INVOLUCIONES Y ANILLOS DE GRUPO CLEAN

CRISTIAN ALEXANDER SARMIENTO OJEDA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2022

INVOLUCIONES Y ANILLOS DE GRUPO CLEAN

CRISTIAN ALEXANDER SARMIENTO OJEDA

Trabajo de Grado para optar al tÃtulo de
Matemático

Director
Alexander Holguín Villa
Doctor en Ciencias Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
BUCARAMANGA
2022

AGRADECIMIENTOS

Agradezco a mis padres Beatriz y Gustavo por darme siempre su apoyo, a mis hermanos Carlos y Diana por ser inspiración y darme su confianza. Agradezco también al profesor Holguín por tenerme paciencia y brindarme su experiencia y conocimiento durante el desarrollo de este trabajo. Por último, a mis compañeros y amigos quienes mejoraron la experiencia de la universidad y con quienes batallamos en equipo para llegar al final.

CONTENIDO

RESUMEN

TÍTULO: INVOLUCIONES Y ANILLOS DE GRUPO CLEAN [*]

AUTOR: CRISTIAN ALEXANDER SARMIENTO OJEDA [**]

PALABRAS CLAVE: ANILLOS DE GRUPO, ANILLOS CLEAN, ANILLOS $*$-CLEAN.

DESCRIPCIÓN:

Un anillo es llamado clean si cada uno de sus elementos puede ser escrito como la suma de una unidad y un idempotente. Entre los anillos con involución y la propiedad clean existe una conexión que permite obtener una generalización de esta propiedad, conocida como propiedad $*$-clean. Un anillo con involución $*$ es llamado $*$-clean si cada uno de sus elementos puede ser escrito como la suma de una unidad y una proyección.

El trabajo consta de tres capítulos. En el primero se abarcan los conceptos necesarios para el desarrollo del tema. En el segundo capítulo, se introduce la propiedad clean tanto en anillos como en anillos de grupo y se presentan algunas de sus propiedades. En el tercer y último capítulo se presentan condiciones necesarias y suficientes para que el anillo de grupo RG sea $*$-clean, donde R es un anillo local conmutativo, G es uno de los grupos C_3, C_4, S_3 o $\mathbb{Q}_8$ y $*$ es la involución clásica en RG, es decir, la extención R lineal de $* : G \to G, g \mapsto g^{-1}$ para todo $g \in G$.

---

[*] Trabajo de grado

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

ABSTRACT

TITLE: INVOLUTIONS AND CLEAN GROUP RINGS [*]

AUTHOR: CRISTIAN ALEXANDER SARMIENTO OJEDA [**]

KEYWORDS: GROUP RINGS, CLEAN RINGS, $*$-CLEAN RINGS.

DESCRIPTION:

A ring is called clean if each of its elements is the sum of a unit and an idempotent. There is a conection between rings with involution and clean rings that allow us to get a generalization of this property, known as $*$-clean property. A ring with involution $*$ is called $*$-clean if each of its elements can be written as the sum of a unit and a projection.

This work consists of three chapters. The first covers the concespts needed for the development of the topics. In the second chapter, we introduce the clean property in both rings and group rings presenting some of its properties. Finally, in the third chapter we present necessary and sufficient conditions for the group ring RG to be clean, where R is a commutative local ring, G is one of the groups C_3, C_4, S_3 or $\mathbb{Q}_8$ and $*$ is the classical involution on RG, that is, the R-linear extension of $* : G \to G, g \mapsto g^{-1}$, for all $g \in G$.

---

[*] Bachelor Thesis

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

INTRODUCCIÓN

Un elemento a en un anillo R (asociativo con unidad) es llamado clean si este puede escribirse como la suma de una unidad y un idempotente de R. Un anillo R es llamado anillo clean si todos sus elementos son clean.

Probablemente el concepto de anillo clean aparece por primera vez en el trabajo de W. K. Nicholson *Lifting Idempotents and Exchange Rings* [1]. Su objetivo en ese artículo era probar que un anillo A es un anillo “exchange"si y solo si los elementos idempotentes pueden ser levantados módulo todo ideal a izquierda.

Este estudio no finalizó ahí, sino que motivó a diversos autores a estudiar estos anillos desde diferentes perspectivas, como por ejemplo la dada por W. W. McGovern en [2] que hace un estudio de los anillos conmutativos clean. En esa misma línea se encuentran trabajos como el desarrollado por D. D. Anderson y V. P. Camillo, *Commutative rings whose elements are a sum of a unit and idempotent* [3], donde entre los resultados, para R anillo conmutativo, se establece que $R[x]$ (anillo de polinomios sobre R) nunca es un anillo clean y que el anillo de series formales $R[[x]]$ es clean si y solo si R es anillo clean.

En general, saber cuándo el anillo de grupo RG es clean es una pregunta abierta. Por ejemplo se sabe que para todo anillo conmutativo clean R y el grupo cíclico C_2, RC_2

---

[1] W. K. Nicholson. “Lifting idempotents and exchange rings”. En: *Transactions of the American Mathematical Society* 229 (1977), págs. 269-278.

[2] W. W. McGovern. “Neat rings”. En: *Journal of Pure and Applied Algebra* 205.2 (2006), págs. 243-265.

[3] D. D. Anderson y V. P. Camillo. “Commutative rings whose elements are a sum of a unit and idempotent”. En: *Comm. Algebra* 30.7 (2002), págs. 3327-3336.

es anillo clean, sin embargo, para R anillo arbitrario tal respuesta no se sabe.

La pregunta de ser anillo clean en el contexto de los anillos de grupo, fue considerada por primera vez por *Han y Nicholson* en [4], donde por ejemplo es probado que para un anillo R Booleano y G un grupo localmente finito, RG es un anillo clean, más exactamente, es demostrado que $\mathbb{Z}_{(7)}C_3$ no es un anillo clean, donde $\mathbb{Z}_{(7)}$ denota el anillo $\mathbb{Z}$ localizado en el ideal primo (7) y C_3 el grupo cíclico de orden 3, usando que RG no es semiperfecto, hecho demostrado por S. Woods en [5].

En 2010 *Vaš* introdujo los anillos $*$-clean en [6]. En [7] se investiga la propiedad $*$-clean en anillos de grupo. Es interesante determinar cuándo un anillo de grupo de un grupo cíclico finito sobre un anillo local conmutativo es $*$-clean. Parece que en general esta es una pregunta extremadamente desafiante, sin embargo es posible determinar cuándo ciertos anillos de grupo de grupos pequeños son $*$-clean. Sean C_n, S_3 y $\mathbb{Q}_8$ los grupos cíclico de orden n, simétrico de grado 3 y cuaternio de orden 8, respectivamente. En [7] se obtienen condiciones necesarias y suficientes para que RG sea $*$-clean en términos de la solubilidad de ciertas ecuaciones en R, donde R es un anillo local conmutativo, y G es uno de los grupos C_3, C_4, S_3 y $\mathbb{Q}_8$. Como consecuencia de la clasificación allí presentada, se tiene una gran cantidad de ejemplos de anillos de grupo que son clean pero no $*$-clean.

---

[4] J. Han y W. Nicholson. “Extensions of clean rings”. En: *Comm. Algebra* 29.6 (2001), págs. 2589-2595.

[5] S. M. Woods. “Some Results on Semi-Perfect Group Rings”. En: *Canad. J. of Math* 26.1 (1974), 121â€“129.

[6] L. Vaš. “$*$-Clean rings; some clean and almost clean Baer$*$-rings and von Neumann algebras”. En: *Journal of Algebra* 324.12 (2010), págs. 3388-3400.

[7] Y. Gao, J. Chen e Y. Li. “Some $*$-clean group rings”. En: *Algebra Colloquium*. Vol. 22. World Scientific. 2015, págs. 169-180.

Esta monografía se basa principalmente en el artículo [7], donde se dan resultados sobre la propiedad $*$-clean para anillos de grupo de grupos abelianos y no abelianos. Para anillos de grupo de grupos abelianos, se estudia el caso en el que R es un anillo local conmutativo y G es C_3 o C_4, los grupos cíclicos de orden 3 y 4 respectivamente. En este caso, los resultados proveen condiciones necesarias y suficientes para que los anillos de grupo mencionados sean $*$-clean. En el caso de anillos de grupo no conmutativos, se considera de nuevo a R siendo anillo local conmutativo y $G = S_3$, el grupo simétrico de orden 3, o $G = \mathbb{Q}_8$, el grupo cuaternio de orden 8. Nuestro objetivo es entender las técnicas y resultados de este trabajo y demostrarlos en detalle.

1. PRELIMINARES

En esta parte se presentan las notaciones, definiciones y propiedades básicas que se usarán a lo largo de los capítulos siguientes.

1.1. Grupos

Los grupos representan entre las estructuras abstractas con una operación binaria, aquellas con mayores propiedades algebraicas y son de vital importancia para este trabajo. Siguiendo [8], se tiene la siguiente definición

Definición 1.1. Sea G un conjunto no vacío junto con una operación binaria. Se dice que G es un **grupo** si satisface las siguientes condiciones.

1. Para todos $a, b, c \in G, (ab)c = a(bc)$. (**Asociatividad**)
2. Existe un elemento $e \in G$, tal que $ea = ae = a$ para todo $a \in G$. (**Existencia de neutro**)
3. Para todo $a \in G$, existe $b \in G$ tal que $ab = ba = e$. (**Existencia de inverso**)

Si adicionalmente G satisface que, $ab = ba$ para todo par de elementos $a, b \in G$, se dice que G es un **grupo abeliano**. Se llamará **semigrupo** al conjunto G si la operación binaria definida sobre él es únicamente asociativa. Si el conjunto G es finito, entonces el número de elementos de G es llamado su **orden** y es denotado por $|G|$. 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 y será denotado por $|a|$.

---

[8] J. Gallian. *Contemporary abstract algebra*. Nelson Education, 2009.

A continuación se mencionan algunos ejemplos de grupos conocidos.

Ejemplo 1.2. Los conjuntos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son grupos con la suma usual. En cada caso el elemento identidad es el 0 y el inverso de a es $-a$. Más aún, todos ellos son grupos abelianos.
El conjunto de los enteros $\mathbb{Z}$ con la multiplicación usual no es grupo ya que no satisface la propiedad 3 en la Definición 1.1. Por ejemplo, no existe $a \in \mathbb{Z}$ tal que $4a = 1$.

Definición 1.3. Sea M un conjunto. Una función biyectiva de M en M es llamada una **permutación** de M. Claramente la función identidad es una permutación y tanto la composición de dos permutaciones como la inversa de una permutación son permutaciones. Por tanto, es fácil demostrar que el conjunto de todas las permutaciones de un conjunto M es un grupo bajo la composición de funciones, denotado por S_M y llamado **grupo simétrico sobre** M. En el caso particular $M = \{1, 2, ..., n\}$, S_M es llamado **grupo simétrico de orden** n y es denotado simplemente por S_n.

Ejemplo 1.4. Es de particular importancia para este trabajo el grupo simétrico de orden 3

$$S_3 = \langle a, b \mid a^3 = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle,$$

que por extensión viene dado por

$$\{1, a, a^2, b, ab, a^2b\},$$

y que claramente es un grupo finito. Además S_3 es un grupo no abeliano, dado que de la relación $b^{-1}ab = a$, se sigue que $ab = ba^{-1} \neq ba$.

Definición 1.5. 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 restricta a él. En tal caso se escribe $H \leq G$.

A continuación se presenta una clase de grupos de mucha importancia en este trabajo.

Definición 1.6. Un grupo G es llamado **cíclico** si existe un elemento $a \in G$ tal que $G = \{a^n | n \in \mathbb{Z}\}$. En este caso a es llamado un **generador** de G.
Sea $\emptyset \neq S \subseteq G$ con S finito. Se dice que G es un grupo finitamente generado si se puede escribir como $G = \langle g_1, g_2, ..., g_k \rangle = \{g_1^{r_1} g_2^{r_2} ... g_k^{r_k} \mid g_k \in S, r_k = \pm 1, k \geq 1\} \cup \{e\}$.

El siguiente resultado exhibe las principales características de los grupos cíclicos. Más aún este es considerado un teorema clave en el estudio de esta clase de grupos.

Teorema 1.7. *Todo subgrupo de un grupo cíclico es cíclico. Si además, el orden del grupo es n, para cada divisor k de n, el grupo tiene un subgrupo de orden k.*

Dado un subgrupo H de G y un elemento en G, es posible definir una partición del grupo G por subconjuntos disjuntos.

Definición 1.8. Sea H un subgrupo de un grupo G. Dado un elemento $a \in G$, los subconjuntos de la forma

$$aH = \{ah \mid h \in H\} \qquad \text{y} \qquad Ha = \{ha \mid h \in H\},$$

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

Sea $H \subset G$. La cardinalidad de los conjuntos de clases laterales a izquierda y de clases laterales a derecha, denotado por $[G : H]$, coinciden y es llamado **índice** de H en

G.

El siguiente teorema debido a J. Lagrange es fundamental en la teoría de grupos finitos y provee una lista de candidatos a ser subgrupos entre los subconjuntos de orden divisor el orden de G.

Teorema 1.9 (Teorema de Lagrange)**.** *Si G es un grupo finito y H es un subgrupo de G, entonces $|H|$ divide a $|G|$. Además, el número de clases laterales a izquierda (o derecha) de H en G es $|G|/|H|$.*

Definición 1.10. Sea H un subgrupo de un grupo G, se dice que H es **normal** en G si $aH = Ha$ para todo $a \in G$, y se denota por $H \trianglelefteq G$.

A continuación se presenta un subconjunto especial de un grupo G de gran importancia en la teoría de grupos y de particular relevancia en este trabajo.

Definición 1.11. Sea G un grupo. Se define el **centro** de G por

$$\mathcal{Z}(G) = \{x \in G \mid xg = gx, \forall g \in G\}.$$

Es posible demostrar que $\mathcal{Z}(G)$ es un subgrupo de G, más exactamente $\mathcal{Z}(G)$ es un grupo normal de G.

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

$$G/H = \{gH \mid g \in G\}.$$

Es un ejercicio simple establecer que el conjunto G/H de todas las clases laterales

tiene estructura de grupo con la operación

$$aHbH = (ab)H;\ a, b \in G,$$

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

A continuación se presenta un resultado que permite catalogar grupos al dar condiciones a uno de sus grupos cocientes.

Proposición 1.12. *Si G es un grupo con centro $\mathcal{Z}(G)$ y si $G/\mathcal{Z}(G)$ es cíclico, entonces G es abeliano.*

Demostración. Suponga $G/\mathcal{Z}(G)$ generado por $x\mathcal{Z}(G)$ para $x \in G$ y, sean $a, b \in G$. Entonces $a\mathcal{Z}(G)$ y $b\mathcal{Z}(G)$ como elementos de $G/\mathcal{Z}(G)$ son de la forma $a\mathcal{Z}(G) = x^m\mathcal{Z}(G)$ y $b\mathcal{Z}(G) = x^n\mathcal{Z}(G)$ para algunos enteros m y n. Por tanto,

$$a = x^m z_1, \quad b = x^n z_2; \quad z_1, z_2 \in \mathcal{Z}(G).$$

Dado que $z_1, z_2 \in \mathcal{Z}(G)$ y que $x^m x^n = x^n x^m$, se tiene que

$$ab = (x^m z_1)(x^n z_2) = x^{m+n} z_1 z_2 = x^{n+m} z_2 z_1 = (x^n z_2)(x^m z_1) = ba.$$

Como a y b son arbitrarios, se concluye que G es abeliano.

Definición 1.13. Un **homomorfismo** ϕ de un grupo G en un grupo H es una función de G en H que preserva la operación de grupo, es decir, $\phi(ab) = \phi(a)\phi(b)$ para todos $a, b \in G$. Si además ϕ es inyectiva (sobreyectiva o biyectiva), ϕ es llamado un **monomorfismo** (**epimorfismo** o **isomorfismo**), respectivamente. En el último caso, se dice que G y H son grupos isomorfos, denotando este hecho por $G \cong H$.

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

$$Ker(\phi) = \{g \in G \mid \phi(g) = 1_H\} \qquad \text{y} \qquad Im(\phi) = \{\phi(g) \mid g \in G\}.$$

Algunas de las principales características de los homomorfismos de grupos se enuncian a continuación.

Proposición 1.14. *Sea $\phi : G \to H$ un homomorfismo de grupos, entonces:*

1. $\phi(e_G) = e_H$.
2. $\phi(g^{-1}) = \phi(g)^{-1}$.
3. *Si $n \in \mathbb{Z}$ entonces* $\phi(g^n) = \phi(g)^n$
4. $Ker(\phi) \trianglelefteq G$.
5. ϕ *es inyectiva si y solo si* $Ker(\phi) = \{e_G\}$.
6. $Im(\phi) \leq H$

Teorema 1.15 (Primer Teorema de Isomorfismos)**.** *Sea $\phi : G \to H$ un homomorfismo de grupos, entonces*

$$G/Ker(\phi) \cong Im(\phi).$$

En particular, si ϕ es un epimorfismo, entonces $G/Ker(\phi) \cong H$.

A continuación se presenta un concepto que será de utilidad más adelante.

Definición 1.16. Sean G un grupo y p un entero primo.

1. Un elemento $x \in G$ es llamado p**-elemento** si su orden es una potencia de p, y x se dice p'**-elemento** si su orden es infinito o no divisible por p.
2. Si G es finito, se dice que G es p**-grupo**, si su orden $|G|$ es una potencia de p.

3. Se dice que G es p**-abeliano elemental**, si G es abeliano y todo elemento $g \in G$, exceptuando la identidad, tiene orden p.

