DESCOMPOSICIÓN ESPECIAL DE MATRICES SOBRE ANILLOS CONMUTATIVOS

CAMILO ANDRÉS ROMERO MANTILLA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMáTICAS
BUCARAMANGA
2025

DESCOMPOSICIÓN ESPECIAL DE MATRICES SOBRE ANILLOS CONMUTATIVOS

CAMILO ANDRÉS ROMERO MANTILLA

Trabajo de grado para optar al título de
Matemático

Director
Alexander Holguín Villa
Doctor en Ciencias

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE CIENCIAS
ESCUELA DE MATEMáTICAS
BUCARAMANGA
2025

DEDICATORIA

A mis padres y a mi hermana, por su amor incondicional y su constante apoyo. A mis amadas mascotas, Luna, Toby, Max, Lia y Amara, por recordarme siempre la importancia de la ternura y la compañía sincera.

AGRADECIMIENTOS

Deseo expresar mi más profundo agradecimiento a mis padres, cuyo apoyo incondicional fue el pilar fundamental que me permitió culminar esta etapa. No existen palabras suficientes para expresar lo afortunado que me siento de contar con su amor y guía en mi vida. Gracias a su largo trabajo, sacrificio y esfuerzo constante, hicieron posible que sus hijos tuvieran la oportunidad de convertirse en profesionales, sembrando en nosotros valores de responsabilidad, dedicación y perseverancia. Me encuentro muy feliz de escribir este documento porque cada página refleja el fruto de todo lo que han entregado por nuestra formación. Espero que siempre se sientan orgullosos de su hijo menor, que con todo el corazón dedica este trabajo como un homenaje al inmenso amor y compromiso que han demostrado en cada etapa de mi vida.

A mi hermana Carolina, a quien considero una segunda madre, le debo un reconocimiento muy especial. Su apoyo constante día a día y su acompañamiento en cada decisión han sido determinantes para que hoy pueda escribir este texto. Más que una hermana, ha sido mi amiga incondicional, mi consejera y mi ejemplo de fortaleza y cariño. Su presencia ha iluminado los momentos difíciles y ha multiplicado las alegrías en los buenos tiempos. Carolina siempre estuvo brindándome palabras de aliento, compartiendo mis sueños y recordándome siempre que nunca estoy solo. A ella le dedico con amor y gratitud estas palabras, con la esperanza de que se sienta tan orgullosa de mí como yo lo estoy de tenerla como hermana.

Extiendo también mi gratitud a mis amigos y compañeros, quienes a lo largo de este proceso se convirtieron en tutores, consejeros y compañeros de camino. En particular, quiero agradecer a C.Ruiz, Daniel, Catalina, Jotta, Jeison Amorocho, Jeison Ospino, Jhonnier, Reinaldo, Edward, Javier, Juan Carlos, Natalí, Angie, Jacksymar, Yineth, Zareth, Thomas y Sofía, pues cada uno de ellos dejó una huella importante en este camino. A todas aquellas personas que no he mencionado de manera explícita, quiero que sepan que las tengo presentes y que estoy profundamente agradecido por su compañía y apoyo.

De igual manera, extiendo un especial reconocimiento a mis profesores, quienes con sus enseñanzas contribuyeron de manera significativa a mi formación. En particular, al profesor Holguín, por su paciencia, disposición , orientación, buena energía y consejos durante la realización de este trabajo de grado, y al profesor Elder, a quien considero el mejor docente que tuve en este recorrido, no solo por su calidad académica, sino también por su calidad humana.

Finalmente, y no por ello menos importante, agradezco a mis amadas mascotas: Luna, Toby, Max, Lia y Amara, quienes con su mera existencia me cambiaron la vida.

RESUMEN

TíTULO: DESCOMPOSICIÓN ESPECIAL DE MATRICES SOBRE ANILLOS CONMUTATIVOS[*]

AUTOR: CAMILO ANDRÉS ROMERO MANTILLA[**]

PALABRAS CLAVE: ANILLOS, ANILLOS DE MATRICES, MATRICES IDEMPOTENTES, MATRICES INVOLUTIVAS, SUMA DE TRES IDEMPOTENTES, FORMA CANóNICA RACIONAL, FORMA CANóNICA DE JORDAN, ANILLOS CONMUTATIVOS, CUERPOS, ANILLOS INDESCOMPONIBLES.

DESCRIPCIóN: Este trabajo estudia la descomposición especial de matrices sobre anillos conmutativos, centrando su desarrollo en la comprensión y análisis de los resultados principales propuestos por Tang, Zhou y Su (2019), relativos a la representación de matrices como sumas de tres idempotentes o tres involutivas. Con este propósito, se construye un marco teórico que integra los fundamentos necesarios para entender y justificar dichos resultados, apoyándose en la teoría de anillos, la estructura de los anillos de matrices y las formas canónicas racional y de Jordan.

La investigación se sustenta en los aportes teóricos de Atiyah y Macdonald (1989) en álgebra conmutativa, Dummit y Foote (2004) en álgebra abstracta y Lezama (2020) en álgebra lineal, cuya combinación permite establecer las bases formales sobre anillos conmutativos, dominios enteros, cuerpos, ideales, anillos locales e indescomponibles. Asimismo, se integran resultados previos de G. Song y Xue-Jün Guo (1999), Robert E. Hartwig y Mohan S. Putcha (1990), y Clément de Séguin Pazzis (2010), cuyos trabajos sobre matrices idempotentes, involutivas y combinaciones lineales de idempotentes constituyen antecedentes fundamentales para los resultados principales de Tang, Zhou y Su (2019).

De manera particular, se destacan las contribuciones de McCoy (1938) y Birkhoff (1944), esenciales para la comprensión de los productos y subproductos directos de anillos, nociones que resultan claves en la caracterización de los anillos de matrices. Además, se abordan nociones esenciales del álgebra matricial, tales como la traza, el rango, la similitud y los polinomios característico y minimal, las cuales resultan indispensables para comprender la estructura interna de las matrices y su relación con las propiedades del anillo base.

El documento desarrolla de manera detallada la base algebraica necesaria para formalizar y demostrar los teoremas de Tang, adaptando su exposición al nivel de pregrado mediante un tratamiento riguroso. Finalmente, se analizan las implicaciones teóricas de los resultados obtenidos y se proponen líneas de trabajo futuro, orientadas a la extensión de estas descomposiciones hacia otras clases de anillos y estructuras algebraicas con propiedades análogas.

[*]Trabajo de grado

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

ABSTRACT

TITLE: SPECIAL DECOMPOSITION OF MATRICES OVER COMMUTATIVE RINGS.[*]

AUTHOR: CAMILO ANDRÉS ROMERO MANTILLA [**]

KEYWORDS: RINGS, MATRIX RINGS, IDEMPOTENT MATRICES, INVOLUTORY MATRICES, SUM OF THREE IDEMPOTENTS, RATIONAL CANONICAL FORM, JORDAN CANONICAL FORM, COMMUTATIVE RINGS, FIELDS, INDECOMPOSABLE RINGS.

DESCRIPTION: This work studies the special decomposition of matrices over commutative rings, focusing on the understanding and analysis of the main results proposed by Tang, Zhou, and Su (2019) concerning the representation of matrices as sums of three idempotent or three involutory matrices. For this purpose, a theoretical framework is constructed that integrates the necessary foundations to comprehend and justify these results, relying on ring theory, the structure of matrix rings, and the rational and Jordan canonical forms.

The research is supported by the theoretical contributions of Atiyah and Macdonald (1989) in commutative algebra, Dummit and Foote (2004) in abstract algebra, and Lezama (2020) in linear algebra, whose combination establishes the formal basis for understanding commutative rings, integral domains, fields, ideals, local rings, and indecomposable rings. Likewise, previous results by G. Song and Xue-Jün Guo (1999), Robert E. Hartwig and Mohan S. Putcha (1990), and Clément de Séguin Pazzis (2010) are integrated, as their works on idempotent matrices, involutory matrices, and linear combinations of idempotents provide essential precedents for the main results of Tang, Zhou, and Su (2019).

In particular, the contributions of McCoy (1938) and Birkhoff (1944) are highlighted as fundamental for understanding direct products and subdirect products of rings, concepts that are key to the structural characterization of matrix rings. Moreover, the study addresses essential notions of matrix algebra, such as trace, rank, similarity, and the characteristic and minimal polynomials, which are indispensable for understanding the internal structure of matrices and their relationship with the properties of the underlying ring.

