SOBRE ANILLOS DE GRUPO CLEAN

JORGE ANDRÉS ROJAS GÓMEZ

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
MAESTRíA EN MATEMÁTICAS
BUCARAMANGA
2018

SOBRE ANILLOS DE GRUPO CLEAN

JORGE ANDRÉS ROJAS GÓMEZ

Trabajo de grado presentado para optar al
título de Magister en Matemáticas

Director
ALEXANDER HOLGUÍN-VILLA
Doctor en Matemáticas

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMÁTICAS
MAESTRíA EN MATEMÁTICAS
BUCARAMANGA
2018

Agradecimientos

- Agradezco primeramente a Abigail Gómez Silva, por ser la mejor madre: su amor y paciencia son un conjunto infinito numerable.
- Agradezco especialmente a mi director de proyecto, el profesor Alexander Holguín-Villa por su colaboración, interés en este trabajo y por su gran paciencia.
- Agradezco a los profesores que contribuyeron en mi formación académica y personal.

Índice General

LISTA DE SÍMBOLOS

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	—	Conjunto de los enteros, racionales, reales y complejos respectivamente.
$\mathbb{Z}_n$	—	El conjunto de los enteros módulo n.
$G, R \ldots$	—	Conjuntos, grupos, anillos, etc.
$\mathcal{Q}_8$	—	Grupo de los cuaternios de orden 8.
$\zeta(G)$	—	El centro del grupo G.
C_n	—	El grupo cíclico de orden n.
G_p	—	La p-componente primaria del grupo G.
$\|G\|$	—	El orden del grupo G.
$exp(G)$	—	El exponente del grupo G.
S_n	—	El grupo simétrico de orden n.
$\simeq$	—	"isomorfo a".
$\prod_{i\in I} X_i$	—	El producto de $(X_i)_{i\in I}$.
$M_n(R)$	—	Matriz de orden n con coeficientes en el anillo R.
$\mathcal{J}(R)$	—	El radical de Jacobson del anillo R.

$\mathcal{U}(R)$	—	Conjunto de todas las unidades de del anillo R.
$\mathcal{I}d(R)$	—	EL conjunto de todos los idempotentes del anillo R .
RG	—	Anillo de grupo de un grupo G sobre un anillo R.
Δ	—	El ideal de aumento.

RESUMEN

TÍTULO: SOBRE ANILLOS DE GRUPO CLEAN[*]

AUTOR: JORGE ANDRÉS ROJAS GÓMEZ[**]

PALABRAS CLAVES: anillo clean, anillo de grupo clean.

DESCRIPCIÓN:
Un elemento a en un anillo R (asociativo con unidad) es llamado **clean** si él puede escribirse como la suma de una unidad y un elemento 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* [20]. 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.

El anillo $\mathbb{Z}$ con las operaciones usuales no es clean, aunque tiene elementos clean.
En efecto, dado que la ecuación $x = x^2$ en $\mathbb{Z}$ sólo se satisface para $x = 0$ o $x = 1$, entonces $\mathcal{ID}(\mathbb{Z}) = \{1, 0\}$. Además, sus elementos invertibles o unidades son 1,-1.
Usando la definición, los elementos clean se obtienen al hacer todas las posibles sumas de elementos invertibles con idempotentes:

$$\begin{aligned} 0 &= (-1) + 1, & 2 &= 1 + 1, \\ -1 &= (-1) + 0, & 1 &= 1 + 0. \end{aligned}$$

Por tanto, los únicos elementos clean en $\mathbb{Z}$ son $\{-1, 0, 1, 2\}$.

El propósito de este trabajo es estudiar algunas propiedades de los anillos clean y en particular verlas en el contexto de los anillos de grupo, situación en la que detallamos las pruebas de los resultados expuestos y en algunos casos los presentamos de otra forma.
Nuestro trabajo está compuesto por tres capítulos:
En el Capítulo 1 presentamos las definiciones y resultados conocidos que necesitaremos para desarrollar el presente trabajo. En el Capítulo 2 mostramos algunas caracterizaciones y, condiciones necesarias o suficientes para que un anillo R con unidad sea clean. Finalmente, en el último Capítulo presentamos algunos resultados conocidos para anillos de grupo clean, haciendo contraste con los enfoques hallados en la literatura. Además presentamos algunos resultados parciales en anillos de grupo clean no-conmutativos.

---

[*] Proyecto de grado

[**] Facultad de Ciencias. Escuela de Matemáticas. **Director** Dr. Alexander Holguín-Villa.

ABSTRACT

TITLE: ON CLEAN GROUP RINGS[***]

AUTHOR: JORGE ANDRÉS ROJAS GÓMEZ[****]

KEYWORDS: clean rings, clean group rings

DESCRIPTION:
A element a in a ring R(associative with unity) is called **clean** if it can be written as a sum of a unit and a idempotent element of R. A ring R is called **clean ring** if all its elements are clean.
Probably the concept of clean ring appeared for the first time in the work of W.K Nicholson *Lifting idempotents and Exchange Rings* [20]. His objective in that article was to prove that a ring A is "exchange" if and only if the idempotents could be lifted modulo every left ideal.

$\mathbb{Z}$ with usual operations is not clean, although it has clean elements.
Indeed, given that the equation $x = x^2$ is only satisfied by $x = 0$ or $x = 1$, then $\mathcal{ID}(\mathbb{Z}) = \{1, 0\}$.
Also, the units in $\mathbb{Z}$ are $1, -1$ only.
Using the definition, the clean elements of $\mathbb{Z}$ are obtained making every sum possible of invertible elements with idempotents:

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

Therefore the only clean elements of $\mathbb{Z}$ are $\{-1, 0, 1, 2\}$.

The purpose of this report is to study some properties of clean rings and clean group rings. Our monography is composed by three chapters:
In chapter 1, we will show some definitions and results which will be needed later in our work. In chapter 2, we will show some characterizations and, necessary or sufficient conditions to make a ring R with unity be clean. Finally, in the last chapter we present some known results about clean group rings, making a contrast with some approaches found in the literature. Moreover we give some results in non commutative group rings .

[***] Graduation project

[****] Faculty of Sciences. Department of Mathematics. **Advisor** Dr. Alexander Holguín Villa.

INTRODUCCIÓN

Un elemento a en un anillo R (asociativo con unidad) es llamado **clean** si él puede escribirse como la suma de una unidad y un elemento 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* [20]. 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. Wm. McGovern en [17] 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" [1], donde por ejemplo si A es anillo conmutativo, puede mostrarse que $A[x]$ (anillo de polinomios sobre A) nunca es un anillo clean y que el anillo de series formales $A[[x]]$ es clean si y solo si A es anillo clean.

Otra perspectiva es el estudio de los anillos clean en general, es decir, con o sin identidad. Estudios de ese tipo han sido abordados por *Nicholson y Y. Zhou* en su artículo "Clean general rings" [22], donde se extienden algunas propiedades conocidas de los anillos clean y se exhibe la relación que existe entre los anillos Booleanos y aquellos anillos clean, con la propiedad adicional de que cada elemento en dichos anillos tiene representación única.

En general, saber cuándo el anillo de grupo RG es clean es una pregunta abierta [29, p.336]. Por ejemplo se sabe que para todo anillo conmutativo clean R y el grupo cíclico C_2, RC_2 es anillo clean, sin embargo para R anillo arbitrario, tal respuesta no se sabe.
Esta pregunta fue considerada por primera vez, en el contexto de los anillos de grupo, por *Han y Nicholson* [9], donde por ejemplo es probado que para un anillo R Boo-

leano y G un grupo localmente finito, RG es un anillo clean. Entre otras propiedades encontradas, es presentado un ejemplo de un anillo clean R y un grupo finito G con orden $|G|$ siendo una unidad en R tal que RG no es un anillo clean, más exactamente, ellos comentan el trabajo de Woods [27] donde se muestra que $\mathbb{Z}_{(7)}C_3$ no es un anillo clean, en el cual $\mathbb{Z}_{(7)}$ es el anillo localizado de $\mathbb{Z}$ en el ideal primo (7) y C_3 el grupo cíclico de orden 3.

Un aspecto importante en el estudio de los anillos clean es el concepto de "regularidad" en el sentido de von Neumann, que es necesario para el estudio de anillos "fuertemente clean". Un elemento a es fuertemente clean si se puede expresar como $a = e + u$ con e idempotente y u una unidad, con la condición adicional de que $eu = ue$. Esto generó preguntas en muchos investigadores como *Yuang, Camillo, Zhou y Nicholson*, quienes estudiaron propiedades comunes y diferencias entre los anillos fuertemente clean y los anillos clean. Este enfoque en particular no será cubierto en este trabajo, lo cual no quiere decir que no sea importante.

Resulta curioso y fascinante que con la noción de anillo semiclean introducida por Ye en [28], pueda demostrarse de manera más simple que el anillo de grupo $\mathbb{Z}_{(7)}C_3$ no es clean en contraste a la prueba exhibida por Woods [27], desde el punto de vista polinomial años atras. Además Ye también demuestra que $\mathbb{Z}_{(7)}C_3$ es semiclean y así esta última clase de anillos contiene estrictamente a la clase de anillos clean. Algunas de estas propiedades, como por ejemplo la de ser anillo semiperfecto están siendo estudiadas actualmente y son motivo de interés en la teoría de anillos.

Nuestra motivación inicial, es estudiar los resultados conocidos (Estado del Arte) para así entender las ideas allí plasmadas que nos permitan organizar la teoría de los anillos clean, en particular la de los anillos de grupo con esa propiedad, destacando resultados claves que puedan aclarar preguntas como las anteriormente mencionadas, y si es posible, obtener resultados parciales (o totales) para anillos o anillos de grupo clean.

Capítulo 1

PRELIMINARES

Nuestro interés en este capítulo es presentar algunas definiciones básicas y resultados bien conocidos en la teoria de grupos, anillos y anillos de grupo, necesarios para el desarrollo de los capítulos siguientes. Es muy probable que estos conceptos se encuentren en cualquier plan de estudios de asignaturas como álgebra moderna I y II, por ello suponemos que el lector no experto tiene conocimientos básicos en grupos y anillos.
A lo largo del texto serán usadas las letras G y H para denotar grupos. Usaremos R y S para denotar anillos y, para el caso particular del anillo de los enteros, como es usual, $\mathbb{Z}$. En todos estos anillos los ideales serán denotados por I y J. Finalmente, por $\mathbb{F}$ denotaremos un cuerpo. La mayoria de los resultados serán asumidos sin demostración, sin embargo serán indicadas las respectivas referencias bibliográficas. Muchas de las pruebas podrán ser consultadas en [23], [7] y [6].

1.1. Grupos

Los grupos son estructuras algebraicas que en la actualidad son ampliamente estudiados dado a las diversas aplicaciones que se han encontrado no solo en matemáticas, sino en diversas disciplinas de la ciencia y tecnología.
Siguiendo Gallian [7], tenemos 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

- (*Asociatividad*) Para todos $a, b, c \in G$, $(ab)c = a(bc)$.
- (*Identidad*) Existe un elemento $e \in G$, tal que $ea = ae = a$ para todo $a \in G$.
- (*Inverso*) Para todo $a \in G$, existe $b \in G$ tal que $ab = ba = e$.

Si adicionalmente el grupo G satisface que, $ab = ba$ para todos a, b en G, G es llamado *grupo abeliano*. En el caso de que el conjunto G solo cumpla con la asociatividad, diremos que G es un *semigrupo*.

A continuacion se mencionan algunos ejemplos de grupos bien conocidos

Ejemplo 1.2.

$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ son grupos con la suma usual. más aún, todos ellos son abelianos.

El conjunto de los enteros $\mathbb{Z}$ con la multiplicación usual no es grupo, dado que por ejemplo, no existe $x \in \mathbb{Z}$ tal que $3x = 2$.

Un grupo de interés en la teoría de anillos de grupo y, en particular en este trabajo, es el grupo de los cuaternios de orden 8, que tiene la siguiente presentación: (ver [23])

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

Por extenso tenemos,

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

y así es un grupo finito. Además $\mathcal{Q}_8$ es un grupo no abeliano, dado que, de la presentación $ba = a^{-1}b$, de modo que

$$\begin{aligned} &a(a^3b) = b \quad \text{y} \\ &(a^3b)a = a^3(ba) = a^3(a^{-1}b) = a^2b. \end{aligned}$$

Una caracteristica relevante de $\mathcal{Q}_8$ es que todos sus subgrupos son normales. Entre otras propiedades que tiene $\mathcal{Q}_8$:

- a^2 es el único elemento no trivial que conmuta con los restantes y asi, el centro de $\mathcal{Q}_8$ es $\zeta(\mathcal{Q}_8) = \{1, a^2\}$.
- Para todo $x \in \mathcal{Q}_8$, $x^{2^k} = 1$ para algún $k \in \mathbb{N}$.
- es un 2-grupo, esto es, todo elemento de $\mathcal{Q}_8$ tiene como orden una potencia de 2, en particular, a^2 tiene orden $2^1 = 2$. Ver 1.6.

A continuación presentamos una clase de grupos muy importantes para este trabajo.

Definición 1.3. Un grupo G es llamado cíclico si existe un elemento $a \in G$ tal que $G = \{a^n \mid n \in \mathbb{Z}\}$. a es llamado un *generador* de G.
Sea $\emptyset \neq S \subseteq G$ con S finito. G se dice que es un *grupo finitamente generado* si G se puede escribir como $G = (g_1, g_2, \ldots, g_k) = \{g_1^{r_1} g_2^{r_2} \cdots g_k^{r_k} : g_k \in S,\, r_k = \pm 1,\, k \geq 1\} \cup \{1_G\}$.

Si el grupo tiene notación aditiva y es cíclico, como es usual, denotamos $G = \{na \mid n \in \mathbb{Z}\}$, grupo cíclico generado por a. Algunos ejemplos bien conocidos son

Ejemplo 1.4. El conjunto de los enteros con la suma usual es un grupo cíclico con 1 siendo uno de sus generadores, más aún, $\mathbb{Z}$ es finitamente generado. El grupo $\mathcal{Q}_8$ no lo es.

El siguiente resultado exhibe las principales características de los grupos cíclicos. Autores como Joseph Gallian (ver [7, Teorema 4.3]) consideran que este teorema es fundamental en el estudio de grupo cíclicos:

Teorema 1.5. *Todo subgrupo de un grupo cíclico es cíclico. Si el orden del grupo es n, para cada divisor k de n, el grupo tiene un subgrupo de orden k.*

Se presenta un concepto que será muy útil en la noción de anillos semiperfectos (ver sección 3.1).

Definición 1.6. Sea p o un primo o cero. La p-componente primaria de un grupo G abeliano es el subgrupo

$$G_p = \{a \in G \mid \exists k \in \mathbb{N},\ a^{p^k} = e\}.$$

Un grupo finito G es llamado $p-$grupo si su orden $|G|$ es una potencia de p. Si G es abeliano, será llamado *p-abeliano elemental* si todos los elementos diferentes de la identidad e son de orden p.

Ejemplo 1.7. Considere el grupo cíclico $C_3 = \{e, a, a^2\}$ con generador a.
Su 7-componente primaria es el subgrupo de C_3

$$(C_3)_7 = \{a \in C_3 \mid a^{7^k} = e,\ k \in \mathbb{N}\}$$

En efecto, consideremos la congruencia $7 \equiv 1 \mod 3$. De esta última congruencia obtenemos que

$$7^k \equiv 1 \mod 3$$

Luego $7^k = 3m + 1$ para algún $m \in \mathbb{Z}$ y así,

$$a^{7^k} = a^{3m+1} = a^{3m}a = (a^3)^m a = ea = a,$$

$$(a^2)^{7^k} = a^{6m+2} = a^{6m}a^2 = a^2.$$

De modo que,

$$(C_3)_7 = \{e\}.$$

Se presenta el concepto de exponente de G

Definición 1.8. Sea G un grupo en notación multiplicativa. El exponente de G es el menor entero positivo n, si existe, tal que $g^n = e$ para todo elemento de $g \in G$ y escribimos $exp(G) = n$.

Note que, de la definición de p-grupo abeliano elemental, G es un $p-$grupo abeliano elemental es una condición necesaria y suficiente para que $exp(G) = p$.
Suponga que G es un grupo abeliano con $exp(G) = p^m$ y considere el grupo $G^p = \{x^p \mid x \in G\}$. Tome $y \in G$, de la manera en que fue definido G^p, se sigue que y^p pertenece a G^p. Observe el lector lo siguiente:

$$(y^p)^{p^{m-1}} = y^{p(p^{m-1})} = y^{p^m} = e,$$

y esto se da si y solamente si $exp(G^p) = p^{m-1}$. Finalmente, si C_n denota el grupo cíclico de orden n, entonces $exp(C_n) = n$.

Ejemplo 1.9. Tome a C_3 y su 7-componente primaria $(C_3)_7$. Como C_3 es abeliano, todo subgrupo es normal, de modo que $C_3/(C_3)_7$ es un grupo.

$$C_3/(C_3)_7 = \{a^2\{e\}, a\{e\}, \{e\}\ \} \simeq \{e, a, a^2\}$$

Así, $exp(C_3/(C_3)_7) = exp(C_3) = 3$.
Considere el grupo $\mathbb{Z}_4$ con notación aditiva. Encontremos a $(\mathbb{Z}_4)_7$. Para esto, observe que $7 \equiv -1 \mod 4$, de aquí, tenemos la congruencia $7^k \equiv (-1)^k \mod 4$. Entonces tenemos que, si k es par, entonces existe $t \in \mathbb{N}$ tal que $7^k = 4t + 1$. De manera análoga, si k es impar, entonces existe $k_1 \in \mathbb{N}$ tal que $7^k = 4k_1 - 1 = 4k_1 + 3$. Por lo tanto,

$$(\mathbb{Z}_4)_7 = \begin{cases} \overline{1} & si \quad k \text{ es par.} \\ \overline{3} & si \quad k \text{ es impar.} \end{cases}$$

De lo anteriormente mencionado, tenemos que $\mathbb{Z}_4/(\mathbb{Z}_4)_7 = \mathbb{Z}_4/\{\overline{1}\}$ o $\mathbb{Z}_4/(\mathbb{Z}_4)_7 = \mathbb{Z}_4/\{\overline{3}\}$. Este último caso es no trivial, pues $\mathbb{Z}_4/(\mathbb{Z}_4)_7 = \mathbb{Z}_4/\{\overline{3}\} = \{\{3\}, 1 + \{3\}, 2 + \{3\}\}$.

Por lo mencionado en esta sección, el grupo de los cuaternios no es un grupo abeliano y se caracteriza por tener todos sus subgrupos normales, esto motiva la siguiente definición.

Definición 1.10. Un grupo no abeliano en el cual todos sus subgrupos son normales, se llama grupo *Hamiltoniano*.

Presentamos un teorema muy importante dado por R. Dedekind y R. Baer, el cual puede ser consultado en [23, teorema 1.8.5].

Teorema 1.11. *Un grupo G es hamiltoniano si y solo si G es isomorfo a*

$$G \simeq \mathcal{Q}_8 \times E \times A,$$

donde

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

Observación 1.12.

1. Cabe destacar que cuando $A = \{1\}$ es el grupo trivial, $G = \mathcal{Q}_8 \times E$ es llamado grupo 2-Hamiltoniano.
2. Sea E un grupo finito donde cada elemento diferente a la identidad tiene orden 2 y suponga que $x \in E$ con $x \neq e$. Entonces, tenemos que $x^2 = e$, y así $x = x^{-1}$. De esta manera, si $a, b \in E$, entonces $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$. Por lo tanto, E es abeliano.
   Entonces, en virtud a [2, Teorema 3.1], obtenemos que $|E| = 2^k$ y E puede ser escrito como el producto directo $E = C_2 \times C_2 \times \cdots \times C_2$.
3. Consideremos $A = C_{p^t}$, el grupo cíclico de orden p^t, $t \in \mathbb{N}$ y p un entero primo. De la definición de exponente (ver Definición 1.8), $exp(C_{p^l}) = p^{t-l}$, con $l < t$. Así, cada elemento de C_{p^t} tiene orden una potencia de p, que es impar.