Definición 1.17. Sea G un grupo, el **exponente** de G, es el menor entero positivo k tal que $g^k = 1$, para todo $g \in G$. Si tal entero existe se denota por $exp(G) = k$.

Note que si G es un grupo, la condición de ser p-abeliano elemental es necesaria y suficiente para que $exp(G) = p$.

Ejemplo 1.18. Un grupo de interés en la teoría de anillos de grupo y, en particular de este trabajo, es el grupo de los cuaternios de orden 8, que tiene la siguiente presentación, [9]

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

que por extensión viene dado por

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

y así es un grupo finito. Además, de la relación $b^{-1}ab = a^{-1}$, $ba = a^{-1}b \neq ab$.
Lo que muestra que $\mathbb{Q}_8$ es un grupo no abeliano. Una característica relevante de $\mathbb{Q}_8$ es que todos sus subgrupos son normales.

Algunas otras propiedades de $\mathbb{Q}_8$ son las siguientes:

- a^2 es el único elemento diferente de la identidad que conmuta con los restantes y así, $\mathcal{Z}(\mathbb{Q}_8) = \{1, a^2\}$.
- Para todo $x \in \mathbb{Q}_8, x^{2^k} = 1$ para algún $k \in \mathbb{N}$, es decir, $\mathbb{Q}_8$ es un 2-grupo.

---

[9] C. Polcino Millies y S. K. Sehgal. *An introduction to group rings*. Vol. 1. Springer Science & Business Media, 2002.

- Como $|\mathbb{Q}_8/\mathcal{Z}(\mathbb{Q}_8)| = 4$, entonces

$$\mathbb{Q}_8/\mathcal{Z}(\mathbb{Q}_8) \cong C_4 \quad \text{o} \quad \mathbb{Q}_8/\mathcal{Z}(\mathbb{Q}_8) \cong C_2 \times C_2.$$

  Como $\mathbb{Q}_8$ no es abeliano, sigue de la Proposición 1.12 y de la caracterización de grupos de orden 4, que $\mathbb{Q}_8/\mathcal{Z}(\mathbb{Q}_8)$ es isomorfo al 4-grupo de Klein[10], es decir, $\mathbb{Q}_8/\mathcal{Z}(\mathbb{Q}_8) \cong C_2 \times C_2$.

Como ya se notó, el grupo cuaternio, $\mathbb{Q}_8$ es no abeliano y todo subgrupo H de él es normal. Esta característica motiva la siguiente definición.

Definición 1.19. Un grupo no abeliano G en el cual todos sus subgrupos son normales, es llamado grupo **Hamiltoniano**.

El siguiente resultado, debido a R. Dedekind y R. Baer caracteriza los grupos Hamiltonianos. Para una demostración de este hecho ver [9].

Teorema 1.20. *Un grupo G es Hamiltoniano si y solo si*

$$G \cong \mathbb{Q}_8 \times E \times A,$$

donde E es un 2-grupo abeliano elemental y A es un grupo abeliano en el cual todos sus elementos son de orden impar.

Cuando $A = \{1\}, G$ es llamado grupo 2-Hamiltoniano. Note que todo grupo Hamiltoniano o 2-Hamiltoniano contiene una copia de $\mathbb{Q}_8$.

---

[10] Llamado así en honor al matemático alemán F. Klein, y denotado generalmente con la letra V, por la palabra en alemán *Vierergruppe*, que significa “grupo de cuatro". Una característica importante del grupo V es que todos sus elementos diferentes de la identidad son de orden 2, es decir, cada uno de ellos es su propio inverso. Usando una tabla de Cayley se puede observar que el tercer elemento no trivial es el producto de los dos primeros y así, una presentación para este es $V = \langle x, y | x^2 = y^2 = (xy)^2 = e \rangle$.

A continuación se define una aplicación de especial interés para este trabajo.

Definición 1.21. Sea G un grupo. La aplicación $* : G \to G$ es llamada una **involución** si $*$ es un anti-homomorfismo de orden 2, es decir, si para todos $g, h \in G$ se verifica que

$$(gh)^* = h^* g^* \qquad \text{y} \qquad (g^*)^* = g.$$

Ejemplo 1.22. Sea G un grupo. Entonces la aplicación $* : G \to G$ definida por $g^* = g^{-1}$, verifica que para todos $g, h \in G$

$$(gh)^* = (gh)^{-1} = h^{-1}g^{-1} = h^* g^* \qquad \text{y} \qquad (g^*)^* = (g^{-1})^{-1} = g,$$

es decir, $*$ es una involución sobre G, conocida en la literatura como la **involución clásica**.

1.2. Anillos

Otro concepto de vital importancia para este trabajo es el de anillo. A continuación se presenta dicha noción y algunas de sus propiedades mas importantes.

Definición 1.23. Un **anillo** es una tripleta $(R, +, \cdot)$ que consiste de un conjunto no vacío R y dos operaciones binarias definidas sobre R que verifican:

1. $(R, +)$ es un grupo abeliano.
2. $(R, \cdot)$ es un semigrupo.
3. La operación " $\cdot$ " es distributiva sobre la operación " $+$ ".

Si además, $xy = yx$ para todos $x, y \in R$, el anillo es llamado conmutativo. Por otro lado, si en R existe un elemento identidad, usualmente denotado por $1 = 1_R$, tal que $1x = x1 = x$, para todo $x \in R$, se llama a R anillo con unidad o identidad.

Ejemplo 1.24. Algunos ejemplos de anillos son los siguientes.

- $\mathbb{Z}$ con la suma y producto usuales, es un anillo conmutativo con unidad .
- Dado un anillo $(R, +, \cdot)$, 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.
- Dado $n \in \mathbb{N}$, $\mathbb{Z}_n$, el conjunto de los enteros módulo n, es un anillo conmutativo con unidad con la suma y el producto módulo n.

Algunos elementos distinguidos en un anillo que serán de uso frecuente a lo largo del trabajo son los siguientes.

Definición 1.25. Sea R un anillo.

1. Si R tiene identidad $1 = 1_R$ y para $u \in R$, existe $v \in R$ tal que $uv = vu = 1$, entonces se dice que u es una unidad de R
2. Un elemento $e \in R$ es llamado **idempotente**, si $e^2 = e$. Claramente 0 y 1 (en caso de que R sea un anillo con unidad) son elementos idempotentes. Un idempotente distinto de estos es llamado **idempotente no trivial**.
3. Un elemento $x \in R$ es llamado **nilpotente**, si existe un entero $n > 0$ tal que $x^n = 0$.
4. Un elemento $x \in R$ es **cuasi-regular**, si existe $y \in R$, tal que $x + y = xy$.

Como es usual en la literatura, se denotarán respectivamente por $\mathcal{U}(R)$, $\mathcal{I}d(R)$, η_R y $Q_{reg}(R)$, al grupo de unidades, a los conjuntos de elementos idempotentes, nilpotentes y cuasi-regulares.

En un anillo R, un **divisor de cero** es un elemento x para el cual existe $y \neq 0_R$ en R tal que $xy = 0$. Un anillo conmutativo R que no tenga divisores de cero (excluyendo a 0_R) es llamado **dominio entero**. Por otro lado, R es llamado **anillo de división**, si todos sus elementos no cero son invertibles, es decir, si $R \setminus \{0\} = \mathcal{U}(R)$. En este último caso, si R es conmutativo, R es denominado **cuerpo**.

Es importante notar que todo cuerpo es un dominio entero, más aún, es un anillo de división. Sin embargo, la recíproca no siempre es cierta. Para el primer caso, el anillo de los enteros $\mathbb{Z}$ es un dominio que no es un cuerpo. A continuación un ejemplo concreto de un anillo de división que no es cuerpo.

Ejemplo 1.26. Sean $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ símbolos dados y considere $\mathcal{H}_{\mathbb{R}}$ el conjunto de todas las expresiones de la forma $x_0 + x_1 i + x_2 j + x_3 k$ donde los coeficientes x_0, x_1, x_2, x_3 son números reales.

Se define la suma de dos elementos de $\mathcal{H}_{\mathbb{R}}$ por

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

Ahora bien, la multiplicación (usando la ley distributiva) queda totalmente definida por el producto entre los símbolos $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ definido como sigue

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1, \quad \boldsymbol{ij} = \boldsymbol{k} = -\boldsymbol{ji}, \quad \boldsymbol{jk} = \boldsymbol{i} = -\boldsymbol{kj}, \quad \boldsymbol{ki} = \boldsymbol{j} = -\boldsymbol{ik}. \tag{1}$$

Mediante un cálculo directo se muestra que $\mathcal{H}_{\mathbb{R}}$ con las operaciones definidas anteriormente es un anillo, llamado el anillo de los cuaternios reales y de la ecuación (1) que es no conmutativo. Dado un cuaternio $\alpha = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k}$, se define su conjugado

$\overline{\alpha}$ y norma $||\alpha||$, respectivamente por

$$\overline{\alpha} = x_0 - x_1\boldsymbol{i} - x_2\boldsymbol{j} - x_3\boldsymbol{k} \quad \text{y} \quad ||\alpha|| = \alpha\overline{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

Usando las definiciones anteriores, es fácil probar que

- $||\alpha\beta|| = ||\alpha||\,||\beta|| = ||\beta\alpha||$
- $||\alpha|| \geq 0$ y $||\alpha|| = 0$ si y solo si $\alpha = 0$

Por otro lado, si $\alpha \in \mathcal{H}_{\mathbb{R}}$ es diferente de cero, se tiene que $||\alpha|| \neq 0$, por lo tanto se puede definir $\alpha' = \overline{\alpha}/||\alpha||$. Y así,

$$\alpha\alpha' = \alpha\frac{\overline{\alpha}}{||\alpha||} = \frac{||\alpha||}{||\alpha||} = 1 = \frac{\overline{\alpha}}{||\alpha||}\alpha = \alpha'\alpha.$$

De lo anterior sigue que $\alpha' = \alpha^{-1}$, el inverso multiplicativo de α. En otras palabras, todo elemento diferente de cero en $\mathcal{H}_{\mathbb{R}}$ es invertible, es decir, $\mathcal{H}_{\mathbb{R}}$ es un anillo de división.
Si en el razonamiento anterior, se restringen los coeficientes al cuerpo de los números racionales $\mathbb{Q}$, todos los argumentos anteriores siguen funcionando, obteniendo el anillo $\mathcal{H}_{\mathbb{Q}}$ de cuaternios racionales, es decir, $\mathcal{H}_{\mathbb{Q}}$ también es un anillo de división. Por otro lado, si los coeficientes se toman en el cuerpo de los números complejos $\mathbb{C}$, se sigue obteniendo un anillo $\mathcal{H}_{\mathbb{C}}$. Sin embargo, $\alpha = 1 + i = 1 + i(1) \in \mathcal{H}_{\mathbb{C}}$ es no cero y $||\alpha|| = 1 + i^2 = 0$, por lo que no es un anillo de división. De hecho, se puede mostrar que $\mathcal{H}_{\mathbb{C}}$ es isomorfo a $M_2(\mathbb{C})$, el anillo de matrices 2×2 con entradas en $\mathbb{C}$, vía la aplicación

$$\alpha = x_0 + x_1\boldsymbol{i} + x_2\boldsymbol{j} + x_3\boldsymbol{k} \quad \mapsto \quad \begin{bmatrix} x_0 & x_1 \\ x_2 & x_3 \end{bmatrix}.$$

Ejemplo 1.27. Considere la familia de anillos $\{R_i\}_{i\in\Lambda}$. El conjunto

$$\prod_{i\in\Lambda} R_i = \{(a_i)_{i\in\Lambda} = (a_1, a_2, ...,) \mid a_i \in R_i, \forall i \in \Lambda\},$$

con la suma y el producto componente a componente es un anillo, llamado el **producto directo** de la familia $\{R_i\}_{i\in\Lambda}$.
Por otro lado, considere el conjunto $S \subseteq \prod_{i\in\Lambda} R_i$ tal que si $(a_i)_{i\in\Lambda} \in S$, solo un número finito de sus componentes son diferentes de cero. Es un ejercicio sencillo verificar que S es un subanillo de $\prod_{i\in\Lambda} R_i$. Este anillo es llamado la **suma directa** de la familia $\{R_i\}_{i\in\Lambda}$ y es denotado por

$$\bigoplus_{i\in\Lambda} R_i.$$

Note que si la familia $\{R_i\}_{i\in\Lambda}$ es finita, entonces $\prod_{i\in\Lambda} R_i = \bigoplus_{i\in\Lambda} R_i$.

La noción de ideal que se considera a continuación, se debe a R. Dedekind, un alumno de K. F. Gauss, quien la introdujo mientras desarrollaba la teoría de números algebraicos. Su aplicación a otras ramas de las matemáticas comenzó a hacerse evidente en 1882, cuando L. Kronecker (1823-1891), un estudiante de E. Kummer, introdujo ideales de polinomios en sus estudios de geometría algebraica.

Definición 1.28. Un subconjunto I de un anillo R es llamado **ideal a izquierda** de R, denotado por $I \preccurlyeq_{\mathfrak{l}} R$ si

1. $a, b \in I$ implica que $(a - b) \in I$
2. $a \in I$ y $r \in R$ implica que $ra \in I$.

Análogamente se define un **ideal a derecha** de R ($I \preccurlyeq_{\mathfrak{r}} R$). Finalmente, un subconjunto no vacío I de R es llamado un ideal o ideal bilateral de R si es a la vez un ideal a izquierda y a derecha de R.
Los subconjuntos $\mathcal{O} = \{0\}$ y R siempre son ideales de R, llamados ideales triviales. Si un ideal I es diferente de R, es llamado **ideal propio**.

Nota 1.29. Si un ideal I de un anillo R contiene un elemento invertible a, entonces $I = R$. En efecto, suponga que I es un ideal a izquierda de R y que $a \in I$ es invertible.

Luego $1 = a^{-1}a \in I$ y así $x \cdot 1 = x \in I$ para todo $x \in R$, i.e, $R \subseteq I$, de lo cual sigue la igualdad. En particular, si $R = D$ un anillo de división o $R = \mathbb{F}$ un cuerpo, sigue que sus únicos ideales son triviales.

Ejemplo 1.30.

1. Sea a un elemento de un anillo R. Entonces $Ra = \{xa \mid x \in R\}$, el conjunto de múltiplos a izquierda de a, es un ideal a izquierda. También el conjunto RaR de todas las sumas finitas de la forma $\sum_i x_i a y_i$ con $x_i, y_i \in R$, es un ideal de R.

2. Si R es un anillo con 1, entonces todo ideal del anillo de matrices $M_n(R)$ es de la forma $M_n(I)$, donde I es ideal de R. [11]

Proposición 1.31. *Si D es un anillo de división, entonces $M_n(D)$ no tiene ideales no triviales.*

Demostración. Si $\mathcal{I}$ es un ideal no cero de $M_n(D)$, entonces por el Ejemplo 1.30, $\mathcal{I} = M_n(I)$, donde I es un ideal no cero de D. Por la Nota 1.29 los únicos ideales de D son $\mathcal{O}$ y D, por lo tanto $I = D$, de lo que se concluye que $\mathcal{I} = M_n(D)$ y esto a su vez muestra que los únicos ideales en el anillo $M_n(D)$ son $\mathcal{O}$ y $M_n(D)$.

Sean R un anillo e I un ideal de R. El conjunto de todas las clases, $R/I = \{r+I \mid r \in R\}$ es un anillo bajo las operaciones $(s + I) + (t + I) = s + t + I$ y $(s + I)(t + I) = st + I$, llamado **anillo cociente** de R módulo I.

Definición 1.32. Sean $\mathfrak{p}$ y $\mathfrak{m}$ ideales propios de un anillo conmutativo con unidad R. El ideal $\mathfrak{p}$ es llamado **ideal primo** de R si dados $a, b \in R$ y $ab \in \mathfrak{p}$, implica que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$. Además, $\mathfrak{m}$ es llamado **ideal maximal** de R, si no existe otro ideal propio J del

---

[11] Phani Bhushan Bhattacharya, Surender Kumar Jain y SR Nagpaul. *Basic abstract algebra*. Cambridge University Press, 1994.

anillo R que lo contenga, es decir, si existe J ideal de R tal que $\mathfrak{m} \subset J \subset R$, entonces $J = R$.

Un anillo R es llamado **local** si contiene un único ideal maximal $\mathfrak{m}$. Al anillo cociente $\mathbf{k} = R/\mathfrak{m}$ se le llama el cuerpo residual de R. Es usual denotar por $(R, \mathfrak{m}, \mathbf{k})$ al anillo local R con ideal maximal $\mathfrak{m}$ y cuerpo residual $\mathbf{k}$.

Los siguientes resultados caracterizan los ideales primos y maximales de un anillo conmutativo R.

Proposición 1.33. *Sean R un anillo conmutativo con unidad y $\mathfrak{p}, \mathfrak{m}$ ideales de R,*

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

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

Como consecuencia de la proposición anterior, si R es un anillo con unidad 1_R, cada ideal maximal es primo. Sin embargo, la recíproca no siempre es cierta. Por ejemplo, en el anillo $\mathbb{Z}$ el ideal $\{0\}$ es primo y no es maximal, lo que muestra que los conjuntos de ideales primos y maximales, denotados respectivamente por $Spec(R)$ y $Specm(R)$, son distintos.

Definición 1.34. Sean R y S anillos, Una aplicación $\gamma : R \to S$ es llamada un **homomorfismo de anillos**, si para todos $a, b \in R$ se tiene que:

1. $\gamma(a + b) = \gamma(a) + \gamma(b)$.
2. $\gamma(ab) = \gamma(a)\gamma(b)$.