The document develops in detail the algebraic foundation necessary to formalize and demonstrate Tang's theorems, adapting its exposition to the undergraduate level through a rigorous and systematic treatment. Finally, the theoretical implications of the results obtained are analyzed, and future research directions are proposed, aimed at extending these decompositions to other classes of rings and algebraic structures with analogous properties.

[*] Bachelor Thesis

[**] Faculty of Science. School of Mathematics. Advisor: Alexander Holguín Villa, Ph.D. in Science.

Índice general

1. Introducción

En el siglo XIX, como respuesta a la necesidad de generalizar los resultados ya establecidos en el álgebra elemental, así como los obtenidos en otras ramas de las matemáticas, surge el álgebra abstracta, cuyo objetivo es identificar las propiedades algebraicas comunes entre estructuras matemáticas tales como grupos, anillos y cuerpos, entre otras. Específicamente, una de las estructuras algebraicas más importantes son los anillos, que son conjuntos no vacíos dotados de dos operaciones binarias llamadas usualmente suma y producto, con ciertos postulados que deben verificar dichas operaciones; resaltando entre los axiomas la ley distributiva del producto respecto a la suma.

En general, la operación producto no requiere unidad, sin embargo, cuando esta última existe se dice que el anillo es unitario. Existen anillos con más estructura como los anillos conmutativos, los anillos de división y los cuerpos. En lo que respecta al presente estudio, se abordarán específicamente los anillos de matrices que son un tipo concreto de anillos cuyo producto no conmuta y que en general, son un conjunto de matrices con entradas en un anillo o un cuerpo específico. En el presente trabajo se busca estudiar cómo expresar los anillos de matrices $M_n(R)$ de orden n, con R anillo conmutativo o cuerpo, como suma de tres matrices especiales (matrices idempotentes o involutivas).

La tesis está estructurada de la siguiente manera: en la primera parte se introducen algunas definiciones básicas sobre los espacios vectoriales, los anillos y los cuerpos, conceptos necesarios en el desarrollo de este trabajo y lograr que el mismo sea de autocontenido. En el segundo capítulo se hace un repaso sobre las formas canónicas y su relación con las matrices cuadradas. Finalmente, en el último capítulo se demuestran en detalle los resultados principales de Tang [1].

[1] Gaohua Tang, Yiqiang Zhou y Huadong Su. «Matrices over a commutative ring as sums of three idempotents or three involutions». En: *Linear and Multilinear Algebra* 67.2 (2019), págs. 267-277. DOI: 10.1080/03081087.2017.1417969.

2. Preliminares

Recuerde que una operación binaria sobre un conjunto S es una aplicación $\circ : S \times S \to S$ que asigna a cada par $(s,t) \in S \times S$ el elemento $s \circ t \in S$, i.e, S es cerrada bajo dicha operación.

Definición 2.0.1. *Un **anillo** R es un conjunto no-vacío con dos operaciones binarias, usualmente denotadas por "$+$" y "$\cdot$", i.e,*

$$+ : (a,b) \longmapsto a+b \qquad \textit{y} \qquad \cdot : (a,b) \longmapsto a \cdot b, \quad \textit{(por brevedad, } a \cdot b = ab),$$

tales que:

1. $(R,+)$ *es un grupo abeliano*[*]*.*
2. $(R,\cdot)$ *es un semigrupo, i.e.,* $ab \in R$ *y* $(ab)c = a(bc)$ *para todo* $a,b,c \in R$
3. *Se cumple la ley distributiva del producto respecto a la suma, i.e., para todo* $a,b,c \in R$ *se verifican*

$$a(b+c) = ab + ac \qquad \textit{y} \qquad (b+c)a = ba + ca.$$

Ahora bien, un anillo R es llamado *conmutativo*, si para $a,b \in R$ se tiene que $ab = ba$. Si en R existe $1 = 1_R$ tal que para todo $a \in R$, $a1 = 1a = a$, se dice que R es un *anillo con unidad* o *anillo unitario*. Por otro lado, a un elemento no-cero $a \in R$ se le llama *divisor de cero*, si existe $b \in R$ no-cero tal que $ab = 0$. Se denotará por $\mathcal{ZD}(R)$ al conjunto de todos los divisores de cero de R.

De lo anterior es posible definir algunos tipos especiales de anillo.

Definición 2.0.2. *Sea R un anillo.*

1. *Si R es conmutativo con unidad y sin divisores de cero, R es llamado dominio entero.*
2. *Si en R todo elemento no nulo es invertible, R es llamado anillo de división. Si además, R es conmutativo R es llamado cuerpo y usualmente se denota por $R = \mathbf{F}$ (por su nombre en inglés).*

A continuación algunos ejemplos que clarifican los conceptos anteriores.

Ejemplo 2.0.3.

[*] El adjetivo abeliano es en honor al matemático noruego Niels Henrik Abel (1802-1829), quien usó estos grupos para estudiar las ecuaciones algebraicas que pueden resolverse por radicales.

1. *El anillo $\mathbb{Z}_p$ de los enteros módulo p, con p primo, es un dominio entero, puesto que al tomar $a, b \in \mathbb{Z}_p$ tales que $ab = 0$, sigue que $ab \equiv 0 \pmod{p}$, i.e, $p \mid ab$ y del Lema de Euclides, $p \mid a$ ó $p \mid b$. Por tanto, $a \equiv 0 \pmod{p}$ ó $b \equiv 0 \pmod{p}$ y así, $a = 0$ ó $b = 0 \in \mathbb{Z}_p$. Por otro lado, si $n \in \mathbb{N}$ es tal que $n = kt$, $0 < k, t < n$, entonces $kt = 0$ en $\mathbb{Z}_n$, i.e, si $n \in \mathbb{N}$ es compuesto $\mathbb{Z}_n$ siempre tiene divisores de cero.*

2. *De acuerdo con el Teorema 13.2 de Gallian [1] (2021, p. 239), todo dominio entero finito es cuerpo y así, del ejemplo anterior $\mathbb{Z}_p$ con p primo es un cuerpo.*

Note que $4x = 0$, para todo $x \in \mathbb{Z}_4$, mientras que en $\mathbb{Z}$ no existe $n \in N$ tal que $nk = 0$, para todo $k \in \mathbb{Z}$. Lo anterior motiva la siguiente definición.

Definición 2.0.4. *La característica de un anillo R es el menor entero positivo n tal que $nx = 0$, para todo $x \in R$. Si dicho entero no existe, se dice que R tiene característica 0. La característica de R se denotará por $car(R)$.*

A continuación algunas observaciones del concepto de característica.

Observación 1.

1. *Es posible demostrar, (véase Teorema 13.3, p. 241, en [1]), que dado R anillo con unidad 1, si 1 no tiene orden aditivo finito, entonces $car(R) = 0$. En caso contrario, i.e., si $n \cdot 1 = 0$, para algún $n \in N$, se sigue que $car(R) = n$.*

2. *Según el Teorema 13.4, pág. 241 de [1] , si R es un dominio entero entonces $car(R) = 0$ ó $car(R) = p$, donde p es un entero primo . De lo anterior se concluye que los cuerpos tienen característica 0 ó p.*

3. *Un anillo R es llamado* **anillo de Boole***, si todos los elementos son idempotentes, i.e, $a^2 = a$, para todo $a \in R$. Además, en este caso R es anillo conmutativo y $car(R) = 2$. De hecho, para todo $a \in R$, $(a+a)^2 = a+a$ y así, $a^2+2a+a^2 = a+a$, i.e., $2a = 0$, para todo $a \in R$ o, en otras palabras, $a = -a$ y por tanto $car(R) = 2$. Usando el mismo argumento para el elemento $a + b$, con $a, b \in R$, se sigue $ab + ba = 0$ y así, para todo $a, b \in R$, $ab = ba$, y R es conmutativo.*

Recuerde que un subconjunto no vacío S de un anillo R es llamado subanillo si él mismo es un anillo al restringir las operaciones de R a S. En este caso se denotará por $S \preceq_{sub.} R$. Además, si $I \preceq_{sub.} R$ y verifica que para todo $a \in I$ y todo $r \in R$ $ar, ra \in I$, I es llamado *ideal bilateral*, denotado $I \triangleleft R$. A los ideales $\{0\}$ y R se les llamarán *triviales*. Todo ideal $\{0\} \neq I$ de R anillo con unidad es llamado **ideal propio**.