De lo mencionado anteriormente, el grupo $\mathcal{Q}_8 \times E \times A$ es un grupo Hamiltoniano.

1.2. Anillos

A continuación presentamos el concepto de anillo, el cual es muy importante para el presente trabajo. Presentaremos el enfoque dado por Burton y Dummit en [3] y [6], respectivamente.

Definición 1.13 (Anillo)**.** Un anillo es una tripla $(R, +, \cdot)$ que consiste de un conjunto no vacío R y dos operaciones binarias definidas en R tales que

- $(R, +)$ es un grupo abeliano.
- $(R, \cdot)$ es un semigrupo.
- la operación $\cdot$ es distributiva(en ambos sentidos) sobre la operación $+$.
- Si $xy = yx$ para todo $x, y \in R$, el anillo se dice conmutativo.
- Si en R existe un elemento identidad, usualmente representado por $1 = 1_R$, tal que $1x = x1 = x$, para todo $x \in R$, se dice que R es anillo con unidad.

Ejemplo 1.14. Algunos ejemplos clásicos son:

- $\mathbb{Z}$ 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 coeficientes e R, denotado $M_n(R)$, es un anillo con la suma y producto usuales.
- Dado $n \in \mathbb{N}$, el conjunto de los enteros módulo n, $\mathbb{Z}_n$, es un anillo conmutativo con unidad, con la suma y producto módulo n.
- Dados R anillo conmutativo con 1_R y x una variable, el conjunto $R[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in R, n \in \mathbb{N}\}$ con la suma y producto de polinomios usual, es también un anillo conmutativo con 1_R.
- Dados R anillo conmutativo con 1_R y x una variable, el conjunto $R[[x]] = \{\sum a_ix^i \mid a_i \in R\}$ de series de potencia formales sobre R, con las operaciones usuales, también es un anillo conmutativo con 1_R.

Presentamos algunos elementos distinguidos en un anillo que son útiles en lo sucesivo.

Definición 1.15. Sea R un anillo

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

Adicionalmente, mencionamos que:

- Si R tiene $1 = 1_R$, entonces (-1) es una unidad, dado que $(-1)(-1) = 1$.
- En $M_2(\mathbb{R})$, la matriz $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ verifica que $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, y así es un elemento nilpotente de $M_2(\mathbb{R})$.
- En $\mathbb{Z}_{12}$, tenemos que $(30 + 12\mathbb{Z}) + (18 + 12\mathbb{Z}) = 48 + 12\mathbb{Z} = 12\mathbb{Z}$ y $(30 + 12\mathbb{Z}) \cdot (18 + 12\mathbb{Z}) = 540 + 12\mathbb{Z} = 12\mathbb{Z}$, luego $30 + 12\mathbb{Z}$ es cuasiregular en $\mathbb{Z}_{12}$.

En un anillo R, un *divisor de cero* en R es un elemento x para el cual existe $y \neq 0_R$ en R tal que $xy = 0$. Un anillo R que no tenga divisores de cero(a excepción de 0_R) es llamado dominio entero.
Un anillo R es llamado *anillo de división* si si todos sus elementos no cero son invertibles. En este último caso, si R tiene $1 = 1_R$ y es conmutativo, R es llamado un *cuerpo*.
Hacemos un énfasis en los siguientes items

Observación 1.16.

1. Notemos 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.

2. Para el segundo caso, considere los símbolos i, j, k y el conjunto $\mathbb{H}_{\mathbb{R}}$ de todas las expresiones de la forma $x_0+x_1i+x_2j+x_3k$, donde los coeficientes x_0, x_1, x_2, x_3 son números reales. Se define la suma de dos elementos en $\mathbb{H}_{\mathbb{R}}$ como sigue:

$$(x_0 + x_1i + x_2j + x_3k) + (y_0 + y_1i + y_2j + y_3k) =$$
$$(x_0 + y_0) + (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k.$$

La multiplicación es definida de forma distributiva, teniendo en cuenta que los símbolos i, j, k cumplen las siguientes reglas:

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

Se puede demostrar que, $\mathbb{H}_{\mathbb{R}}$ con las operaciones anteriormente mencionadas, es un anillo(no conmutativo), llamado el **anillo de cuaternios reales**.
Ahora bien, dado un cuaternio $\alpha = x_0+x_1i+x_2j+x_3k$, definimos el conjugado y la norma de α, respectivamente por

$$\overline{\alpha} = x_0 - x_1i - x_2j - x_3k,$$
$$\|\alpha\| = \alpha\overline{\alpha} = x_0^2 + x_1^2 + x_2^2 + x_3^2.$$

De la definición anterior es fácil demostrar que :

i) $\|\alpha\beta\| = \|\alpha\| \, \|\beta\| = \|\beta\alpha\|$,

ii) $\|\alpha\| \geq 0$ y $\|\alpha\| = 0$ si y solo si $\alpha = 0$.

Ahora si $0 \neq \alpha \in \mathbb{H}_{\mathbb{R}}$, del inciso ii), se sigue que $\|\alpha\| \neq 0$, y así es posible definir $\alpha' = \overline{\alpha}/\|\alpha\|$. Luego

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

De manera análoga, obtenemos que $\alpha'\alpha = 1$. Con esto, hemos mostrado que $\mathbb{H}_{\mathbb{R}}$ es un anillo de división.

La noción de ideal que consideramos a continuación, se debe a Richard Dedekind (1831-1916), un alumno de 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 Leopold Kronecker (1823-1891), un estudiante de Ernst Kummer, introdujo ideales de polinomios en sus estudios de geometría algebraica.

Definición 1.17 (ideal)**.** Un subconjunto I de un anillo R es llamado **ideal a izquierda** de R si

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

Análogamente podemos definir un **ideal a derecha** de R. Un subconjunto I de R es llamado un **ideal** de R (algunas veces, **un ideal bilateral**) si I es un ideal a izquierda y a derecha de R.
Los subconjuntos $\{0\}$ y R siempre son ideales de R. Un ideal I diferente de estos, es llamado un ideal propio. Note que si un ideal I de un anillo R contiene un elemento invertible a, entonces $I = R$. En efecto, supongamos que es un ideal a izquierda de R y que $a \in I$ es invertible. Entonces $1 = a^{-1}a \in I$ y así $x \cdot 1 = x \in I$ para todo $x \in R$, i.e, $R \subseteq I$ y de la definición 1.17, $I \subseteq R$.

Ejemplo 1.18. Sea a un elemento de un anillo R. Entonces $Ra = \{xa : x \in R\}$, 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.

Un ideal propio I de un anillo conmutativo R es llamado *ideal primo* de R si dados $a, b \in R$ y $ab \in I$, implica que $a \in I$ o $b \in I$. Además, M es llamado ideal maximal de R, si no existe otro ideal propio J del anillo R que lo contenga, i.e, si existe J ideal tal que $M \subset J \subseteq R$, implica que $J = R$. Para este trabajo utilizaremos la notación (R, M) para indicar un anillo local con ideal maximal M. Damos un resultado que nos sirve para caracterizar dichos ideales

Proposición 1.19. *Sean R un anillo conmutativo con unidad e I un ideal de R,*

- *I es un ideal primo si y solo si R/I es un dominio entero.*
- *I es un ideal maximal si y solo si R/I es un cuerpo.*

Como una consecuencia de la proposición anterior, si R con 1_R, cada ideal maximal es primo. En particular, en los enteros $\mathbb{Z}$ el ideal (0) es primo y no es maximal.

Sea I un ideal del anillo R. Entonces el grupo cociente aditivo R/I se torna un anillo al definir la multiplicación de manera natural por:

$$\overline{r} \cdot \overline{s} = (r + I)(s + I) = rs + I = \overline{rs}.$$

Al anillo R/I construido arriba se le llama anillo cociente de R por I.

A continuación consideramos anillos conmutativos con unidad de tipo especial: anillos noetherianos y anillos artinianos. Estos aparecen en la teoría general de anillos con la intención de obtener resultados más profundos con respecto a ideales. Los primeros son particularmente versátiles y satisfacen cierta condición de finitud, a saber, es que cada ideal del anillo debe ser finitamente generado. Los segundos, son el tipo de anillos más simples después de los cuerpos. Es posible mostrar que todo anillo artiniano es necesariamente noetheriano de un tipo muy especial.
Como punto de partida conveniente tenemos la siguiente definición Sea $(R, \leq)$ un conjunto parcialmente ordenado bajo " $\leq$".

Definición 1.20. Un anillo R satisface *la condición de cadena ascendente*, **C.C.A.** por brevedad, para ideales si, dada cualquier sucesión de ideales $I_1, I_2, \ldots$ de R con

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots,$$

existe un entero positivo n tal que $I_m = I_n$ para todo $m \geq n$. Un anillo que satisfaga la condición **C.C.A** se dice que es *noetheriano*.

Se puede demostrar que, si un anillo R satisface **C.C.A.**, entonces cada subconjunto de R tiene un elemento maximal.

De manera análoga, si para un anillo R, cualquier sucesión de ideales $I_1, I_2, \ldots$ satisface que

$$I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n \supseteq \cdots,$$

Se dice que R satisface la *condición de cadena descendente*, por brevedad, se notará como **C.C.D**. Un anillo R que satisfaga la condición de cadena descendente se dice que es un anillo *artiniano*. A continuación presentamos algunos ejemplos clásicos de dichos anillos

Ejemplo 1.21. 1. Cada cuerpo es a la vez artiniano y noetheriano. También lo son los anillos finitos. El anillo $\mathbb{Z}$ es noetheriano pero no artiniano. En efecto, si $a \in \mathbb{Z}$ y $a \neq 0$ se sigue que $(a) \supsetneq (a^2) \supsetneq \ldots \supsetneq (a^n) \supsetneq \ldots$, lo cual nos muestra que $\mathbb{Z}$ no es artiniano.

2. Cada dominio de ideales principales es noetheriano.

3. El anillo $\mathbb{K}[x]$ ($\mathbb{K}$ es un cuerpo, x es una variable)satisface **C.C.A** y por tanto es noetheriano.

4. EL anillo $\mathbb{K}[[x]]$ no es ni noetheriano ni artiniano. En efecto, la sucesión $(x_1) \subset (x_1, x_2) \subset \ldots$ nunca se estabiliza y, por otra parte, la sucesión $(x_1) \supsetneq (x_1^2) \supsetneq (x_1^3) \ldots$ tampoco se estabiliza.

Presentamos una propiedad que tienen los anillos noetherianos que es utilizada después en nuestro trabajo:

Proposición 1.22. *Un anillo R noetheriano no puede tener un conjunto infinito de idempotentes ortogonales.*

Demostración. Supongamos lo contrario, i.e. supongamos que R tiene un conjunto infinito de idempotentes ortogonales, digamos $e_1, e_2, \ldots$. Para un ideal I de R se tiene

$$e_1 I \subset (e_1 + e_2)I \subset \cdots$$

y esta es una cadena ascendente que no se estabiliza. Así, contradice su condición de noetheriano.
Por lo tanto, todo anillo noetheriano no admite un conjunto infinito de idempotentes ortogonales. □

A continuación introducimos el radical de Jacobson.

Definición 1.23 (Radical de Jacobson)**.** Sea R un anillo. El radical de Jacobson, denotado por $\mathcal{J}(R)$ es la intersección de todos su ideales a izquierda maximales.

Un primer ejemplo es $\mathcal{J}(\mathbb{Z})$. Como en $\mathbb{Z}$, los ideales maximales son de la forma (p), para p número primo, se sigue de la definición que

$$\mathcal{J}(\mathbb{Z}) = \cap(p) = (0) = \{0\}.$$

La última igualdad se justifica recordando que, para p primo dado, existe un entero no nulo que no es divisible por éste; excepto el cero pues $0 = 0p$ para todo primo p. De la definición, es claro que $\mathcal{J}(R)$ es un ideal a izquierda de R. La verdad es posible establecer que $\mathcal{J}(R)$ es un ideal bilateral, [23, Prop. 2.7.4].

Recordemos que si $\mathcal{F}$ es una colección de subconjuntos de un conjunto dado, un elemento $A \in \mathcal{F}$ es llamado **maximal** si A no está propiamente contenido en ningún miembro de $\mathcal{F}$. Dada una subfamilia $\mathcal{L}$ de miembros de $\mathcal{F}$, un conjunto $A \in \mathcal{F}$ es llamado una **cota superior** de los miembros de $\mathcal{L}$ si $A_i \subset A$ para todo $A_i \in \mathcal{L}$. La siguiente afirmación es conocida como **Lema de Zorn** (también llamado **Principio Maximal**) y es demostrado, en teoría de conjuntos, que es equivalente al **Axioma de elección**.

Lema 1.24 (Zorn). *Sea $\mathcal{F}$ una colección no-vacía de subconjuntos de un conjunto dado tal que toda familia totalmente ordenada* [1] *de miembros de $\mathcal{F}$ tiene una cota superior (en $\mathcal{F}$). Entonces $\mathcal{F}$ tiene un elemento maximal.*

Como una aplicación del Lema de Zorn, tenemos el siguiente resultado que garantiza que en un anillo R con 1_R, el radical de Jacobson $\mathcal{J}(R)$ siempre existe.

Lema 1.25. *Todo anillo $R \neq \{0\}$ con 1_R contiene ideales maximales propios.*

Demostración. Sea $\mathcal{F}$ el conjunto de todos los ideales I de R con $I \neq R$. Si $\{I_i\}_{i\in\Lambda}$ es una familia totalmente ordenada de miembros de $\mathcal{F}$, consideremos la unión $J = \cup_{i\in\Lambda} J_i$. Verifiquemos que J es un ideal. Sean $x, y \in J$. Entonces existen índices $r, s \in \Lambda$ tales que $x \in J_r$ y $y \in J_s$. Si $r = s$, $x - y \in J$ y para $r \in R$ se tiene que $rx \in J$; pues cada J_i es un ideal. Por el contrario, suponga que $r \neq s$. Como la familia $\{I_i\}_{i\in\Lambda}$ es totalmente ordenada, entonces puede ocurrir una de las dos cosas: o $J_r \subseteq J_s$ o $J_s \subseteq J_r$. Sin pérdida de generalidad, suponga que $J_r \subseteq J_s$. En efecto, como $x \in J_r$ y $J_r \subseteq J_s$, entonces $x \in J_s$. Como J_s es ideal, tenemos que $x - y \in J_s$, y como $J_s \subseteq J$, concluímos que $x - y \in J$. Ahora, suponga que $z \in R$. como $x \in J_r$ y J_r es ideal, entonces $zx \in J_r$, lo cual implica que $zx \in J$.
Dado que $J_i \neq R$, para todo $i \in \Lambda$. Vemos que $1_R \notin J_i$ y así $1 \notin J$, luego $J \in \mathcal{F}$. Claramente J es una cota superior de $\{J_i\}_{i\in\Lambda}$ y del Lema de Zorn $\mathcal{F}$ tiene un elemento maximal (ideal). □

Es bien conocido que si I es un ideal de R, entonces existe una correspondencia biyectiva que preserva el orden entre los ideales J de R que contienen a I, y los ideales $\overline{J}$ de R/I. Más exactamente , $\overline{J} = J/I$. Como una consecuencia de este teorema de correspondencia y el lema anterior, para todo ideal $I \neq (1)$ de R, existe un ideal maximal de R que lo contiene. En efecto, si $I \neq (1)$ es un ideal de R, entonces $R/I \neq \{0\}$.
Por tanto, del lema anterior, R/I tiene ideales maximales. Sea $\overline{M}$ un ideal maximal. Se sigue del teorema de la correspondencia que $\overline{M} = M/I$ con $I \subseteq M$ y maximal en R.

Recordemos que dados $I_1, I_2, \ldots I_n$ (a izquierda, a derecha o bilaterales) ideales de R, su producto es el conjunto de todas las sumas finitas de términos de la forma $a_1 a_2 \cdots a_n$, donde $a_i \in I$, $1 \leq i \leq n$.
Tal producto de ideales es denotado por $I_1 I_2 \cdots I_n$ y es posible demostrar que es un ideal a izquierda (a derecha o bilateral) respectivamente, y que en el caso de ser

[1] Si $(\mathcal{F}, \leq)$ es un conjunto parcialmente ordenado, una familia $\mathcal{L}$ de miembros de $\mathcal{F}$ es totalmente ordenada, si todo par de elementos son comparables, i.e, para todo $A_i, A_j \in \mathcal{L}$, $A_i \leq A_j$ o $A_j \leq A_i$.

todos los I_i $1 \leq i \leq n$ bilaterales, entonces

$$I_1 I_2 \cdots I_n \subseteq \bigcap_{i=1}^{n} I_i.$$

En particular si $I_i = I$, $1 \leq i \leq n$, entonces

$$I^n = \left\{ \sum_{\text{finita}} a_1 a_2 \cdots a_n : a_i \in I,\ 1 \leq i \leq n \right\}.$$

Proposición 1.26. *En un anillo con identidad todo ideal propio está contenido en un ideal maximal*

Demostración. Sea R un anillo con identidad y además sea I un ideal de R no trivial, esto es, un ideal propio del anillo R. Sea

$$S = \{M \mid I \subseteq M \text{ siendo } M \text{ ideal de } R\}.$$

Primero, observe el lector que $S \neq \emptyset$, pues $I \in S$. Además S está parcialmente ordenado bajo la inclusión $\subseteq$, pues $\subseteq$ es reflexiva, antisimétrica y transitiva.
Sea $\mathcal{C}$ una cadena de S. A continuación definamos

$$J = \bigcup_{A \in \mathcal{C}} A$$

Se procede a mostrar que J es un ideal de R. Es inmediato que $J \neq \emptyset$ pues como cada $A \in \mathcal{C}$ es ideal, entonces el cero del anillo está en esos ideales, lo que muestra que $0 \in J$. Sean a, b elementos de J. Por la forma como fue definido J, existen ideales A, B en $\mathcal{C}$ tales que $a \in A$ y $b \in B$. Como $\mathcal{C}$ es una cadena, se tiene que $A \subseteq B$ o $B \subseteq A$. En cualquiera de los dos casos, se concluye que $a - b$ está en J, pues A y B son ideales. Sea $c \in R$ y $d \in J$. Como $d \in J$, existe algún ideal D en $\mathcal{C}$ tal que $d \in D$. Entonces $cd \in D$, lo que implica que $cd \in J$.
Como cada ideal de S, es propio, entonces 1 del anillo no está en nigún ideal de S. De esta, manera, cualquier cadena $\mathcal{C}$ de S, está acotada superiormente en S. Del lema de Zorn, se sigue que S tiene elemento maximal, el cual es el ideal maximal que se quería mostrar. □

Antes de enunciar algunas propiedades relevantes del radical de Jacobson, tenemos las siguientes definiciones:

Definición 1.27.
- Decimos que un ideal I de un anillo R es **nil** si, para todo elemento $x \in I$, existe un entero positivo n tal que $x^n = 0$. I es llamado **nil de exponente acotado**, si existe un entero positivo n tal que $x^n = 0$ para todo $x \in I$.

- El ideal I del anillo R es llamado **nilpotente** si existe un entero positivo n tal que $I^n = \{0\}$.