Como en el caso de grupos, un homomorfismo de anillos $\gamma : R \to S$ es llamado monomorfismo (epimorfismo e isomorfismo), si γ es inyectivo (sobreyectivo y biyectivo). En el último caso R y S se dicen isomorfos y se denota por $R \cong S$. Si $\gamma : R \to S$ es un

homomorfismo de anillos, se definen el **kernel** y la **imagen** de γ respectivamente por:

$$Ker(\gamma) = \{r \in R \mid \gamma(r) = 0\} \qquad \text{y} \qquad Im(\gamma) = \{\gamma(r) \mid r \in R\}.$$

Proposición 1.35. *Sean $\phi : R \to S$ un epimorfismo de anillos y $I \preccurlyeq R$, entonces $\phi(I) \preccurlyeq S$.*

Demostración. Sean $y_1, y_2 \in \phi(I)$, luego $y_1 = \phi(r_1), y_2 = \phi(r_2)$ con $r_1, r_2 \in I$ y así

$$y_1 - y_2 = \phi(r_1) - \phi(r_2) = \phi(r_1 - r_2),$$

es decir, $y_1 - y_2 \in \phi(I)$.
Por otro lado, si $y \in \phi(I)$ y $s \in S$, como ϕ es epimorfismo $s = \phi(x)$ y $y = \phi(r)$, para algunos $x \in R$ y $r \in I$. Por lo tanto, $sy = \phi(x)\phi(r) = \phi(xr) \in \phi(I)$. Así $\phi(I) \preccurlyeq S$.

A continuación se establece una biyección, bajo cierta condición que será explícita en el enunciado, entre los conjuntos de ideales de los anillos de un epimorfismo ϕ dado.

Teorema 1.36 (Teorema de Correspondencia de Ideales - TCI's)**.** *Sea $\phi : R \to S$ un epimorfismo de anillos. Entonces, la aplicación $\Psi : I \mapsto \phi(I)$ define una correspondencia biyectiva entre el conjunto de todos los ideales (izquierdos o derechos) de R que contienen a $Ker(\phi)$ y el conjunto de todos los ideales (izquierdos o derechos) de S. Mas aún, esta correspondencia preserva el orden, en el sentido de que $I_1 \subsetneq I_2$ si y solo si $\phi(I_1) \subsetneq \phi(I_2)$.*

El siguiente resultado es un caso particular del TCI's y por ello una consecuencia del mismo. Sin embargo, Por una cuestión de completez y debido a que es la versión más usada, se establecerá su demostración.

Teorema 1.37. *Si I es un ideal de un anillo R, entonces todo ideal (izquierdo o derecho) en R/I es de la forma $\overline{J} = J/I$, donde J es un ideal (izquierdo o derecho) de R que contiene a I.*

Demostración. En efecto, sea $\pi_I : R \to R/I$ el epimorfismo canónico. Ahora bien,

$$Ker(\pi_I) = \{r \in R \mid \pi_I(r) = r + I = I\} = \{r \in R \mid r \in I\} = I.$$

Del teorema anterior, todo ideal (izquierdo o derecho) de R/I es de la forma

$$\pi_I(J) = \overline{J} = \{a + I \mid a \in J\} = J/I,$$

donde J es un ideal (izquierdo o derecho) de R que contiene a I. Además, I es un ideal de J, visto este último como anillo sobre si mismo, lo que demuestra el teorema.

Nota 1.38. Recuerde que un *conjunto parcialmente ordenado*, también llamado **poset**, es un conjunto no vacío S dotado de una **relación de orden**, usualmente denotada por "$\preceq$", es decir, "$\preceq$" es reflexiva, anti-simétrica y transitiva. Además, una cadena $\mathcal{C}$ en el **poset** S es cualquier subconjunto de S tal que, para todos $a, b \in \mathcal{C}$, ellos son comparables, en otras palabras, $a \preceq b$ o $b \preceq a$. Finalmente, un elemento $u \in S$ es una *cota superior* de $\mathcal{C}$ si $a \preceq u$ para todo $a \in \mathcal{C}$ y, un elemento $m \in S$ es un *elemento maximal* del **poset** si $m \preceq a$, $a \in S$, implica $m = a$.

A continuación un famoso axioma de la teoría de conjuntos acerca de los posets, el cual es ampliamente usado en matemáticas.

Teorema 1.39 (Lema de Zorn)**.** *Si toda cadena $\mathcal{C}$ del* **poset** $\left(S, \preceq\right)$ *tiene una* **cota superior** *en S, entonces $\left(S, \preceq\right)$ tiene un elemento maximal.*

Como un simple ejemplo del uso del Lema de Zorn, se prueba el siguiente resultado.

Teorema 1.40. *Todo anillo conmutativo con unidad $R \neq 0$ tiene por lo menos un ideal maximal.*

Demostración. Sea $(S, \subseteq)$ el poset de todos los ideales propios de R ordenados por inclusión. S es no vacío dado que $\mathcal{O} = \{0\} \in S$. Considere $\{I_i\}_{i\in\Lambda}$ una cadena de ideales en S.

Afirmación: $I = \bigcup I_i$ es un ideal de R y $1 \notin I$. En efecto, dado que $1 \notin I_i$ para todo $i \in \Lambda$, sigue que $1 \notin I$. Ahora bien si $a, b \in I$, entonces $a \in I_i$ y $b \in I_j$ para algunos $i, j \in \Lambda$. Sin perdida de generalidad se puede suponer que $I_i \subseteq I_j$, y por tanto $a - b \in I_j \subseteq I$. Sean $a \in I$ y $r \in R$, entonces $a \in I_i$ para algún $i \in \Lambda$, luego $ra \in I_i \subseteq I$. Por lo tanto $I \in S$ y es una cota superior de la cadena. Así, por el Lema de Zorn y la definición del conjunto S, este contiene un ideal maximal $\mathfrak{m}$.

Corolario 1.41. *Sea R un anillo conmutativo con 1.*

1. *Si $I \neq \langle 1\rangle$ es un ideal de R, entonces existe $\mathfrak{m}$ ideal maximal de R que contiene a I.*

2. *Todo $x \in R$ no unidad está contenido en un ideal maximal.*

Demostración.

1. *Como $I \neq \langle 1\rangle = R$, entonces $R/I \neq \mathcal{O}$ y del Teorema 1.40, este tiene al menos un ideal maximal $\overline{\mathfrak{m}}$. Sigue del TCI's que $\overline{\mathfrak{m}} = \mathfrak{m}/I$ con $I \subseteq \mathfrak{m} \preccurlyeq R$.*

2. *Sea $x \in R \setminus \mathcal{U}(R)$, entonces $\langle x\rangle \neq \langle 1\rangle = R$. Usando el inciso anterior se concluye que $\langle x\rangle \subseteq \mathfrak{m}$, para algún $\mathfrak{m} \in Specm(R)$.*

Definición 1.42. Sea R un anillo conmutativo. El radical de Jacobson de R, denotado por $J = J(R)$ es la intersección de todos sus ideales maximales a izquierda.

Ejemplo 1.43. Como en el anillo de los enteros $\mathbb{Z}$ los ideales maximales son de la forma $\langle p \rangle$, para p número primo, sigue que

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

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

De la definición, es claro que $J(R)$ es un ideal a izquierda de R. Más aún, es posible demostrar que $J(R)$ es un ideal bilateral. [9]

Se dice que un ideal I de un anillo R es **nil** si para todo elemento $x \in I$, existe un entero positivo n_x tal que $x^{n_x} = 0$. Además, I es llamado 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 llamado **nilpotente** si existe un entero positivo n tal que $I^n = \{0\}$.

Ahora, si I es nilpotente se sigue que para todos $a_{i_1}, a_{i_2}, a_{i_3}, ..., a_{i_n} \in I$,

$$a_{i_1} a_{i_2} a_{i_3} ... a_{i_n} = 0.$$

En particular, si $a_{i_j} = a$ para $1 \leq j \leq n$, entonces $a^n = 0$ para todo $a \in I$, lo que muestra que todo ideal nilpotente es nil. La recíproca no siempre es cierta.
Si $\mathbb{F}$ es un cuerpo, un ejemplo simple de ideal nilpotente se da en $R = \left\{ \begin{bmatrix} r & r \\ 0 & r \end{bmatrix} \mid r \in \mathbb{F} \right\}$, el anillo de matrices 2×2 triangulares superiores. $I = \left\{ \begin{bmatrix} 0 & r \\ 0 & 0 \end{bmatrix} \mid r \in \mathbb{F} \right\}$, es un ideal de R diferente de cero, con $I^2 = \mathcal{O}$.

Un anillo R puede tener elementos nilpotentes diferentes de cero y sin embargo, no

tener un ideal nilpotente no nulo, como lo ilustra el siguiente ejemplo.

Ejemplo 1.44. Sean $\mathbb{F}$ un cuerpo y $R = M_n(\mathbb{F})$. Entonces R tiene elementos nilpotentes diferentes de cero, tales como $E_{ij}, i \neq j, 1 \leq i, j \leq n$, las matrices con valor 1 en la entrada e_{ij} y 0 en las restantes. Suponga $\mathcal{I}$ un ideal a derecha de R, tal que $\mathcal{I}^k = \mathcal{O}$ para k un entero positivo. Considere el ideal $(R\mathcal{I})^k$, luego

$$\mathcal{O} \subseteq \overbrace{(R\mathcal{I})(R\mathcal{I})(R\mathcal{I})...(R\mathcal{I})}^{k \text{ veces}} = R\overbrace{(\mathcal{I}R)...(\mathcal{I}R)}^{k-1 \text{ veces}}\mathcal{I} \subseteq R\overbrace{\mathcal{I}\mathcal{I}...\mathcal{I}}^{k \text{ veces}} = R\mathcal{I}^k = \mathcal{O}.$$

Por lo tanto, $R\mathcal{I}$ es un ideal nilpotente de R. De la Proposición 1.31 $R = M_n(\mathbb{F})$ no tiene ideales no triviales. Entonces, $R\mathcal{I} = \mathcal{O}$ o $R\mathcal{I} = R$. Dado que R tiene $1_R = I_n$, la matriz identidad de orden n, $R\mathcal{I} \neq R$. Se sigue que $R\mathcal{I} = \mathcal{O}$. Luego para todo $A \in \mathcal{I}, A = I_n A \in R\mathcal{I} = \mathcal{O}$ y así, $\mathcal{I} = \mathcal{O}$.

Algunas propiedades del radical de Jacobson son.

Proposición 1.45. *Sean R un anillo conmutativo con 1_R, $I \preccurlyeq R$ y $a \in R$. Las siguientes afirmaciones son válidas.*

1. $I \subseteq J(R)$ *si y solo si cada elemento de la clase lateral* $1 + I$ *tiene inverso en* R.
2. $a \in J(R)$ *si y solo si* $1 - ra \in \mathcal{U}(R)$, *para todo* $r \in R$.
3. *El único idempotente en* $J(R)$ *es el cero del anillo.*
4. *Todo ideal nil de* R *está contenido en* $J(R)$.

Demostración.

1. Suponga que $I \subseteq J(R)$ y que existe algún elemento de la clase $1 + I$ que no es invertible en R, es decir, existe $r \in I$ tal que $1+r \notin \mathcal{U}(R)$. Como R es un anillo con unidad, entonces $1+r \in \mathfrak{m}$, para algún $\mathfrak{m} \in Specm(R)$. Como $r \in I \subset J(R)$, sigue

de la definición de radical de Jacobson que $r \in \mathfrak{m}$. Finalmente, $1 = (1 + r) - r$ está en $\mathfrak{m}$, es decir, $\mathfrak{m} = R$, que es una contradicción.

Por otro lado, si todo elemento de la clase $1+I$ es invertible y $I \nsubseteq J(R)$, entonces existe un ideal maximal $\mathfrak{m}$ tal que $I \nsubseteq \mathfrak{m}$. Sea $a \in I$ con $a \notin \mathfrak{m}$. Del hecho que $\mathfrak{m}$ es un ideal maximal, el conjunto

$$T = \{m + ra \mid m \in \mathfrak{m}, r \in R\},$$

es un ideal de R y verifica que $\mathfrak{m} \subset T \subset R$ y así, $T = R$. Por lo tanto, existen $m \in \mathfrak{m}$ y $r_1 \in R$ tales que $1 = m + r_1 a$. Luego $m = 1 + (-r_1 a) \in 1 + I$ y por tanto, $m \in \mathfrak{m}$ es unidad, lo cual es de nuevo una contradicción.

2. Si $a \in J(R)$, entonces para $r \in R$ arbitrario, el elemento $-ra$ pertenece a $J(R)$. Del inciso (1), se sigue que $1 + (-ra) = 1 - ra$ es invertible para todo $r \in R$.

   Suponga que $1 - ra \in \mathcal{U}(R)$, para todo $r \in R$. Sea $I = \{ra \mid r \in R\}$ el cual es un ideal a izquierda de R. Como cada elemento de la clase $1 + I$ es de la forma $1 + (ra) = 1 - (-ra)$, se sigue del inciso (1) que $I \subseteq J(R)$. Además, $1_R \in R$ y así, $a = 1_R a \in I \subseteq J(R)$.

3. Sea $a \in J(R)$ tal que $a^2 = a$. Como a pertenece al radical de Jacobson, entonces $1 - a$ es invertible en R. Por lo tanto, existe $b \in R$ que es el inverso de $1 - a$ y se

tiene lo siguiente:

$$\begin{aligned}(1-a)b &= 1\\ a(1-a)b &= a\\ (a-a^2)b &= a\\ 0b &= a\\ 0 &= a.\end{aligned}$$

Es decir, el único idempotente que pertenece al radical de Jacobson es $0 \in R$.

4. Suponga N un ideal nil de R y sea $a \in N$. Entonces, para $r \in R$, el elemento $(-ra)$ es nilpotente. Así, existe $n \in \mathbb{N}$ tal que $(-ra)^n = 0$. Se observa que

$$(1+(-ra))(1-(-ra)+(-ra)^2+...+(-1)^{n-1}(-ra)^{n-1}) = 1.$$

Por tanto, $1 - ra \in \mathcal{U}(R)$, para todo $r \in R$. Del inciso (2), se concluye que $a \in J(R)$.

El siguiente resultado, el cual se usara en el Capitulo 2 establece que los homomorfismos de anillos se comportan bien con unidades y elementos idempotentes.

Proposición 1.46. *Sean R, S anillos y $\gamma : R \to S$ un homomorfismo de anillos, entonces γ envía unidades en unidades e idempotentes en idempotentes.*

Demostración.

1. Note primero que si $a \in R$, entonces

$$\gamma(a) = \gamma(1a) = \gamma(1)\gamma(a).$$

Análogamente, $\gamma(a) = \gamma(a)\gamma(1)$. Por tanto $\gamma(1)$ es la identidad de $\gamma(R)$.

Sea $u \in \mathcal{U}(R)$, entonces $\gamma(1) = \gamma(uu^{-1}) = \gamma(u)\gamma(u^{-1}) = \gamma(u^{-1})\gamma(u) = \gamma(1)$. Luego $\gamma(u)$ es una unidad de $\gamma(R)$.

2. Sea e un idempotente de R, entonces $\gamma(e) = \gamma(e^2) = \gamma(e)\gamma(e)$. Se concluye que $\gamma(e)$ es un idempotente de $\gamma(R)$.

Definición 1.47. Sea R un anillo y M un grupo abeliano (aditivo). Se dice que M tiene estructura de R**-módulo unitario a izquierda**, si existe una aplicación $\mu : R \times M \to M$, dada por $(r, m) \mapsto rm$, que verifica para todos $a, b \in R$ y $m, m_1, m_2 \in M$ las siguientes condiciones:

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

De manera similar se definen los módulos-R unitarios o **módulos unitarios 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 adelante todo módulo será unitario.

Definición 1.48. Sea R un anillo conmutativo. Se dice que el anillo A es una R-**álgebra**, si A tiene estructura de R-módulo y además, verifica la siguiente condición de compatibilidad:

$$r(ab) = (ra)b = a(rb), \text{ para todo } r \in R \text{ y todos } a, b \in A.$$

Observe que, si A es un anillo con 1 y dado que el conjunto $R \cdot 1 \cong R$, entonces

$R \subset \mathcal{Z}(A)$. En efecto, dados $r \in R$ y $a \in A$ arbitrarios,

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

1.3. Anillos de Grupo

El anillo de grupo RG es un anillo asociativo, que presenta propiedades tanto del grupo G como del anillo de coeficientes R. Como su nombre lo indica, es un lugar de encuentro entre la teoría de grupos y la teoría de anillos y por tal motivo, ha sido abordado desde diferentes puntos de vista. Por ejemplo, el teórico de grupos finitos lo hace desde la teoría de caracteres y el analista desde la teoría de operadores y análisis de Fourier.

Sea 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 denote por RG al conjunto de todas las combinaciones lineales formales finitas de la forma

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

donde $a_g \in R$ y $a_g = 0$ casi siempre, es decir, solo un número finito de coeficientes son diferentes de 0 en cada una de estas sumas.

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

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

Note que para $\alpha = \sum_{g\in G} a_g g$ y $\beta = \sum_{g\in G} b_g g$ elementos de RG, reorganizando las expresiones de ser necesario, si α=β se tiene que $\sum_{g\in G}(a_g - b_g)g = 0$, y por tanto, del hecho que *supp*$(\alpha) =$ *supp*$(\beta) \subseteq G$, que es base de RG $a_g - b_g = 0$, es decir, $a_g = b_g$ para cada $g \in G$. 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 dos elementos en RG componente a componente, es decir,

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

Además, dados dos elementos $\alpha = \sum_{g\in G} a_g g$ y $\beta = \sum_{g\in G} b_g g$ en RG, su **producto** es dado por:

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

donde,

$$c_u = \sum_{gh=u} a_g b_h.$$

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

Ahora bien, si $\alpha, \beta, \gamma \in RG$ sigue que:

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

es decir, el producto en RG es asociativo.