Existen algunos tipos interesantes de ideales, entre los cuales se destacan los siguientes.

[1] J. Gallian. *Contemporary abstract algebra*. Chapman y Hall/CRC, 2021.

Definición 2.0.5. *Sean R un anillo conmutativo con unidad, $\mathfrak{p}$ y $\mathfrak{m}$ ideales propios de R.*

1. *$\mathfrak{p}$ es llamado ideal primo, si para todo $a, b \in R$ con $ab \in \mathfrak{p}$, se tiene que $a \in \mathfrak{p}$ o $b \in \mathfrak{p}$.*

2. *$\mathfrak{m}$ es llamado ideal maximal, si para todo ideal J tal que $\mathfrak{m} \subseteq J \subseteq R$, implica que $J = \mathfrak{m}$ ó $J = R$.*

Ahora, dado un anillo R e I ideal de R el conjunto $R/I = \{a + I : a \in R\}$, con suma $(a + I) + (b + I) = (a + b) + I$, $a, b \in R$ tiene estructura de grupo abeliano y junto al producto $(a + I)(b + I) = (ab) + I$, $a, b \in R$ dan a R/I estructura de anillo, denominado **anillo cociente**.

A continuación se introducen algunos otros elementos y subconjuntos distinguidos de un anillo.

Definición 2.0.6. *Sea R un anillo con unidad, un elemento $a \in R$, a es llamado nilpotente si $a^n = 0$, para algún $n > 1$. Al conjunto de todos sus elementos nilpotentes se le llama el* **nilradical** *de R y se le denota por η_R, i.e, $\eta_R = \{a \in R : a^n = 0, \exists\, n > 1\}$.*

Observación 2. *Sean R un anillo conmutativo con unidad, I un ideal de R, $Spec(R)$ y $Specm(R)$ los conjuntos de todos los ideales primos y maximales, respectivamente de R, i.e, $Spec(R) = \{\mathfrak{p} \leq R : \mathfrak{p}$-ideal primo $\}$ y $Specm(R) = \{\mathfrak{m} \leq R : \mathfrak{m}$-ideal maximal $\}$.*

1. *Para ideales primos y maximales se conoce el siguiente resultado. Sean $\mathfrak{p}, \mathfrak{m}$ ideales propios del anillo conmutativo R. Entonces:*
   a) *$\mathfrak{p} \in Spec(R)$ si y solo si, $R/\mathfrak{p}$ es un dominio entero (ver [1],Teorema 14.3, pág. 285).*
   b) *$\mathfrak{m} \in Specm(R)$ si y solo si, $R/\mathfrak{m}$ es un cuerpo, (ver [1],Teorema 14.4, pág. 286).*

2. *De acuerdo con la Proposición 1.8, página 5 de Atiyah [2], es posible demostrar que el nilradical de un anillo conmutativo R es la intersección de todos los ideales primos de R , i.e., $\eta_R = \bigcap_{\mathfrak{p} \in Spec(R)} \mathfrak{p}$.*

3. *Un ideal I es llamado **nil**, si todos los elementos son nilpotentes, i.e., para todos $x \in I$, existe un entero positivo n_x tal que $x^{n_x} = 0$. Además, I es **nil de exponente acotado**, si existe un entero positivo n tal que $x^n = 0$, para todo $x \in I$. Finalmente, el ideal I es llamado* **nilpotente**, *si $I^n = \{0\}$ para algún $n \in N$. Note que en este caso se tiene que existe $n \in N$ tal que $x_{i_1} x_{i_2} \cdots x_{i_n} = 0$, para todo $x_{i_1}, x_{i_2}, \cdots, x_{i_n} \in I$. En particular, si $x_{i_j} = x$, para $1 \leq j \leq n$, entonces $x^n = 0$, para todo $x \in I$. Lo que demuestra que todo ideal nilpotente es nil.*

[2] Michael Francis Atiyah y Ian Grant Macdonald. *Introducción al álgebra conmutativa*. Reverté, 1989.

4. *No todo ideal nil es nilpotente. En efecto, considere* $R = \bigoplus_{i\geq 1} \mathbb{Z}/(p^i)$ *la suma directa de los anillos* $\mathbb{Z}/(p^i)$*, donde* p *es un número primo. Note que* R *contiene elementos nilpotentes no-cero, como por ejemplo* $(0+(p),\ p+(p^2),\ 0+(p^3),\ldots)$*. Sea* I *el conjunto de todos los elementos nilpotentes de* R*. Como* R *es anillo conmutativo, sigue de la Observación 2 que* I *es un ideal y por tanto, un ideal nil. Sin embargo,* I *no es nilpotente, dado que si existe un entero* $k > 1$ *tal que* $I^k = 0$*, entonces el elemento*

$$x = \big(0+(p), 0+(p^2), 0+(p^k), p+(p^{k+1}), 0+(p^{k+2}), \cdots\big),$$

es nilpotente y por tanto $x \in I$*. No obstante,* $x^k \neq 0$*, lo cual es una contradicción y se sigue que* I *no es nilpotente.*

Recuerde que el radical de Jacobson $J(R)$ de un anillo R es la intersección de todos los ideales maximales de R. Además, de la *Proposición. 1.9, página 6* de Atiyah[2], un elemento $a \in R$ pertenece a $J(R)$ si, y sólo si, $1 - ax$ es una unidad del anillo, para todo $x \in R$, .

Los cuerpos presentan el rasgo particular que $\mathcal{O} = \{0\}$ es su único ideal maximal. Lo anterior motiva la siguiente definición.

Definición 2.0.7. *Un anillo conmutativo* R *es llamado* **anillo local** *si, y solo si,* R *tiene exactamente un único ideal maximal* $\mathfrak{m}$*. Al cuerpo* $\mathbf{k} = R/\mathfrak{m}$ *se le llamará cuerpo residual de* R*.*

Ejemplo 2.0.8. *Un anillo* R *con* 1 *donde cada elemento es una unidad o un nilpotente es un anillo local. En efecto, considere el conjunto* $I = \{r \in R : r$ *no es unidad* $\}$*. Por hipótesis, para todo* $r \in I$*,* r *es nilpotente, por la Proposición. 1.7, página 5 de [2],* I *es un ideal de* R *. Note que* $1 \notin I$*, luego* I *es un ideal propio. Por construcción, para cada* $x \in R \setminus I$*,* x *es unidad y de la Proposición. 1.6, página 5 de [2],* R *es anillo local.*

Ahora bien, un **homomorfismo** ϕ del anillo R hacia el anillo S, es una función $\phi : R \to S$ que preserva las operaciones, ie , para todo $a, b \in R$

$$\phi(a+b) = \phi(a) + \phi(b) \quad \text{y} \quad \phi(ab) = \phi(a)\phi(b).$$

Definición 2.0.9. *Un anillo R es* **indescomponible** *si no puede ser escrito como* $R \cong R_1 \times R_2$ *con* R_1 *ó* R_2 *anillos no cero.*

Ejemplo 2.0.10. *El anillo de los enteros* $\mathbb{Z}$*, los cuerpos* $\mathbf{F}$ *y el anillo de las matrices* $M_n(\mathbf{F})$ *con* $\mathbf{F}$ *cuerpo y* $n \geq 2$ *son ejemplos de anillos indescomponibles.*

En general para R un anillo, el conjunto:

$$M_n(R) = \big\{[a_{ij}] : a_{ij} \in R, i, j = 1, \cdots, n\big\},$$

de todas las matrices $n \times n$ con entradas en R, también es un anillo con la suma y producto usual de matrices. Más aún, si R tiene 1, entonces $1_{M_n(R)} = I_n$ la matriz identidad de orden n.

En particular, el anillo $M_2(\mathbb{Z})$ de matrices 2×2 con entradas enteras verifica para las matrices $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ y $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ que:

$$AB = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix} \neq BA = \begin{bmatrix} ae+fc & be+df \\ ag+ch & bg+dh \end{bmatrix}.$$

Además, si ahora A y B vienen dadas por $A = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ y $B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, se tiene que $AB = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \mathcal{O}$ y sin embargo, $A \neq \mathcal{O} \neq B$. En otras palabras, A y B son divisores de cero en $M_2(\mathbb{Z})$. De lo anterior es claro que los anillos de matrices $M_n(R)$, en general, no son ni conmutativos ni son dominios enteros y, solo tienen unidad en el que caso que $1 \in R$.