De la definición, un ideal I de un anillo R es nilpotente si y solo si existe un entero positivo n tal que $a_1a_2\cdots a_n = 0$, para toda escogencia de elementos $a_1, a_2, \ldots a_n \in I$. Para explicar esto, como I es nilpotente, entonces $\sum_{\text{finita}} a_1a_2\cdots a_n = 0_R$. En particular, $a_1a_2\cdots a_n = 0$, para cualquier escogencia de elementos $a_1, a_2, \ldots a_n$ en I. Entonces, para $a \in I$ se concluye que $a^n = 0$, lo cual nos dice que todo ideal nilpotente es nil, sin embargo la afirmación recíproca no es cierta.
Recordemos que para p número primo y $n \in \mathbb{Z}^+$, en el anillo $\mathbb{Z}_{p^n}$ podemos encontrar ideales de la forma $p^k\mathbb{Z}_{p^n}$ para $1 \leq k \leq n$. Ahora, observe el lector lo siguiente:

$$(p^k\mathbb{Z}_{p^n})^n = p^{kn}\mathbb{Z}_{p^n} = p^n\mathbb{Z} = 0_{\mathbb{Z}_{p^n}}$$

Esto nos muestra que el anillo $\mathbb{Z}_{p^n}$ tiene muchos ideales nilpotentes. Más aún, se puede demostrar que todos los ideales propios de $\mathbb{Z}_{p^n}$ son nilpotentes. Fijemos a p y considere ahora la siguiente colección de sucesiones[2]

$$\mathcal{S} = \{(a_n)_{n\in\mathbb{N}} \mid\ a_n \in \mathbb{Z}_{p^n},\ n \geq 1\},$$

Este conjunto con las operaciones

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} = (x_n + y_n)_{n\in\mathbb{N}}, \qquad (x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} = (x_ny_n)_{n\in\mathbb{N}}$$

Es un anillo el cual tiene como $0_{\mathcal{S}}$ la sucesión formada por los ceros de cada $\mathbb{Z}_{p^n}$, además de que el negativo de $(x_n)_{n\in\mathbb{N}}$ es $(-x_n)_{n\in\mathbb{N}}$. Considere el conjunto I formado por sucesiones que tienen la siguiente forma

$$x = (px_1, px_2, \ldots, px_n, 0, 0, 0, \ldots)$$

Esto es, sucesiones que, a partir de cierto momento, sus valores son cero y cada $x_k \in \mathbb{Z}_{p^k}$. Probemos que I es un ideal de $\mathcal{S}$. Sean $a, b \in I$. Entonces, existen $n, m \in \mathbb{N}$ tales que

$$a = (pa_1, pa_2, \ldots, pa_n, 0, 0, 0, \ldots)$$
$$b = (pb_1, pb_2, \ldots, pb_m, 0, 0, 0, \ldots).$$

para $a_i, b_i \in \mathbb{Z}_{p^i}$. Sin pérdida de generalidad, suponga que $n > m$. En efecto,

$$(pa_1 - pb_1, pa_2 - pb_2, \ldots, pa_m - pb_m, pa_{m+1}, pa_{m+2}, \ldots, pa_n, 0, 0, 0, \ldots)$$

[2]Utilizaremos la siguiente notación para sucesiones: $(x_n)_{n\in\mathbb{N}}$.

Como cada uno de los elementos pa_k y pb_k pertenece al ideal en $\mathbb{Z}_{p^n}$ generado por p, entonces se obtiene que $a - b \in I$. Sea $z = (z_n)_{n\in\mathbb{N}} \in \mathcal{S}$. Entonces,

$$za = (z_1, z_2, \ldots)\cdot(pa_1, pa_2, \ldots, pa_n, 0, 0, 0, \ldots) = (p(a_1z_1), p(a_2z_2), \ldots, p(z_na_n), 0, 0, 0, \ldots)$$

Esto nos muestra que $za \in I$. tome el elemento $a \in I$ anteriormente mencionado. Como todo ideal de $\mathbb{Z}_{p^n}$ es nil, cada término de a es nilpotente en su anillo respectivo, lo cual no indica que, para un n lo suficientemente grande, obtenemos que

$$a^n = (0, 0, 0, \ldots).$$

Hemos mostrado que I es nil.
Por otra parte, considere la sucesión $c = (c_n)_{n\in\mathbb{N}}$ definida de la siguiente manera:

$$c = \begin{cases} c_k = p & si \quad 1 \leq k \leq n+1 \\ c_k = 0 & si \quad k > n+1 \end{cases}$$

Observe el lector que $c \in I$ y que satisface lo siguiente,

$$c^n = (0, 0, 0, \ldots, p^n, 0, 0, 0, \ldots)$$

Donde encontramos que, en la n-ésima posición hay un elemento distinto de cero. Como $p^n \neq 0$ en $\mathbb{Z}_{p^{n+1}}$, la sucesión c cumple que $c^n \neq 0$, lo cual implica que $I^n \neq 0$. Por lo tanto, para cada entero positivo n, existen sucesiones $c \in I$ que satisfacen $c^n \neq 0$. Se concluye que I no es nilpotente.

Algunas propiedades del radical de Jacobson son

Proposición 1.28. *Si R es conmutativo con 1_R, entonces*

1. *Sea I es un ideal de R. Entonces $I \subseteq \mathcal{J}(R)$ si y sólo si cada elemento de la clase lateral $1 + I$ tiene inverso en R.*

2. *Si $a \in R$, entonces $a \in \mathcal{J}(R)$ si y solo si $1 - ra \in \mathcal{U}(R)$, $\forall r \in R$.*

3. *El único idempotente en $\mathcal{J}(R)$ es el cero del anillo.*

4. *Todo ideal nil R está contenido en $\mathcal{J}(R)$.*

Demostración. Para la demostración del primer inciso, suponga que $I \subseteq \mathcal{J}(R)$ y que existe algún elemento de la clase $1 + I$ que no sea invertible en R, es decir, existe $r \in I$ tal que $1+r$ no es unidad de R. Como R es un anillo con unidad, entonces $1+r$ pertenece a algún ideal maximal M de R (ver [3, Teorema 5.3]), y como $r \in I$, por hipótesis, se tiene que $r \in \mathcal{J}(R)$. De la definición de radical de Jacobson, concluímos

que $r \in M$. Como M es un ideal de R, entonces el elemento $(1+r)-r$ está en M, por lo tanto, el ideal M contiene una unidad y se tiene que $M = R$. Esto es una contradicción.
Ahora suponga que cada elemento de la clase $1+I$ es invertible y que $I \nsubseteq \mathcal{J}(R)$. Entonces, existe un ideal maximal M tal que $I \nsubseteq M$. Sea $a \in I$ con $a \notin M$. Teniendo en cuenta que M es maximal, es fácil probar que el conjunto

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

es un ideal y que $T = R$. Por lo tanto, existe $r_1 \in R$ tal que $1 = m + r_1 a$, con lo que se obtiene que $m = 1 + (-r_1 a)$. Así, observe que $m \in 1 + I$, lo cual por hipótesis nos dice que m es invertible. De nuevo, esto es una contradicción.
Para demostrar el inciso 2, suponga $a \in R$ tal que $a \in \mathcal{J}(R)$. Como $\mathcal{J}(R)$ es ideal, entonces para $r \in R$, elemento $(-ra)$ pertenece a $\mathcal{J}(R)$. Del inciso 1, se sigue que cada elemento de la clase lateral $1 + \mathcal{J}(R)$ tiene inverso en R, s decir, existe $v \in R$ tal que $(1 + (-ra))v = 1$. De la última ecuación vemos que $1 - ra$ es invertible, para todo $r \in R$.
Por otra parte, sea I un ideal de R tal que para $a \in I$, el elemento $1 - ra$ es invertible en R para todo $r \in R$. Entonces, existe $v \in R$ tal que $(1 - ra)v = (1 + (-r)a)v = 1$. De este modo, observe que todo elemento de la clase lateral $1 + I$ tiene inverso en R. Del inciso 1, se concluye que $I \subseteq \mathcal{J}(R)$, de lo cual podemos concluir que $a \in \mathcal{J}(R)$.
Para la prueba del inciso 3, sea $a \in \mathcal{J}(R)$ 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 observemos lo siguiente

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

Concluimos que el único idempotente presente en el radical de Jacobson es el cero.
Para el último inciso, suponga N un nilideal 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 $(-ra)^n = 0$. Observe el lector lo siguiente

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

De modo que el elemento $1 - ra$ es invertible para todo $r \in R$. Del inciso 2, se concluye que $a \in \mathcal{J}(R)$, que era lo que se quería mostrar. □

1.3. Anillo de Fracciones y Localización.

El procedimiento por el cual se construye el cuerpo de números racionales $\mathbb{Q}$ a partir del anillo de enteros $\mathbb{Z}$ se extiende fácilmente a un **dominio entero** R y da lugar al cuerpo de fracciones de R. La construcción consiste en tomar todos los pares ordenados (a, s) donde $a, s \in R$ y $s \neq 0$,y establecer la relación de equivalencia entre tales pares:

$$(a, s) \sim (b, t) \text{ si y solo si } (at - bs) = 0$$

Para la verificación de la propiedad transitiva en $\sim$ se necesita el hecho que R no tenga divisores de cero diferentes al 0. Y así, la necesidad de R de ser dominio entero.
Sin embargo tal procedimiento se puede generalizar como sigue: Sea R un anillo conmutativo con 1_R. Un **subconjunto multiplicativamente cerrado** de R es un subconjunto D de R tal que $1 \in S$ y D es cerrado respecto a la multiplicación.
Se define una relación $\equiv$ en $R \times D$ como sigue:

$$(r, d) \equiv (s, e) \text{ si y solo si } \exists u \in S \ (re - sd)u = 0.$$

Claramente esta relación es reflexiva y transitiva. Veamos que $\equiv$ es transtiva. En efecto, sean (a, s), (b, t) y (c, u) elementos en $R \times D$ tales que

$$(a, s) \equiv (b, t) \quad \text{y} \quad (b, t) \equiv (c, u).$$

Entonces existen $v, w \in S$ tales que

$$(at - bs)v = 0 \quad \text{y} \quad (bu - ct)w = 0,$$

Eliminando b entre estas ecuaciones se tiene que $(au - cs)tvw = 0$. Dado que D es cerrado respecto a la multiplicación, se tiene que $tvw \in S$ y así $(a, s) \equiv (c, u)$. Por tanto, "$\equiv$" define una relación de equivalencia en $R \times D$. Indicaremos por $[a/s]$ la clase de equivalencia de (a, s) y por $D^{-1}R$ el conjunto de las clases de equivalencia. Ahora bien en $D^{-1}R$ definimos la suma y producto dadas por

$$[a/s] + [b/t] = [at + bs/st] \quad \text{y} \quad [a/s][b/t] = [ab/st].$$

Es posible demostrar que estas definiciones no dependen de la elección de los representantes (a, s) y (b, t) y que $D^{-1}R$ es un anillo conmutativo con $1_{S^{-1}R} = [1/1]$. El cero de este anillo es $[0/1] = [0/a]$, $a \in D$.
El anillo $D^{-1}R$ es llamado **anillo de fracciones** de R con respecto a D.

Observación 1.29. Si R es un dominio entero y si $D = R\backslash\{0\}$, entonces $D^{-1}R$ es el cuerpo de fracciones de R.

Ejemplo 1.30. Considere R un anillo conmutativo con 1_R y sea P un ideal primo de R. Primero, se probará que el conjunto $D = R\backslash P$ es multiplicativamente cerrado. En efecto, $1 \in D$, pues P es un ideal y no puede tener unidades. Suponga que $a, b \in R$ tales que $a, b \notin P$. Esto implica que $ab \notin P$, ya que P es un ideal primo. Por lo tanto, para elementos $a, b \in R$ tales que $a, b \in R\backslash P$, se sigue que $ab \in R\backslash P$. Por consiguiente, D es multiplicativamente cerrado. Escribiremos R_P en lugar de $D^{-1}R$ para indicar la localización de R en P.
Los elementos $[a/s]$ con $a \in P$ forman un ideal $P_D = PR_P$ en R_P. Si $[b/t] \notin P_D$, entonces $b \notin P$, por tanto $b \in D$ y por consiguiente $[b/t]$ es una unidad de R_P. Luego, si $P_D \nsubseteq I$, entonces I contiene una unidad y así $I = R_P$.
Se ha obtenido que si I es un ideal en $R_{\mathfrak{p}}$ y $PR_P \nsubseteq I$, entonces I contiene una unidad de R_P, y por tanto $I = R_P$. Así las cosas, PR_P es el único ideal maximal en R_P.

Un ejemplo más concreto es el siguiente: sea $R = \mathbb{Z}$, el anillo de los enteros y sea P el ideal generado por p, con p entero primo. Así, $D = \mathbb{Z}\backslash P$ es un conjunto multiplicativamente cerrado y $\mathbb{Z}_P$ viene dado por:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$$

En este caso, el único ideal maximal es

$$P\mathbb{Z}_{(p)} = \{a/b : a \in P, b \notin P\}$$

Introducimos a continuación un concepto que permite explicar porque el anillo localizado $\mathbb{Z}_{(p)}$ es Noetheriano, propiedad importante por derecho propio en la teoría general de anillos y, en particular, relevante para nuestro trabajo al exponer *anillos de grupo clean* en el Capítulo 3.

Sean R, S anillos conmutativos y $\phi : R \to S$ un homomorfismo. Si I es un ideal de R, $\phi(I)$ no necesariamente es un ideal de S. Si I es un ideal de R, entonces definimos la extensión de I a S es el ideal $\phi(I)S$ en S. De manera explícita los elementos de $\phi(I)S$ son de la forma $\sum \phi(x_i)y_i$, donde $y_i \in S$ y $x_i \in I$; denotaremos a dicho conjunto como ${}^eI$.
Si J es un ideal de S, entonces definimos la contracción en R de J como el ideal $\phi^{-1}(J)$. Se denota por ${}^cJ$. A continuación, mencionamos dos propiedades útiles para este trabajo:

Observación 1.31. Se tienen las siguientes contenencias

- $I \subseteq {}^c({}^eI)$.
- ${}^e({}^cJ) \subseteq J$.

En efecto, sea J un ideal de S y $\phi : R \to S$ un homomorfismo de anillos. Note que, $\phi(\phi^{-1}(J)) \subseteq J$. De forma que, escribir ${}^e({}^cJ)$ es equivalente por definición, a escribir $\phi(\phi^{-1}(J))S$. Tenemos entonces que $\phi(\phi^{-1}(J))S \subseteq JS$. Como J es ideal, note que $JS \subseteq J$. Hemos probado que ${}^e({}^cJ) \subseteq J$

El siguiente resultado es parte de la Proposición 38 del Capítulo 15 de la referencia [6]

Proposición 1.32. *Teniendo en cuenta la notación precedente se sigue que*

- *Para un ideal J de $D^{-1}R$ se tiene que ${}^e({}^cJ) = J$.*
- *Si R es Noetheriano, entonces $D^{-1}R$ también lo es.*

Demostración. Sea J un ideal de $D^{-1}R$ y sea $\pi : R \to D^{-1}R$ el epimorfismo canónico de R en $D^{-1}R$, definido de la siguiente manera: para $r \in R$, $r \to [r/1]$.
Debido a la observación 1.31, es suficiente para la primera afirmación mostrar que $J \subseteq {}^c({}^eJ)$. En efecto, sea $a/d \in J$. Entonces $d\frac{a}{d} = \frac{a}{1} \in J$, dado que J es ideal en $D^{-1}R$. Como π es sobreyectivo, y de la definición de contracción, se sigue que $a \in \pi^{-1}(J) = {}^cJ$. Para la otra contenencia, suponga que $\frac{a}{d} \in J$. Entonces $d\frac{a}{d} \in J$, pues J es ideal, lo cual implica que $\frac{a}{1} \in J$. Como $\pi^{-1}(\frac{a}{1}) = a$, pues π es sobreyectivo, note que $a \in \pi^{-1}(J) =^c J$. Al tomar imagen por π, se obtiene que $\pi(a) = \frac{a}{1} \in^e ({}^cJ)$. Finalmente con ${}^e({}^cJ)$ es un ideal en $D^{-1}R$, $(\frac{a}{1})(\frac{1}{d}) = \frac{a}{a} \in^e ({}^cJ)$, y así $J \subseteq {}^e({}^cJ)$.

Para la segunda afirmación, considere la cadena ascendente de ideales en $D^{-1}R$,

$$J_1 \subseteq J_2 \subseteq \ldots J_n \subseteq \ldots$$

Al tomar ls pre-imágenes por π obtenemos, la cadena ascendente en R

$${}^cJ_1 \subseteq {}^cJ_2 \subseteq \ldots {}^cJ_n \subseteq \ldots$$

R es noetheriano, entonces la última cadena estaciona o para, i.e., existe $k \in \mathbb{N}$ tal que

$${}^cJ_1 \subseteq {}^cJ_2 \subseteq \ldots \subseteq {}^cJ_k = {}^cJ_{k+1} = {}^cJ_{k+1} = \ldots$$

Por tanto la siguiente cadena de ideales en $D^{-1}R$ también estaciona:

$${}^e({}^cJ_1) \subseteq {}^e({}^cJ_2) \subseteq \ldots \subseteq {}^e({}^cJ_k) = {}^e({}^cJ_{k+1}) = {}^e({}^cJ_{k+2}) = \ldots$$

Como ya establecimos que ${}^e({}^cJ_i) = J_i$, para todo i, entonces la cadena ascendente de ideales en $D^{-1}R$ es estacionaria y por tanto $D^{-1}R$ es un anillo Noetheriano. $\square$

En este punto vale la pena mencionar que, dependiendo del anillo, éste puede tener un conjunto finito(el anillo de entero módulo n), infinito (el anillo de enteros $\mathbb{Z}$) de ideales maximales. En particular, existen anillos con exactamente un ideal maximal; por ejemplo, $\mathbb{Z}_{(p)}$ para p número primo . Este comportamiento sugiere la existencia de una clase especial de anillos que se define a continuación

Definición 1.33. Un anillo R conmutativo con unidad es *Local* si posee un único ideal maximal M.

Un ejemplo de un anillo local que es de interés para este trabajo es $\mathbb{Z}_{(p)}$. Para finalizar, algunas propiedades algebraicas de este tipo de anillos pueden ser consultadas en la referencia [6, pág. 717].

1.4. 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 donde la teoría de grupos y de la teoría de anillos se unen, y por tal motivo ha sido abordado desde varios puntos de vista diferentes. Por ejemplo, el teórico de grupos finito lo hace desde la teoría de caracteres y el analista desde la teoría de operadores y análisis de Fourier.
El estudio algebraico de los anillos de grupo fue iniciado en 1949 por I. Kaplansky y fue potencializado doce años después por el trabajo de S. A. Amitsur. Desde entonces, estudiar anillos de grupo se ha tornado llamativo entre un número creciente de investigadores de Colombia, Bélgica, Italia, Brasil, Canadá, Estados Unidos, etc, como Castillo, Jespers, Giambruno, Gonçalves, Goodaire, Lee, Passman, Polcino Milies, Spinelli, Sehgal, etc.
Dado un grupo G y un anillo R, deseamos construir un R-módulo, teniendo los elementos de G como base, y usando conjuntamente las operaciones de G y R para definir una estructura de anillo sobre él. Denotaremos por RG al siguiente conjunto:

$$RG = \left\{ \sum_{g \in G} \alpha_g g : \alpha_g \in R \text{ y } \alpha_g \neq 0 \text{ para un número finito de } \alpha_g \right\}.$$

Note que los elementos en RG son sumas finitas. Dado un elemento $\alpha = \sum_{g \in G} \alpha_g g$ el *soporte de* α es el subconjunto de los elementos de G que efectivamente aparecen en la suma, es decir,

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

De la definición es claro que dos elementos $\sum_{g\in G}\alpha_g g$ y $\sum_{g\in G}\beta_g g$ de RG son iguales si y solo si, $\alpha_g = \beta_g$ para todo $g \in G$. Es fácil verificar que el conjunto RG es un anillo con unidad con las operaciones de suma y producto dadas por:

$(+)$ $\left(\sum_{g\in G}\alpha_g g\right) + \left(\sum_{g\in G}\beta_g g\right) = \sum(\alpha_g + \beta_g)g,$

$(\cdot)$ $\left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{h\in G}\beta_h h\right) = \sum_{g,h\in G}(\alpha_g\beta_h)gh = \sum_{u\in G}c_u u$, donde $c_u = \sum_{gh=u}\alpha_g\beta_h.$

con unidad dada por $1_{RG} = \sum_{g\in G}\alpha_g g$, donde $\alpha_1 = 1$ y $\alpha_g = 0$, para todo $g \neq 1$. Además, $0_{RG} = \sum_{g\in G}0_g g$ y $-\alpha = \sum_{g\in G}(-\alpha_g)g$ es el inverso aditivo de $\alpha \in RG$. Notemos que RG tiene estructura de R-módulo, con el producto $\mu : R \times RG \to RG$ definido por la expresión:

$$\left(\lambda, \sum_{g\in G}\alpha_g g\right) \overset{\mu}{\mapsto} \sum_{g\in G}(\lambda\alpha_g)g.$$

Si R es un anillo conmutativo tenemos que RG es un R-álgebra. En particular, si tomamos $R = \mathbb{F}$ un cuerpo, $\mathbb{F}G$ es un $\mathbb{F}$-álgebra, más aún, $\mathbb{F}G$ es un $\mathbb{F}$-espacio vectorial.