Usando la propiedad distributiva válida en R y la definición de producto en RG, es claro que valen las leyes distributivas, a izquierda y derecha, del producto respecto a la suma, es decir,

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

Además, su unidad viene dada por $1_{RG} = \sum_{g\in G} u_g g$, donde $u_= 1_R = 1$ y $u_g = 0$, para todo $g \neq e$. Por tanto, $(RG, +, \cdot)$ es un anillo con unidad $1_{RG} = 1_R e$
Finalmente, RG tiene estructura de R-módulo al considerar el producto $\mu : R \times RG \to RG$ dado por

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

De hecho, si R es conmutativo, RG es una R-álgebra, en particular si $R = \mathbb{F}$ es un cuerpo, $\mathbb{F}G$ es un $\mathbb{F}$-espacio vectorial.
A continuación se presenta la definición transversal al presente trabajo.

Definición 1.49. El conjunto RG, con las operaciones suma y producto definidas anteriormente, es llamado el **anillo de grupo** de G sobre R. En el caso donde R es un anillo conmutativo y en particular cuando $R = \mathbb{F}$ es un cuerpo, RG también es llamado el **álgebra de grupo** de G sobre R.

Puede verse a G inmerso en RG mediante la aplicación $i : G \hookrightarrow RG$, definida para todo elemento $x \in G$ por $i(x) = \sum_{g\in G} a_g g$, donde $a_x = 1$ y $a_g = 0$ si $g \neq x$. Ahora bien, la aplicación $\nu : R \to RG$ dada por $\nu(r) = \sum_{g\in G} a_g g$, donde $a_e = r$ y $a_g = 0$ si $g \neq e$, define un homomorfismo de anillos inyectivo y así, R puede verse como un subanillo de RG.
Note que de la definición de suma y producto en RG, Re es un subanillo de RG, dado que, $R \cong R \cdot e = Re$ vía la aplicación

$$r \mapsto re.$$

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

$$gr = (1g)(re) = (1 \cdot r)(g \cdot e) = rg.$$

Por lo tanto, si R es conmutativo, $R \subseteq \mathcal{Z}(RG)$. En efecto, si $r \in R$ y $\alpha = \sum_{g\in G} a_g g \in RG$, se tiene que

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

Si $H = \{e\}$, entonces la aplicación $G \to \{e\}$ induce un homomorfismo de anillos $\varepsilon : RG \to R$ dado por:

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

Definición 1.50. El homomorfismo $\varepsilon : RG \to R$ definido anteriormente, es llamado la **aplicación de aumento** de RG y su kernel, $Ker(\varepsilon) = \Delta(G)$, es llamado **ideal de aumento** de RG.

Considere $\alpha = \sum_{g\in G} a_g g \in RG$. Si $\alpha \in \Delta(G)$ entonces $\varepsilon\left(\sum_{g\in g} a_g g\right) = \sum_{g\in G} a_g = 0$. Luego, se obtiene que:

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

Es claro que todos los elementos de la forma $g-1$, con $g \in G$ pertenecen a $\Delta(G)$, es decir, $\{g-1 \mid g \in G,\ g \neq 1\}$ es un conjunto de generadores para $\Delta(G)$ sobre R. Note que la expresión $\sum_{g\in G} a_g(g-1) = 0_{RG}$ se satisface si todos los coeficientes a_g con $g \in G$ son iguales a 0_R. Por consiguiente, el conjunto $\{g-1 \mid g \in G,\ g \neq 1\}$ es linealmente independiente. Más exactamente se ha probado el siguiente resultado.

Proposición 1.51. *El conjunto* $\{g-1 \mid g \in G,\ g \neq 1\}$ *es una base para* $\Delta(G)$ *sobre* R *y por tanto,*

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

donde como es usual, se asume que $a_g \neq 0$ *solo para un número finito de coeficientes.*

En general, dado $H \leq G$, se denota por $\Delta(G,H)$ al ideal a izquierda de RG generado por el conjunto $\{h-1 \mid h \in H\}$, es decir, $\Delta_R(G,H) = \Delta(G,H) = \left\{\sum_{h\in H} \alpha_h(h-1) \mid \alpha_h \in RG\right\}$.

Es posible demostrar que si $H \trianglelefteq G$, entonces $\Delta(G,H) \preccurlyeq RG$. Más aún, el epimorfismo canónico $\omega : G \to G/H$, induce el epimorfismo de anillos $\omega^* : RG \to R(G/H)$ dado por

$$\sum_{g\in G} \alpha_g g \mapsto \sum_{g\in G} \alpha_g \omega(g) = \sum_{g\in G} \alpha_g \overline{g},$$

donde $\overline{g}$ es la imagen de g en G/H. Note que $Ker(\omega^*) = \Delta(G,H)$ y así $RG/\Delta(G,H) \cong R(G/H)$. En particular, tomando $H = G$, $G \to \{e\}$, induce el epimorfismo $RG \to R$, que es la aplicación de aumento y $RG/\Delta(G) \cong R$. Es decir, se ha probado lo siguiente.

Proposición 1.52. *Sea $H \trianglelefteq G$, entonces el kernel de $\omega^* : RG \to R(G/H)$ es $\Delta(G,H)$, que es generado como ideal a izquierda de RG por el conjunto $\{h-1 \mid h \in H\}$, es decir, $\Delta(G,H) = \left\{\sum_{h\in H} \alpha_h(h-1) \mid \alpha_h \in RG\right\}$. Más aún, $\Delta(G,H) \preccurlyeq RG$ y $RG/\Delta(G,H) \cong R(G/H)$. En particular, si $H = G$ se sigue que $RG/\Delta(G) \cong R$.*

Es importante para este trabajo saber que condiciones son necesarias sobre el anillo R y el grupo G, para que el anillo de grupo RG sea local. W. K. Nicholson en el año 1972, dio respuesta a esta pregunta en su artículo dedicado a los anillos de grupo locales [12]. El resultado es el siguiente.

Teorema 1.53. *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[13] y $p \in J(R)$, entonces RG es local.*

---

[12] W. K. Nicholson. "Local group rings". En: *Canadian Mathematical Bulletin* 15.1 (1972), págs. 137-138.

[13] Recuerde que un grupo G es **localmente finito** si todos sus subgrupos finitamente generados son finitos.

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

Para establecer el teorema anterior, W. K. Nicholson inicialmente demuestra los siguientes resultados, los cuales dependen de los subgrupos H de G y los ideales de aumento $\Delta(G, H)$ y $\Delta(G)$, más precisamente él prueba lo siguiente.

1. Sea $\phi : R \to A$ un epimorfismo no nulo de anillos. Entonces R es local si y solo si A es local y $Ker(\phi) \subset J(R)$.

2. Si H es subgrupo normal de G, entonces, RG es local si y solo si $R(G/H)$ es local y $\Delta(G, H) \subset J(RG)$. En particular, RG es local si y solo si R es local y $\Delta(G) \subset J(RG)$.

3. RG es local si y solo si RH es local para todo subgrupo finitamente generado H de G.

2. Propiedad Clean

En este capítulo se introduce la propiedad clean tanto en anillos como en anillos de grupo y se estudiaran las características que estas estructuras adquieren cuando poseen dicha propiedad anillo teórica.

2.1. Anillos Clean

Sea $(R, +, \cdot)$ un anillo con unidad 1. Recuerde que los siguientes conjuntos

$$\mathcal{U}(R) = \{r \in R \mid r \text{ es invertible}\} \qquad \text{y} \qquad \mathcal{I}d(R) = \{e \in R \mid e^2 = e\},$$

denotan respectivamente el **grupo de unidades** y el **conjunto de idempotentes** de R.
Dado que $1 \in R$, $\mathcal{U}(R)$ y $\mathcal{I}d(R)$ son no vacíos. Observe que $\mathcal{U}(R) \neq \mathcal{I}d(R)$ debido a que $0 \notin \mathcal{U}(R)$.

Definición 2.1. Un anillo R es llamado **clean** si todo elemento de R puede ser escrito como la suma de una unidad y un idempotente. Más generalmente, un elemento $r \in R$ es llamado **clean** si existen $u \in \mathcal{U}(R)$ y $e \in \mathcal{I}d(R)$ tales que

$$r = u + e.$$

Como un primer ejemplo se tiene:

Ejemplo 2.2. El anillo $\mathbb{Z}$ con las operaciones usuales no es clean, aunque tiene elementos clean.

En efecto, dado que $\mathbb{Z}$ es un dominio entero, la ecuación $x = x^2$ en $\mathbb{Z}$ solo se satisface para $x = 0$ y $x = 1$, por lo tanto $\mathcal{I}d(\mathbb{Z}) = \{0, 1\}$.
Ahora bien, los elementos invertibles en $\mathbb{Z}$ son $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$.
De la Definición 2.1, los elementos clean se obtienen al hacer todas las posibles sumas de elementos invertibles con idempotentes:

$$0 = (-1) + 1 \qquad 2 = 1 + 1 \qquad -1 = (-1) + 0 \qquad 1 = 1 + 0.$$

Se concluye que los únicos elementos clean en $\mathbb{Z}$ son {-1,0,1,2}.

Nota 2.3. Para un anillo R con $1 \neq 0$, su conjunto de idempotentes $\mathcal{I}d(R)$ y su grupo de unidades $\mathcal{U}(R)$ son subconjuntos clean.
En efecto:

1. Para todo $e \in \mathcal{I}d(R)$, se tiene que $(1-e)^2 = (1-e) \in \mathcal{I}d(R)$; además, $(2e-1)^2 = 1$, por tanto,

$$e = \underbrace{(2e-1)}_{\in \mathcal{U}(R)} + \underbrace{(1-e)}_{\in \mathcal{I}d(R)}.$$

   Luego todo elemento idempotente es clean.

2. Dado que $0 \in \mathcal{I}d(R)$ y que para todo $u \in \mathcal{U}(R)$, $u = u + 0$ se sigue que toda unidad es clean.

A continuación algunas propiedades elementales que aparecen en la literatura y que en el presente trabajo se demuestran en detalle.

Proposición 2.4. *Sea R un anillo con unidad $1 \neq 0$. Si R es anillo de división o anillo local, entonces R es clean.*

Demostración.

i) Si R es un anillo de división, todo $x \in R \setminus \{0\}$ es unidad y por tanto sigue de la Nota 2.3 que x es clean. En el caso que $x = 0$ se tiene que $0 = -1 + 1$, es decir, 0 es clean.

ii) Sea $(R, \mathfrak{m})$ un anillo local.

Dado $x \in R$, se tienen dos posibilidades:

a) Si $x \in \mathcal{U}(R)$, sigue nuevamente de la Nota 2.3 que x es un elemento clean.

b) Si $x \in \mathfrak{m}$, entonces, sigue de la Proposición 1.45 que $x - 1 \in \mathcal{U}(R)$, y así $x = (x - 1) + 1$ es clean.

A continuación se establece que la propiedad clean se mantiene por imágenes homomorfas y formación de productos directos.

Proposición 2.5. *Sean R, S anillos con unidad y $\{R_i\}_{i\in\Lambda}$ una familia de anillos.*

1. *Si R es un anillo clean y $\phi : R \to S$ es un homomorfismo de anillos, entonces, $\phi(R)$ es un anillo clean. En particular, si ϕ es un epimorfismo S es un anillo clean.*

2. *El producto directo $\prod_{i\in\Lambda} R_i$ es clean si y solo si cada R_i es un anillo clean.*

Demostración.

1. Sean R, S anillos y $\phi : R \to S$ un homomorfismo de anillos.

Como R es anillo clean, dado $r \in R$ este puede escribirse como $r = u + e$, donde $u \in \mathcal{U}(R)$ y $e \in \mathcal{I}d(R)$. Ahora bien, todo homomorfismo de anillos envía unidades en unidades e idempotentes en idempotentes, es decir,

$$\phi(r) = \phi(u) + \phi(e) = \hat{u} + \hat{e},$$

donde $\hat{u} \in \mathcal{U}(S)$ y $\hat{e} \in \mathcal{I}d(S)$, por tanto $\phi(r)$ es clean y se sigue que $\phi(R) = \{\phi(r) : r \in R\} \leq S$ es clean.

2. ($\Rightarrow$) Sigue del hecho que $\pi_i \mid \prod_{i\in I} R_i \to R_i$ es la i-ésima proyección, que es epimorfismo, luego del ítem anterior, cada R_i es clean.

   ($\Leftarrow$) Sea $\{R_i\}_{i\in I}$ una familia de anillos clean. Como R_i es clean, $x_i \in R_i$ puede escribirse como $x_i = u_i + e_i$ donde $u_i \in \mathcal{U}(R_i)$ y $e_i \in \mathcal{I}d(R_i)$. Ahora bien, de la definición de suma en $\prod_{i\in I} R_i$ se tiene que:

$$\begin{aligned}(x_1, x_2, ..., x_i, ...) &= (u_1 + e_1, u_2 + e_2, ..., u_i + e_i, ...) \\ &= (u_1, u_2, ..., u_i, ...) + (e_1, e_2, ..., e_i, ...),\end{aligned}$$

   que son elementos unidad e idempotente respectivamente en $\prod_{i\in I} R_i$, lo que demuestra que $\prod_{i\in I} R_i$ es clean.

Como una aplicación del resultado anterior se tiene el siguiente ejemplo.

Ejemplo 2.6. 1. Considere la aplicación $\phi : \mathbb{Z}_3 \to \mathbb{Z}_{12}$ definida como $x + 3\mathbb{Z} \mapsto 4x + 12\mathbb{Z}$. Se concluirá que $\phi(\mathbb{Z}_3)$ es clean.

   En efecto, $\phi((x+3\mathbb{Z})(y+3\mathbb{Z})) = \phi(xy+3\mathbb{Z}) = 4xy+12\mathbb{Z}$. Como $12xy = 16xy-4xy$, entonces $4xy + 12\mathbb{Z} = 16xy + 12\mathbb{Z}$ en $\mathbb{Z}_{12}$, lo cual implica que: $\phi((x + 3\mathbb{Z})(y + 3\mathbb{Z})) = 16xy + 12\mathbb{Z} = (4x + 12\mathbb{Z})(4y + 12\mathbb{Z}) = \phi(x + 3\mathbb{Z})\phi(y + 3\mathbb{Z})$. Como $\mathbb{Z}_3$ es un cuerpo, sigue de la Proposición 2.4 que es un anillo clean y dado que ϕ es un homomorfismo, por la proposición anterior se tiene que $\phi(\mathbb{Z}_3) = \{12\mathbb{Z}, 4+12\mathbb{Z}, 8+12\mathbb{Z}\}$ es clean.

2. Del Ejemplo 2.2 y la Proposición 2.4 no todo subanillo de un anillo clean es clean. Más exactamente, se tiene que el anillo de enteros racionales $\mathbb{Q}$ es clean,

mientras que $\mathbb{Z}$ no lo es.

2.2. Anillos de Grupo Clean

Â¿Cuándo un anillo de grupo es clean? Esta pregunta parece un poco difícil en general. Por ejemplo, se desconoce cuando el anillo de grupo del grupo cíclico de orden 2 es clean. Si RG es clean, entonces R es clean, dado que es imagen homomorfa de RG vía la aplicación de aumento $\varepsilon : RG \to R$. En este capítulo se presentaran en detalle algunas respuestas parciales a esta pregunta.

Se iniciará con un resultado bien conocido de I. G. Connell, que relaciona los radicales de Jacobson de un anillo de grupo y su anillo de coeficientes, hecho que permitirá demostrar que el ideal de aumento $\Delta(G)$ está contenido en el radical $J(RG)$. Así mismo, se enunciará un resultado que relaciona al radical de Jacobson de un anillo con sus ideales cuasi-regulares.

Lema 2.7. *1.* [14] *Si R es un anillo y G es un grupo localmente finito, entonces $J(R) = J(RG) \cap R$. En particular, $J(R)(RG) \subseteq J(RG)$. Además, si $H \leq G$ $RH \cap J(RG) \subseteq J(RH)$.*

2. [9] *Sea R un anillo, entonces $J(R)$ es el único ideal cuasi-regular maximal a izquierda de R.*

Lema 2.8. *Sea p un primo con $p \in J(R)$. Si G es un p-grupo localmente finito, entonces $\Delta(G) \subseteq J(RG)$.*

Demostración. Suponga que G es un p-grupo, se presentan dos casos:

---

[14] I. G. Connell. “On the group ring”. En: *Canad. J. Math* 15.3 (1963), págs. 650-685.

Caso 1: G finito: Se procede por inducción sobre el orden de G. Como G es un p-grupo, existe $z \in \mathcal{Z}(G)$ con $|z| = p$, [9]. Considere $\langle z \rangle$ el subgrupo de G generado por z. Entonces el grupo $\overline{G} = G/\langle z \rangle$ tiene orden menor y así, $J(R\overline{G}) \supseteq \Delta(\overline{G})$ por hipótesis de inducción. Por otro lado, la aplicación $\varphi : RG \to R\overline{G}, \sum r_g g \mapsto \sum r_g \overline{g}$ es un epimorfismo de anillos cuyo kernel por la Proposición 1.52 es $\Delta(G, \langle z \rangle) = (RG)(1 - z)$. Dado que $z^p = 1$ y que los coeficientes binomiales $\binom{p}{k}$, $2 \leq k \leq p - 1$, en la expansión de $(1 - z)^p$ son múltiplos de p, se tiene por Lema 2.7 que $(1-z)^p \in p(RG) \subseteq J(R)(RG) \subseteq J(RG)$. Dado que $z \in \mathcal{U}(RG)$, por la Proposición 1.45 $1 - z \in J(RG)$ y así, $\Delta(G, \langle z \rangle) = (RG)(1 - z) \subseteq J(RG)$. Luego, por el T.C.I. 1.36 $J(R\overline{G}) = \varphi(J(RG))$. Ahora bien, para todo $h \in G$, $\varphi(1-h) = 1-\overline{h} \in \Delta(\overline{G}) \subseteq \varphi(J(RG))$. Esto demuestra que $\Delta(G) \ni (1 - h) \in (RG)(1 - z) + J(RG) = J(RG)$, donde la última igualdad sigue del isomorfismo $RG/\Delta(G, \langle z \rangle) \cong R\overline{G}$. Es decir, $\Delta(G) \subseteq J(RG)$.