Definición 2.0.11. *Sea $A \in M_n(R)$ con R anillo.*

- *Una matriz A es llamada matriz* **triangular superior** *(análogamente* **triangular inferior***) si los elementos situados debajo (encima) de la diagonal principal son cero. Una* **matriz diagonal** *es aquella matriz donde todos los elementos situados por debajo y encima de la diagonal principal son nulos. Los siguientes ejemplos presentan matrices triangulares superiores, inferiores y diagonales de orden n con entradas $a_{ij} \in R$:*

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix}, \quad \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \quad y \quad \begin{bmatrix} a_{11} & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{nn} \end{bmatrix}.$$

- *Una* **Matriz escalar** *A es una matriz diagonal donde los elementos de la diagonal principal son iguales, i.e, para algún $a \in R$ dichas matrices tienen la forma:*

$$\begin{bmatrix} a & 0 & \cdots & 0 & 0 \\ 0 & a & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a & 0 \\ 0 & 0 & \cdots & 0 & a \end{bmatrix} = aI_n,$$

  donde I_n es la matriz identidad de orden n.

  Observación 3. *Las matrices escalares conmutan entre ellas. Más aún, si $A = aI_n$ para algún $n \in R$, $A \in \zeta\big(M_n(R)\big) = \big\{X \in M_n(R) : XB = BX, \forall\, B \in M_n(R)\big\}$, el centro del anillo $M_n(R)$. Es posible demostrar que $\zeta\big(M_n(R)\big) = \big\{aI_n : a \in \zeta(R)\big\}$.*

- *Una matriz cuadrada A se denomina* ***invertible****, si existe otra matriz llamada la matriz inversa, denotada por A^{-1}, tal que $AA^{-1} = A^{-1}A = I_n$. Algunos ejemplos*

de matrices invertibles son la matriz identidad I_n, las matrices diagonales no nulas y las matrices ortogonales, ver definición abajo.

- *Una **Matriz involutiva** es una matriz cuadrada que es su propia inversa, i.e, $A = A^{-1}$ o equivalentemente que $A^2 = I_n$. Algunas matrices involutivas para $M_2(\mathbb{Z})$, $M_3(\mathbb{Z})$ y $M_4(\mathbb{Z})$ son, respectivamente:*

$$\begin{bmatrix} 2 & 3 \\ -1 & -2 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 & 1 \\ -1 & 0 & -1 \\ -2 & -2 & -1 \end{bmatrix} \quad y \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

- *Una* **Matriz ortogonal** A *es una matriz cuadrada cuya inversa coincide con su transpuesta, i.e, $A^{-1} = A^t$. Una matriz $A \in M_2(\mathbb{R})$ que sirve de ejemplo es la matriz de rotación para un ángulo θ:*

$$A = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}.$$

Observación 4. *Es posible demostrar que las matrices triangulares superiores, inferiores y diagonales con coeficientes un anillo R, con la suma y el producto usual de matrices, son anillos.*

Dada una matriz cuadrada $A \in M_n(\mathbf{F})$ con $\mathbf{F}$ cuerpo, existen varias nociones fundamentales asociadas a su estructura algebraica. En primer lugar, la **traza** de A, denotada por $tr(A)$, se define como la suma de los elementos de su diagonal principal, i.e, $tr(A) = \sum_{i=1}^{n} a_{ii}$. Por otro lado, el **rango** de A, denotado $ran(A)$, es el número de pivotes que aparecen en su forma escalonada por renglones, lo cual equivale al número de filas (o columnas) linealmente independientes.

Dado un anillo conmutativo R, el conjunto de símbolos $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R,\ n$ es un número entero no negativo$\}$ se llama el **anillo de polinomios sobre** R. Las operaciones de suma y multiplicación que hacen de $R[x]$ un anillo son las mismas operaciones conocidas del álgebra elemental, i.e, la suma es:

$$(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)$$

$$= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x + (a_0 + b_0),$$

(a_n o b_n pueden ser cero para que tenga sentido la suma de polinomios de distintos grados).

La multiplicación se realiza primero definiendo $(ax^i)(bx^j) = abx^{i+j}$ para polinomios con un solo término no nulo, y luego extendiéndola a todos los polinomios mediante las leyes distributivas:

$$(a_0+a_1x+a_2x^2+\cdots)(b_0+b_1x+b_2x^2+\cdots) = a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\cdots$$

(En general, el coeficiente de x^k en el producto será $\sum_{i=0}^{k} a_i b_{k-i}$).

Dada una matriz $A \in M_n(\mathbf{F})$, con $\mathbf{F}$ cuerpo, se define el **polinomio característico** $\chi_A(x)$ de la matriz $A \in M_n(\mathbf{F})$ como $\chi_A(x) = \det(A - xI) \in \mathbf{F}[x]$. Note que χ_A es un polinomio que anula a A, i.e, $\chi_A(A) = 0$. Entre todos los polinomios con coeficientes en $\mathbf{F}$ que anulan a A existe un único polinomio mónico de *menor grado* con esta propiedad y se le llamará el **polinomio minimal** de A, denotado por $m_A(x)$.

Ejemplo 2.0.12.

1. *Considere la matriz diagonal* $A = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$*. Calculando su polinomio característico se obtiene que*

$$\chi_A(x) = \det\left(\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} - x\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = \det\left(\begin{bmatrix} 2-x & 0 \\ 0 & 2-x \end{bmatrix}\right),$$

$$\chi_A(x) = (2-x)(2-x) = (2-x)^2 = x^2 - 4x + 4$$

Buscando el polinomio mónico de menor grado que anule A*, considere el polinomio* $q(x) = x - 2$*. Así:*

$$q(A) = A - 2I = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} - 2\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} - \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Dado que $q(A) = 0$*,* $q(x) = x - 2$ *es mónico y es de grado 1, se concluye que el polinomio minimal de* A *es* $m_A(x) = x - 2$*.*

2. *Sea la matriz* $B = \begin{bmatrix} 4 & 1 \\ 0 & 4 \end{bmatrix}$*, con polinomio característico* $\chi_B(x) = \det(B - xI) = \begin{vmatrix} 4-x & -1 \\ 0 & 4-x \end{vmatrix} = (4-x)^2$*. Ahora suponga que el polinomio mínimo es* $m_B(x) = 4 - x$*. Por definición,* $m_B(B) = B - 4I = 0$*, pero* $B - 4I = \begin{bmatrix} 4 & 1 \\ 0 & 4 \end{bmatrix} - \begin{bmatrix} 4 & 0 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \mathcal{O}$*. Observe que* $(B - 4I)^2 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$*. De lo anterior* $\chi_B(x) = m_B(x) = (4-x)^2$*.*

3. *Sea la matriz* $A = \begin{bmatrix} 4 & -2 & 4 \\ -2 & 1 & -2 \\ 4 & -2 & 4 \end{bmatrix}$*. Su polinomio característico es* $\chi_A(x) = -x^2(x-9)$*. Las posibles opciones para el polinomio minimal son:* $q_1(x) = x(x-9)$ *ó* $q_2(x) = x^2(x-9)$*.*

Calculando para $q_1(x)$*:*

$$A^2(A-9) = A^3 - 9A = \begin{bmatrix} 4 & -2 & 4 \\ -2 & 1 & -2 \\ 4 & -2 & 4 \end{bmatrix}^3 - 9\begin{bmatrix} 4 & -2 & 4 \\ -2 & 1 & -2 \\ 4 & -2 & 4 \end{bmatrix}$$
$$= \begin{bmatrix} 288 & -144 & 288 \\ -144 & 72 & -144 \\ 288 & -244 & 288 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

En cambio, para $q_2(x)$*:*

$$A(A-9) = A^2 - 9A = \begin{bmatrix} 36 & -18 & 36 \\ -18 & 9 & -18 \\ 36 & -18 & 36 \end{bmatrix} - 9\begin{bmatrix} 4 & -2 & 4 \\ -2 & 1 & -2 \\ 4 & -2 & 4 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

De lo anterior $m_A(x) = x(x-9)$.