Definición 1.34. El conjunto RG con las operaciones anteriormente definidas es llamado el **anillo de grupo del grupo** G **sobre el anillo** R. Además, si R es un anillo conmutativo, entonces RG también es llamado el **álgebra de grupo de** G **sobre** R.

Observación 1.35. La aplicación $i : G \to RG$ dada por $x \mapsto i(x) = \sum_{g\in G}\alpha_g g$ donde $\alpha_x = 1$ y $\alpha_g = 0$ si $g \neq x$, nos permite ver a G inmerso en RG, que denotaremos por $G \hookrightarrow RG$. Esta inmersión muestra claramente que G resulta ser una R-base para RG. Sea M un módulo libre con base finita sobre un anillo conmutativo R. El número de elementos de cualquier base de M es llamado el *rank* de M. Si R es conmutativo y G finito entonces se puede establecer que el rango de RG sobre R, $rank(RG)$, es precisamente $|G|$.
Ahora, consideremos $\upsilon : R \to RG$ la función dada por $\upsilon(r) = \sum_{g\in G}\alpha_g g$ donde $\alpha_{1_G} = r$ y $\alpha_g = 0$ si $g \neq 1_G$. Así, v define un monomorfismo de anillos y R puede verse como subanillo de RG.

Teniendo presente las anteriores identificaciones, dados $r \in R$ y $g \in G$, se tiene que $rg = gr$ en RG. Por tanto, si R es conmutativo, $R \subseteq \zeta(RG)$. Si $H = \{1\}$, entonces, la aplicación $G \to \{1\}$ induce el homomorfismo de anillos $\varepsilon : RG \to R$ dado por:

$$\varepsilon\Big(\sum_{g\in G} \alpha_g g\Big) = \sum_{g\in G} \alpha_g.$$

Definición 1.36. El homomorfismo $\varepsilon : RG \to R$ definido arriba, es llamado la *aplicación de aumento de* RG y su núcleo, $Ker(\varepsilon) = \Delta(G)$, es llamado *ideal de aumento de* RG.

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

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

Claramente, todos los elementos de la forma $g-1$ con $g \in G$, pertenecen a $\Delta(G)$, es decir, $\{g-1 : g \in G \text{ y } g \neq 1\}$ es un conjunto de generadores de $\Delta(G)$ sobre R. Note el lector que, la ecuación $\sum_{g\in G} \alpha_g (g-1) = 0_{RG}$ se satisface si todos los coeficientes α_i con $i \in G$ son iguales a 0_R. Por consiguiente, el conjunto $\{g-1 : g \in G, \quad g \neq 1\}$ es linealmente independiente. En efecto, se sigue el siguiente resultado:

Proposición 1.37. *El conjunto* $\{g-1 : g \in G, \quad g \neq 1\}$ *es una base para* $\Delta(G)$ *sobre* R *y, por tanto:*

$$\Delta(G) = \Big\{ \sum_{g\in G} \alpha_g (g-1) : g \in G,\ \alpha_g \in R \Big\},$$

donde como es usual, asumimos que sólo un número finito de coeficientes $\alpha_g \neq 0$.

Una pregunta que es pertinente a este trabajo es saber que condiciones en el anillo R, y en el grupo G hacen del anillo de grupo RG local. Nicholson en el año 1972, dio respuesta a esta pregunta en su artículo dedicado a los anillos de grupo locales (ver [21]). Es de nuestro interés en este trabajo el resultado principal de Nicholson [21], el cual dice:

Teorema 1.38. *Sea* R *un anillo y sea* G *un grupo.*

a) Si R *es local,* G *es un* p*-grupo localmente finito y* $p \in \mathcal{J}(R)$*, entonces* RG *es local.*

b) Si G es abeliano, entonces RG es local si y solo si R es local, G es un p-grupo y $p \in \mathcal{J}(R)$.

En efecto, Nicholson en su artículo [21] demuestra dos resultados(ver Lema y Corolario en [21]) que nos dan dos caracterizaciones de ser local para un anillo de grupo que, dependen del ideal de aumento de ese anillo y de los subgrupos de G; más precisamente Nicholson prueba que

1. Sea $\varphi : R \to A$ un epimorfismo no nulo de anillos. Entonces R es local si y solo si A es local y $\ker(\varphi) \subset \mathcal{J}(R)$.

2. RG es local si y solo si $\Delta(RG) \subset \mathcal{J}(RG)$ y R es local.

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

De la propiedad 3, G puede ser asumido finitamente generado y como por hipótesis G es localmente finito[3], entonces G es finito. Sea $\overline{R} = R/\mathcal{J}(R)$ y consideremos el epimorfismo canónico $\pi : R \to \overline{R}$, el cual extiende al epimorfismo $\overline{\pi} = RG \to \overline{R}G$. Recordemos que

$$\overline{R}G \simeq RG/\mathcal{J}(R)G,$$

lo cual nos permite presentar el kernel de φ de la siguiente manera

$$\begin{aligned}\ker(\overline{\pi}) &= \left\{ \alpha \in RG : \overline{\pi}\left(\sum_{g\in G} \alpha_g g\right) = \sum_{g\in G} \alpha_g g + \mathcal{J}(R)G = \mathcal{J}(R)G \right\} \\ &= \{\alpha \in RG : \alpha_g \in \mathcal{J}(R),\, \forall j \in G\}\,.\end{aligned}$$

Por Connell [5, Prop. 16], si G es finito, entonces $\ker(\overline{\pi}) \subseteq \mathcal{J}(\overline{R}G)$, lo que implica que $\ker(\overline{\pi})$ es nilpotente. Así, de la propiedad 1. citada arriba, es suficiente mostrar que $\overline{R}G \simeq RG/\mathcal{J}(R)G$ es local.
Dado que $\overline{R} = R/\mathcal{J}(R)$ es local, de la propiedad 2. citada, $\overline{R}G$ es local.

[3]Un grupo G es localmente finito si, todo subgrupo finitamente generado de G es finito

Capítulo 2

ANILLOS CLEAN

Empezamos fijando nuestra convención: En lo que sigue, todos los anillos son asociativos con unidad $1 \neq 0$, si no hay lugar a confusión, $1_R = 1$ con R anillo y se utiliza la notación y terminología dada en [11].

2.1. Anillos Clean

Sea $(R, +, \cdot)$ un anillo y considere los siguientes subconjuntos:

$$\mathcal{U}(R) = \{r \in R \mid r \text{ es invertible}\} \quad \text{y} \quad \mathcal{ID}(R) = \{e \in R \mid e^2 = e\}.$$

$(\mathcal{U}(R), \cdot)$ es llamado el grupo de unidades de R ver [7].
Observe que $\mathcal{U}(R) \neq \emptyset$ y $\mathcal{ID}(R) \neq \emptyset$ ya que $1 \in \mathcal{U}(R) \cap \mathcal{ID}(R)$. Vale la pena mencionar que $\mathcal{U}(R) \neq \mathcal{ID}(R)$ debido que $0 \notin \mathcal{U}(R)$. El concepto de anillo clean, que mencionaremos enseguida, fue introducido por Nicholson [20] en su estudio sobre el levantamiento de idempotentes y anillos exchange.

Definición 2.1. Un elemento en un anillo es llamado **clean** si puede ser escrito como la suma de una unidad y de un idempotente del anillo. Un anillo R es **clean** si todo elemento del anillo es clean.

A continuación presentamos algunos ejemplos iniciales.

Ejemplo 2.2. El anillo $\mathbb{Z}$ con las operaciones usuales no es clean, aunque tiene elementos clean.
Como la ecuación $x = x^2$ en $\mathbb{Z}$ sólo se satisface para $x = 0$ o $x = 1$, entonces $\mathcal{ID}(\mathbb{Z}) = \{1, 0\}$.
Los únicos elementos invertibles en $\mathbb{Z}$ son 1,-1. Así, $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$.

De la definición 2.1, los elementos clean se obtienen al hacer todas las posibles sumas de elementos invertibles con idempotentes.

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

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

Proposición 2.3. *Si R es anillo de división, entonces R es clean.*

Demostración. Como R es anillo de división, entonces R es dominio y esto implica que $\mathcal{ID}(R) = \{0, 1\}$.
Sea $x \in R$. Si $x \neq 0$, entonces x es unidad, por lo que se deduce que $\mathcal{U}(R) = R \setminus \{0\}$.
De acuerdo a lo mencionado, se consideran dos casos para x:

1. $x = 0$. En este caso, $0 = (-1) + 1$. Observe que (-1) es una unidad, ya que $(-1)(-1) = 1$ para todo anillo con 1_R, además 1 es idempotente trivial.

2. $x \neq 0$. Como x es unidad de D, observe que se puede escribir a x como $x = x+0$.

Así, concluimos que todo elemento de R es clean. □

Como todo cuerpo es un anillo de división, entonces los cuerpos son clean.

Sea R un anillo y sea $r \in R$ un elemento clean. Entonces, $r = u + e$, donde u es una unidad de R y e es un idempotente de R. Note que $1 - r = -u + (1 - e)$. Esta última igualdad nos dice que el elemento $1 - r$ también es clean. De manera análoga, se puede demostrar que, si $1 - r$ es clean, entonces r es clean. Presentamos a continuación otro ejemplo de anillo clean que es de interés para este trabajo.

Proposición 2.4. *Si R es un anillo local, entonces R es clean.*

Demostración. Sea M el ideal a izquierda maximal de un anillo R. Si $x \notin M$, entonces x es unidad.
Por otra parte,si $x \in M$, entonces $x \in \mathcal{J}(R)$, debido a que $\mathcal{J}(R) = M$. Entonces $1 - x$ es invertible en R.
Así, $1 - x$ es clean, lo cual implica que x es clean. □

2.2. Primeras propiedades

Ahora presentaremos algunas propiedades básicas y útiles de los anillos clean. Entre otras propiedades, se prueba que toda imagen bajo homomorfismo de un anillo clean es clean, que todo producto directo de anillos clean es clean y que toda matriz cuadrada con entradas en un anillo clean es clean.

Proposición 2.5. *Toda imagen bajo homomorfismo de un anillo clean es clean.*

Demostración. Sea R, S anillos, con R clean y considere $\varphi : R \longrightarrow \varphi(R) \subseteq S$ un homomorfismo.
Sea $r \in R$. Por hipótesis, $r = u + e$ con u unidad de R y e idempotente de R.
Como u es unidad en R, entonces $\varphi(1_R) = \varphi(uu^{-1}) = \varphi(u)\varphi(u^{-1})$. Observe el lector que $\varphi(1_R) = 1_{\varphi(R)}$. Así, $\varphi(u)$ es una unidad de $\varphi(R)$. En palabras, un homomorfismo de anillos envía unidades en unidades.
Como e es idempotente en R, entonces $\varphi(e) = \varphi(e^2) = \varphi(e)\varphi(e)$. Se concluye que $\varphi(e)$ es idempotente de $\varphi(R)$. Esto nos indica que un homomorfismo de anillos envía idempotentes en idempotentes.
Como $\varphi(r) = \varphi(u + e) = \varphi(u) + \varphi(e)$, por lo anteriormente mencionado en esta prueba, φ envía elementos clean en elementos clean, es decir, $\varphi(R)$ es clean. □

Ejemplo 2.6. Considere la aplicación $\phi : \mathbb{Z}_3 \to \mathbb{Z}_{12}$ definida como $x+3\mathbb{Z} \mapsto 4x+12\mathbb{Z}$. 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 cuerpo y ϕ es homomorfismo, de los resultados 2.3 y 2.5, se concluye que $\phi(\mathbb{Z}_3) = \{12\mathbb{Z}, 4 + 12\mathbb{Z}, 8 + 12\mathbb{Z}\}$ es clean.

Proposición 2.7. *Todo producto directo de anillos $\prod_{i\in\mathbb{Z}^+} R_i$ es clean si y sólo si cada anillo R_i es clean.*

Demostración. Recuerde el lector que $\prod_{i\in\mathbb{Z}^+} R_i = \{(r_1, r_2, \ldots) \mid r_i \in R_i\}$ con las operaciones de suma y producto componente a componente es un anillo si cada R_i es anillo.
Suponga que para cada i, $\prod_{i\in\mathbb{Z}^+} R_i$ es clean. Considere la aplicación $\psi : \prod_{i\in\mathbb{Z}^+} R_i \to R_i$ definida como $(r_1, r_2, \ldots r_i, \ldots) \mapsto r_i$. En efecto, ψ es un epimorfismo. Tome $(x_1, x_2, \ldots)$ y $(y_1, y_2, \ldots)$ en $\prod_{i\in\mathbb{Z}^+} R_i$. Entonces $\psi((x_1, x_2, \ldots)+(y_1, y_2, \ldots)) = \psi((x_1+y_1, x_2 + y_2, \ldots)) = x_i + y_i = \psi((x_1, x_2, \ldots)) + \psi((y_1, y_2, \ldots))$.
Además, en el producto note que $\psi((x_1, x_2, \ldots)(y_1, y_2, \ldots)) = \psi((x_1y_1, x_2y_2, \ldots)) = x_iy_i = \psi((x_1, x_2, \ldots))\psi((y_1, y_2, \ldots))$. Por lo tanto, ψ es homomorfismo. También ψ es epimorfismo puesto que

$$\psi\left(\prod_{i\in\mathbb{Z}^+} R_i\right) = \{\psi((r_1, r_2, \ldots) \mid r_i \in \mathbb{R}_i \text{ para cada i}\} = \{r_i \mid r_i \in R_i \text{ para cada i}\} = R_i$$

Como $\prod_{i\in\mathbb{Z}^+} R_i$ es clean, de la proposición 2.5 se sigue que $\psi(\prod_{i\in\mathbb{Z}^+} R_i)$ es clean. Por lo tanto, R_i es clean para todo i, consideremos $u_i \in \mathcal{U}(R_i)$ para cada i. Entonces existe $v_i \in R_i$ tal que $u_iv_i = 1_{R_i}$.

Observamos que $(u_1, u_2, \ldots)(v_1, v_2, \ldots) = (1_{R_1}, 1_{R_2}, \ldots)$. Concluimos que un elemento $(u_1, u_2, \ldots)$ en $\prod_{i\in\mathbb{Z}^+} R_i$ es unidad si y sólo si cada u_i es unidad en R_i.
Por otro lado, consideremos $e_i \in \mathcal{ID}(R_i)$ para cada i. Entonces $e_i e_i = e_i$.
Observe que $(e_1, e_2, \ldots)(e_1, e_2, \ldots) = (e_1, e_2, \ldots)$. Se sigue que, un elemento $(e_1, e_2, \ldots)$ en $\prod_{i\in\mathbb{Z}^+} R_i$ es idempotente si y sólo si cada e_i es idempotente en R_i.
Supongamos que cada R_i es clean. Entonces $x_i \in R_i$ puede ser escrito como $x_i = u_i + e_i$ con u_i unidad de R_i y e_i idempotente de R_i. Como la suma esta definida componente a componente en $\prod_{i\in\mathbb{Z}^+} R_i$, note que

$$(x_1, x_2, \ldots) = (u_1 + e_1, u_2 + e_2, \ldots) = (u_1, u_2, \ldots) + (e_1, e_2, \ldots)$$

como $(u_1, u_2, \ldots)$ es unidad de $\prod_{i\in\mathbb{Z}^+} R_i$ y $(e_1, e_2, \ldots)$ es idempotente de $\prod_{i\in\mathbb{Z}^+} R_i$, se concluye que $(x_1, x_2, \ldots)$ es clean. Por lo tanto, $\prod_{i\in\mathbb{Z}^+} R_i$ es un anillo clean. □

Proposición 2.8. *$x \in R$ es cuasiregular si y sólo si $1 - x$ es una unidad de R.*

Demostración. Supongamos que x es cuasiregular. Entonces existe $y \in R$ tal que $x + y = xy$. Note que $(1-x)(1-y) = 1-y-x+xy$, como x e cuasiregular, entonces $(1-x)(1-y) = 1-y-x+(x+y)$. Simplificando, se obtiene que $(1-x)(1-y) = 1$. Así, se ha obtenido que $(1-x)$ es unidad. Recíprocamente, Suponga que $(1-x)$ es una unidad de R; así las cosas, existe $w \in R$ tal que $(1-x)w = 1$. Como R es anillo, entonces $x = 1 \cdot x$, y aprovechando el hecho de que $(1-x)$ es unidad, se sigue que

$$x = 1 \cdot x = ((1-x)w)x = (1-x)(wx)$$

Lo que nos muestra que $1-x$ divide a x. Sea $z = xw$, de manera que, x se puede expresar como $x = (1-x)z$. Luego, $x = (1-x)z = z - xz$. De hecho, $x - z = -xz = x(-z)$. Haga $y = -z$, como $x - z = x(-z)$, concluimos que existe $y \in R$ tal que $x + y = xy$; por tanto x es cuasiregular. □

Recordemos que, un anillo R es *booleano* si $r^2 = r$, para todo $r \in R$; un ejemplo de un anillo booleano es $\mathbb{Z}/2\mathbb{Z}$.
Immormino en su tesis doctoral (ver [11, Corolario 2.2]), afirma que los anillos de división, booleanos y locales están compuestos enteramente de unidades, idempotentes o elementos cuasiregulares. El siguiente lema, el cual fue demostrado por Camillo y Anderson en [1], nos describe algunos elementos destacados de un anillo que son clean:

Proposición 2.9. *Las unidades, los idempotentes y los elementos cuasiregulares de un anillo son clean.*

Demostración. Sea R un anillo. Como 0_R es idempotente, toda unidad u de R se puede escribir como $u = u + 0_R$, por lo que u es clean. Por otro lado, considere el

elemento $2e-1$ con e idempotente de R. Note que $(2e-1_R)^2 = (2e-1_R)(2e-1_R) = 4e^2 - 2e - 2e + 1_R = 4e - 4e + 1_R = 1_R$, lo cual nos dice que $2e - 1_R$ es una unidad. Más aún, $(1_R - e)$ es idempotente, pues e lo es. De este modo, e puede ser escrito como $e = (2e - 1_R) + (1_R - e)$, lo que implica que e es clean.
Sea x un elemento cuasiregular de R. Entonces la proposición 2.8 nos afirma que $(1_R - x)$ es una unidad de R, y note que $(-1_R)(1_R - x) = -(1_R - x)$ es unidad también; además se hace notar que x puede ser escrito como $x = -(1_R - x) + 1_R$. □

En este punto haremos un paréntesis para realizar una descripción de todo anillo con unidad 1_R que posea por lo menos un idempotente no trivial e, conocida en la literatura como la descomposición de Peirce. Tal descripción es un resultado clásico de la teoría "Corner Ring Theory". Para detalles ver [15] y [16].