Caso 2: G arbitrario: Sea $r \in \Delta(G)$. Si H es el subgrupo de G generado por el soporte de r, entonces $r \in \Delta(H)$ y como H es un p-grupo finito, $\Delta(H) \subseteq J(RH)$ como se probó en el Caso 1. Por lo tanto $r \in J(RH)$ es cuasi-regular $(1 + r) \in \mathcal{U}(RH)$. Como r en $\Delta(G)$ es arbitrario, sigue que $\Delta(G)$ es un ideal cuasi-regular y así, por el ítem (2) del Lema 2.7 $\Delta(G) \subseteq J(RG)$.

Antes de establecer el próximo lema, se necesita el siguiente resultado.

Proposición 2.9. *Sean R un anillo, G un grupo y N un subgrupo normal de G tal que G/N es localmente finito. Entonces $J(RN) \subseteq J(RG)$.*

Lema 2.10. *Sea p un número primo con $p \in J(R)$. Sea G un grupo localmente finito tal que $G = KH$ donde K es un p-subgrupo normal de G y H es un subgrupo de G. Si RH es clean, entonces RG es clean.*

Demostración. Dado $g \in G$, existen $k \in K$ y $h \in H$ tales que $g = kh = (k-1)h + h \in \sum_{k\in K}(1-k)(RG) + RH$.
Entonces,

$$RG = \sum_{k\in K}(1-k)(RG) + RH. \tag{1}$$

Del Lema 2.8, $\Delta(K) \subseteq J(RK)$. Como G es un grupo localmente finito, entonces G/K es localmente finito, y por la Proposición 2.9 $J(RK) \subseteq J(RG)$. Así, $\Delta(K) \subseteq J(RG)$, de lo cual usando que $J(RG)$ es ideal sigue que

$$\sum_{k\in K} \underbrace{(1-k)}_{\in\Delta(K)}(RG) \subseteq \Delta(K)(RG) \subseteq J(RG). \tag{2}$$

Por tanto de las expresiones (1) y (2) se obtiene que

$$RG = J(RG) + RH. \tag{3}$$

Por el ítem (1) del Lema 2.7, $RH \cap J(RG) \subseteq J(RH)$. Ahora bien, la aplicación $\phi : RH \to RG/J(RG)$, dada por $h \mapsto h + J(RG)$ es un epimorfismo de anillos cuyo kernel

$$Ker(\phi) = \{\alpha \in RH \mid \alpha + J(RG) = J(RG)\} = RH \cap J(RG).$$

Por lo tanto $RH/[RH \cap J(RG)] \cong RG/J(RG)$, el cual tiene radical de Jacobson cero, y así $J(RH) = RH \cap J(RG)$, de lo cual sigue que $RH/J(RH) \cong RG/J(RG)$. Finalmente, suponga que RH es clean, y dado que la propiedad clean es cerrada por imágenes homomorfas entonces $RH/J(RH)$ es clean y así $RG/J(RG)$ también lo es. Siguiendo a Han y Nicholson [4], "RG es clean si y solo si $RG/J(RG)$ es clean y levanta idempo-

tentes[15] módulo $J(RG)$".

Sea $x \in RG$ tal que $x^2 - x \in J(RG)$. Por (3), $x = y + z$ con $y \in J(RG)$ y $z \in RH$. Entonces

$$z^2 - z = x^2 - x - (y^2 - y + 2yz) \in J(RG) \cap RH = J(RH).$$

Dado que RH es clean, existe $e^2 = e \in RH \subseteq RG$ tal que $z - e \in J(RH)$. Así $x - e = y + (z - e) \in J(RG)$.

Note que si en el lema anterior G es adicionalmente un p-grupo, es decir $H = \{1\}$, en realidad se tiene el siguiente teorema.

Teorema 2.11. *Sea p un primo con $p \in J(R)$. Si R es un anillo clean y G es un p-grupo localmente finito, entonces RG es clean.*

Nota 2.12. Recuerde que un subconjunto multiplicativamente cerrado es un subconjunto S de un anillo conmutativo con unidad R tal que $1 \in S$ y S es cerrado bajo el producto. Defina la relación " $\equiv$ " en $R \times S$ como sigue

$$(r, s) \equiv (x, y) \iff (ry - xs)u = 0, \text{ para algún } u \in S.$$

Es un ejercicio de rutina ver que " $\equiv$ " es una relación de equivalencia, [16]. Se denotarán respectivamente por $\frac{r}{s}$ y $S^{-1}R$ a la clase de equivalencia de (r, s) y al conjunto de todas las clases de equivalencia.

---

[15] Se dice que un subgrupo aditivo L de un anillo R **levanta** idempotentes módulo L si dado $x \in R$ tal que $x^2 - x \in L$, existe $e \in \mathcal{I}d(R)$ tal que $e - x \in L$.

[16] M. Atiyah. *Introduction to commutative algebra*. CRC Press, 2018.

Se definen la suma y el producto de elementos en $S^{-1}R$ como

$$(+): \ \left(\frac{r}{s}\right)+\left(\frac{x}{y}\right)=\frac{(ry+xs)}{sy} \quad \text{y} \quad (\cdot): \ \left(\frac{r}{s}\right)\left(\frac{x}{y}\right)=\frac{rx}{sy},$$

las cuales no dependen de los representantes de clase y dan a $(S^{-1}R,+,\cdot)$ estructura de anillo conmutativo con $1_{S^{-1}R}=\frac{1}{1}$, llamado **anillo de fracciones** de R respecto a S.

La aplicación $\Phi: R\to S^{-1}R$, dado por $r\mapsto \frac{r}{1}$, es un homomorfismo de anillos que en general no es inyectivo.

Ejemplo 2.13. Sea $\mathfrak{p}$ un ideal primo de R. Entonces $S=R\setminus\mathfrak{p}$ es multiplicativamente cerrado (en efecto si $a,b\in R\setminus\mathfrak{p}$, se tiene por la primalidad de $\mathfrak{p}$ que $ab\in R\setminus\mathfrak{p}$). En este caso se denotará por $R_{\mathfrak{p}}$ al anillo $S^{-1}R$. Los elementos $\frac{r}{s}$ donde $r\in\mathfrak{p}$ forman un ideal $\mathfrak{m}$ en $R_{\mathfrak{p}}$. Si $\frac{x}{y}\notin\mathfrak{m}$, entonces $x\notin\mathfrak{p}$, es decir $x\in S$ y por lo tanto $\frac{x}{y}$ es una unidad de $R_{\mathfrak{p}}$. Sigue que si I es un ideal de $R_{\mathfrak{p}}$ y $I\nsubseteq\mathfrak{m}$, entonces I contiene una unidad y así $I=R_{\mathfrak{p}}$. Por tanto $\mathfrak{m}$ es el único ideal maximal de $R_{\mathfrak{p}}$, es decir, $(R_{\mathfrak{p}},\mathfrak{m})$ es un anillo local conocido como la localización del anillo R en el ideal primo $\mathfrak{p}$.

Ejemplo 2.14. Un caso particular del ejemplo anterior es la localización de $\mathbb{Z}$ en el ideal primo $\mathfrak{p}$ generado por el número primo p, que se define como el conjunto $\mathbb{Z}_{(p)}=\{\frac{m}{n}\mid p\nmid n\}$.
En este caso, el único ideal maximal es

$$\mathfrak{p}\mathbb{Z}_{(p)}=\left\{\frac{m}{n}\mid m\in\mathfrak{p},n\notin\mathfrak{p}\right\}=\left\{\frac{m}{n}\mid p\mid m \text{ y } p\nmid n\right\}.$$

Los siguientes resultados obtenidos por Y. Ye [17] dan condiciones sobre los elementos

[17] Y. Ye. “Semiclean rings”. En: *Communications in Algebra* 34.9 (2006), pág. 3487.

de $\mathbb{Z}_{(p)}C_3$, para determinar la condición clean de este anillo de grupo.

Proposición 2.15. *Sea G un grupo cíclico finito.*

1. *Si $G = \{1, g, g^2\}$ es el grupo cíclico de orden 3, entonces los elementos idempotentes del anillo de grupo $\mathbb{Z}_{(p)}G$ con p número primo diferente de 3 son*

$$\mathcal{I}d(\mathbb{Z}_{(p)}G) = \left\{0, 1, \frac{1}{3} + \frac{1}{3}g + \frac{1}{3}g^2, \frac{2}{3} - \frac{1}{3}g - \frac{1}{3}g^2\right\}.$$

2. *Si $G = \{1, g, g^2, ..., g^{q-1}\}$ es el grupo cíclico de orden q, entonces*

$$\mathbb{Z}_{(p)}G = \left\{\sum_{i=0}^{q-1} k_i g^i \mid k_i \in \mathbb{Z}_{(p)}\right\}.$$

Un elemento $x \in \mathbb{Z}_{(p)}G$ es una unidad si y solo si p no divide al determinante

$$|circ(k_0, k_1, k_2, ..., k_{q-1})^t| = \begin{vmatrix} k_0 & k_{q-1} & k_{q-2} & ... & k_1 \\ k_1 & k_0 & k_{q-1} & ... & k_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ k_{q-1} & k_{q-2} & k_{q-3} & ... & k_0 \end{vmatrix},$$

donde $circ(k_0, k_1, k_2, ..., k_{q-1}) = \begin{bmatrix} k_0 & k_1 & ... & k_{q-1} \\ k_{q-1} & k_0 & ... & k_{q-2} \\ \vdots & \vdots & \vdots & \vdots \\ k_1 & k_2 & ... & k_0 \end{bmatrix}$ *es llamada la matriz circulante generada por el elemento* $x = \sum_{i=0}^{q-1} k_i g^i$.

Ejemplo 2.16. $\mathbb{Z}_{(7)}C_3$ no es clean. En efecto, considere el elemento $2+3g$ con g generador de C_3. De la Proposición 2.15 ítem (1), $\mathcal{I}d(\mathbb{Z}_{(7)}C_3) = \left\{0, 1, \frac{1}{3} + \frac{1}{3}g + \frac{1}{3}g^2, \frac{2}{3} - \frac{1}{3}g - \frac{1}{3}g^2\right\}$.

Luego el elemento $2+3g$ tiene las siguientes presentaciones:

$$\begin{aligned} 2+3g &= 0+(2+3g) \\ &= 1+(1+3g) \\ &= \left(\tfrac{1}{3}+\tfrac{1}{3}g+\tfrac{1}{3}g^2\right)+\left(\tfrac{5+8g-g^2}{3}\right) \\ &= \left(\tfrac{2}{3}-\tfrac{1}{3}g-\tfrac{1}{3}g^2\right)+\left(\tfrac{4+10g+g^2}{3}\right). \end{aligned}$$

Así las cosas, es suficiente demostrar que los elementos $2+3g, 1+3g, \frac{5+8g-g^2}{3}$ y $\frac{4+10g+g^2}{3}$ no son unidades de $\mathbb{Z}_{(7)}C_3$. Note que para los casos de $\frac{5+8g-g^2}{3}$ y $\frac{4+10g+g^2}{3}$ solo es necesario ver que los numeradores no son unidades. Para el caso del elemento $2+3g$, $k_0=2, k_1=3$ y $k_2=0$. Y así, 7 divide a $|circ(2,3,0)^t| = \begin{vmatrix} 2 & 0 & 3 \\ 3 & 2 & 0 \\ 0 & 3 & 2 \end{vmatrix} = 2^3+3^3+0^3-3(2\cdot 3\cdot 0)=35$. De forma análoga para los demás casos se obtiene que:

- 7 divide a $|circ(1,3,0)^t| = 1^3+3^3+0^3-3(1\cdot 3\cdot 0)=28.$
- 7 divide a $|circ(5,8,-1)^t| = 5^3+8^3+(-1)^3-3\cdot 5\cdot 8\cdot(-1)=756.$
- 7 divide a $|circ(4,10,1)^t| = 4^3+10^3+1^3-3\cdot 4\cdot 10\cdot 1=945.$

Por tanto, los elementos $2+3g, 1+3g, \frac{5+8g-g^2}{3}$ y $\frac{4+10g+g^2}{3}$ no son unidades de $\mathbb{Z}_{(7)}C_3$. Así, el elemento $2+3g$ no es clean.

En el ejemplo anterior $C_3=\{1,g,g^2\}$ es un 3-grupo y como $3 \notin \langle 7\rangle = \mathfrak{p}$, ver Ejemplo 2.13, entonces $3 \notin J(\mathbb{Z}_{(7)})$, lo cual muestra que la condición $3 \in J(\mathbb{Z}_{(7)})$ en el Teorema 2.11 es esencial.

3. Anillos de Grupo $*$-clean

Definición 3.1. Un anillo R es un $*$-**anillo** (o **anillo con involución**) si existe una aplicación $* : R \to R$ tal que:

$$(\mathsf{I}_1)\ (x+y)^* = x^* + y^*. \qquad (\mathsf{I}_2)\ (xy)^* = y^*x^*. \qquad (\mathsf{I}_3)\ (x^*)^* = x,$$

para todos $x, y \in R$; es decir, $*$ es un anti-homomorfismo de orden 2. Como es usual, se denota por $R^+ = \{r \in R \mid r^* = r\}$ al conjunto de los elementos simétricos de R bajo la involución $*$.

Un elemento p de un $*$-anillo R es llamado una **proyección** si p es un idempotente simétrico, es decir, $p^* = p = p^2$. Se denotará por $proy(R) = \{p \in R \mid p \text{ es proyección}\}$ al conjunto de todas las proyecciones del anillo R.

Definición 3.2. Un $*$-anillo R es llamado $*$-**clean** si todo elemento en R puede expresarse como la suma de una unidad y una proyección.

Dado que toda proyección p es un idempotente del anillo es decir, $proy(R) \subseteq \mathcal{I}d(R)$, sigue de la Definición 3.2, que todo anillo $*$-clean R es clean. Por otro lado de la Proposición 2.4 todo anillo local R es clean, luego si este es $*$-anillo, él será $*$-clean (los únicos idempotentes de R son 0 y 1).
Recordando que un anillo cuyos elementos idempotentes pertenecen al centro es llamado **anillo abeliano**, es posible contrastar esta propiedad en los $*$-anillos.
Más exactamente, sigue de lo anterior que en un $*$-anillo abeliano, toda proyección es central, lo que es conocido comúnmente como un anillo $*$-abeliano. En un $*$-anillo la involución es llamada propia si $x^*x = 0$ implica que $x = 0$.
Note que si R es un anillo conmutativo y si $* : G \to G$ es una involución, ver Definición

1.21, la extensión R-lineal $* : RG \to RG, \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^*$, da al anillo de grupo RG estructura de $*$-anillo. En particular, en el anillo de grupo RG la aplicación $* : RG \to RG$ dada por $\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g g^{-1}$, define una involución y así, RG es un $*$-anillo. Esta involución es conocida como involución clásica y será la utilizada de ahora en adelante cuando se hable de $*$-anillos.

3.1. Anillos de Grupo Abelianos

En esta sección se estudiará cuando un anillo de grupo abeliano RG es $*$-clean, donde R es un anillo local conmutativo y G es uno de los grupos cíclicos C_3 o C_4.

Lema 3.3. *Un $*$-anillo R conmutativo es $*$-clean si y solo si R es clean y todo idempotente es una proyección.*

Demostración. ($\Rightarrow$) Es claro que R es clean por ser $*$-clean. Ahora, sea $e \in R$ idempotente. Como R es $*$-clean, se tiene que $e = p + u$, donde $p \in proy(R)$ y $u \in \mathcal{U}(R)$. Luego $u = e - p$ y $(e-p)(e+p-1) = e^2 - p^2 - (e-p) = 0$. Por lo tanto, $e + p - 1 = 0$. De lo anterior, $e = 1 - p = (1-p)^*$, es decir $e \in proy(R)$.
($\Leftarrow$) Por hipótesis, si $a \in R$, entonces $a = e+u$ donde $e \in \mathcal{I}d(R) = proy(R)$ y $u \in \mathcal{U}(R)$. Sigue que R es un anillo $*$-clean.

El siguiente lema caracteriza los elementos simétricos de RC_3, $(RC_3)^+$, bajo la involución clásica.

Lema 3.4. *Sea R un anillo local conmutativo y $C_3 = \langle g \rangle$ el grupo cíclico de orden 3. Suponga que $x = a_0 + a_1 g + a_2 g^2$ es un idempotente de RC_3, donde $a_0, a_1, a_2 \in R$. Entonces $x^* = x$ si y solo si $a_2 - a_1 \in J(R)$.*

Demostración. ($\Rightarrow$) Como $x^* = a_0+a_1g^{-1}+a_2(g^2)^{-1} = a_0+a_1g^2+a_2g = a_0+a_1g+a_2g^2 = x$, se concluye que $a_1 = a_2$ y por lo tanto, $a_2 - a_1 = 0 \in J(R)$.
($\Leftarrow$) Dado que $x = a_0 + a_1g + a_2g^2 \in RC_3$ es idempotente, sigue que,

$$x^2 = a_0^2 + 2a_0a_1g + a_1^2g^2 + 2(a_0 + a_1g) + a_2g^2 + a_2^2g = a_0 + a_1g + a_2g^2 = x.$$

Y así,

$$a_0^2 + 2a_1a_2 = a_0 \tag{1}$$

$$a_2^2 + 2a_0a_1 = a_1 \tag{2}$$

$$a_1^2 + 2a_0a_2 = a_2. \tag{3}$$

Restando las últimas dos ecuaciones, $a_2^2 - a_1^2 + 2a_0(a_1 - a_2) = a_1 - a_2$ es decir,

$$a_2 - a_1 + a_2^2 - a_1^2 + 2a_0(a_1 - a_2) = (a_2 - a_1)(1 + a_2 + a_1 - 2a_0) = 0. \tag{4}$$

Se tienen los siguientes dos casos.