Sea $\mathbf{F}$ un cuerpo y considere $A, B \in M_n(\mathbf{F})$. Se dice que A y B son **similares**, denotado por $A \sim B$, si existe $P \in M_n(\mathbf{F})$ invertible tal que $B = P^{-1}AP$.

Ejemplo 2.0.13. *Al considerar las matrices* $A = \begin{bmatrix} 5 & 2 \\ 0 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 5 & 4 \\ 0 & 3 \end{bmatrix}$, $P = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *y* $P^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$*. Se dice que* $A \sim B$ *puesto que:*

$$B = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 5 & 2 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 5 & -1 \\ 0 & 3 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 4 \\ 0 & 3 \end{bmatrix}.$$

A continuación se presentan algunas propiedades fundamentales que satisfacen las matrices semejantes.

Observación 5. *Sea* $\mathbf{F}$ *un cuerpo y* $A, B \in M_n(\mathbf{F})$ *tales que* $A \sim B$*. Entonces:*

- $ran(A) = ran(B)$.
- $det(A) = det(B)$.
- A *y* B *son ambas invertibles o ambas no invertibles.*
- $\chi_A = \chi_B$.
- *Para cada* $\lambda \in \mathbf{F}, \lambda I_n - A \sim \lambda I_n - B$.

La siguiente proposición permitirá ver bajo qué condiciones propiedades como la traza o el rango de una matriz cuadrada se preserva bajo similitud.

Observación 6. *Sean R un anillo conmutativo y $A, B \in M_n(R)$ tales que $A \sim B$.*

- $tr(A) = tr(B)$. *Para ver esto recuerde que, para cualquier $X, Y \in M_n(R)$, $tr(XY) = tr(YX)$. Como $A \sim B$, existe $P \in M_n(R)$ invertible tal que $B = P^{-1}AP$, luego $tr(B) = tr(P^{-1}AP) = tr(P^{-1}PA) = tr(A)$.*
- *Si R es un anillo local se cumple que $ran(A) = ran(B)$. En efecto, Sea $\mathfrak{m}$ el único ideal maximal de R y sea $\mathbf{k} = R/\mathfrak{m}$ su cuerpo residual. Dado que $A \sim B$, existe una matriz invertible $P \in M_n(R)$ tal que $B = P^{-1}AP$. Al considerar la reducción módulo $\mathfrak{m}$, se obtiene que $\overline{B} = \overline{P^{-1}AP} = \overline{P}^{-1}\,\overline{A}\,\overline{P}$, i.e, $\overline{A} \sim \overline{B}$ en $M_n(\mathbf{k})$. Como $\mathbf{k}$ es un cuerpo, de la Observación 5 se sigue que $ran(\overline{A}) = ran(\overline{B})$. Por otra parte, dado que R es local, el rango de una matriz sobre R coincide con el rango de su reducción módulo $\mathfrak{m}$. En particular, se cumple que $ran(A) = ran(\overline{A})$ y $ran(B) = ran(\overline{B})$. De lo anterior $ran(A) = ran(B)$.*

Definición 2.0.14. *Sea $\mathbf{F}$ es un cuerpo y $A \in M_n(\mathbf{F})$. Una matriz A es* **diagonalizable** *si existe una matriz diagonal D y una matriz invertible $P \in M_n(\mathbf{F})$ tales que*

$$A = PDP^{-1}.$$

Ejemplo 2.0.15. *Dadas las matrices*

$$A = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 2 & 1 \\ 1 & 5 & 6 \end{bmatrix}, \quad P = \begin{bmatrix} 1 & -3 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix},$$

Note que $det(P) \neq 0$, por lo que P es invertible y además $D = P^{-1}AP$, i.e , $A \sim D$ y, más aún, D es una matriz diagonal cuyas entradas en su diagonal principal son los valores propios de A.

Con el propósito de establecer un marco conceptual sólido y favorecer la comprensión de los resultados presentados en [3] y [4], se exponen a continuación una serie de definiciones fundamentales que constituyen la base teórica sobre la cual se apoyan dichos desarrollos. Estas nociones resultarán esenciales para la formulación y justificación de las demostraciones centrales incluidas en el Capítulo 3.

Dado $P = x^n - \sum_{k=0}^{n-1} a_k x^k \in \mathbf{F}[X]$ un polinomio mónico de grado n. Su **matriz compañera** $C(P)$ es

[3] Clément de Seguins Pazzis. «On decomposing any matrix as a linear combination of three idempotents». En: *Linear algebra and its applications* 433.4 (2010), págs. 843-855. DOI: 10.1016/j.laa.2010.04.017.

[4] Clément de Seguins Pazzis. «On sums of idempotent matrices over a field of positive characteristic». En: *Linear algebra and its applications* 433.4 (2010), págs. 856-866. DOI: 10.1016/j.laa.2010.04.018.

$$C(P) := \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & a_{n-2} \\ 0 & \cdots & 0 & 1 & a_{n-1} \end{bmatrix},$$

cuyo polinomio característico es precisamente P y también es su polinomio minimal. Se define $tr(P) := tr(C(P)) = a_{n-1}$, y $\deg(P) = n$ (el grado de P).

Dada una lista $(A_1, \ldots, A_p)$ de matrices cuadradas, se denotará por

$$D(A_1, \ldots, A_p) := \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \\ 0 & \cdots & \cdots & A_p \end{bmatrix},$$

A la matriz en bloques diagonal con bloques diagonales $A_1, \ldots, A_p$. Además, $H_{n,p}$ denotará la matriz elemental:

$$H_{n,p} := \begin{bmatrix} 0 & \cdots & 0 & 1 \\ \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 \end{bmatrix} \in M_{n,p}(\mathbf{F}),$$

con único coeficiente no nulo ubicado en la primera fila y la columna p.

Para $k \in N^*$, se define $F_k := D(0, \ldots, 0, 1) \in M_k(\mathbf{F})$.

Es un resultado conocido que, cuando P y Q son polinomios mónicos primos entre sí, se cumple que

$$C(PQ) \sim \begin{bmatrix} C(P) & 0 \\ 0 & C(Q) \end{bmatrix}.$$

Sea $A \in M_n(\mathbf{F})$. Se dirá que una matriz A es **cíclica** cuando $A \sim C(P)$ para algún polinomio P (y entonces $P = \chi_A$). Una **buena matriz cíclica** es una matriz de la forma

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & \cdots & a_{1,n} \\ 1 & a_{2,2} & \ddots & \cdots & \vdots \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \cdots & 0 & 1 & a_{n,n} \end{bmatrix},$$

sin ninguna condición sobre los $a_{i,j}$ para $j \geq i$.

El siguiente lema será de vital importancia a la hora de comprender la demostración presente en la Proposición 4.1.6. Para una exposición detallada y rigurosa de la demostración de este lema, puede consultarse en el *Lema 11, página 848* de [3].

Lema 2.0.16. *(Lema de elección de polinomio). Sea $A \in M_n(\mathbf{F})$ y $B \in M_r(\mathbf{F})$ dos matrices cíclicas buenas, y sea P un polinomio mónico de grado $n + r$ tal que $tr(P) =$*

$tr(A) + tr(B)$. *Entonces existe una matriz* $D \in M_{n,r}(\mathbf{F})$ *tal que*

$$\begin{bmatrix} A & D \\ H_{r,n} & B \end{bmatrix} \sim C(P).$$

Definición 2.0.17. *Sea* $\mathbf{F}$ *un cuerpo tal que* $car(\mathbf{F}) = p \neq 0$ *y sea* $\mathcal{A}$ *una* $\mathbf{F}$*-álgebra y* $(\alpha_1, \ldots, \alpha_n) \in (\mathbf{F}^*)^n$*. Un elemento* $x \in \mathcal{A}$ *se llama un* $(\alpha_1, \ldots, \alpha_n)$-compuesto *si existen idempotentes* $p_1, \ldots, p_n$ *tales que*

$$x = \sum_{k=1}^{n} \alpha_k \cdot p_k.$$

Ejemplo 2.0.18.