Sea R un anillo con 1_R y sea e un idempotente no trivial, entonces

$$R \simeq eRe \oplus (1-e)Re \oplus eR(1-e) \oplus (1-e)R(1-e).$$

Veamos primero que el conjunto $\widetilde{R} = eRe \oplus (1-e)Re \oplus eR(1-e) \oplus (1-e)R(1-e)$ es anillo con unidad bajo las siguientes operaciones:

"+" Suma componente a componente.

"·" Dados $(a,b,c,d), (a',b',c',d') \in \widetilde{R}$ definimos su producto como

$$(aa' + bc', ab' + bd', ca' + dc', cb' + dd').$$

Identificando (de forma natural) $(a,b,c,d), (a',b',c',d') \in \widetilde{R}$ con dos matrices de orden 2×2, vemos que su producto es

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}.$$

Es claro que las entradas de la matriz resultado coinciden con las componentes del producto definido arriba en $\widetilde{R}$. Así las cosas, la asociatividad del producto y distributividad de la suma con respecto al producto en $\widetilde{R}$ se satisfacen.

Ahora bien, la función

$$\phi : R \to eRe \oplus (1-e)Re \oplus eR(1-e) \oplus (1-e)R(1-e),$$

definida por $\phi(r) = (ere, (1-e)re, er(1-e), (1-e)r(1-e))$ es un isomorfismo.

Primeramente, no es difícil ver que ϕ preserva la suma. Veamos que preserva el producto.
En efecto, sean $x, y \in R$. Entonces

$$\phi(x)\phi(y) = \begin{bmatrix} exe & ex(1-e) \\ (1-e)xe & (1-e)x(1-e) \end{bmatrix} \cdot \begin{bmatrix} eye & ey(1-e) \\ (1-e)ye & (1-e)y(1-e) \end{bmatrix}.$$

Al realizar el producto en la primera fila y primera columna anterior tenemos que:

$$exeye + ex(1-e)ye = ex[e + (1-e)]ye = exye.$$

Continuando con el proceso, obtenemos

$$\phi(x)\phi(y) = \begin{bmatrix} exye & exy(1-e) \\ (1-e)xye & (1-e)xy(1-e) \end{bmatrix} = \phi(xy),$$

lo que demuestra que ϕ es un homomorfismo. Por otra parte, note que el único elemento $x \in R$ que verifica simultáneamente las ecuaciones

$$\begin{aligned} exe &= 0 \\ ex(1-e) &= 0 \\ (1-e)xe &= 0 \\ (1-e)x(1-e) &= 0, \end{aligned}$$

es $x = 0_R$. Por lo tanto $\ker(\phi) = \{0\}$, es decir, ϕ es inyectiva. De la definición ϕ es sobreyectiva. Y así, ϕ es un isomorfismo de anillos.

Teniendo en cuenta la descomposición de Peirce, presentamos el esquema propuesto por Nicholson y Han en [9], para saber cuando un anillo de matrices cuadradas es clean. Para ello necesitamos el siguiente resultado.

Lema 2.10. *Sea $e \in R$ un idempotente tal que eRe y $(1-e)R(1-e)$ son anillos clean. Entonces R es clean.*

Demostración. Por conveniencia en la notación, se denota $\overline{r} = 1 - r$ para cada $r \in R$. De la descomposición de Peirce descrita arriba, R puede ser identificado con un anillo de matrices 2×2. Más exactamente se tiene que

$$R \simeq \begin{bmatrix} eRe & eR\overline{e} \\ \overline{e}Re & \overline{e}R\overline{e} \end{bmatrix}$$

Sea $A = \begin{bmatrix} a & x \\ y & b \end{bmatrix} \in R$. Como eRe es clean, a puede escribirse como $a = u + f$ donde $f^2 = f \in eRe$ y u es una unidad de eRe con inverso u_1. Como $u_1 \in eRe$, entonces

existe $u_2 \in R$ tal que $u_1 = eu_2e$.
Probaremos que $yu_1x \in \overline{e}R\overline{e}$. En efecto, como $y \in \overline{e}Re$, existe $y_1 \in R$ tal que $y = \overline{e}y_1e$. Además, al tener que $x \in eR\overline{e}$, existe $x_1 \in R$ tal que $x = ex_1\overline{e}$. Así las cosas, tenemos entonces que

$$yu_1x = (\overline{e}y_1e)u_1(ex_1\overline{e}) = \overline{e}y_1(eu_1e)x_1\overline{e}.$$

Note lo siguiente para el término eu_1e:

$$eu_1e = e(eu_2e)e = eu_2e = u_1,$$

de manera que yu_1x se puede escribir como

$$yu_1x = \overline{e}(y_1u_1x_1)\overline{e}.$$

De nuevo, advierta el lector que $y_1u_1x_1 = y_1eu_2ex_1$, lo cual nos dice que el término $y_1u_1x_1$ es un producto de elementos de R, lo cual implica que $y_1u_1x_1 \in R$. Por lo tanto, $yu_1x \in \overline{e}R\overline{e}$. Entonces, $b - yu_1x \in \overline{e}R\overline{e}$ y por hipótesis se puede escribir como $b - yu_1x = g + v$ donde $g^2 = g \in \overline{e}R\overline{e}$ y v es unidad de $\overline{e}R\overline{e}$ con inverso v_1. De manera que

$$A = \begin{bmatrix} f+u & x \\ y & g+v+yu_1x \end{bmatrix} = \begin{bmatrix} f & 0 \\ 0 & g \end{bmatrix} + \begin{bmatrix} u & x \\ y & v+yu_1x \end{bmatrix}$$

Como f y g son idempotentes en sus respectivos anillos, note que $\begin{bmatrix} f & 0 \\ 0 & g \end{bmatrix}$ es idempotente en R. Probaremos que $\begin{bmatrix} u & x \\ y & v+yu_1x \end{bmatrix}$ es unidad en R. Para este fin, observe el lector lo siguiente

$$\begin{bmatrix} e & 0 \\ -yu_1 & \overline{e} \end{bmatrix} \begin{bmatrix} e & 0 \\ yu_1 & \overline{e} \end{bmatrix} = \begin{bmatrix} e & 0 \\ 0 & \overline{e} \end{bmatrix}$$

debido a que $-yu_1e + \overline{e}yu_1 = -yu_1 + yu_1 = 0$. Más aún

$$\begin{bmatrix} e & -u_1x \\ 0 & \overline{e} \end{bmatrix} \begin{bmatrix} e & u_1x \\ 0 & \overline{e} \end{bmatrix} = \begin{bmatrix} e & 0 \\ 0 & \overline{e} \end{bmatrix}$$

ya que $eu_1x - u_1x\overline{e} = 0$. Adicionalmente,

$$\begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix} \begin{bmatrix} u_1 & 0 \\ 0 & v_1 \end{bmatrix} = \begin{bmatrix} e & 0 \\ 0 & \overline{e} \end{bmatrix}$$

De este modo, las matrices $\begin{bmatrix} e & 0 \\ -yu_1 & \overline{e} \end{bmatrix}$, $\begin{bmatrix} e & -u_1x \\ 0 & \overline{e} \end{bmatrix}$ y $\begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix}$ son unidades de $\begin{bmatrix} eRe & eR\overline{e} \\ \overline{e}Re & \overline{e}R\overline{e} \end{bmatrix}$. Estas matrices nos sirven porque

$$\begin{bmatrix} e & 0 \\ -yu_1 & \overline{e} \end{bmatrix} \begin{bmatrix} u & x \\ y & v+yu_1x \end{bmatrix} \begin{bmatrix} e & -u_1x \\ 0 & \overline{e} \end{bmatrix} = \begin{bmatrix} u & x \\ 0 & v \end{bmatrix} \begin{bmatrix} e & -u_1x \\ 0 & \overline{e} \end{bmatrix} = \begin{bmatrix} u & 0 \\ 0 & v \end{bmatrix}$$

De este producto es posible obtener a $\begin{bmatrix} u & x \\ y & v+yu_1x \end{bmatrix}$ y verla como un producto de matrices invertibles. □

Como una consecuencia de este resultado se obtiene lo siguiente

Lema 2.11. *Si* $1 = e_1 + e_2 + \cdots + e_n$ *en un anillo* R *donde cada* e_i *es idempotente,* $e_ie_j = 0$ *para todo* $1 \leq i, j \leq n$*, y cada* e_iRe_i *es clean, entonces* R *es clean.*

Demostración. Según lo exigido en el resultado anterior, lo que hace falta probar es que cada $(1-e_i)R(1-e_i)$ es clean. Se probará mediante inducción sobre n.
Si $n = 1$ caso trivial. Suponga que $n = 2$, es decir, suponga que $1 = e_1 + e_2$ y que e_1Re_1 y e_2Re_2 son ambos clean. De este modo, se sigue que $e_2 = 1 - e_1$ y por lo tanto $e_2Re_2 = (1-e_1)R(1-e_1)$ es clean. Del Lema 2.10, concluimos que R es clean.
Supongamos ahora que para $2 < k \leq n$ se cumple el resultado, esto es, R es clean si $1 = e_1 + e_2 + \cdots + e_k$ donde los e_i idempotentes ortogonales y cada e_iRe_i es clean.
Se probará que en el caso $n+1$ se cumple. Para esto, suponga que $1 = e_1 + e_2 + \cdots + e_n + e_{n+1}$ y que cada e_iRe_i es clean para $1 \leq i \leq n+1$. Considere el elemento $1 - e_{n+1} = e_1 + e_2 + \cdots + e_n$. Se afirma que $e_1 + e_2 + \cdots + e_n$ es un idempotente de R. Para ver esto, tome el producto $(e_1 + e_2 + \cdots + e_n)(e_1 + e_2 + \cdots + e_n)$. Observe el lector que

$$(e_1 + e_2 + \cdots + e_n)(e_1 + e_2 + \cdots + e_n) = (e_1e_1 + \sum_{2 \leq i_1 \leq n} e_1e_{i_1}) + (e_2e_1 + e_2e_2 +$$

$$\sum_{3 \leq i_2 \leq n} e_2e_{i_2}) + (e_3e_1 + e_3e_2 + e_3e_3 + \sum_{4 \leq i_3 \leq n} e_3e_{i_3}) + \cdots + (\sum_{1 \leq i_{n-1} \leq n-1} e_ke_{i_{n-1}} + e_ne_n) =$$

$$e_1e_1 + e_2e_2 + \cdots + e_ne_n = e_1 + e_2 + \cdots + e_n$$

Además de la propiedad distributiva, $1 = (e_1+e_2+\cdots+e_n)+e_{n+1}$ con $(e_1+e_2+\cdots+e_n)$ y e_{n+1} idempotentes de R. De aquí, como en el caso $n = 2$ llegamos a que $(e_1 + e_2 + \cdots + e_n)R(e_1 + e_2 + \cdots + e_n)$ es clean. Como $1 - e_{n+1} = e_1 + e_2 + \cdots + e_n$, entonces se obtiene que $(1-e_{n+1})R(1-e_{n+1})$. Del Lema 2.10, se cumple el resultado. □

Con lo anteriormente mencionado, tenemos las herramientas suficientes para demostrar que:

Proposición 2.12. *Si* R *es clean, entonces* $M_n(R)$ *es clean.*

Demostración. Consideremos el subconjunto de $M_n(R)$ de la forma $\{E_{ii}\}_{i=1}^n$, donde la matriz E_{ii} tiene exactamente una entrada igual a 1 en la fila i y en la columna i y en las demás posiciones sus entradas son iguales a cero. Observe que $E_{ii}E_{jj} = 0_{n \times n}$

con $0_{n\times n}$ la matriz cero, si $i \neq j$. Además de que $E_{ii}E_{ii} = E_{ii}$ y que la matriz identidad se puede ver como $I_{n\times n} = E_{11} + E_{22} + \cdots + E_{nn}$. El conjunto $E_{ii}M_n(R)E_{ii}$ es de matrices cuadradas cuya entrada es distinta de cero en la fila i y la columna i y en las entradas restantes su valor es cero.
Sea $D \in E_{ii}M_n(R)E_{ii}$. Entonces el elemento $(D)_{ii} \neq 0$, y además $(D)_{ii} \in R$. Se puede definir una función cuyo dominio sea $E_{ii}M_n(R)E_{ii}$ y recorrido sea R, de manera natural: tome el elemento no nulo $d = (D)_{ii}$ y asignelo a $d \in R$. Esta función así definida nos da un isomorfismo, y como R es clean entonces de 2.5 se obtiene que $E_{ii}M_n(R)E_{ii}$ es clean. Por lo tanto, todas las hipótesis del lema 2.11 se tienen para el anillo $M_n(R)$ y se concluye que $M_n(R)$ es clean si R es clean. □

Recordemos que un $R-$módulo es llamado *semisimple* si todo submódulo de M es un sumando directo. Un anillo R es llamado *semisimple* si visto R como $R-$módulo es semisimple. Los espacios vectoriales de dimensión finita son semisimples, pues todo subespacio es sumando directo.
Probaremos que

Proposición 2.13. *Todo anillo semisimple es clean.*

Demostración. Sea R anillo semisimple. Del teorema de Wedderburn-Artin, [23, Teorema 2.6.18], se obtiene que

$$R \simeq M_{n_1}(D_1) \oplus \cdots \oplus M_{n_s}(D_s)$$

Donde cada $M_{n_i}(D_i)$ es un anillo de matrices sobre cada anillo de división D_i, $i = 0, 1, \cdots, s$.
Del resultado 2.12, cada $M_{n_i}(D_i)$ es clean pues las entradas en las matrices son anillos de división. Además como todo producto de anillos clean también lo es, por lo visto en la proposición 2.7, y la imagen bajo homomorfismo de anillos clean también lo es, entonces en virtud de la proposición 2.5 se concluye que R es clean. □

2.3. Levantamiento de idempotentes y anillos exchange

El concepto que vamos a introducir es importante en adelante y ya apareció en textos de álgebra desde finales de los $60's$, como por ejemplo en el libro de D. M. Burton *A First Course in RINGS AND IDEALS* [3]. Resaltamos que los anillos R a considerar son conmutativos con unidad, excepto que se mencione explicítamente lo contrario. Antes de continuar, definimos otro radical asociado a un anillo R, el llamado *Radical Primo*.

Definición 2.14. El radical primo de R, denotado por $Rad(R)$, viene dado por

$$Rad(R) = \bigcap_{\mathfrak{p} \in Spec(R)} \mathfrak{p},$$

donde $Spec(R)$ denota el conjunto de todos los ideales primos del anillo R.

Es posible demostrar que $Rad(R)$ es un ideal de R, $Rad(R) \subseteq \mathcal{J}(R)$ y además que $Rad(R)$ coincide con el ideal de todos los elementos nilpotentes [3, Teorema 8.8].

Suponga que I es un ideal de un anillo R tal que $I \subseteq Rad(R)$, y sea e un idempotente de R no nulo. Entonces $e + I = e^2 + I = (e + I)(e + I)$, es decir, $e + I$ es un idempotente en R/I. Una pregunta natural es si ¿$e + I$ es un idempotente no nulo? La respuesta es afirmativa, dado que si e idempotente no nulo tal que $e + I = I$, usando que $I \subseteq Rad(R)$, obtenemos que $e = 0$, lo cual es una contradicción.

Antes de continuar necesitamos el siguiente lema.

Lema 2.15. *Sea R anillo con unidad. Si $a \in R$ es nilpotente y si $u \in \mathcal{U}(R)$, entonces $u + a \in \mathcal{U}(R)$. En particular, $1 + a \in \mathcal{U}(R)$.*

Demostración. Como a es nilpotente, existe $n \in \mathbb{N}$ tal que $a^n = 0$. Además, como u es unidad de R, existe $v \in R$ tal que $uv = vu = 1$.
Ahora bien, dado que

$$(u + a)(u^{n-1} - u^{n-2}a + \cdots + (-1)^{n-1}a^{n-1}) = u^n - a^n = u^n,$$

es fácil ver que

$$(u + a)^{-1} = (u^{n-1} - u^{n-2}a + \cdots + (-1)^{n-1}a^{n-1})v^n.$$

□

A continuación presentamos algunas propiedades que aparecen en [3, Capítulo 8], que están relacionadas con nuestro trabajo.

Proposición 2.16. *Si e y e' son dos idempotentes del anillo R tales que $(e - e') \in Rad(R)$, entonces $e = e'$.*

Demostración. Supongamos que e y e' son dos idempotentes del anillo R tales que $(e - e') \in Rad(R)$. Observe el lector que $(e - e')(1 - (e + e')) = 0$. En efecto,

$$\begin{aligned}(e - e')(1 - (e + e')) &= (e - e') - (e - e')(e + e') \\ &= (e - e') - [e^2 + ee' - e'e - (e')^2] \\ &= (e - e') - [e - e'] \\ &= 0_R.\end{aligned}$$

La idea de esta prueba es verificar que el elemento $1-(e+e')$ es invertible en R y así la ecuación $(e-e')(1-(e+e'))=0$ implica que $e-e'=0$.
En efecto, $1-(e+e')$ la podemos escribir como

$$1-(e+e')=(1-2e)+(e-e')$$

como $e-e'$ pertenece al radical primo de R, entonces R es nilpotente. Además, $(1-2e)^2=1-4e+4e^2=1$. Entonces $1-(e+e')$ es la suma de un nilpotente y una unidad de R. Ahora hacemos lo siguiente

$$\begin{aligned}1-(e+e')&=(1-2e)+(e-e')\\(1-(e+e'))(1-2e)&=(1-2e)^2+(e+e')(1-2e)\\(1-(e+e'))(1-2e)&=1+(e+e')(1-2e).\end{aligned}$$

como $e-e'$ es nilpotente y R es conmutativo, entonces $(e-e')(1-2e)$ es nilpotente, lo cual implica que $1+(e+e')(1-2e)$ es invertible en R. De lo anteriormente mencionado, concluimos que $1-(e+e')$ es un elemento invertible en R. □

Recordemos que, de la proposición 1.28, el único idempotente en $\mathcal{J}(R)$ es 0_R.
Suponga que $I\subseteq\mathcal{J}(R)$. En efecto, $e\notin I$ y, por lo tanto, concluimos que $e+I\neq I$.
Ahora bien, si $x+I$ es un idempotente no nulo de R/I, ¿existe algún idempotente de $e\in R$ tal que $e+I=x+I$? Lo mencionado motiva la siguiente

Definición 2.17. Sea un ideal I de un anillo R. se dice que los idempotentes de R/I pueden ser *levantados* a R, si todo idempotente de R/I es de la forma $e+I$ donde e es un idempotente de R.

Observe el lector que la definición se puede reescribir de la siguiente manera: para cada elemento $x\in R$ tal que $(x-x^2)\in I$ existe un idempotente e de R tal que $e-x$ está en I.
Decir que para cada elemento $x\in R$ tal que $(x-x^2)\in I$ es equivalente a tomar x de manera que $x+I=x^2+I=(x+I)(x+I)$. Así, para cada idempotente de R/I, existe un idempotente e de R tal que $e+I=x+I$.