Caso 1: Si $2 \in J(R)$, al usar que $a_1 = 2a_1 - a_1$, se tiene de la Proposición 1.45 (2) que

$$1 + a_2 + a_1 - 2a_0 = 1 + (a_2 - a_1) + 2(a_1 - a_0) \in \mathcal{U}(R).$$

Luego de la expresión (4) $a_1 = a_2$ y así, $x^* = x$.

Caso 2: Si $2 \in \mathcal{U}(R)$, suponga que $1 + a_1 + a_2 - 2a_0 \notin \mathcal{U}(R)$, es decir,

$$1 + a_1 + a_2 - 2a_0 \in J(R). \tag{5}$$

Como $x^2 = x$, se cumple que $\varepsilon(x)^2 = \varepsilon(x^2) = \varepsilon(x)$, es decir, $(a_0+a_1+a_2)^2 = (a_0+$

$a_1+a_2)$. Dado que R es anillo local, $a_0+a_1+a_2=0$ o $a_0+a_1+a_2=1$. Al reemplazar x por $1-x$, de ser necesario, siempre es posible asumir que $a_0+a_1+a_2=0$ y así, $a_1+a_2=-a_0$. De la expresión (5), se obtiene que $(1-3a_0)\in J(R)$ y de nuevo por la Proposición 1.45(2), $3a_0\in\mathcal{U}(R)$, de lo cual sigue que $a_0\in\mathcal{U}(R)$, caso contrario $3a_0\in J(R)$, lo cual no es posible.

Ahora bien, al usar la ecuación (1) y las igualdades $a_1+a_2=-a_0$ y $(a_2-a_1)^2=(a_2+a_1)^2-4a_1a_2$, se obtiene que $(-a_0)^2-2(a_0-a_0^2)=a_0(3a_0-2)$. Como por hipótesis $(a_2-a_1)\in J(R)$, también $a_0(3a_0-2)\in J(R)$ y así, $(3a_0-2)\in J(R)$ dado que $a_0\in\mathcal{U}(R)$. Por consiguiente, $-1=(3a_0-2)+(1-3a_0)\in J(R)$, que es de nuevo una contradicción. Así, $1+a_1+a_2-2a_0\in\mathcal{U}(R)$ y por tanto, de la ecuación (4) sigue que $a_1=a_2$, lo que implica que $x^*=x$.

Del último lema, $x\in\mathcal{I}d(R)$ es proyección si y solo si $a_2-a_1\in J(R)$, lo que es equivalente a decir que $a_1+J(R)=a_2+J(R)$. En realidad se tiene el siguiente resultado.

Corolario 3.5. *Sea R un anillo local conmutativo y $C_3=\langle g\rangle$ el grupo cíclico de orden 3. Asuma que x es un idempotente de RC_3. Entonces $x^*=x$ si y solo si $\overline{x}^*=\overline{x}$, donde $\overline{x}$ es la imagen de x en $(R/J(R))C_3$.*

Note que del último corolario y la Proposición 1.33, para el estudio de la propiedad $*$-clean en RC_3 es posible asumir que R es un cuerpo, en el caso que R es un anillo local conmutativo.

El siguiente teorema condiciona al radical de Jacobson de un anillo R para que el anillo de grupo RC_3 sea $*$-clean.

Teorema 3.6. *Sea R un anillo local conmutativo y $C_3=\langle g\rangle$ el grupo cíclico de orden 3.*

1. *Si $3\in J(R)$, entonces RC_3 es $*$-clean*

2. *Si $3 \notin J(R)$, entonces RC_3 es $*$-clean si y solo si RC_3 es clean y la ecuación $x^2 + x + 1 = 0$ no tiene soluciones en R.*

Demostración.

1. Como $3 \in J(R)$, del Teorema 1.53(2), RC_3 es local y así, sus únicos idempotentes son 0 y 1 que son proyecciones. Sigue que RC_3 es $*$-clean.

2. $(\Rightarrow)$ Dado que RC_3 es $*$-clean, entonces también es clean. Ahora bien, suponga que existe $a \in R$ tal que $a^2+a+1 = 0$, es decir, $a^2 = -(a+1)$ y así, $a^3 = 1$. Al tomar $e = \frac{1}{3}(1+ag+a^2g^2)$, se tiene que $e^2 = [\frac{1}{3}(1+ag+a^2g^2)]^2 = \frac{1}{9}(3+3ag+3a^2g^2) = e$. Sin embargo, $e^* \neq e$ ya que $a_2 - a_1 = \frac{1}{3}a(a-1) \neq 0$, pues $a^3 = 1$ y $a \neq 1$. Del Lema 3.3, RC_3 no es $*$-clean, lo que contradice la hipótesis inicial.

   $(\Leftarrow)$ Suponga que RC_3 no es $*$-clean, entonces c De la misma forma que en la demostración del Lema 3.4, se tiene que $(a_2-a_1)(1+a_1+a_2-2a_0) = 0$ y además $a_2 - a_1 \in \mathcal{U}(R)$. Luego

   $$1 + a_1 + a_2 - 2a_0 = 0. \tag{6}$$

   Como $e^2 = e$, $\varepsilon(e)^2 = \varepsilon(e^2) = \varepsilon(e)$, es decir, $(a_0 + a_1 + a_2)^2 = a_0 + a_1 + a_2$ y con R local, $a_0 + a_1 + a_2 = 0$ o 1.

   Como fue justificado en el último lema, siempre se puede asumir que $a_0 + a_1 + a_2 = 0$. Entonces de (6) $a_0 = \frac{1}{3}$ y $a_1 + a_2 = -\frac{1}{3}$. Ahora bien, de la expresión (2) $a_2^2 = (1-2a_0)a_1 = (1-\frac{2}{3})(-\frac{1}{3}-a_2) = \frac{1}{3}(-\frac{1}{3}-a_2)$ y por tanto, $9a_2^2+3a_2+1 = 0$, es decir, la ecuación $x^2+x+1 = 0$ tiene como solución a $x = 3a_2$, lo que contradice la hipótesis inicial.

A continuación la definición de una propiedad anillo-teórica, la cual será conectada con la cualidad del anillo ser clean.

Definición 3.7. Un anillo R es llamado fuertemente π-regular si toda sucesión decreciente de ideales $aR \supseteq a^2R \supseteq ... \supseteq a^kR$ estaciona para cada $a \in R$, es decir existe $k \in \mathbb{N}$ tal que $a^kR = a^{k+n}R$ para $n > 0$.

El siguiente resultado probado por primera vez por Burgess y Menal, [18] usando elementos de geometría algebraica, establece que un elemento fuertemente π-regular es clean con una propiedad adicional.

Teorema 3.8. *Si $a \in R$ es fuertemente π-regular, entonces $a = e + u$ donde $e \in \mathcal{I}d(R)$ y $u \in \mathcal{U}(R)$ y además $eu = ue$.*

Es un resultado conocido que si R es un anillo Artiniano y G es un grupo finito, entonces RG es Artiniano [14]. Por lo tanto, de la Definición 3.7 RG es fuertemente π-regular. Así las cosas, si R es un cuerpo, RC_3 es Artiniano y así es un anillo clean.
Como una consecuencia del Teorema 3.6 y del Teorema 3.8 se tiene.

Corolario 3.9. *Sea R un cuerpo*

(1) Si $char(R) = 3$, entonces RC_3 es $*$-clean

(2) Si $char(R) \neq 3$, entonces RC_3 es $*$-clean si y solo si la ecuación $x^2 + x + 1 = 0$ no tiene soluciones en R.

Ejemplo 3.10. Dado que la ecuación $x^2 + x + 1 = 0$ tiene discriminante -3, se tiene que $x^2 + x + 1 = 0$ no tiene soluciones en $\mathbb{R}$. Además $char(\mathbb{R}) = 0$, lo que permite concluir usando el corolario anterior que $\mathbb{R}C_3$ es $*$-clean. Por otro lado, los anillos de grupo $\mathbb{C}C_3$ y RC_3, donde $R = \mathbb{Q}\left[\sqrt{-3}\right] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\}$, no son $*$-clean, dado que $char(\mathbb{C}) = 0 = char(R)$ y la ecuación $x^2 + x + 1 = 0$ si tiene solución tanto en $\mathbb{C}$

---

[18] W. K. Nicholson. "Strongly clean rings and Fitting's lemma". En: *Communications in algebra* 27.8 (1999), págs. 3583-3592.

como en R. Sin embargo, el Teorema 3.8 garantiza que ambos anillos de grupo $\mathbb{C}C_3$ y RC_3, siendo Artinianos, son clean.

Ejemplo 3.11. 1. Sea R un cuerpo de 4 elementos, el cual es isomorfo a $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$. Por el Teorema de Kroneker existe $a \in R$ tal que $a^2+a+1=0$. Entonces RC_3 es clean, pero no $*-$clean.

2. $\mathbb{Z}_pC_3$ es $*-$clean, con $p = 2, 3$. En efecto, si $p = 2$, $\mathbb{Z}_2C_3$ es $*$-clean ya que $x^2+x+1=0$ no tiene soluciones en $\mathbb{Z}_2$ y $\mathbb{Z}_2C_3$ es clean. Si $p=3$, del Corolario 3.9 se deduce que $\mathbb{Z}_3C_3$ es $*$-clean.

3. Recuerde que si p es un primo impar y a un entero no divisible por p, el símbolo de Legendre denotado por $\left[\frac{a}{p}\right]$[19] viene dado por

$$\left[\frac{a}{p}\right] = \begin{cases} 1, & \text{si } a \text{ es residuo cuadrático de } p, \\ -1, & \text{si } a \text{ no es residuo cuadrático de } p. \end{cases}$$

Un resultado debido a Euler, $\left[\frac{a}{p}\right] \equiv a^{\frac{p-1}{2}} (\text{mod } p)$ [20], permite decidir cuando el entero a es o no residuo cuadrático de un primo p.

Considere $p > 3$ primo y el anillo $R = \mathbb{Z}_p$. Por el Teorema 3.8 RC_3 es clean.

(i) Si $(-3)^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$, sigue del criterio de Euler que $x^2+3=0$ tiene solución en R. Al tomar $x = 2y+1$, se tiene que $0 = x^2+3 = 4(y^2+y+1)$.

---

[19] Si m es un entero positivo, se dice que el entero a es un *residuo cuadrático* de m, si a y m son primos relativos y la congruencia $x^2 \equiv a \ (\text{mod } m)$ tiene una solución.

[20] K. H. Rosen. *Elementary number theory and its applications*. Vol. 1. Pearson/Addison Wesley, 2005.

Por lo tanto $x^2 + 3 = 0$ tiene solución en R si y solo si $y^2 + y + 1 = 0$ tiene solución en R. El resultado ahora sigue por el Corolario 3.9.

(ii) Si $(-3)^{\frac{p-1}{2}} \equiv -1 (\text{mod } p)$, nuevamente por el criterio de Euler $x^2 + 3 = 0$ no tiene solución en R. Al tomar $x = 2y + 1$ y razonando análogamente al ítem anterior, se tiene que $x^2 + 3 = 0$ no tiene solución en R si y solo si $y^2 + y + 1 = 0$ no tiene solución en R.

Por lo tanto, en este caso RC_3 es $*$-clean.

Ejemplo 3.12. 1. $\mathbb{Z}_{(7)}C_3$ no es $*$-clean. En efecto, como se mostró en el Ejemplo 2.16, $\mathbb{Z}_{(7)}C_3$ no es clean, por lo tanto no es $*$-clean.

2. $\mathbb{Z}_{(p)}C_3$ es $*$-clean, donde $p = 2, 3, 5$. Si $p = 2$, $\mathbb{Z}_{(2)}C_3$ es semiperfecto siguiendo [5]. Entonces $\mathbb{Z}_{(2)}C_3$ es clean[21] y la ecuación $x^2 + x + 1 = 0$ no tiene soluciones en $\mathbb{Z}_{(2)}$. Así, por Teorema 3.6, $\mathbb{Z}_{(2)}C_3$ es $*$-clean.

   Si $p = 3$, por Teorema 3.6 se tiene que $\mathbb{Z}_{(3)}C_3$ es $*$-clean. Por último, si $p = 5$ la prueba es análoga al caso $p = 2$.

A continuación se estudia cuando el anillo de grupo RC_4 es $*$-clean.

Lema 3.13. *Sea R un anillo local conmutativo y $C_4 = \langle g \rangle$, el grupo cíclico de orden 4. Asuma que $x = a_0 + a_1 g + a_2 g^2 + a_3 g^3$ es un idempotente de RC_4, donde $a_0, a_1, a_2, a_3 \in R$. Entonces $x^* = x$ si y solo si $a_1 - a_3 \in J(R)$.*

---

[21] "Un anillo R es semiperfecto si y solo si R es clean y no contiene un conjunto infinito de idempotentes ortogonales." ver V. P. Camillo y H. P. Yu (V.P. Camillo y H.P. Yu. "Exchange rings, units and idempotents". En: *Comm. Algebra* 22.12 [1994], págs. 4737-4749)

Demostración. ($\Rightarrow$) Aplicando la involución clásica se obtiene:

$$\begin{aligned} x^* &= a_0^* + (a_1g)^* + (a_2g^2)^* + (a_3g^3)^* = a_0 + a_1g^{-1} + a_2g^{-2} + a_3g^{-3} \\ &= a_0 + a_1g^3 + a_2g^2 + a_3g = a_0 + a_1g + a_2g^2 + a_3g^3 = x. \end{aligned}$$

Por lo tanto, $a_1 = a_3$ y así, $a_1 - a_3 = 0 \in J(R)$.

($\Leftarrow$) Sea $x = a_0 + a_1g + a_2g^2 + a_3g^3 \in \mathcal{I}d(RC_4)$. Entonces

$$\begin{aligned} x^2 &= (a_0 + a_1g + a_2g^2 + a_3g^3)^2 \\ &= a_0^2 + 2a_1a_3 + a_2^2 + (2a_0a_1 + 2a_2a_3)g + (a_1^2 + 2a_0a_2 + a_3^2)g^2 + (2a_0a_3 + 2a_1a_2)g^3 \\ &= a_0 + a_1g + a_2g^2 + a_3g^3 = x. \end{aligned}$$

Y así,

$$a_0^2 + 2a_1a_3 + a_2^2 = a_0, \tag{7}$$

$$2a_0a_1 + 2a_2a_3 = a_1, \tag{8}$$

$$2a_0a_2 + a_1^2 + a_3^2 = a_2, \tag{9}$$

$$2a_0a_3 + 2a_1a_2 = a_3. \tag{10}$$

Luego, de restar (10) de (8), se obtiene $2a_0(a_1 - a_3) + 2a_2(a_3 - a_1) = a_1 - a_3$, es decir,

$$(a_1 - a_3)(2a_0 - 2a_2 - 1) = 0. \tag{11}$$

De forma similar, restando (9) de (7), se obtiene $(a_0 - a_2)^2 - (a_1 - a_3)^2 = a_0 - a_2$, y así,

$$(a_0 - a_2)(a_0 - a_2 - 1) = (a_1 - a_3)^2. \tag{12}$$

Como $a_1 - a_3 \in J(R)$, sigue que $(a_0 - a_2)(a_0 - a_2 - 1) \in J(R)$. Luego $a_0 - a_2 \in J(R)$ o $a_0 - a_2 - 1 \in J(R)$. En el primer caso, si $a_0 - a_2 \in J(R)$, también $2(a_0 - a_2) \in J(R)$, por lo tanto $2a_0 - 2a_2 - 1 \in \mathcal{U}(R)$, y de (11), $a_1 = a_3$. En el segundo caso, donde $a_0 - a_2 - 1 \in J(R)$ se cumple que $2(a_0 - a_2 - 1) \in J(R)$ y por lo tanto $2a_0 - 2a_2 - 1 \in \mathcal{U}(R)$. Nuevamente de (11), $a_1 = a_3$. De lo cual se concluye que $x^* = x$.

Teorema 3.14. *Sea R un anillo local conmutativo y $C_4 = \langle g \rangle$ el grupo cíclico de orden 4.*

1. *Si $2 \in J(R)$, RC_4 es $*$-clean.*
2. *Si $2 \notin J(R)$, RC_4 es $*$-clean si y solo si RC_4 es clean y la ecuación $x^2 + 1 = 0$ no tiene soluciones en R.*

Demostración.

1. Como $2 \in J(R)$, por el Teorema 1.53(2), RC_4 es local. Así, RC_4 es $*$-clean.
2. $(\Rightarrow)$ Es claro que RC_4 es clean por ser $*$-clean. Suponga que la ecuación $x^2 + 1 = 0$ tiene por solución a $\alpha \in R$, entonces $\alpha^2 = -1$ y $\alpha^4 = 1$. Al tomar $e = \frac{1}{4} + \frac{1}{4}\alpha g - \frac{1}{4}g^2 - \frac{1}{4}\alpha g^3$. Se tiene que $e^2 = (\frac{1}{4} + \frac{1}{4}\alpha g - \frac{1}{4}g^2 - \frac{1}{4}\alpha g^3)^2 = 4(\frac{1}{16}) + 4(\frac{1}{16}\alpha g) - 4(\frac{1}{16}g^2) - 4(\frac{1}{16}\alpha g^3) = e$. Se afirma que $e^* \neq e$, de lo contrario, se tendría que $\frac{1}{4}\alpha = -\frac{1}{4}\alpha$ y por lo tanto $\alpha = 0$, lo que contradice que α es solución de $x^2 + 1 = 0$. Así, usando el Lema 3.3 RC_4 no es $*$-clean, contradiciendo la hipótesis inicial.