- *La matriz* $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in M_2(\mathbb{Z}_3)$ *es un* $(1, -1)$*-compuesto. En efecto, si* $P_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, P_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ *entonces* $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = P_1 - P_2$*, ya que* $-1 \equiv 2 \mod 3$*.*
- *En* $M_2(\mathbb{Z}_3)$*, considerando los mismos idempotentes del ejemplo anterior, sigue que la matriz* $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ *es un* $(2, 1)$*-compuesto, dado que* $A = 2P_1 + P_2$*.*
- *Al considerar la matriz* $A = \begin{bmatrix} 2 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \in M_3(\mathbb{Z}_3)$*, se dice que* A *es un* $(1, 1, -1)$*-compuesto porque las matrices idempotentes* $P_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$*,* $P_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ *y* $P_3 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ *verifican que* $A = P_1 + P_2 - P_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} -1 & -1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 2 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \pmod 3$.

3. Formas Canónicas

En este capítulo se presentan algunos conceptos conocidos asociados a *Formas Canónicas*, los cuales no son parte de los contenidos de los cursos de Álgebra de pregrado y que son necesarios para el desarrollo de la presente monografía.

3.1. La forma canónica racional

La forma canónica racional de una matriz es una representación que permite expresar una matriz cuadrada como una combinación de bloques estructurados que reflejan sus propiedades algebraicas esenciales. Este tipo de matrices son importantes porque permiten clasificar matrices vía semejanza sin requerir que el cuerpo sea algebraicamente cerrado, proporcionando una herramienta poderosa para el estudio estructural de operadores lineales. A continuación se enunciarán algunas definiciones y resultados extraídos del *Capítulo 12* del libro de Dummit y Foote [1].

Teorema 3.1.1. *Sean $\mathbf{F}$ un cuerpo y $A \in M_n(\mathbf{F})$*

1. *La matriz A es similar a una matriz en* **forma canónica racional***, i.e, existe una matriz invertible $P \in M_n(\mathbf{F})$ tal que $P^{-1}AP$ es una matriz diagonal por bloques, donde cada bloque diagonal es una matriz compañera de polinomios mónicos $a_1(x), a_2(x), \ldots, a_m(x)$ de grado al menos uno, y tales que $a_1(x) \mid a_2(x) \mid \cdots \mid a_m(x)$. Los polinomios $a_i(x)$ son llamados* **factores invariantes** *de la matriz.*
2. *La forma canónica racional es única.*

Definición 3.1.2. *Los factores invariantes de una matriz $n \times n$ sobre un cuerpo $\mathbf{F}$ son los factores invariantes de su forma canónica racional.*

Teorema 3.1.3. *Sean $A, B \in M_n(\mathbf{F})$. Entonces $A \sim B$ si y solo si A y B tienen la misma forma canónica racional.*

La próxima proposición muestra cómo se relaciona el polinomio característico de una matriz con sus factores invariantes, lo cual es especialmente útil para identificarlos en el caso de matrices pequeñas.

Lema 3.1.4. *Sea $a(x) \in \mathbf{F}[x]$ un polinomio mónico cualquiera.*

1. *El polinomio característico de la matriz compañera de $a(x)$ es $a(x)$.*

[1] David Steven Dummit, Richard M Foote et al. *Abstract algebra*. Vol. 3. Wiley Hoboken, 2004.

2. *Si M es la matriz diagonal por bloque*

$$M = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_k \end{bmatrix},$$

dada por la suma directa de las matrices $A_1, A_2, \ldots, A_k$, entonces el polinomio característico de M es el producto de los polinomios característicos de $A_1, A_2, \ldots, A_k$, i.e. $\chi_M = \prod_{i=1}^{k} \chi_{A_i}$.

Ejemplo 3.1.5.

- *Para buscar la forma canónica racional de la matriz $A = \begin{bmatrix} 1 & -2 & 10 \\ 0 & 2 & 6 \\ 0 & 0 & 2 \end{bmatrix}$ se calcula el polinomio característico $\chi_A(x) = det(A - xI) = (x-1)(x-2)^2$. Luego, los candidatos a ser el polinomio minimal son $q_1(x) = (x-1)(x-2)$ ó $q_2(x) = (x-1)(x-2)^2$. Rápidamente $m_A(x) = (x-1)(x-2)^2 = x^3 - 5x^2 + 8x - 4$, dado que*

$$m_A(A) = (A-I)(A-2I)^2 = \begin{bmatrix} 1-1 & -2 & 10 \\ 0 & 2-1 & 6 \\ 0 & 0 & 2-1 \end{bmatrix} \begin{bmatrix} 1-2 & -2 & 10 \\ 0 & 2-2 & 6 \\ 0 & 0 & 2-2 \end{bmatrix}^2$$
$$= \begin{bmatrix} 0 & -2 & 10 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & -2 & 10 \\ 0 & 0 & 6 \\ 0 & 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Como $\chi_A = m_A$, se sigue que la forma canónica racional de A es la matriz compañera de m_A, i.e,

$$C(m_A) = \begin{bmatrix} 0 & 0 & 4 \\ 1 & 0 & -8 \\ 0 & 1 & 5 \end{bmatrix}.$$

- *Si $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}$, se sigue que $\chi_B(x) = det(B - xI) = (x-1)(x-2)^2 \neq (x-1)(x-2) = m_B(x)$. Como $\chi_B \neq m_B(x)$ y $\frac{\chi_B}{m_B} = \frac{(x-1)(x-2)^2}{(x-1)(x-2)} = (x-2)$, los factores invariantes serán $x-2$ y $(x-1)(x-2) = x^2 - 3x + 2$. Así, las matrices compañeras respectivas asociadas a los factores invariantes vienen dadas por*

$$C(x-2) = [2] \qquad \text{y} \qquad C(x^2 - 3x + 2) = \begin{bmatrix} 0 & -2 \\ 1 & 3 \end{bmatrix}.$$

De esta manera, la forma canónica racional de la matriz A es $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{bmatrix}$.

3.1.1. Matrices cuadradas y matrices en forma canónica racional El propósito de esta sección es exponer algunos resultados fundamentales del álgebra lineal que permitirán establecer rigurosamente la relación entre las matrices cuadradas y su forma canónica racional. Para ello, se presentan algunas definiciones y proposiciones tomadas de [2].

Sea $A = [a_{ij}]$ una matriz de orden $n \geq 1$. Se dice que A es una matriz **diagonal en bloques** si $n = 1$ o si para $n \geq 2$ existen $r \geq 2$ enteros positivos $k_1, \ldots, k_r$ tales que A es de la forma

$$A = \begin{bmatrix} A_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A_r \end{bmatrix}, \tag{1}$$

donde A_i es una matriz de orden k_i. Note que $2 \leq r \leq n$, $1 \leq k_i \leq n-1$, $1 \leq i \leq r$.

Recuerde que una transformación lineal $T : V \to V$ de un espacio V de dimensión finita $n \geq 1$ es *diagonalizable en bloques* si existe una base para V tal que la matriz de T en dicha base es diagonal en bloques. Además, una matriz cuadrada A de orden $n \geq 1$ es **diagonalizable en bloques** si A es similar a una matriz diagonal en bloques.

A continuación algunas propiedades iniciales de las trasformaciones diagonalizables.

Observación 7.

1. *Si T es una transformación lineal de un espacio de dimensión 1, entonces T es trivialmente diagonalizable en bloques.*
2. *Sea $T : V \to V$ una transformación lineal de un espacio V de dimensión finita $n \geq 1$. Sea $\mathcal{X}$ una base cualquiera de V. Entonces, T es diagonalizable en bloques si y sólo si $M_{\mathcal{X}}(T)$ es diagonalizable en bloques.*
3. *Sea $T : V \to V$ una transformación lineal de un espacio V de dimensión finita $n \geq 2$. Entonces, T es diagonalizable en bloques si y sólo si V es suma directa de $2 \leq r \leq n$ subespacios invariantes no triviales.*

Sea V un espacio vectorial de dimensión finita $n \geq 1$, $T : V \to V$ una transformación lineal y v un vector cualquiera de V. El conjunto $[v]_T = \{p(T)(v) \mid p(x) \in K[x]\}$ es, claramente, el menor subespacio invariante de V que contiene el vector v; este subespacio se conoce con el nombre de el **T-subespacio cíclico generado por v**. Cuando no haya lugar a confusión, se dirá simplemente que $[v]$ es el subespacio cíclico generado por el vector v.