Ejemplo 2.18. Considere el lector a $\mathbb{Z}_2$. Este anillo es el resultado de hacer el cociente $\mathbb{Z}/2\mathbb{Z}$. Los idempotentes de $\mathbb{Z}$ son $\{0,1\}$ y los idempotentes de $\mathbb{Z}_2$ son todo $\mathbb{Z}_2$ pues este anillo es booleano.
Para el caso de $1+2\mathbb{Z}$, que es idempotente en $\mathbb{Z}_2$, el uno de los enteros verifica que $1-1=0\in 2\mathbb{Z}$.
En el caso de $0+2\mathbb{Z}$, el cero de los enteros verifica que $0-0=0\in 2\mathbb{Z}$. Por lo tanto, se concluye que $\mathbb{Z}_2$ levanta idempotentes módulo $2\mathbb{Z}$.

2.4. Algunas propiedades de los anillos exchange

El concepto de *anillo exchange* que presentaremos en esta sección, probablemente nació con el artículo de Crawley y Jónsson [26], pues fue usado por Warfield en [25] para definir anillo exchange como los anillos que satisfacen lo dicho por Crawley y Jónsson, vistos como un módulo a izquierda sobre si mismo. De manera más precisa, tenemos

Definición 2.19. Un $R-$módulo M tiene la propiedad de ser **exchange** si para todo $R-$módulo A y cualesquiera dos descomposiciones $A = M' \oplus N = \oplus_{i\in I} A_i$, con $M' \simeq M$, existen submódulos $A'_i \subset A_i$ tales que

$$A = M' \oplus (\oplus_{i\in I} A'_i).$$

Un anillo R es exchange si R visto como $R-$módulo tiene la propiedad exchange.

Una caracterizacón dada por Monk [18] es

Proposición 2.20. *Un anillo R es exchange si y solo si para todo $a \in R$, existen $b, c \in R$ tales que $bab = b$ y $c(1-a)(1-ba) = 1-ba$.*

Considere el anillo $\mathbb{Z}$. Para el valor $a = -2$, tenemos de la anterior proposición que $0 = (2b+1)b$, y como $\mathbb{Z}$ es dominio, concluímos que $b = 0$, lo cual implica que $-3c = 1$. Por lo tanto, $\mathbb{Z}$ no es exchange. De forma análoga, se puede probar que $\mathbb{Q}$ es exchange.
Toda esta información fue tomada por Nicholson en [20] y pudo reformular el concepto inicial de anillo exchange mediante el siguiente resultado en el cual omitiremos su demostración.

Proposición 2.21. *Un anillo es **exchange** si y solo si levanta idempotentes módulo todo ideal a izquierda (equivalentemente, derecha) del anillo.*

Veamos una relación importante que tienen los anillos exchange y los anillos clean.

Proposición 2.22. *Todo anillo clean es exchange.*

Demostración. Sea R clean, $x \in R$, I un ideal a izquierda de R tal que $x - x^2 \in I$. De la proposición 2.21 basta mostrar que existe un idempotente e de R tal que $e - x$ está en I.
En efecto, como R es clean, x se puede escribir como $x = u + f$ donde $f^2 = f$ y v el inverso de u. Verifiquemos que $e = v(1-f)u$ es idempotente.

$$e^2 = v(1-f)(uv)(1-f)u = v(1-f)1(1-f)u = v(1-f)^2u = v(1-f)u = e.$$

ahora verifiquemos que $e - x = v(x - x^2)$. Por un lado

$$\begin{aligned} v(x - x^2) &= v(u + f - (u + f)^2) = v(u + f - u^2 - uf - fu - f^2) \\ &= v(u - u^2 - uf - fu) = vu - vu^2 - vuf - vfu = 1 - u - f - vfu. \end{aligned}$$

para el término $e - x$ tenemos que

$$e - x = v(1 - f)u - (u + f) = vu - vfu - u - f = 1 - u - f - vfu$$

Así, $e-x = v(x-x^2) \in I$. Se concluye que para $x = u+f$ clean tal que $x-x^2 \in I$ para un ideal I a izquierda de R, existe $e = v(1-f)u$ idempotente tal que $e-x = v(x-x^2)$ está en I. De la proposición 2.21 se concluye que R es exchange si R es clean. □

En general no es cierto que todo anillo exchange sea clean. El ejemplo encontrado en la literatura es bien técnico y se debe a un aporte hecho por George Bergman al artículo de David Handelman en [10].

Definición 2.23. Para un ideal I de un anillo R, se dice que R levanta unidades módulo I si para cada elemento $x \in R$ tal que $x + I$ es una unidad del anillo cociente R/I, existe una unidad u de R tal que $u - x$ está en I.

A continuación, veremos cómo el radical de Jacobson nos puede servir para nuestro estudio de levantamiento de idempotentes.

Proposición 2.24. *Para un anillo R y todo ideal $I \subseteq \mathcal{J}(R)$, un elemento $x + I$ es una unidad de R/I si y solo si x es una unidad de R.*

Demostración. Supongamos que $x + I$ es una unidad de R/I y que $I \subseteq \mathcal{J}(R)$. Entonces existe $y + I \in R/I$ tal que $(x + I)(y + I) = (y + I)(x + I) = 1 + I$. En efecto, $xy + I = 1 + I$, lo que implica que $(1 - xy) \in I$.
Como I está contenido en el radical de Jacobson, $1 - r(1 - xy)$ es invertible para todo $r \in R$, en particular, para $r = 1$. Se obtiene que $1 - (1 - xy)$ es invertible. Pero $1 - (1 - xy) = xy$, de modo que xy es unidad de R. Así, existe $z \in R$ tal que $(xy)z = 1$. De la propiedad asociativa se obtiene que $x(yz) = 1$, con lo que se concluye que x es unidad de R.
Para probar el recíproco, si x es unidad de R, existe $z \in R$ tal que $xz = zx = 1$. De modo que

$$(x + I)(z + I) = xz + I = 1 + I$$

Se concluye que $x + I$ es unidad de R/I. □

El siguiente resultado, es una consecuencia de lo escrito en esta sección. Nos da una propiedad útil para el estudio de levantamiento de idempotentes.

Corolario 2.25. *Todo anillo clean levanta idempotentes módulo todo ideal a izquierda (respectivamente, derecha) del anillo.*

Demostración. Sea R anillo clean. Como R es clean, es exchange por la proposición 2.22. Así, R levanta idempotentes módulo todo ideal a izquierda(respectivamente derecha) del anillo por la proposición 2.21. □

Se presenta a continuación una caracterización de los anillos clean que depende de la propiedad de levantamiento de idempotentes.

Teorema 2.26. *Sea I un ideal a izquierda del anillo R, tal que $I \subseteq \mathcal{J}(R)$. Entonces R es clean si y solamente si el anillo cociente R/I es clean y R levanta idempotentes módulo I.*

Demostración. Suponga que R es clean. La función

$$\begin{aligned} \pi : R &\to R/I \\ r &\mapsto r + I \end{aligned}$$

es un homomorfismo sobreyectivo. Como $\pi(R) = R/I$, entonces de 2.5 se concluye que R/I es clean.
Del corolario 2.25 se obtiene que R levanta idempotents módulo I.
Suponga que R/I es clean y que R levanta idempotentes módulo I. Tome $r \in R$, entonces $r + I$ se puede escribir como $r + I = (x + I) + (e + I)$ con $x + I$ unidad de R/I y $e + I$ idempotente de R/I. Por un lado, como R levanta idempotentes módulo I, existe y idempotente de R tal que $(y - e) \in I$.
Entonces se puede asumir que e es un idempotente de R pues $e - e = 0_R$ y $0_R \in I$.
Como $x + I$ es una unidad de R/I y $I \subseteq \mathcal{J}(R)$, de la proposición 2.24 se deduce que x es unidad de R. Como $(r - e) + I = (r + I) - (e + I) = x + I$, entonces $x = r - e$ es una unidad de R. Por lo tanto, para $r \in R$, r se puede escribir como $r = (r - e) + e$, con lo cual r se puede ver como la suma de una unidad y de un idempotente de R. Por lo tanto, R es clean. □

Como consecuencia inmediata del resultado anterior, se obtiene el siguiente resultado clásico de Nicholson sobre su trabajo en levantamiento de idempotentes. (ver [20, pág. 272.])

Corolario 2.27. *Un anillo R es clean si y solamente si $R/\mathcal{J}(R)$ es clean y R levanta idempotentes módulo $\mathcal{J}(R)$.*

A continuación se presenta un resultado debido a Koh [14], en el que se prueba que los nil ideales tienen la propiedad de levantar idempotentes.

Proposición 2.28. *Sea N un ideal de un anillo R. Si todo elemento de N es nilpotente, entonces R levanta idempotentes módulo N.*

Demostración. Sea $r \in R$ tal que $(r - r^2) \in N$, y N un nil ideal de R. Entonces, existe $m \in \mathbb{N}$ tal que $(r - r^2)^m = 0_R$, de manera que $r^m(1 - r)^m = 0$.
Escriba a 1_R como $1 = r + (1 - r)$. Observe que $r(1 - r) = (1 - r)r$, lo cual nos permite hacer lo siguiente

$$1 = 1^{2m} = (r + (1 - r))^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} r^{2m-i}(1 - r)^i$$

Observe el lector que

$$1 = \sum_{i=0}^{m-1} \binom{2m}{i} r^{2m-i}(1 - r)^i + \sum_{j=1}^{m} \binom{2m}{m+j} r^{m-j}(1 - r)^{m+j}$$

Denote a

$$e = \sum_{i=0}^{m-1} \binom{2m}{i} r^{2m-i}(1 - r)^i$$

y

$$f = \sum_{j=1}^{m} \binom{2m}{m+j} r^{m-j}(1 - r)^{m+j}$$

verifiquemos que $ef = fe = 0_R$ para esto, observemos los productos que aparecen

$$ef = \left(\binom{2m}{0} r^{2m} + \binom{2m}{1} r^{2m-1}(1 - r) + \ldots + \binom{2m}{m-1} r^{m+1}(1 - r)^{m-1} \right)$$
$$\left(\binom{2m}{m+1} r^{m-1}(1 - r)^{m+1} + \binom{2m}{m+2} r^{m-2}(1 - r)^{m+2} + \ldots + (1 - r)^{2m} \right).$$

como r y $1 - r$ conmutan, entonces $r^a(1 - r)^b = (1 - r)^b r^a$, para a y b naturales, lo que implica que los diferentes productos que se forman en ef se hacen cero. De forma análoga se puede verificar que $fe = 0_R$.
De modo que $ef = fe = 0_R$ y $1 = e + f$. Observe que $(e + f)^2 = e^2 + f^2$, además

$$\begin{aligned} (1 - e)^2 &= 1 - 2e + e^2 \\ f^2 &= (e^2 + f^2) - 2e + e^2 \\ 2e &= 2e^2 \\ e &= e^2. \end{aligned}$$

Se concluye que e es un idempotente de R. De manera análoga, se prueba que f también es idempotente de R.
De lo anteriormente mencionado, se concluye que $e - r$ está en N, ya que $r + N = r^2 + N = e + N$. □

Corolario 2.29. *Sea N un nil ideal de un anillo R. Entonces R es clean si y solamente si el anillo cociente R/N es clean.*

Demostración. Como toda imagen bajo homomorfismo de un anillo clean es clean, entonces si R es clean, el epimorfismo canónico nos garantiza que R/N es clean. Para el reciproco, suponga que R/N es clean. De la proposición 2.28, se sigue que R levanta idempotentes módulo N. Siendo este el caso, del Teorema 2.26 se concluye que R es clean. □

2.5. Anillos con condiciones de cadena

Recuerde el lector que del ejemplo 2.2, $\mathbb{Z}$ no es clean. Así, no todo anillo Noetheriano es clean. El objetivo de esta sección es buscar conectar los conceptos estudiados de anillo artiniano con la condición clean.
Una caracteristica importante de los anillos artinianos es

Proposición 2.30. *Todo anillo artiniano a izquierda (derecha) es clean.*

Demostración. Sea R un anillo artiniano a izquierda. Entonces, es un hecho conocido que $\mathcal{J}(R)$ es nilpotente(para una demostración de este hecho, ver [3, Teorema 11-11]). Del resultado 2.29, hay que probar que $R/J(R)$ es clean para garantizar que R sea clean.
Como $R/\mathcal{J}(R)$ es semisimple cuando R es artiniano a izquierda (equivalentemente, derecha), entonces $R/\mathcal{J}(R)$ es clean por la proposición 2.13. Por lo tanto, todo anillo artiniano a izquierda (derecha) es clean. □

El siguiente resultado es muy útil para dar ejemplos de anillos clean:

Corolario 2.31. *Todo anillo finito es clean.*

Demostración. De la Proposición 2.30, basta con probar que todo anillo finito es artiniano.
para esto, suponga que R es un anillo finito. Como R es finito, el número posible de subconjuntos que se puede hacer con sus elementos también es finito. De manera que el número de ideales es menor que el número de subconjuntos de R. Entonces, toda cadena descendente de ideales de R finaliza, pues solo se cuenta con un número finito de ideales. Por lo tanto, R es artiniano. □

En virtud al resultado 2.31, se obtiene de manera inmediata que $\mathbb{Z}_n$ es clean. Presentaremos un resultado que se utliza más adelante en nuestro trabajo, pues nos da información de cuando un anillo de grupo es artiniano, su demostración se debe a Connell en [5, Teorema 1].

Proposición 2.32. *RG es artiniano si y solo si R es un anillo artiniano y G es un grupo finito*

2.6. Breve comentario acerca de elementos clean en anillos de polinomios.

El ánimo de esta sección es dar un ejemplo concreto de como la teoría de anillos clean puede usarse para resolver problemas concretos en matemáticas.
En el artículo "Commutative rings whose elements are a sum of a unit and a idempotent", Camillo y Anderson hacen una demostración acerca de la propiedad clean de anillos de polinomios. Para empezar, si R es un anillo conmutativo con 1_R y x es una variable, se tiene lo siguiente

$$\mathcal{ID}(R) = \mathcal{ID}(R[x]),$$
$$\mathcal{U}(R[x]) = \left\{ r_0 + r_1 x + \ldots r_n x^n : \ r_0 \in \mathcal{U}(R) \quad \text{y} \quad r_i \in \sqrt{(0)};\ i = 1, 2, \ldots, n \right\}.$$

Donde $\sqrt{(0)}$ es el nilradical[1] del ideal (0).
Sea $e = e^2$ un idempotente, entonces

1. caso $e = 0$. x se puede escribir como $x = 0 + (0 + 1x)$. El elemento $(0 + 1x)$ no es unidad en $R[x]$.

2. caso $e = 1$. x se puede escribir como $x = 1 + ((-1) + 1x)$. El elemento $((-1) + 1x)$ no es unidad de $R[x]$.

3. caso $e^2 = e$ no trivial. x se puede escribir como $x = e + ((-e) + 1x)$. El elemento $((-e) + 1x)$ no es unidad de $R[x]$.

hemos demostrado que x no es clean, lo que implica que $R[x]$ no es clean. Es de interés mencionar que hay elementos clean en $R[x]$, como por ejemplo el elemento $2 + ax = 1 + (1 + ax)$, donde a es un elemento nilpotente en R. Por otra parte, supongamos que $R[[x]]$ es clean y considere el ideal (x) de $R[[x]]$. Es posible probar que $(x) = \mathcal{J}(R[[x]])$ (ver [3, ejemplo 8-4]).
Así las cosas, la proposición 2.26 nos garantiza que $R[[x]]/(x)$ es clean, y como

[1] Sea I un ideal de un anillo R. El nilradical de I, se define como $\sqrt{I} = \{x \in I : x^n \in I \quad \exists n \in \mathbb{N}\}$.,

$R[[x]]/(x) \simeq R$, entonces podemos concluir que R es clean. Más aún, es posible demostrar que R clean implica que $R[[x]]$ es clean (ver [1, prop. 12].

A principios del siglo XX, el matemático Gottfried Köthe $(1905 - 1989)$, conjeturó que en cualquier anillo, la suma de dos nil ideales a izquierda es nil; resultado conocido como la "conjetura de Köthe". Los temas mencionados en esta sección interesaron a Kanwar, Leroy y Matczuk tanto que publicaron un artículo llamado "Clean elements in polynomial rings", [13], en el cual dan respuesta afirmativa parcial a la conjetura de Köthe.
Ellos demuestran que, para un anillo R en el cual no tenga nilpotentes no triviales, i.e., $x^2 = 0$ solo se satisface para $x = 0$; la suma de dos nil ideales a izquierda es nil si y solo si el conjunto de todos los elementos clean del anillo $R[x]$ es un subanillo de $R[x]$, [13, Teorema 2.15].

Capítulo 3

SOBRE ANILLOS DE GRUPO CLEAN

Una forma de estudiar la propiedad de ser clean en un anillo de grupo es por medio de la propiedad de ser semiperfecto. Mostraremos en detalle este primer camino para estudiar anillos de grupo clean.

3.1. Acerca de Anillos Semiperfectos

El trabajo conocido acerca de los anillos semiperfectos probablemente empieza con el trabajo hecho por Woods y Mueller en [27] y [19] respectivamente.

Definición 3.1. Un anillo R es llamado *semiperfecto* si levanta idempotentes módulo $\mathcal{J}(R)$ y $R/\mathcal{J}(R)$ es artiniano.

Ejemplo 3.2. Un ejemplo de anillos semiperfectos son los cuerpos. Como los únicos ideales en un cuerpo son los triviales, para $\mathbb{F}$ cuerpo, se tiene que $\mathcal{J}(\mathbb{F}) = \{0\}$, además $\mathbb{F}/\mathcal{J}(\mathbb{F}) = \mathbb{F}/\{0\} = \mathbb{F}$, el cual es artiniano. De este modo los cuerpos son semiperfectos.
Sea R un anillo artiniano a izquierda(derecha). De la Proposición 2.30 se obtiene que R es clean. Por lo tanto, R levanta idempotentes módulo $\mathcal{J}(R)$ en virtud del Corolario 2.25. Además, recuerde el lector que $R/\mathcal{J}(R)$ es artiniano a izquierda(derecha) también. Por lo tanto, los anillos artinianos a izquierda(derecha) son semiperfectos.

A continuación presentamos una propiedad que poseen los anillos exchange que es útil en nuestro trabajo. Su demostración se omite pues involucra conceptos que no son una prioridad en nuestro trabajo, [4, Corolario 2]).

Lema 3.3. *Todo anillo exchange o es semiperfecto o contiene un conjunto infinito de idempotentes ortogonales.*

Note el lector que a partir de la definición, es tedioso averiguar si un anillo es semiperfecto. Un resultado debido al trabajo hecho por Camillo y Yu en su estudio de anillos exchange [4], nos facilita el trabajo y utiliza herramientas ya conocidas por el lector en este momento del trabajo

Teorema 3.4. *Un anillo R es semiperfecto si y sólo si R es clean y no contiene un conjunto infinito de idempotentes ortogonales.*

Demostración. Supongamos que R es clean y que no contiene un conjunto infinito de idempotentes ortogonales. Como todo anillo clean es exchange (ver proposición2.22), del Lema 3.3 se concluye que R es semiperfecto.
Ahora supongamos que R es semiperfecto. Entonces $R/\mathcal{J}(R)$ es artiniano. Como todo anillo artiniano es clean, Proposición 2.30, se obtiene que $R/\mathcal{J}(R)$ es clean. Además, como R es semiperfecto, los idempotentes de R son levantados módulo $\mathcal{J}(R)$. De este modo, hemos obtenido por lo anteriormente mencionado que $R/\mathcal{J}(R)$ es clean y R levanta idempotentes módulo $\mathcal{J}(R)$. Del Corolario 2.27 se obtiene que R es clean.
Mueller en su artículo, [19], sobre anillos semiperfectos, prueba que dichos anillos no pueden tener un conjunto infinito de idempotentes ortogonales. □

Ejemplo 3.5. Otro ejemplo de anillos semiperfectos son los anillos finitos. Del Corolario 2.31 se sabe que todo anillo finito es clean. Por otra parte, los anillos finitos no pueden tener un conjunto infinito de idempotentes ortogonales. Así, los anillos finitos son semiperfectos.