   $(\Leftarrow)$ Suponga que RC_4 no es $*$-clean, entonces existe un idempotente $e = a_0 + a_1 g + a_2 g^2 + a_3 g^3$ tal que $e^* \neq e$. Del Lema 3.13, se tiene que $a_1 - a_3 \in \mathcal{U}(R)$. Se deduce de (11) que $2a_0 - 2a_2 - 1 = 0$, es decir, $a_0 - a_2 = \frac{1}{2}$ y de (12) se obtiene $[2(a_1 - a_3)]^2 + 1 = 0$. De esta forma, la ecuación $x^2 + 1 = 0$ tiene por solución a $x = 2(a_1 - a_3)$, lo que es una contradicción.

De nuevo al usar el resultado de I. G. Conell [14], al caso de RC_4, sigue de forma análoga al caso de RC_3 que RC_4 es fuertemente pi-regular y clean. Como consecuencia del Teorema 3.14 se tiene.

Corolario 3.15. *Sea $R = \mathbb{Z}_p$, donde $p > 2$ primo*

1. *Si $p \equiv 1(mod\ 4)$, RC_4 es clean pero no $*$-clean.*

2. *Si $p \equiv 3(mod\ 4)$, RC_4 es $*$-clean.*

Demostración. Del Teorema 3.8 se deduce que RC_4 es clean. Es conocido en la teoría de números que si p es primo, el símbolo de Legendre $\left[\frac{-1}{p}\right]$ es 1 si $p \equiv 1(\text{mod } 4)$ o -1 si $p \equiv -1(\text{mod } 4)$ [20], es decir, $x^2 + 1 = 0$ no tiene soluciones en R si y solo si $p \equiv 3(\text{mod } 4)$. Así, el resultado sigue del Teorema 3.14.

Ejemplo 3.16. $\mathbb{R}C_4$ es clean siguiendo el Teorema 3.8 y además es $*$-clean ya que $2 \in \mathcal{U}(\mathbb{R})$ y la ecuación $x^2 + 1 = 0$ no tiene soluciones en $\mathbb{R}$. Por el contrario, $\mathbb{C}C_4$ no es $*$-clean, dado que $2 \in \mathcal{U}(\mathbb{C})$ y $x^2 + 1 = 0$ tiene solución en $\mathbb{C}$. Sin embargo, del Teorema 3.8 $\mathbb{C}C_4$ es clean.

3.2. Anillos de Grupo No Abelianos

En esta sección se estudia cuando un anillo de grupo RG es $*$-clean, donde R es un anillo local conmutativo y G es S_3 o $\mathbb{Q}_8$. Primero se asume que $G = S_3$, el grupo simétrico de orden 3. Sea

$$S_3 = \langle a, b \mid a^3 = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle.$$

El siguiente resultado da condiciones sobre los elementos idempotentes de RS_3.

Lema 3.17. *Sea R un anillo conmutativo. Suponga que*

$$\alpha = x_0 + x_1a + x_2a^2 + x_3b + x_4ab + x_5a^2b \in RS_3,$$

donde $x_i \in R, i = 0, 1, ..., 5$. Entonces $\alpha^2 = \alpha$ si y solo si

$$\begin{aligned}
x_0^2 + 2x_1x_2 + x_3^2 + x_4^2 + x_5^2 &= x_0, \\
2x_0x_1 + x_2^2 + x_3x_4 + x_4x_5 + x_5x_3 &= x_1, && (13)\\
2x_0x_2 + x_1^2 + x_3x_4 + x_4x_5 + x_5x_3 &= x_2, && (14)\\
2x_0x_3 + x_1x_4 + x_1x_5 + x_2x_4 + x_2x_5 &= x_3, && (15)\\
2x_0x_4 + x_1x_3 + x_2x_3 + x_1x_5 + x_2x_5 &= x_4, && (16)\\
2x_0x_5 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 &= x_5. && (17)
\end{aligned}$$

Demostración.

$$\begin{aligned}
\alpha^2 = \; & (x_0 + x_1a + x_2a^2 + x_3b + x_4ab + x_5a^2b)^2 \\
= \; & (x_0^2 + 2x_0x_1a + 2x_0x_2a^2 + 2x_0x_3b + 2x_0x_4ab + 2x_0x_5a^2b + x_1^2a^2 + 2x_1x_2 + x_1x_3ab \\
& + x_1x_4a^2b + x_1x_5b + x_2^2a + x_2x_3a^2b + x_2x_4b + x_2x_5ab + x_1x_3ba + x_2x_3ba^2 + x_3^2 \\
& + x_3x_4bab + x_3x_5ba^2b + x_1x_4aba + x_2x_4aba^2 + x_3x_4a + x_4^2(ab)^2 + x_4x_5aba^2b \\
& + x_1x_5a^2ba + x_2x_5a^2ba^2 + x_3x_5a^2 + x_4x_5a^2bab + x_5^2(a^2b)^2) \\
= \; & x_0^2 + 2x_1x_2 + x_3^2 + x_4^2 + x_5^2 + (2x_0x_1 + x_2^2 + x_3x_4 + x_4x_5 + x_5x_3)a \\
& + (2x_0x_2 + x_1^2 + x_3x_4 + x_4x_5 + x_5x_3)a^2 + (2x_0x_3 + x_1x_4 + x_1x_5 + x_2x_4 + x_2x_5)b \\
& + (2x_0x_4 + x_1x_3 + x_2x_3 + x_1x_5 + x_2x_5)ab + (2x_0x_5 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4)a^2b \\
& = x_0 + x_1a + x_2a^2 + x_3b + x_4ab + x_5a^2b = \alpha.
\end{aligned}$$

Luego, el resultado sigue de comparar los respectivos coeficientes.

Lema 3.18. *Sea R un anillo local conmutativo con $2 \in J(R)$. Suponga que $\alpha = x_0 + x_1a + x_2a^2 + x_3b + x_4ab + x_5a^2b$ es un idempotente de RS_3, donde $x_i \in R, i = 0, 1, ..., 5$. Entonces*

1. $x_3 + x_4 + x_5 = 0$.
2. *Si $x_2 - x_1 \in J(R)$, entonces $x_1 = x_2$.*
3. *Si $x_2 - x_1 \in \mathcal{U}(R)$, entonces $x_0 = \frac{1}{3}$ y $x_1 + x_2 = -\frac{1}{3}$, o, $x_0 = \frac{2}{3}$ y $x_1 + x_2 = \frac{1}{3}$.*

Demostración.

1. Sumando (15), (16) y (17) se tiene

$$2x_0(x_3 + x_4 + x_5) + 2x_1(x_3 + x_4 + x_5) + 2x_2(x_3 + x_4 + x_5) = x_3 + x_4 + x_5.$$

   Luego $(x_3 + x_4 + x_5)[1 - 2(x_0 + x_1 + x_2)] = 0$. Del hecho de que $2 \in J(R)$, se tiene que $1 - 2(x_0 + x_1 + x_2) \in \mathcal{U}(R)$. Por lo tanto $x_3 + x_4 + x_5 = 0$

2. Restando (14) de (13), se obtiene $2x_0(x_1 - x_2) + (x_2 - x_1)(x_1 + x_2) = x_1 - x_2$, es decir

$$(x_2 - x_1)(x_1 + x_2 - 2x_0 + 1) = 0. \tag{18}$$

   Ya que 2 y $x_2 - x_1 \in J(R)$, sigue que $x_1 + x_2 - 2x_0 + 1 = 1 + (x_2 - x_1) - 2(x_0 - x_1) \in \mathcal{U}(R)$. Así, $x_1 = x_2$.

3. Si $x_1 - x_2 \in \mathcal{U}(R)$ de (18) se obtiene

$$x_1 + x_2 - 2x_0 + 1 = 0. \tag{19}$$

   Como $\alpha^2 = \alpha$, $\varepsilon(\alpha)^2 = \varepsilon(\alpha^2) = \varepsilon(\alpha)$, entonces $(x_0 + x_1 + x_2 + x_3 + x_4 + x_5)^2 = (x_0 + x_1 + x_2 + x_3 + x_4 + x_5)$. Como R es local se puede afirmar que $x_0 + x_1 +$

$x_2 + x_3 + x_4 + x_5 = 0$ o 1. Así por Lema 3.18(1), se reduce a $x_0 + x_1 + x_2 = 0$ o 1. Sigue de (19) que

$$x_0 = \frac{1}{3} \text{ y } x_1 + x_2 = -\frac{1}{3} \quad \text{o} \quad x_0 = \frac{2}{3} \text{ y } x_1 + x_2 = \frac{1}{3}.$$

Lema 3.19. *Sea R un anillo local conmutativo con $2 \in J(R)$. Suponga que $\alpha = x_0 + x_1a + x_2a^2 + x_3b + x_4ab + x_5a^2b \in RS_3$, donde cada $x_i \in R$. Entonces $\alpha^2 = \alpha = \alpha^*$ si y solo si $\alpha = x_0 + x_1a + x_1a^2$, donde $x_0 = -2x_1$ y $3x_1^2 + x_1 = 0$, o, $x_0 = 1 - 2x_1$ y $3x_1^2 - x_1 = 0$.*

Demostración.

$$\begin{aligned}
\alpha^* &= (x_0 + x_1a + x_2a^2 + x_3b + x_4ab + x_5a^2b)^* \\
&= x_0 + x_1a^* + x_2(a^2)^* + x_3b^* + x_4(ab)^* + x_5(a^2b)^* \\
&= x_0 + x_1a^2 + x_2a + x_3b + x_4ab + x_5a^2b \\
&= x_0 + x_1a + x_2a^2 + x_3b + x_4ab + x_5a^2b = \alpha.
\end{aligned}$$

Luego, al comparar con el Lema 3.17 se tiene que

$$x_0^2 + 2x_1^2 + x_3^2 + x_4^2 + x_5^2 = x_0, \tag{20}$$

$$2x_0x_1 + x_1^2 + x_3x_4 + x_4x_5 + x_5x_3 = x_1, \tag{21}$$

$$2x_0x_3 + 2x_1x_4 + 2x_1x_5 = x_3, \tag{22}$$

$$2x_0x_4 + 2x_1x_3 + 2x_1x_5 = x_4,$$

$$2x_0x_5 + 2x_1x_3 + 2x_1x_4 = x_5,$$

$$x_1 = x_2.$$

$(\Rightarrow)$ Sumando (20) y $2\times$(21) se tiene

$$x_0^2 + 4x_0x_1 + 4x_1^2 + (x_3 + x_4 + x_5)^2 = x_0 + 2x_1.$$

Del Lema 3.18(1), se tiene que $(x_0 + 2x_1)^2 = x_0 + 2x_1$. Por lo tanto, $x_0 + 2x_1 = 0$ o 1 ya que R es local.

Caso 1: Si $x_0 + 2x_1 = 0$, $x_0 = -2x_1$. Sigue de (22) que $-4x_1x_3 + 2x_1x_4 + 2x_1x_5 = x_3$. Como $x_3 + x_4 + x_5 = 0$, se tiene que $-6x_1x_3 = x_3$, entonces $x_3(1 + 6x_1) = 0$. Ya que $2 \in J(R)$, se obtiene $1 + 6x_1 \in \mathcal{U}(R)$, luego $x_3 = 0$. De forma análoga se obtiene que $x_4 = x_5 = 0$. También de (21), se tiene que $3x_1^2 + x_1 = 0$. Así, $\alpha = x_0 + x_1a + x_1a^2$ donde $x_0 = -2x_1$ y $3x_1^2 + x_1 = 0$.

Caso 2: Si $x_0 + 2x_1 = 1$, $x_0 = 1 - 2x_1$. Sigue de (22) que $2(1-2x_1)x_3 + 2x_1x_4 + 2x_1x_5 = x_3$. Ya que $x_3 + x_4 + x_5 = 0$, se obtiene $x_3 - 6x_1x_3 = 0$, entonces $x_3(1 - 6x_1) = 0$. Como $2 \in J(R)$, $1 - 6x_1 \in \mathcal{U}(R)$, entonces $x_3 = 0$. Similarmente se muestra que $x_4 = x_5 = 0$. También de (21) se obtiene que $3x_1^2 - x_1 = 0$. Así, $\alpha = x_0 + x_1a + x_1a^2$, donde $x_0 = 1 - 2x_1$ y $3x_1^2 - x_1 = 0$.

$(\Leftarrow)$ Note que $\alpha^* = (x_0 + x_1a + x_1a^2)^* = x_0 + x_1a^{-1} + x_2(a^2)^{-1} = x_0 + x_1a^2 + x_1a = \alpha$, y $\alpha^2 = (x_0 + x_1a + x_1a^2)^2 = 2x_1^2 + x_0^2 + (2x_0x_1 + x_1^2)a + (2x_0x_1 + x_1^2)a^2$. En el primer caso donde $x_0 = -2x_1$ y $x_1 = -3x_1^2$ se tiene que

$$\begin{aligned} \alpha^2 &= 2x_1^2 + (-2x_1)^2 + (2(-2x_1)x_1 + x_1^2)a + (2(-2x_1)x_1 + x_1^2)a^2 \\ &= 6x_1^2 - 3x_1^2a + 3x_1^2a^2 = -2x_1 - 3x_1^2a + 3x_2^2a^2 \\ &= x_0 + x_1a + x_1a^2 = \alpha. \end{aligned}$$

Para el segundo caso en donde $x_0 = 1 - 2x_1$ y $3x_1^2 - x_1 = 0$ se tiene que

$$\begin{aligned}\alpha^2 &= 1 + 6x_1^2 - 4x_1 + (2x_1 - 3x_1^2)a + (2x_1 - 3x_1^2)a^2 \\ &= 1 - 2x_1 + x_1a + x_1a^2 \\ &= x_0 + x_1a + x_1a^2 = \alpha.\end{aligned}$$

Teorema 3.20. *Sea R un anillo local conmutativo tal que $2 \in J(R)$. Entonces RS_3 es clean pero no $*$-clean.*

Demostración. De [5] se tiene que RS_3 es semiperfecto y por lo tanto clean. Sea

$$e = \frac{1}{3} + \frac{2}{3}a - a^2 - b + \frac{2}{3}ab + \frac{1}{3}a^2b.$$

Es sencillo comprobar que $e^2 = e$. Como $\varepsilon(e) = \frac{1}{3} + \frac{2}{3} - 1 - 1 + \frac{2}{3} + \frac{1}{3} = 0$, e no es una unidad. Se necesita probar que $e \neq f + u$ para cualquier $f \in proy(RS_3)$ y $u \in \mathcal{U}(RS_3)$. Suponga que $e = f + u$, como $e \neq 0$, se debe tener que $f \neq 1$, de lo contrario se tiene que $1 - e = f - e = -u \in \mathcal{U}(RS_3)$. Note también que $1 - e \neq 1$ es un idempotente, lo que produce una contradicción. Como $e \neq 1$, se tiene que $f \neq 0$, de otra forma $u = e \in \mathcal{U}(RS_3)$, que es una contradicción. Del lema 3.19 se sabe que $f = x_0 + x_1a + x_1a^2$, donde $x_0 = -2x_1$, $3x_1^2 + x_1 = 0$, o $x_0 = 1 - 2x_1$, $3x_1^2 - x_1 = 0$.
Caso 1: Suponga que $f = -2x_1 + x_1a + x_1a^2$, donde $3x_1^2 + x_1 = 0$. Entonces

$$u = e - f = \left(\frac{1}{3} + 2x_1\right) + \left(\frac{2}{3} - x_1\right)a + (-x_1 - 1)a^2 - b + \frac{2}{3}ab + \frac{1}{3}a^2b.$$

Ahora, $\varepsilon(u) = (\frac{1}{3} + 2x_1) + (\frac{2}{3} - x_1) + (-x_1 - 1) - 1 + \frac{2}{3} + \frac{1}{3} = 0$, por lo tanto $u \notin \mathcal{U}(RS_3)$ lo que es una contradicción.