Note que $[v]_T = \langle T^k(v) \mid k \geq 0 \rangle$ Más exactamente $[v]_T = \langle T^k(v) \mid 0 \leq k \leq m-1 \rangle$, donde m es el grado del polinomio mínimo de la transformación T. El vector v se dice que es un **vector cíclico** de T si $[v]_T = V$. De manera similar se define el subespacio

[2] Lezama Serrano José Oswaldo. *Álgebra lineal*. 2020.

$[\alpha]_A$, donde A es una matriz cuadrada de orden $n \geq 1$ sobre el cuerpo $\mathbf{F}$ y α es un vector cualquiera de $\mathbf{F}^n$. En este contexto, α es un vector cíclico de la matriz A si $[\alpha]_A = \mathbf{F}^n$.

Proposición 3.1.6. *Sea $T : V \to V$ una transformación lineal de un espacio V de dimensión finita $n \geq 1$ y sea $X = \{v_1, \ldots, v_n\}$ una base de V. Entonces, el vector $v = c_1 v_1 + \cdots + c_n v_n$ es un vector cíclico de T si y sólo si $\alpha = (c_1, \ldots, c_n)$ es un vector cíclico de la matriz de T en la base X.*

Observación 8. *A continuación se presentan algunas propiedades de $[v]$.*

1. $[0] = 0$.
2. $\dim([v]) = 1$ *si, y solo si, v es un vector propio de T.*
3. *Sea $v \neq 0$, y $q_v(x)$ su polinomio anulador. Entonces* $\dim([v]) =$ *grado*$(q_v(x))$*. Más exactamente, si grado*$(q_v(x)) = k$*, entonces $\{v, T(v), \ldots, T^{k-1}(v)\}$ es una base de $[v]$.*
4. *Sea $T_{[v]}$ la restricción de T a $[v]$. Entonces, el polinomio mínimo de $T_{[v]}$ coincide con el anulador $q_v(x)$ del vector v.*
5. *Si v es un vector cíclico de T, entonces $q_v(x) = q_T(x) = p_T(x)$.*

Con fundamento en los resultados previamente establecidos, se enuncia a continuación el siguiente teorema. Una demostración completa y rigurosa de este resultado puede consultarse en el *Capítulo 6, Teorema 5* de [2].

Teorema 3.1.7. *(Teorema de Descomposición Cíclica) Sea $T : V \to V$ una transformación lineal de un espacio V de dimensión finita $n \geq 1$. Entonces existen $r \geq 1$ vectores no nulos $v_1, \ldots, v_r$ en V con polinomios anuladores $q_{v_1}(x), \ldots, q_{v_r}(x)$ tales que:*

a) $V = [v_1] \oplus \cdots \oplus [v_r]$

b) $q_{v_1}(x) \mid q_{v_2}(x) \mid \cdots \mid q_{v_r}(x), \quad 1 \leq i \leq r-1.$

c) $q_{v_1}(x) = q_T(x)$.

Además, el entero r y los polinomios anuladores $q_{v_1}(x), \ldots, q_{v_r}(x)$ están ***unívocamente determinados*** *por a) y b); i.e, si existen otros vectores no nulos $w_1, \ldots, w_s$ con anuladores $q_{w_1}(x), \ldots, q_{w_s}(x)$ tales que se cumplen a) y b), entonces $r = s$ y $q_{v_i}(x) = q_{w_i}(x)$ para cada $1 \leq i \leq r$.*

Nótese que, por el Teorema de Descomposición Cíclica, existe un vector v_1 en V tal que $q_{v_1}(x)$ coincide con el polinomio mínimo de T. Esta observación y el hecho que $\dim([v_1]) =$ grado$(q_{v_1}(x))$, permite entonces sacar las siguientes conclusiones.

Corolario 3.1.8. *Sea $T : V \to V$ una transformación lineal de un espacio V de dimensión $n \geq 1$. Entonces,*

a) Existe un vector v_1 en V tal que $q_{v_1}(x)$ coincide con el polinomio mínimo de T.

b) T tiene un vector cíclico si y solo si $p_T(x) = q_T(x)$.

Las mismas afirmaciones son válidas para matrices.

Proposición 3.1.9. *Sea A una matriz cuadrada de orden $n \geq 1$. Si A es la matriz compañera de un polinomio mónico $p(x)$, entonces $p(x)$ es el polinomio mínimo y característico de la matriz A.*

La proposición que se presenta a continuación constituye el objetivo principal de esta sección, en tanto que establece, de manera rigurosa, la relación entre toda matriz cuadrada y su correspondiente forma canónica racional. Dicho resultado adquiere especial relevancia, pues servirá como fundamento esencial para la demostración de la Proposición 4.1.6 y el Teorema 4.

Proposición 3.1.10. *Toda matriz cuadrada B de orden $n \geq 1$ es similar a una y sólo una matriz racional de la forma (1) descrita arriba. Los polinomios mónicos $p_1(x), \ldots, p_r(x)$ se conocen como los **factores invariantes** de la matriz B.*

Demostración. Sea Y la base canónica de $\mathbf{F}^n$ y $T : \mathbf{F}^n \to \mathbf{F}^n$ una transformación lineal tal que B es la matriz de T en la base Y. Sea A una matriz racional de la forma (1) similar a la matriz B. Existe entonces una base X en K^n tal que $A = m_X(T)$. Se demostrará que $\mathbf{F}^n$ tiene una descomposición cíclica en la forma

$$\mathbf{F}^n = [v_1] \oplus \cdots \oplus [v_r].$$

En efecto, si la matriz racional A tiene un solo bloque, entonces según la Proposición 3.1.9 y el Corolario 3.1.8, T tiene un vector cíclico y así $\mathbf{F}^n = [v]$. Si el número de bloques de A es $r \geq 2$, entonces de acuerdo a la Proposición 7(3), $\mathbf{F}^n$ se descompone en la forma

$$\mathbf{F}^n = W_1 \oplus \cdots \oplus W_r,$$

de tal manera que si T_i es la restricción de T a W_i y X_i es una base de W_i, el bloque A_i de A es $A_i = m_{X_i}(T_i)$. Aplicando nuevamente la Proposición 3.1.9 y el Corolario 3.1.8, se obtiene que W_i tiene un vector cíclico no nulo v_i, de donde $W_i = [v_i]$, $1 \leq i \leq r$. Esto completa la prueba de la descomposición enunciada arriba.

Si B fuese similar a otra matriz racional C, entonces $\mathbf{F}^n$ tendría otra descomposición *cíclica*, pero por la unicidad del *Teorema de Descomposición Cíclica* se tiene que $C = B$. □

3.2. La forma reducida de Jordan

Como ya se expresó anteriormente, la forma canónica racional permite expresar una matriz como equivalente a una forma compuesta por bloques controlados por su

polinomio mínimal. Cuando el cuerpo base es algebraicamente cerrado, esta forma puede refinarse aún más: cada bloque cíclico asociado a un factor lineal del polinomio mínimo se reemplaza por un bloque de Jordan. Así, la forma de Jordan se presenta como una descomposición más precisa que refleja tanto la estructura algebraica como la geométrica de la matriz.

Definición 3.2.1. *La matriz $k \times k$ denotada por $j_k(\lambda)$ con λ en la diagonal principal y 1 en la primera superdiagonal se llama* **matriz de Jordan** *elemental de tamaño k con valor propio λ ó* **bloque de Jordan** *de tamaño k con valor propio λ.*

Ejemplo 3.2.2. *A continuación, se presentan algunos ejemplos ilustrativos de matrices de Jordan $j_k(\lambda)$ para distintos valores de λ y tamaños k.*

$$j_1(3) = \begin{bmatrix} 3 \end{bmatrix}, \qquad j_2(-1) = \begin{bmatrix} -1 & 1 \\ 0 & -1 \end{bmatrix},$$

$$j_3(0) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \qquad j_4(5) = \begin{bmatrix} 5 & 1 & 0 & 0 \\ 0 & 5 & 1 & 0 \\ 0 & 0 & 5 & 1 \\ 0 & 0 & 0 & 5 \end{bmatrix}.$$

Teorema 3.2.3. *Sea $\mathbf{F}$ un cuerpo y $A \in M_n(\mathbf{F})$, y supongamos que $\mathbf{F}$ contiene todos los valores propios de A.*

1. *La matriz A es similar a una matriz en forma canónica de Jordan; i.e, existe una matriz invertible $P \in M_n(\mathbf{F})$ tal que $P^{-1}AP$ es una matriz diagonal por bloques, cuyas bloques diagonales son los bloques de Jordan para los divisores elementales de A.*

2. *La forma canónica de Jordan para A es única salvo por una permutación de los bloques de Jordan a lo largo de la diagonal.*

Note que la forma canónica de Jordan difiere de una matriz diagonal únicamente por la posible presencia de unos (1) en la primera superdiagonal (y esto solo si existen bloques de Jordan de tamaño mayor que uno), por lo tanto, está lo más cerca posible de ser una matriz diagonal. El siguiente resultado muestra en particular que la forma de Jordan de una matriz A es tan cercana como sea posible a ser una matriz diagonal.