Una de las razones por las cuales se estudian los anillos semiperfectos es por el impacto que tienen en los anillos de grupo de la forma $\mathbb{Z}_{(p)}C_n$, donde $\mathbb{Z}_{(p)}$ denota la localización de los enteros en el primo p y C_n es el grupo cíclico de orden n, como lo veremos en la siguiente sección.

3.2. ¿Es el anillo de grupo RG clean?

El ánimo de esta sección es convencer al lector de que, en general, la mera condición de que R sea clean no basta para que RG sea clean para un grupo dado G.

Proposición 3.6. *Sea R un anillo y G un grupo. Si RG es clean, entonces R es clean.*

Demostración. De la Definición 1.36 y la Proposición 1.37 tenemos que $\epsilon : RG \to R$ es un homomorfismo, y del primer Teorema del isomorfismo, $RG/\Delta(G) \simeq R$. Dado que toda imagen homomorfa de un anillo clean es clean, Proposición 2.5, entonces R es un anillo clean. □

Esta proposición nos da un criterio muy útil: Si R no es clean, entonces RG no es clean.
Una observación hecha por Mcgovern en su estudio de anillos clean conmutativos, [12], es que si R es un anillo conmutativo, G un grupo abeliano y si RG es clean, entonces G es de torsión(localmente finito). Mostraremos a continuación que no basta tener un anillo R solo con la condición clean para obtener, en general, un anillo de grupo RG.
Recordemos que $\mathbb{Z}_{(p)}$ para p primo es un anillo local, y por tanto clean. Explicaremos porqué el anillo de grupo $\mathbb{Z}_{(p)}C_n$ no es clean para todo p y para todo n.

Si tomamos anillos noetherianos y grupo abelianos finitamente generados, se pueden encontrar en la literatura afirmaciones muy interesantes. El siguiente resultado se debe al trabajo de Immormino y McGovern en [12]:

Proposición 3.7. *Sea R un anillo noetheriano, y sea G un grupo abeliano finitamente generado. El anillo de grupo RG es clean si y solo si es semiperfecto.*

Demostración. Suponga que RG es semiperfecto. Entonces RG es clean del Teorema 3.4.
Suponga ahora que RG es clean. El teorema 3.4 nos pide probar que RG no contenga un conjunto infinito de idempotentes ortogonales. Como R es un anillo noetheriano y G es finitamente generado, Connell en el inciso c) de [5, Teorema 2], nos permite concluir que RG es noetheriano. Como los anillos noetherianos no admiten un conjunto infinito de idempotentes ortogonales, Proposición 1.22, entonces en virtud del Teorema 3.4 se concluye que RG es semiperfecto, lo cual completa la demostración. □

Un resultado importante que se puede deducir a partir del resultado anterior es

Corolario 3.8. *Sea p primo, $n \in \mathbb{Z}^+$. Entonces el anillo de grupo $\mathbb{Z}_{(p)}C_n$ es clean si y solamente si es semiperfecto.*

Demostración. Como $\mathbb{Z}_{(p)}$ es noetheriano ya que es la localización de los enteros en el primo p (ver Proposición 1.32) y C_n es un grupo abeliano finitamente generado, de la Proposición 3.7 obtenemos el resultado. □

Como vemos, para determinar cuando $\mathbb{Z}_{(p)}C_n$ es clean es suficiente demostrar que es semiperfecto. Woods en su artículo sobre anillos semiperfectos(ver [27, Teorema 5.8]) sugiere el siguiente método. Omitimos su demostración.

Teorema 3.9. *Sea R un anillo conmutativo local con $char(R/\mathcal{J}(R)) = p \geq 0$, y sea G un grupo abeliano con p-componente primaria G_p. Entonces el anillo de grupo RG es semiperfecto si y solamente si G/G_p es un grupo finito de exponente n y cada factor mónico de $\overline{x^n - 1} \in (R/\mathcal{J}(R))[x]$ puede ser levantado a un factor mónico de $x^n - 1 \in R[x]$.*

Mostramos a continuación un ejemplo de como se aplica este teorema

Ejemplo 3.10. $\mathbb{Z}_{(7)}C_3$ no es semiperfecto

Demostración. El anillo $\mathbb{Z}_{(7)}$ es local conmutativo, su único ideal maximal es $\mathcal{J}(\mathbb{Z}_{(7)}) = 7\mathbb{Z}_{(7)}$. Por lo tanto, el anillo cociente $\mathbb{Z}_{(7)}/\mathcal{J}(\mathbb{Z}_{(7)})$ es un cuerpo de caracteristica 7, lo cual hace que este anillo sea isomorfo a $\mathbb{F}_7[x]$.
Con respecto a C_3 ya se sabe que es abeliano, y que su 7 componente primaria está dada por $(C_3)_7 = \{e\}$. De esta manera, el grupo $C_3/(C_3)_7$ es un grupo finito de exponente 3.
Veamos el polinomio $x^3 - 1$ en $\mathbb{F}_7$. Note que

$$(x-1)(x-2)(x-4) = (x^2 - 3x + 2)(x-4) = x^3 - 7x^2 + 14x - 8 = x^3 - 1$$

Por otra parte como $\mathbb{Z}_{(7)} \subset \mathbb{Q}$,

$$(x-1)(x^2 + x + 1) = x^3 - 1$$

Del criterio de Eisenstein se sigue que $x^2 + x + 1$ es irreducible en $\mathbb{Q}[x]$, en particular en $\mathbb{Z}_{(7)}[x]$. □

Por tanto, viendo conjuntamente los dos resultados anteriores podemos determinar cuando el anillo de grupo $\mathbb{Z}_{(p)}C_n$ es clean. Además, dado un anillo de grupo RG en las condiciones del Teorema 3.9 tenemos que él es clean y que no admite un conjunto infinito de idempotentes ortogonales, por el Teorema 3.4.

Presentamos a continuación unos resultados que pueden ser útiles a la hora de determinar cuando un anillo de grupo es clean. Vale la pena mencionar que un idempotente en un anillo R es *local* si eRe es un anillo local. El primer resultado es debido a Han y Nicholson en [9, Proposición 2.]:

Proposición 3.11. *Sea R un anillo semiperfecto y sea G un grupo. Si $(eRe)G$ es clean para cada idempotente local $e \in R$, entonces RG es clean.*

Demostración. la función $\gamma : (eRe)G \to e(RG)e$ definida como $\gamma(\sum a_g g) = \sum a_g g$ es un isomorfismo. Para ver que la función así definida tiene sentido, observe que $a_g \in eRe$ y por tanto $a_g = er_g e$, para $r_g \in R$. De manera que $\sum a_g g = \sum (er_g e)g =$

$\sum e(r_g g)e$. γ es claramente un isomorfismo pues es la función identidad.
Como R es semiperfecto, entonces $1_R = e_1 + e_2 + \cdots + e_n$, [9, Corolario 4], donde cada e_i es un idempotente local y $e_i e_j = 0$ para $i \neq j$. Como $(eRe)G \simeq e(RG)e$, y las imágenes isomorfas de anillos clean son también clean, se obtiene que $e_i(RG)e_i$ es clean para cada i. Por lo tanto se tienen todas las hipótesis del Lema 2.11, por lo cual concluímos que RG es clean. □

El siguiente resultado aparece en un trabajo de Zhou, [29, Corolario 16], en anillos de grupo.

Proposición 3.12. *Sea R un anillo semiperfecto y sea $G = H \times K$ donde H es un $2-$grupo abeliano elemental y K es el producto directo de un número finito de copias de S_3. Entonces RG es clean.*

Demostración. Es sabido que, [23, Sección 3.2]

$$R(H \times K) \simeq (RH)K \simeq (RK)H \simeq R(K \times H).$$

Lo anterior se puede justificar al definir una función $\delta : H \times K \to K \times H$ definida de la siguiente manera: $\delta((a, b)) = (b, a)$. Observe que δ es un isomorfismo.
De lo anteriormente mencionado se sigue que RK es semiperfecto, en virtud a un resultado demostrado por Woods, [27, Lema 6.1]. Como e es un idempotente local, el anillo $e(RK)e$ es local. Así las cosas, obtenemos que $(e(RK)e)H$ es clean, a partir de lo encontrado por Zhou en [29, Lema 14.]. Entonces, en virtud del Lema 2.11, obtenemos que $(RK)H$ es clean. Por lo tanto, RG es clean. □

3.3. Acerca de los anillos semiclean

En la literatura existe otra forma de resolver parcialmente la pregunta de encontrar condiciones sobre R y G que hagan del anillo de grupo RG un anillo clean. Este camino es mediante el concepto de anillos semiclean que presentamos a continuación. Tomaremos algunos resultados concretos del trabajo hecho por Ye en su artículo [28].

Definición 3.13. Un elemento a se llama periódico si $a^k = a^l$ para algunos k, l enteros positivos con $k \neq l$.
Un elemento r de un anillo R es llamado "semiclean" si se puede expresar como $r = a + u$, donde a es un elemento periódico y u es una unidad de R.

Observación 3.14. Observe que ejemplos de elementos periódicos en un anillo son los idempotentes, pues $e^2 = e$.
Es claro de la definición que todo elemento clean es semiclean y así todo anillo clean es semiclean, lo cual nos hace pensar que el concepto de anillo semiclean es más general. Esto último será establecido luego.

A continuación mencionaremos algunas propiedades de estos anillos

Proposición 3.15. *Toda imagen bajo homomorfismo de un anillo semiclean es semiclean*

Demostración. Esta prueba es muy parecida a la presentada en la demostración de la Proposición 2.5. Se demostrará que la imagen de un elemento periódico es también periódico.
Sea a un elemento periódico y sea $\phi : R \to S$ un homomorfismo de anillos, con R semiclean. Entonces $a^k = a^l$, con $k \neq l$. Esto implica que $a^k - a^l = 0_R$, lo cual nos dice que $\phi(0_R) = \phi(a^k - a^l) = 0_S$, de modo que $\phi(a^k) - \phi(a^l) = 0$. Como $\phi(a^k) = \phi(a)^k$ y $\phi(a^l) = \phi(a)^l$, note el lector que $\phi(a)^k = \phi(a)^l$. Esto nos muestra que $\phi(a)$ es periódico, como se quería mostrar. □

Recordemos que del Teorema 2.26, una caracteristica que tienen los anillos clean R es que, dado un ideal I que esté contenido en el radical de Jacobson $\mathcal{J}(R)$, R/I es también es clean y los idempotentes de R pueden ser levantados módulo ese ideal I. ¿qué ocurre en el caso de los anillos semiclean?
En su artículo *Semiclean Rings* [28], Ye demuestra el siguiente resultado.

Proposición 3.16 (Proposición 2.2)**.** *Sea I un ideal de R, con $I \subseteq \mathcal{J}(R)$. Si R/I es semiclean y los elementos periódicos en R pueden ser levantados módulo I, entonces R es semiclean.*

Demostración. Escriba $\overline{r} = r + I$ para r en R. ComoR/I es semiclean, entonces $\overline{r} = \overline{f} + \overline{u}$ donde $\overline{f}$ es un periódico en R/I y $\overline{u}$ es una unidad. Como $\overline{u} = \overline{r - f}$, vamos a ver que $r - f$ es unidad en R.
Para esto, como $\overline{r - f}$ es unidad de R/I, existe $\overline{w}$ tal que $\overline{(r-f)w} = \overline{1}$. Entonces $1-(r-f)w$ está en I. Como $I \subseteq \mathcal{J}(R)$, el elemento $1-(1-(r-f)w)$ es una unidad de R, lo cual implica que existe $m \in R$ tal que $(1-(1-(r-f)w))m = 1$. Observe el lector que

$$\begin{aligned}(1-(1-(r-f)w))m &= 1\\ (1-1+(r-f)w)m &= 1\\ (r-f)wm &= 1.\end{aligned}$$

Lo cual nos muestra que $r - f$ es una unidad de R. Comolos elementos periódicos de R pueden ser levantado módulo I, se obtiene que f es un periódico de R si $\overline{f}$ lo es en R/I.
Además, como el elemento r se puede escribir como $r = (r - f) + f$, esto implica que puede ser escrito como la suma de una unidad y un periódico de R. Así, r es semiclean, y dado que r es arbitrario, se concluye que R es semiclean. □

Observación 3.17. En la teoría de anillos es conocido que el único idempotente que admite el radical de Jacobson es el cero del anillo. Esta misma pregunta en el caso periódico no es satisfactoria, pues el radical de Jacobson contiene a los nilideales que tenga el anillo dado.

Una de las caracteristícas del artículo de Ye, [28, Sección 3], es que pudo encontrar los idempotentes y las unidades de anillos de grupo tipo $\mathbb{Z}_{(p)}C_n$.

Proposición 3.18. *Supongamos que C_3 está generado por a. Los idempotentes de $\mathbb{Z}_{(p)}C_3$ con p primo distinto a 3 son* 0, 1, $\frac{1}{3}+\frac{1}{3}a+\frac{1}{3}a^2$, $\frac{2}{3}-\frac{1}{3}a-\frac{1}{3}a^2$.

Demostración. Sea $x+ya+za^2$ un idempotente de $\mathbb{Z}_{(p)}C_3$. Entonces observe el lector lo siguiente

$$\begin{aligned} x+ya+za^2 &= (x+ya+za^2)^2 \\ &= x^2+xya+xza^2+xya+y^2a^2+yza^3+xza^2+yza^3+z^2a^4 \\ &= (x^2+2yz)+(z^2+2xy)a+(2xz+y^2)a^2. \end{aligned}$$

entonces concluímos que

$$x^2+2yz = x \tag{3.1}$$
$$z^2+2xy = y \tag{3.2}$$
$$2xz+y^2 = z. \tag{3.3}$$

Al multiplicar la ecuación 3.2 por z y la ecuación 3.3 por y se obtienen las siguientes ecuaciones

$$z^3+2xyz = yz$$
$$y^3+2xyz = yz.$$

De las cuales podemos, por medio del método de eliminación, obtener que

$$z^3-y^3 = 0$$

Como $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$, podemos factorizar la última expresión como

$$0 = z^3-y^3 = (z-y)(z^2+zy+y^2). \tag{3.4}$$

queremos probar que la ecuación 3.4 implica que$z = y$, teniendo en cuenta que z, y son racionales. Para este fin, suponga que $z \neq y$. Entonces, como $\mathbb{Q}$ es cuerpo, se debe tener que el término z^2+zy+y^2 sea igual a cero. Por otra parte, de la propiedad

de tricotomía de los racionales, como $z \neq y$, se obtienen dos casos.
El primer caso es que $z > y$.
Para este caso, observe el lector que

$$\begin{aligned} 0 &< z - y \\ 0 &< (z-y)^2 \\ 0 &< z^2 - 2zy + y^2 \\ 0 &< z^2 - 2zy + y^2 < z^2 + zy + y^2. \end{aligned}$$

Se obtiene que $0 < z^2 + zy + y^2$. Esto es contradictorio, pues el término $z^2 + zy + y^2$ es igual a cero. De manera análoga, si se supone que $z < y$, se encontrará una contradicción. Por lo tanto, se concluye que $z = y$.
Reemplazando z por y en la ecuación 3.3, obtenemos $y^2 + 2xy = y$, de lo cual obtenemos la siguiente ecuación

$$y(y + 2x - 1) = 0 \tag{3.5}$$

De la ecuación3.5, se puede afirmar que o $y = 0$ o $y + 2x - 1 = 0$. Si $y = 0$, entonces $z = 0$, lo cual al reemplazar esta información en la ecuación 3.1 se obtiene que $x^2 = x$. Como x es racional, se concluye que $x = 0$ o $x = 1$.
como $z = y$, reemplazando este valor en la ecuación 3.1 se obtiene la siguiente ecuación

$$x^2 + 2y^2 = x \tag{3.6}$$

Por otra parte, si $y + 2x - 1 = 0$, entonces $y = 1 - 2x$. Si reemplazamos este valor en la ecuación 3.6, tenemos lo siguiente

$$\begin{aligned} x^2 + 2y^2 &= x \\ x^2 + 2(1-2x)^2 &= x \\ x^2 + 2(1 - 4x + 4x^2) &= x \\ 9x^2 - 9x + 2 &= 0. \end{aligned}$$

Note que el polinomio $9x^2 - 9x + 2$ se factoriza en $\mathbb{Q}$ como $(3x-2)(3x-1)$, de modo que $9x^2 - 9x + 2 = 0$ implica que $(3x - 2)(3x - 1) = 0$. De lo cual se obtiene que x puede valer $2/3$ o $1/3$.
Si $x = 1/3$, como $y = 1 - 2x$ y $z = y$, se obtiene que $z = 1/3$. Por otra parte, si $x = 2/3$, entonces $z = -1/3$.
Se concluye que para el elemento $x + ya + za^2$, las posibilidades que tiene para valores de x,y y z son 0, 1, $\frac{1}{3} + \frac{1}{3}a + \frac{1}{3}a^2$, $\frac{2}{3} - \frac{1}{3}a - \frac{1}{3}a^2$. □

el siguiente resultado caracteriza a las unidades del anillo $\mathbb{Z}_{(p)}C_3$

Proposición 3.19. *Sea G un grupo cíclico de orden 3 generado por a y sea $x = k + la + ma^2$ que pertenece a $\mathbb{Z}_{(p)}G$. Entonces x es una unidad de $\mathbb{Z}_{(p)}G$ si y solo si p no divide*

$$\begin{vmatrix} k & m & l \\ l & k & m \\ m & l & k \end{vmatrix} = k^3 + l^3 + m^3 - 3klm.$$

Demostración. Suponga que $x = k + la + ma^2$ pertenece a $\mathbb{Z}_{(p)}G$. Entonces x es una unidad de $\mathbb{Z}_{(p)}G$ si y solo si existe $y = h_0 + h_1a + h_2a^2$ que pertenece a $\mathbb{Z}_{(p)}G$ tal que $xy = yx = 1_{\mathbb{Z}_{(p)}G} = 1 + 0a + 0a^2$.
observe el lector lo siguiente

$$\begin{aligned} xy &= 1 \\ (k + la + ma^2)(h_0 + h_1a + h_2a^2) &= 1. \end{aligned}$$

resolviendo el lado izquierdo de la última ecuación tenemos lo siguiente

$$\begin{aligned} (k+la+ma^2)(h_0+h_1a+h_2a^2) &= kh_0+kh_1a+kh_2a^2+lh_0a+lh_1a^2+lh_2a^3+mh_0a^2 \\ &+ mh_1a^3+mh_2a^4 = (kh_0+lh_2+mh_1)+(kh_1+lh_0+mh_2)a+(kh_2+lh_1+mh_0)a^2. \end{aligned}$$

recordando que $a^3 = 1$ y que $a^4 = a$, pues G es cíclico. Se obtiene entonces que

$$(kh_0 + lh_2 + mh_1) + (kh_1 + lh_0 + mh_2)a + (kh_2 + lh_1 + mh_0)a^2 = 1$$

Esta ecuación genera el siguiente sistema de ecuaciones lineales

$$\begin{aligned} kh_0 + mh_1 + lh_2 &= 1 \\ lh_0 + kh_1 + mh_2 &= 0 \\ mh_0 + lh_1 + kh_2 &= 0. \end{aligned}$$

del álgebra lineal sabemos que, este sistema es consistente si y solo si

$$\begin{vmatrix} k & m & l \\ l & k & m \\ m & l & k \end{vmatrix} = w. \tag{3.7}$$

con w distinto a cero o que p no divida a w. De lo contrario, suponga que $p \mid w$. Entonces $w = pr$ con $r \in \mathbb{Z}_{(p)}$. De modo que, r se puede escribir como $r = s/t$ con $p \nmid t$. Así, tenemos que

$$w = p\frac{s}{t} = \frac{p^2}{p}\frac{s}{t} = \frac{p^2 s}{pt}$$

, con lo que conluimos que $w \notin \mathbb{Z}_{(p)}$, pues $p \mid pt$. Esto es una contradicción.
Por otra parte, del método de cofactores aplicado a 3.7 tenemos lo siguiente

$$w = k[k^2 - ml] - m[lk - m^2] + l[l^2 - mk] = \\ k^3 - klm - klm + m^3 + l^3 - klm = k^3 + m^3 + l^3 - 3klm$$

Con esto se completa la demostración. □

Presentamos, por completez, la versión más general encontrada también por Ye en su mencionado trabajo. Su demostración es análoga a la presentada en el resultado inmediatamente anterior, y por lo tanto, se omite. El lector interesado, puede ver dicha demostración en [28].