Caso 2: Suponga que $f = (1 - 2x_1) + x_1a + x_1a^2$, donde $3x_1^2 - x_1 = 0$. Entonces

$$u = e - f = \left(2x_1 - \frac{2}{3}\right) + \left(\frac{2}{3} - x_1\right)a + (-x_1 - 1)a^2 - b + \frac{2}{3}ab + \frac{1}{3}a^2b.$$

Asuma que $uv = 0$ para algún $v = y_0 + y_1a + y_2a^2 + y_3b + y_4ab + y_5a^2b$. Entonces

$$(S_1) = \begin{cases} (2x_1 - \frac{2}{3})y_0 + (-x_1 - 1)y_1 + (\frac{2}{3} - x_1)y_2 - y_3 + \frac{2}{3}y_4 + \frac{1}{3}y_5 & = 0, \\ (\frac{2}{3} - x_1)y_0 + (2x_1 - \frac{2}{3})y_1 + (-x_1 - 1)y_2 + \frac{2}{3}y_3 + \frac{1}{3}y_4 - y_5 & = 0, \\ (-x_1 - 1)y_0 + (\frac{2}{3} - x_1)y_1 + (2x_1 - \frac{2}{3})y_2 + \frac{1}{3}y_3 - y_4 + \frac{2}{3}y_5 & = 0, \\ -y_0 + \frac{2}{3}y_1 + \frac{1}{3}y_2 + (2x_1 - \frac{2}{3})y_3 + (-x_1 - 1)y_4 + (\frac{2}{3} - x_1)y_5 & = 0, \\ \frac{2}{3}y_0 + \frac{1}{3}y_1 - y_2 + (\frac{2}{3} - x_1)y_3 + (2x_1 - \frac{2}{3})y_4 + (-x_1 - 1)y_5 & = 0, \\ \frac{1}{3}y_0 - y_1 + \frac{2}{3}y_2 + (-x_1 - 1)y_3 + (\frac{2}{3} - x_1)y_4 + (2x_1 - \frac{2}{3})y_5 & = 0. \end{cases}$$

Como la matriz de coeficientes del sistema de ecuaciones (S_1) es

$$A = \begin{bmatrix} 2x_1 - \frac{2}{3} & -x_1 - 1 & \frac{2}{3} - x_1 & -1 & \frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} - x_1 & 2x_1 - \frac{2}{3} & -x_1 - 1 & \frac{2}{3} & \frac{1}{3} & -1 \\ -x_1 - 1 & \frac{2}{3} - x_1 & 2x_1 - \frac{2}{3} & \frac{1}{3} & -1 & \frac{2}{3} \\ -1 & \frac{2}{3} & \frac{1}{3} & 2x_1 - \frac{2}{3} & -x_1 - 1 & \frac{2}{3} - x_1 \\ \frac{2}{3} & \frac{1}{3} & -1 & \frac{2}{3} - x_1 & 2x_1 - \frac{2}{3} & -x_1 - 1 \\ \frac{1}{3} & -1 & \frac{2}{3} & -x_1 - 1 & \frac{2}{3} - x_1 & 2x_1 - \frac{2}{3} \end{bmatrix}$$

y $det(A) = 9x_1^2(3x_1 - 1)^2 = 0$, de [22] el sistema de ecuaciones (S_1) tiene soluciones diferentes de cero. Así u es divisor de cero, lo que contradice que $u \in \mathcal{U}(RS_3)$. Por lo tanto, RS_3 no es $*$-clean.

---

[22] W. C. Brown. *Matrices over commutative rings*. Marcel Dekker, Inc., 1993.

Ejemplo 3.21. $\mathbb{Z}_2S_3$ no es abeliano, pero es $*$-abeliano.
En efecto, sea $\alpha = a+b+ab \in \mathbb{Z}_2S_3$. Es sencillo mostrar que $\alpha^2 = \alpha$, pero $b\alpha = 1+a^2+a^2b$ y $\alpha b = 1+a+ab$. Así, $b\alpha \neq \alpha b$, por lo tanto $\mathbb{Z}_2S_3$ no es abeliano. Del Lema 3.19, $proy(\mathbb{Z}_2S_3) = \{0, 1, a+a^2, 1+a+a^2\}$. Como $(a+a^2)b = b(a+a^2)$ y $(a+a^2)a = a(a+a^2)$, se deduce que $a+a^2$ y $1+a+a^2$ son centrales en $\mathbb{Z}_2S_3$. Por lo tanto $\mathbb{Z}_2S_3$ es $*$-abeliano.

Ejemplo 3.22. La involución $*$ en $\mathbb{Z}_2S_3$ no es propia. En efecto, sea $\alpha = 1+a+a^2+b+ab+a^2b \in \mathbb{Z}_2S_3$. Es claro que $\alpha^* = \alpha$. Note que $\alpha^*\alpha = \alpha^2 = 0$ pero $\alpha \neq 0$. Por lo tanto, la involución $*$ no es propia.

A continuación se asumirá que $G = \mathbb{Q}_8$, el grupo cuaternio de orden 8 definido en el Ejemplo 1.18.

Note que si R es conmutativo y $2 \in \mathcal{U}(R)$, entonces el elemento $e = \frac{1}{2}(1+a^2)$ es idempotente. Además, recordando que $a^2 \in \mathcal{Z}(\mathbb{Q}_8)$ es fácil ver que e es central en $R\mathbb{Q}_8$, por lo cual $R\mathbb{Q}_8 = (R\mathbb{Q}_8)e \oplus (R\mathbb{Q}_8)f$, donde $f = 1-e$.

Lema 3.23. *Suponga que $R\mathbb{Q}_8$ se descompone de la forma descrita anteriormente. Para cualquier $\alpha \in (R\mathbb{Q}_8)f$, $\alpha^2 = \alpha \iff \alpha = x_0 + x_1a - x_0a^2 - x_1a^3 + x_4b + x_5ab - x_4a^2b - x_5a^3b$ con $2x_0^2 - 2x_1^2 - 2x_4^2 - 2x_5^2 = x_0$, $4x_0x_1 = x_1$, $4x_0x_4 = x_4$ y $4x_0x_5 = x_5$.*

Demostración. Para cualquier $\alpha = x_0 + x_1a + x_2a^2 + x_3a^3 + x_4b + x_5ab + x_6a^2b + x_7a^3b \in (R\mathbb{Q}_8)f$, donde $x_i \in R, i = 0, 1, ..., 7$, se tiene que $\alpha e = 0$. Por lo tanto, $x_i + x_{i+2} = 0, i = 0, 1, 4, 5$. El resultado sigue directo de las operaciones.

Teorema 3.24. *Sea R un anillo local conmutativo.*

1. *Si $2 \in J(R)$, entonces $R\mathbb{Q}_8$ es $*$-clean.*
2. *Si $2 \in \mathcal{U}(R)$, entonces $R\mathbb{Q}_8$ es $*$-clean si y solo si $R\mathbb{Q}_8$ es clean y la ecuación $x^2+y^2+z^2+1 = 0$ no tiene soluciones en R.*

Demostración.

1. Ya que R es local, $2 \in J(R)$ y $\mathbb{Q}_8$ es un 2-grupo finito, por 1.53(2) $R\mathbb{Q}_8$ es local. Por lo tanto, $R\mathbb{Q}_8$ es $*$-clean.

2. ($\Rightarrow$) Sea $\alpha = x_0 + x_1a + x_2a^2 + x_3a^3 + x_4b + x_5ab + x_6a^2b + x_7a^3b \in R\mathbb{Q}_8$, donde $x_i \in R, i = 0, 1, ..., 7$. Entonces

$$\begin{aligned} \alpha e &= \tfrac{1}{2}[(x_0 + x_2) + (x_1 + x_3)a + (x_0 + x_2)a^2 + (x_1 + x_3)a^3 \\ &\quad +(x_4 + x_6)b + (x_5 + x_7)ab + (x_4 + x_6)a^2b + (x_5 + x_7)a^3b]. \end{aligned}$$

   Es claro que $(\alpha e)^* = \alpha e$, luego cada idempotente de $(R\mathbb{Q}_8)e$ es una proyección. Como $R\mathbb{Q}_8$ es $*$-clean, también es clean. Siguiendo que $R\mathbb{Q}_8 = (R\mathbb{Q}_8)e \oplus (R\mathbb{Q}_8)f$ se deduce que $(R\mathbb{Q}_8)f$ es $*$-clean. Ahora solo se necesita verificar que la ecuación $x^2 + y^2 + z^2 + 1 = 0$ no tiene soluciones en R.

   Suponga que la ecuación $x^2 + y^2 + z^2 + 1 = 0$ tiene por solución $x = 4x_1, y = 4x_4, z = 4x_5$, es decir $16x_1^2 + 16x_4^2 + 16x_5^2 + 1 = 0$. Sea

$$s = \frac{1}{4} + x_1a - \frac{1}{4}a^2 - x_1a^3 + x_4b + x_5ab - x_4a^2b - x_5a^3b.$$

   Es un ejercicio simple ver que $s^2 = s$ pero $s^* \neq s$.(De lo contrario se tendría que $x_1 = x_4 = x_5 = 0$, lo que genera una contradicción). Sigue mostrar que $s \neq t + u$, donde $t^2 = t = t^*$ y $u \in \mathcal{U}((R\mathbb{Q}_8)f)$. Suponga que $s = t + u$, es claro que $t \neq 0$ o f. Del Lema 3.23 se obtiene $t = x_0 - x_0a^2$ con $2x_0^2 = x_0$. Así, $u = s - t = (\frac{1}{4} - x_0) + x_1a - (\frac{1}{4} - x_0)a^2 - x_1a^3 + x_4b + x_5ab - x_4a^2b - x_5a^3b$. Asuma que $uv = 0$ para algún $v = y_0 + y_1a - y_0a^2 - y_1a^3 + y_4b + y_5ab - y_4a^2b - y_5a^3b$.

Entonces

$$(S_2) = \begin{cases} (\frac{1}{4} - x_0)y_0 - x_1y_1 - x_4y_4 - x_5y_5 &= 0, \\ x_1y_0 + (\frac{1}{4} - x_0)y_1 - x_5y_4 + x_4y_5 &= 0, \\ x_4y_0 + x_5y_1 + (\frac{1}{4} - x_0)y_4 - x_1y_5 &= 0, \\ x_5y_0 - x_4y_1 + x_1y_4 + (\frac{1}{4} - x_0)y_5 &= 0. \end{cases}$$

Como la matriz de coeficientes del sistema de ecuaciones (S_2) es

$$A = \begin{bmatrix} \frac{1}{4} - x_0 & -x_1 & -x_4 & -x_5 \\ x_1 & \frac{1}{4} - x_0 & -x_5 & x_4 \\ x_4 & x_5 & \frac{1}{4} - x_0 & -x_1 \\ x_5 & -x_4 & x_1 & \frac{1}{4} - x_0 \end{bmatrix}$$

y $det(A) = [(\frac{1}{4} - x_0)^2 + x_1^2 + x_4^2 + x_5^2]^2 = (\frac{1}{16} - \frac{1}{2}x_0 + x_0^2 - \frac{1}{16})^2 = 0$, de [22] el sistema de ecuaciones (S_2) tiene soluciones diferentes de cero. Así, u es un divisor de cero, lo que es una contradicción. Por lo tanto, la ecuación $x^2 + y^2 + z^2 + 1 = 0$ no tiene solución en R.

$(\Leftarrow)$ Ya que $R\mathbb{Q}_8$ es clean, se deduce que $(R\mathbb{Q}_8)e$ es clean. Para cualquier $\alpha \in (R\mathbb{Q}_8)e, \alpha = c_1(1+a^2)+c_2a(1+a^2)+c_3(1+a^2)b+c_4a(1+a^2)b$. Es claro que $\alpha^* = \alpha$. Entonces $(R\mathbb{Q}_8)e$ es $*$-clean. Sigue mostrar que todo idempotente de $(R\mathbb{Q}_8)f$ es una proyección.

Suponga que $t^2 = t \in (R\mathbb{Q}_8)f$. Del lema 3.23 sigue que

$$t = x_0 + x_1a - x_0a^2 - x_1a^3 + x_4b + x_5ab - x_4a^2b - x_5a^3b$$

y $4x_0x_1 = x_1$. Si $x_1 \in \mathcal{U}(R)$ entonces $4x_0 = 1$, es decir, $x_0 = \frac{1}{4}$. Del Lema 3.23 se tiene que

$$(4x_1)^2 + (4x_4)^2 + (4x_5)^2 + 1 = 0.$$

Por lo tanto la ecuación $x^2 + y^2 + z^2 + 1 = 0$ tiene solución, lo que contradice la hipótesis. Así $x_1 \in J(R)$.

Suponga que $1 - 4x_0 \in J(R)$, por tanto $x_0 \in \mathcal{U}(R)$. Del Lema 3.23 se tiene que

$$\begin{aligned} 2x_1^2 &= 2x_0^2 - 2x_4^2 - 2x_5^2 - x_0 = 2x_0^2 - 32x_0^2x_4^2 - 32x_0^2x_5^2 - x_0 \\ &= x_0(2x_0 - 32x_0x_4^2 - 32x_0x_5^2 - 1) = x_0(2x_0 - 8x_4^2 - 8x_5^2 - 1). \end{aligned}$$

Como $x_1 \in J(R)$, también $2x_1^2 \in J(R)$. Por lo tanto $2x_0 - 8x_4^2 - 8x_5^2 - 1 \in J(R)$ ya que $x_0 \in \mathcal{U}(R)$. Tomando $y = 2x_0 - 8x_4^2 - 8x_5^2 - 1$, se sigue que $2x_0 - 1 = y + 8(x_4^2 + x_5^2)$. Ahora, como $2x_0 \in \mathcal{U}(R)$ y $1 - 4x_0 \in J(R)$, entonces $2x_0 - 1 = (-2x_0) - (1 - 4x_0) \in \mathcal{U}(R)$ y $8(x_4^2 + x_5^2) \in \mathcal{U}(R)$. Así $x_4^2 + x_5^2 \in \mathcal{U}(R)$. Del Lema 3.23 se concluye que $16x_0^2(x_4^2 + x_5^2) = x_4^2 + x_5^2$. Luego, $16x_0^2 = 1$, es decir, $(1 - 4x_0)(1 + 4x_0) = 0$. Como $1 - 4x_0 \in J(R), 1 + 4x_0 = 2 - (1 - 4x_0) \in \mathcal{U}(R)$. Así $1 - 4x_0 = 0$, entonces $x_0 = \frac{1}{4}$. Del Lema 3.23 se tiene

$$(4x_1)^2 + (4x_4)^2 + (4x_5)^2 + 1 = 0.$$

Luego, la ecuación $x^2 + y^2 + z^2 + 1 = 0$ tiene solución, lo que es una contradicción. Por lo tanto, $1 - 4x_0 \in \mathcal{U}(R)$. Ahora del Lema 3.23, se tiene que $(1 - 4x_0)x_i = 0$ para $i = 1, 4, 5$. Entonces $x_1 = x_4 = x_5 = 0$. Así, $t = x_0 - x_0a^2$, por lo cual, $t^* = t$. Con esto todo idempotente en $(R\mathbb{Q}_8)f$ es una proyección. Se concluye que $(R\mathbb{Q}_8)f$ es $*$-clean. Como $R\mathbb{Q}_8 = (R\mathbb{Q}_8)e \oplus (R\mathbb{Q}_8)f$, $R\mathbb{Q}_8$ es $*$-clean.

Ejemplo 3.25.

- $\mathbb{R}\mathbb{Q}_8$ es $*$-clean, dado que la ecuación $x^2 + y^2 + z^2 + 1 = 0$ no tiene solución en $\mathbb{R}$ y por Teorema 3.8 $\mathbb{R}\mathbb{Q}_8$ es clean.

- $\mathbb{C}\mathbb{Q}_8$ es clean pero no $*$-clean. La propiedad clean es garantizada por el Teorema 3.8, y por Teorema 3.24 no es $*$-clean, dado que la ecuación $x^2 + y^2 + z^2 + 1 = 0$

tiene solución en $\mathbb{C}$.

BIBLIOGRAFÍA

Anderson, D. D. y V. P. Camillo. “Commutative rings whose elements are a sum of a unit and idempotent”. En: *Comm. Algebra* 30.7 (2002), págs. 3327-3336 (vid. pág. 7).

Atiyah, M. *Introduction to commutative algebra*. CRC Press, 2018 (vid. pág. 47).

Bhattacharya, Phani Bhushan, Surender Kumar Jain y SR Nagpaul. *Basic abstract algebra*. Cambridge University Press, 1994 (vid. pág. 23).

Brown, W. C. *Matrices over commutative rings*. Marcel Dekker, Inc., 1993 (vid. págs. 67, 70).

Camillo, V.P. y H.P. Yu. “Exchange rings, units and idempotents”. En: *Comm. Algebra* 22.12 (1994), págs. 4737-4749 (vid. pág. 58).

Connell, I. G. “On the group ring”. En: *Canad. J. Math* 15.3 (1963), págs. 650-685 (vid. págs. 44, 56, 61).

Gallian, J. *Contemporary abstract algebra*. Nelson Education, 2009 (vid. pág. 10).

Gao, Y., J. Chen e Y. Li. “Some $*$-clean group rings”. En: *Algebra Colloquium*. Vol. 22. World Scientific. 2015, págs. 169-180 (vid. págs. 8, 9).

Han, J. y W. Nicholson. “Extensions of clean rings”. En: *Comm. Algebra* 29.6 (2001), págs. 2589-2595 (vid. págs. 8, 46).

McGovern, W. W. “Neat rings”. En: *Journal of Pure and Applied Algebra* 205.2 (2006), págs. 243-265 (vid. pág. 7).

Nicholson, W. K. “Lifting idempotents and exchange rings”. En: *Transactions of the American Mathematical Society* 229 (1977), págs. 269-278 (vid. pág. 7).

— “Local group rings”. En: *Canadian Mathematical Bulletin* 15.1 (1972), págs. 137-138 (vid. pág. 38).

— “Strongly clean rings and Fitting’s lemma”. En: *Communications in algebra* 27.8 (1999), págs. 3583-3592 (vid. pág. 56).

Polcino Millies, C. y S. K. Sehgal. *An introduction to group rings*. Vol. 1. Springer Science & Business Media, 2002 (vid. págs. 16, 17, 28, 44, 45).

Rosen, K. H. *Elementary number theory and its applications*. Vol. 1. Pearson/Addison Wesley, 2005 (vid. págs. 57, 61).

Vaš, L. “$*$-Clean rings; some clean and almost clean Baer$*$-rings and von Neumann algebras”. En: *Journal of Algebra* 324.12 (2010), págs. 3388-3400 (vid. pág. 8).

Woods, S. M. “Some Results on Semi-Perfect Group Rings”. En: *Canad. J. of Math* 26.1 (1974), 121â€“129 (vid. págs. 8, 58, 66).

Ye, Y. “Semiclean rings”. En: *Communications in Algebra* 34.9 (2006), pág. 3487 (vid. pág. 48).