitamente generado, y así, dado que G es localmente finito, entonces G es finito. Sea $\bar{R}$ el anillo de división $R/J(R)$, por lo tanto existe un epimorfismo $\phi : RG :\twoheadrightarrow \bar{R}G$ con

$$ker_\phi = \{r \in RG : r_g \in J(R), \forall g \in G\}.$$

Dado que G es localmente finito, entonces $ker_\phi \subset J(RG)$, debido a la Proposición 2.0.9. Como $\bar{R}$ es un anillo de división con característica p y G es un p-grupo finito con $p \in J(R)$, del ítem dos de la Proposición 2.0.10, $\Delta(\bar{R}G)$ es nilpotente. Sigue de la Proposición 1.2.28 que $\Delta(\bar{R}G) \subset J(\bar{R}G)$, por lo tanto $\bar{R}G$ es local por el Corolario 4.0.3. Luego se sigue del Lema 3.0.5 que RG es local.

3. Se sigue de los resultados anteriores.

□

Observación 4.0.7.

1. *La prueba del ítem dos se cumple si se reemplaza la condición de que G es localmente finito por:*

   1) $J(R) \subset J(RG)$;

   2) $\bar{R}G$ es local.

2. *Recuerde que el resultado del ítem tres es la generalización de los resultados propuestos por Gulliksen, Ribenboim y Viswanathan, [3, (h) & (i), pág 153], quienes probaron ésto asumiendo que el anillo R es conmutativo.*

Ejemplo 4.0.8.

1. *Por el primer ítem de la Proposición 3.0.2 el anillo de grupo $\mathbb{F}_2C_2 = \{0, 1, x, 1 + x\}$ es local con único ideal maximal $\mathfrak{m} = \{0, 1 + x\}$, dado que $\{1, x\} \subset \mathcal{U}(\mathbb{F}_2C_2)$.*

2. *Sean $\mathbb{F}$ un cuerpo de $car(\mathbb{F}) = p$ y G un p-grupo abeliano. Dado que $\mathbb{F}$ tiene característica p se sigue que $1 = 1 - pt \in \mathcal{U}(\mathbb{F})$ para todo $t \in \mathbb{F}$, entonces $p \in J(\mathbb{F})$ por la Proposición 1.2.20. Por tanto del Teorema 4.0.6, $\mathbb{F}G$ es un anillo de grupo local.*

3. *Sean $R = \mathbb{Z}_p$ y $G = C_{p^n}$ el grupo cíclico de p^n elementos. Se sabe que $ord(a) = |\langle a \rangle|$ y así del Teorema de Lagrange [*] G es un p-grupo. De las ideas del ejemplo anterior, se tiene que RG es anillo de grupo local.*

4. *Sean $R = \mathbb{Z}_2$ y $G = \mathcal{Q}_8$, luego G es un 2-grupo localmente finito, por lo tanto RG es un anillo de grupo local.*

5. *Sean C_2 el grupo cíclio de orden 2 y $\mathbb{C}$ el cuerpo de los complejos, luego $\mathbb{C}$ es un anillo local con característica 0, entonces,*

$$\mathbb{C}C_2 \cong \mathbb{C}[x]/\langle x^2 - 1\rangle \cong \mathbb{C}[x]/\langle x - 1\rangle \times \mathbb{C}[x]/\langle x + 1\rangle \cong \mathbb{C} \times \mathbb{C},$$

por lo tanto, $\mathbb{C}C_2$ **no es un anillo de grupo local**, *ya que $\langle x-1\rangle$ y $\langle x+1\rangle$ son ideales maximales en $\mathbb{C}[x]/\langle x^2-1\rangle$. De hecho, $J(\mathbb{C}) = 0$, por lo tanto no cumple la condición de que $p \in J(R)$ del Teorema 4.0.6.*

---

[*] Dados un grupo finito G y $H \preceq G$ un subgrupo. Entonces el orden de H divide al orden de G, es decir, $|H|||G|$.

BIBLIOGRAFÍA

AMITSUR, S.A. “On the semi-simplicity of group algebras”. En: 6 (1959), págs. 251-253 (vid. pág. 52).

ATIYAH, Michael. *Introduction to commutative algebra*. 1st Edition. CRC Press, 2018 (vid. págs. 10, 42, 46).

BHATTACHARYA, Phani Bhushan, Surender Kumar JAIN y SR NAGPAUL. *Basic abstract algebra*. 2nd Edition. Cambridge University Press, 1994 (vid. págs. 10, 20).

CONNELL, Ian G. “On the group ring”. En: *CJM* 15 (1963), págs. 650-685 (vid. págs. 39-41).

GALLIAN, J. *Contemporary abstract algebra*. 8th Edition. North-Holland Publishing Company, 2021 (vid. pág. 10).

GULLIKSEN, Tor, Paulo RIBENBOIM y T.M VISWANATHAN. “An elementary note on group-rings.” En: (1970) (vid. págs. 9, 50, 54).

NAGATA, Masayoshi. “Local rings”. En: *Interscience Tracts in Pure and Appl. Math.* (1962) (vid. pág. 8).

NICHOLSON, W. K. “Local group rings”. En: *CMB* 15.1 (1972), 137
bibrangedash 138 (vid. págs. 9, 53).

POLCINO MILIES, César y Sudarshan K SEHGAL. *An introduction to group rings*. 1st Edition. Vol. 1. Springer Science & Business Media, 2002 (vid. págs. 9, 10, 18, 36).