Proposición 3.20. *Suponga el grupo cíclico C_q es generado por a. Entonces, un elemento $x = k_0 + k_1 a + k_2 a^2 + \ldots + k_{q-1} a^{q-1}$ es una unidad en $\mathbb{Z}_{(p)} C_q$ si y solo si p no divide al determinante*

$$\begin{vmatrix} k_0 & k_{q-1} & k_{q-2} & \cdots & k_1 \\ k_1 & k_0 & k_{q-1} & \cdots & k_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ k_{q-1} & k_{q-2} & k_{q-3} & \cdots & k_0 \end{vmatrix}.$$

Además, en su trabajo Ye afirma y demuestra que

Proposición 3.21. *El anillo de grupo $\mathbb{Z}_{(p)} G$ con G grupo cíclico de orden 3 es semiclean.*

Su pregunta natural era saber si todo anillo semiclean estaba contenido en uno clean. Su respuesta fue la opuesta: Los anillos clean están contenidos dentro de los anillos semiclean. Para ver esto, probaremos que

Proposición 3.22. *$\mathbb{Z}_{(7)} C_3$ no es clean.*

Demostración. considere el elemento $2+3a$ con a generador de C_3. De la Proposici"on 3.18, los idempotentes en $\mathbb{Z}_{(7)} C_3$ son

- 0.
- 1.
- $\frac{1}{3} + \frac{1}{3}a + \frac{1}{3}a^2$.
- $\frac{2}{3} - \frac{1}{3}a - \frac{1}{3}a^2$.

teniendo esto en mente, las formas posibles de escribir el elemento $2+3a$ son

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

lo que falta por determinar es que los elementos

- $2+3a$.
- $1+3a$.
- $\frac{5+8a-a^2}{3}$.
- $\frac{4+10a+a^2}{3}$.

son unidades de $\mathbb{Z}_{(7)}C_3$. Para esto, utilizaremos el criterio dado en la Proposición3.19. Observe que para los términos $\frac{5+8a-a^2}{3}$ y $\frac{4+10a+a^2}{3}$ basta verificar que

- $5+8a-a^2$.
- $4+10a+a^2$.

son unidades.
Al hacer las cuentas, se puede ver que

- 7 divide a $2^3+3^3+0^3-(3)(2\cdot 3\cdot 0)=35$.
- 7 divide a $1^3+3^3+0^3-(3)(1\cdot 3\cdot 0)=28$.
- 7 divide a $5^3+8^3+(-1)^3-3\cdot 5\cdot 8\cdot(-1)=756$.
- 7 divide a $4^3+10^3+1^3-3\cdot 4\cdot 10\cdot 1=945$.

Por lo tanto, los elementos $2+3a$, $1+3a$, $\frac{5+8a-a^2}{3}$ y $\frac{4+10a+a^2}{3}$ no son unidades en $\mathbb{Z}_{(7)}C_3$, en virtud de la Proposición 3.19. Por lo tanto, $2+3a$ no es clean. □

Lo que hemos hecho en este trabajo es mostrar dos caminos que hay disponibles en la literatura para determinar cuando ciertos anillos de grupo, en particular $\mathbb{Z}_{(7)}C_n$, son o no son clean.

3.4. ¿Qué ocurre cuando el grupo no es abeliano?

Un camino para poder explicar el comportamiento clean de un anillo de grupo en el cual se tenga un grupo no abeliano, es mediante involuciones, trabajo iniciado por Vaš en su artículo [24].
En el 2015, los profesores Gao, Chen y Li publicaron su trabajo , [8], en el cual se avanzó bastante en el estudio de dichos anillos. Este artículo es necesario para el trabajo de esta sección. Se presenta la noción de $* - clean$, dada en estos artículos

Definición 3.23. Sea R un anillo. Una aplicación $* : R \to R$ es una **involución**, si es un anti-homomorfismo de orden 2.
Un elemento p de un anillo con involución R es llamado una *proyección* si $p^* = p = p^2$.
$r \in R$ es llamado $*-$clean si se puede escribir como la suma de una proyección y una unidad de R. Un anillo con involución es llamado $*-$clean si todo elemento de dicho anillo es $*-$clean.

Ejemplo 3.24. Suponga R anillo local con involución. Como $0^* = 0$ y $1^* = 1$ para $*$ involución del anillo, además de que 0 y 1 son los únicos idempotentes, entonces estos dos elementos son las únicas proyecciones del anillo, pues R es local. Como todo anillo local es clean, todo elemento de un anillo local se puede ver como la suma de una proyección y una unidad. Por lo tanto, es $*-$clean.

Es claro de la definición, que toda proyección es un elemento idempotente, así tenemos lo siguiente

Proposición 3.25. *Todo anillo $*-$clean, es clean.*

El recíproco de esta afirmación no es cierto. Para ver esto, presentamos a continuación un resultado de Gao, Chen y Li, [8, Corolario 2.5], el cual presentamos como

Proposición 3.26. *Sea R un anillo. Si $char(R) \neq 3$, entonces RC_3 es $*-$clean si y sólo si la ecuación $x^2 + x + 1 = 0$ no tiene soluciones en R.*

Ejemplo 3.27. No todo anillo clean es $*-$clean. Dado que $\mathbb{C}C_3$ es un $\mathbb{C}-$espacio vectorial de dimensión finita, se sigue de la Proposición 2.30, que es clean. De la última proposición, vemos que $\mathbb{C}C_3$ no es $*-$clean, pues la ecuación $x^2 + x + 1 = 0$ en $\mathbb{C}$ tiene las soluciones $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ y $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$.

Por otra parte, en [8, Teorema 3.8] se encuentra el siguiente resultado, el cual nos permite demostrar que $R\mathcal{Q}_8$ es clean.

Teorema 3.28. *Sea R un anillo conmutativo local. Si $2 \in \mathcal{J}(R)$, entonces $R\mathcal{Q}_8$ es $*-$clean. En particular, $R\mathcal{Q}_8$ es clean.*

Demostración. Como R es local, $2 \in \mathcal{J}(R)$ y $\mathcal{Q}_8$ es 2-grupo finito, ver Sección 1.1, entonces del Teorema 1.38, se concluye que $R\mathcal{Q}_8$ es local. Del Corolario 3.24, todo anillo local es $*-$clean, y el resultado se sigue. □

Recordemos que si R es un anillo, G y H grupos, [23, Sección 3.2], entonces

$$R(G \times H) \simeq (RG)H.$$

Consideremos el grupo cuaternio $\mathcal{Q}_8$, E un $2-$grupo abeliano elemental y A un grupo abeliano cuyos elementos son de orden impar, entonces

$$R(\mathcal{Q}_8 \times E) \simeq (R\mathcal{Q}_8)E, \tag{3.8}$$

y

$$R((\mathcal{Q}_8 \times E) \times A) \simeq (R(\mathcal{Q}_8 \times E))A. \tag{3.9}$$

Por Polcino [23, Teorema 1.8.5], se obtiene la ecuación

$$R\mathcal{H} \simeq (R(\mathcal{Q}_8 \times E))A. \tag{3.10}$$

En la teoría de grupos, se estudia un teorema que clasifica los grupos de orden $2p$ con $p > 2$ número primo, dependiendo de si son abelianos o no.

Teorema 3.29. *Sea G un grupo, $|G| = 2p$, $p > 2$ número primo. Entonces G es isomorfo a $\mathbb{Z}_{2p}$ o D_p, el grupo dihedral de orden $2p$.*[1]

Una demostración de este resultado está en [7, Teorema 7.2]. Consideremos el caso en el que G no es abeliano de orden $2p$. Del anterior teorema, tenemos que G es isomorfo al grupo dihedral D_p, del cual podemos decir, entre otras cosas, que es un $p-$grupo localmente finito.
Zhou en su artículo "On Clean Group Rings" [29, Teorema 4] tiene un resultado que nos ayuda a encontrar anillos de grupo clean, con un $p-$grupo localmente finito:

Teorema 3.30. *Sea p un primo con $p \in \mathcal{J}(R)$. Si R es un anillo clean y G es un $p-$grupo localmente finito, entonces RG es clean.*

Zhou nos da un ejemplo directo de aplicación de dicho resultado, [29, Ejemplo 5], el cual nos dice que si R un anillo clean con $p \in \mathcal{J}(R)$, entonces RD_p es clean.
Teniendo en cuenta lo anterior, al debilitar un poco la condición sobre el grupo en el Teorema 3.30, es decir, a considerar $p-$grupos no abelianos de orden $2p$, tendriamos una familia de grupos no abelianos que nos pueden servir, es decir, los grupos isomorfos a D_p.

[1] Una manera de definir a este grupo es $D_p = \langle a, b : a^p = 1, \quad b^2 = 1, \quad ba = a^{-1}b \rangle$.

Corolario 3.31. *Sea $p > 2$ un primo con $p \in \mathcal{J}(R)$. Si R es un anillo clean y G es un $p-$grupo no abeliano de orden $2p$, entonces RG es clean.*

Más aún, Connell en su estudio de anillos de grupo [5] demuestra que si R es un anillo y G es un grupo localmente finito entonces $\mathcal{J}(R) = \mathcal{J}(RG) \cap R$. y teniendo en mente la siguiente identificación $R(G \times H) \simeq (RG)H$, podemos construir un anillo de grupo clean tomando como grupo base un grupo Hamiltoniano especial.

Sea $\mathcal{Q}_8 \times E$ con E un $2-$grupo abeliano elemental finito. Entonces $|\mathcal{Q}_8 \times E| = 2^{3+k}$, por lo que tenemos que $\mathcal{Q}_8 \times E$ es un $2-$grupo localmente finito. Por otra parte, suponga R anillo clean con $2 \in \mathcal{J}(R)$ y $q \in \mathcal{J}(R)$ para $q > 2$ primo. Del Teorema 3.30 se obtiene que $R(\mathcal{Q}_8 \times E)$ es clean.
Ahora bien, suponga A un grupo abeliano finito cuyos elementos son de orden q, por lo observado por Connell, tenemos que $2, q \in \mathcal{J}(R(\mathcal{Q}_8 \times E))$. Como A es un $q-$grupo localmente finito, tenemos que $(R(\mathcal{Q}_8 \times E))A$ es clean, en virtud del Teorema 3.30. Por lo tanto, $R(\mathcal{Q}_8 \times E \times A)$ es clean. Enunciamos este hecho mediante la siguiente Proposición:

Proposición 3.32. *Sea R anillo clean con con $2 \in \mathcal{J}(R)$ y $q \in \mathcal{J}(R)$ para $q > 2$ primo. Además, sea G el grupo $\mathcal{Q}_8 \times E \times A$ el grupo compuesto por*

- *$\mathcal{Q}_8$ grupo de cuaternios de orden 8.*
- *E es un $2-$grupo abeliano elemental finito.*
- *A es un grupo abeliano finito cuyos elementos son de orden q.*

Entonces $RG = R(\mathcal{Q}_8 \times E \times A)$ es clean.

Capítulo 4

CONCLUSIONES

1. En varios de los artículos de la literatura estudiada aparecen afirmaciones sin demostración, las cuales son posteriormente usadas para justificar otras aseveraciones, Lemas o Proposiciones. Aquellas afirmaciones que fueron relevantes en el presente trabajo fueron probadas en detalle y nos permitieron establecer y demostrar los Lemas y Proposiciones que algunas veces sólo fueron enunciados, por ejemplo, en la Sección 2.1, demostramos que todo anillo de división R es clean, hecho que unido al Teorema de Wedderburn-Artin, [23, Teorema 2.6.18], nos permite establecer de manera clara y transparente el hecho que todo anillo semisimple R es clean, Proposición 2.13.
   También demostramos el hecho simple de que $r \in R$ es clean, si y solamente si, $1 - r$ también lo es, que es el argumento principal en la demostración de que todo anillo local (R, M), Proposición 2.4, es clean.

2. Un resultado conocido en la literatura es que si R es un anillo clean, su anillo de matrices $n \times n$ asociado $M_n(R)$ también lo es. Para la demostración completa de este hecho, se hizo necesario demostrar un resultado relevante en la teoría general de anillos conocido como la descomposición de Peirce, [16, Sección 21], lo que permite demostrar que un anillo R con idempotente e, se puede identificar con cierto anillo matrices 2×2, Proposición 2.10. Finalmente, usamos la teoría de anillos corner [16, Capítulo 3], para establecer el resultado enunciado al comienzo de este parrafo.

3. ¿Cuándo un anillo de grupo RG es clean? es una pregunta que se han hecho muchos académicos como por ejemplo Han, Nicholson, Mcgovern, Immormimo [29], [17], [11], [9], entre otros. En el artículo de Han y Nicholson, *Extensions of clean rings*, demostraron los siguientes resultados: (1) Si R es un anillo semiperfecto, entonces RC_2 es clean; (2) Si R es un anillo Booleano y G es un grupo localmente finito, entonces RG es clean; (3) $\mathbb{Z}_{(7)}C_3$ no es clean. Como

$\mathbb{Z}_{(7)}$ es local, por lo visto en la Sección 1.3, entonces es clean en virtud de la Proposición 2.4; éste último ejemplo nos muestra una dificultad que hay en el estudio de anillo de grupos clean: No basta con que el anillo base R sea clean para que RG sea clean.
En este trabajo hemos abordado un camino vía anillos semiperfectos en la Sección 3.1; basados en el trabajo [12, Proposición 2.1] y la presentada por Ye con los anillos semiclean en la Sección 3.3 teniendo como referencia a [28]; para explicar de una manera clara y precisa la dificultad de estudiar un anillo de grupo particular de la forma $\mathbb{Z}_{(p)}C_n$, lo cual nos da una idea del problema de estudiar dichas estructuras algebraicas.

4. Zhou en su artículo llamado "On Clean Group Rings" [29] demuestra que, para p primo, si $p \in \mathcal{J}(R)$, R es clean y G es un $p-$grupo localmente finito, entonces RG es clean [29, Teorema 4] y utilizando el bien conocido resultado de que si $p > 2$ es un primo y G un grupo tal que $|G| = 2p$, entonces G es isomorfo a $\mathbb{Z}_{2p}$ o D_p; donde D_p es el grupo dihedral de orden $2p$, [7, Teorema 7.2]; al restringirnos a $p-$grupos no abelianos de orden $2p$, obtenemos el Corolario 3.31.
En el texto de Polcino y Sehgal se presenta una caracterización dada por Dedekind y Baer de los grupos Hamiltonianos, [23, Teorema 1.8.5]; además en dicho libro se da una identificación conocida en anillos de grupos [23, Sección 3.2]; $R(G \times H) \simeq (RG)H$; que junto con $\mathcal{J}(R) = \mathcal{J}(RG) \cap R$, dada por Connell en [5], nos da las herramientas suficientes junto con el Teorema 4 mencionado arriba por Zhou para construir la Proposición 3.32.

Bibliografía

[1] Anderson, D. D. ; Camillo, V. P.: Commutative rings whose elements are a sum of a unit and idempotent. (2002)

[2] Bhattacharya, P. B. ; Jain, S. K. ; Nagpaul, S. : *Basic abstract algebra.* Cambridge University Press, 1994

[3] Burton, D. M.: *A first course in Rings and Ideals.* Bd. 731. Addison-Wesley, 1970

[4] Camillo, V. P. ; Yu, H.-P. : Exchange rings, units and idempotents. In: *Communications in Algebra* 22 (1994), Nr. 12, S. 4737–4749

[5] Connell, I. G.: On the group ring. In: *Canad. J. Math* 15 (1963), Nr. 3, S. 650–685

[6] Dummit, D. S. ; Foote, R. M.: *Abstract algebra.* Bd. 3. Wiley Hoboken, 2004

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

[8] Gao, Y. ; Chen, J. ; Li, Y. : Some $*$-clean group rings. In: *Algebra Colloquium* Bd. 22 World Scientific, 2015, S. 169–180

[9] Han, J. ; Nicholson, W. : Extensions of clean rings. In: *Communications in Algebra* 29 (2001), Nr. 6, S. 2589–2595

[10] Handelman, D. : Perspectivity and cancellation in regular rings. In: *Journal of Algebra* 48 (1977), Nr. 1, S. 1–16

[11] Immormino, N. A.: *Clean Rings\ & Clean Group Rings*, Bowling Green State University, Diss., 2013

[12] Immormino, N. A. ; McGovern, W. W.: Examples of clean commutative group rings. In: *Journal of Algebra* 405 (2014), S. 168–178

[13] Kanwar, P. ; Leroy, A. ; Matczuk, J. : Clean elements in polynomial rings. In: *Contemp. Math* 634 (2015), S. 197–204

[14] KOH, K. : On lifting idempotents. In: *Canadian Mathematical Bulletin* 17 (1974), Nr. 4, S. 607–607

[15] Lam, T.-Y. : *A first course in noncommutative rings*. Bd. 131. Springer Science & Business Media, 2013

[16] Lam, T. : Corner ring theory: a generalization of Peirce decompositions. I. In: *Algebras, rings and their representations* (2006), S. 153–182

[17] McGovern, W. W.: Neat rings. In: *Journal of Pure and Applied Algebra* 205 (2006), Nr. 2, S. 243–265

[18] Monk, G. : A characterization of exchange rings. In: *Proceedings of the American Mathematical Society* 35 (1972), Nr. 2, S. 349–353

[19] Mueller, B. J. u. a.: On semi-perfect rings. In: *Illinois Journal of Mathematics* 14 (1970), Nr. 3, S. 464–467

[20] Nicholson, W. K.: Lifting idempotents and exchange rings. In: *Transactions of the American Mathematical Society* 229 (1977), S. 269–278

[21] Nicholson, W. : Local group rings. In: *Canadian Mathematical Bulletin* 15 (1972), Nr. 1, S. 137–138

[22] Nicholson, W. ; Zhou, Y. : Clean general rings. In: *Journal of Algebra* 291 (2005), Nr. 1, S. 297–311

[23] Polcino, C. M. ; Sehgal, S. K.: *An introduction to group rings*. Bd. 1. Springer Science & Business Media, 2002

[24] Vaš, L. : $*$-Clean rings; some clean and almost clean Baer $*$-rings and von Neumann algebras. In: *Journal of Algebra* 324 (2010), Nr. 12, S. 3388–3400

[25] Warfield, R. : Exchange rings and decompositions of modules. In: *Mathematische Annalen* 199 (1972), Nr. 1, S. 31–36

[26] WLEY, P. C. ; Jónsson, B. : Refinements for infinite direct decompositions of algebraic systems. In: *SUPPORTING INSTITUTIONS* (1964), S. 797

[27] Woods, S. : Some results on semi-perfect group rings. In: *Canad. J. Math* 26 (1974), Nr. 1, S. 121–129

[28] Ye, Y. : Semiclean Rings. In: *Communications in Algebra* 31 (2003), Nr. 11, S. 5609–5625

[29] Zhou, Y. : On clean group rings. In: *Advances in Ring Theory* (2010), S. 335–345