Corolario 3.2.4.

1. *Si una matriz A es similar a una matriz diagonal D, entonces D es la forma canónica de Jordan de A.*

2. *Dos matrices diagonales son similares si y solo si sus entradas diagonales son las mismas salvo por una permutación.*

El siguiente corolario da un criterio para determinar cuándo una matriz A puede ser diagonalizada.

Corolario 3.2.5. *Si $\mathbf{F}$ es un cuerpo, $A \in M_n(\mathbf{F})$ y $\mathbf{F}$ contiene todos los valores propios de A, entonces A es similar a una matriz diagonal sobre $\mathbf{F}$ si, y solo si, el polinomio minimal de A no tiene raíces repetidas.*

Ejemplo 3.2.6.

1. *Para calcular la forma canónica de Jordan de la matriz* $A = \begin{bmatrix} -2 & 1 & 4 \\ -5 & 2 & 5 \\ -1 & 1 & 3 \end{bmatrix}$, *se calcula su polinomio característico*

$$\chi_A = \det(A - \lambda I) = \begin{vmatrix} -2-\lambda & 1 & 4 \\ -5 & 2-\lambda & 5 \\ -1 & 1 & 3-\lambda \end{vmatrix} = \lambda^3 - 3\lambda^2 + 4 = (\lambda - 2)^2(\lambda + 1).$$

El subespacio propio asociado al valor propio -1 es el núcleo de $\begin{bmatrix} 1 & -1 & -4 \\ 5 & -3 & -5 \\ 1 & -1 & -4 \end{bmatrix}$, *el cual es un subespacio generado por* $\begin{bmatrix} 1 & 15 & -2 \end{bmatrix}^T$.

El subespacio propio asociado al valor propio 2 es el núcleo de $\begin{bmatrix} 4 & -1 & -4 \\ 5 & 0 & -5 \\ 1 & -1 & -1 \end{bmatrix}$, *el cual es un subespacio generado por* $\begin{bmatrix} 0 & 1 & 0 \end{bmatrix}^T$.

Estos cálculos de valores y vectores propios muestran que A no es diagonalizable. Ahora, note que $A \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix} = 2 \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$. *Sea* $P = \begin{bmatrix} 1 & 1 & 7 \\ 0 & 1 & 15 \\ 1 & 1 & -2 \end{bmatrix}$, *entonces la forma canónica de Jordan de A es* $J = P^{-1}AP = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{bmatrix}$.

2. *Para la matriz* $A = \begin{bmatrix} 0 & 3 & 1 \\ 2 & -1 & -1 \\ -2 & -1 & -1 \end{bmatrix}$, *su polinomio característico es* $\det(A - xI) = -(x+2)^2(x-2)$. *Entonces, los valores propios son: $x = -2$ (con multiplicidad algebraica 2) y $x = 1$ (con multiplicidad algebraica 1).*

   Calculando los espacios propios:

$$A + 2I = \begin{bmatrix} 2 & 3 & 1 \\ 2 & 1 & 1 \\ -2 & -1 & 1 \end{bmatrix} \quad \text{, y así} \quad \dim(\ker(A + 2I)) = 1.$$

$$A - 2I = \begin{bmatrix} -2 & 3 & 1 \\ 2 & -3 & -1 \\ -1 & 2 & -1 \end{bmatrix}$$ *, de esta manera* $\dim(\ker(A - 2I)) = 1$

De lo anterior se deduce que los valores propios $x = -2$ *y* $x = 2$ *presentan multiplicidad geométrica igual a* 1*. Sin embargo, para* $x = -2$ *la multiplicidad geométrica no coincide con la multiplicidad algebraica y, por tanto, es necesario construir un vector propio generalizado siguiendo el procedimiento ilustrado en el ejemplo anterior. En consecuencia, al determinar la forma canónica de Jordan, este proceso corresponde ubicar un* 1 *en la posición inmediatamente superior al segundo valor propio asociado a* $x = -2$*, i.e,*

$$J = \begin{bmatrix} -2 & 1 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

3. *Al considerar la matriz* $A = \begin{bmatrix} -2 & 1 & -1 \\ -1 & -1 & 0 \\ 0 & 1 & -3 \end{bmatrix}$*, note que* $\chi_A(x) = (x+2)^3$ *y su único valor propio es* $x = -2$ *con multiplicidad algebraica 3. Además, calculando el subespacio propio*

$$A + 2I = \begin{bmatrix} 0 & 1 & -1 \\ -1 & 1 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$ *, luego* $dim(ker(A + 2I)) = 1.$

Así, el valor propio $x = -2$ *tiene multiplicidad gemétrica 1. De los ejemplos anteriores sigue que* $J = \begin{bmatrix} -2 & 1 & 0 \\ 0 & -2 & 1 \\ 0 & 0 & -2 \end{bmatrix}$.

4. *Considere* $A = \begin{bmatrix} 5 & -4 & 4 \\ 1 & 0 & 1 \\ -1 & 2 & 1 \end{bmatrix}$*, note que* $\chi_A(x) = (x-2)(x-3)(x-1)$*. Así,* A *tiene tres valores propios distintos y, por tanto, la matriz* A *es diagonalizable y su la forma canónica de Jordan será* $J = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

5. *Un caso particular de la forma canónica de Jordan está dado por la matriz* $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$*, cuyo polinomio característico* $\chi_A(x) = x^2 + 1$*, el cual tiene raíces complejas* $x = i$ *y* $x = -i$*. Note que* A *no admite valores propios reales y, por tanto, no es similar a ninguna matriz de Jordan definida sobre* $\mathbb{R}$*. No obstante, al considerar el cuerpo de los números complejos, A resulta ser similar a la matriz diagonalizable* $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$*, la cual es una matriz de Jordan.*

4. Resultados

4.1. Algunos resultados previos

A continuación se presentarán algunos resultados citados por el artículo principal [1] con el objetivo de obtener un trabajo de autocontenido.

Definición 4.1.1. *Sea A una matriz de $M_n(\mathbf{F})$, $\lambda \in \mathbf{F}$ y $k \in N^*$. Se denota por:*

$$n_k(A,\lambda) := \dim\ker(A-\lambda\cdot I_n)^k - \dim\ker(A-\lambda\cdot I_n)^{k-1},$$

i.e, $n_k(A,\lambda)$ es el número de bloques de tamaño mayor o igual que k para el valor propio λ en la reducción de Jordan de A (en particular, es cero si λ no es un valor propio de A). También se denotará por $j_k(A,\lambda)$ al número de bloques de tamaño k para el valor propio λ en la reducción de Jordan de A.

Recuerde que dos sucesiones $(u_k)_{k\geq 1}$ y $(v_k)_{k\geq 1}$ se dicen *entrelazadas* si:

$$\forall k \in N^*, \quad v_k \leq u_{k+1} \quad \text{y} \quad u_k \leq v_{k+1}.$$

El siguiente resultado es una generalización de los resultados de Hartwig y Putcha [1].

Teorema 4.1.2. *Suponga que $car(\mathbf{F}) \neq 2$, y sea $A \in M_n(\mathbf{F})$. Entonces A es un $(1,1)$-compuesto si y solo si se cumplen todas las siguientes condiciones:*

(i) Las sucesiones $(n_k(A,0))_{k\geq 1}$ y $(n_k(A,2))_{k\geq 1}$ están entrelazadas.

(ii) Para todo $\lambda \in \mathbb{K}\setminus\{0,1,2\}$ y para todo $k \in N^*$, se cumple que

$$j_k(A,\lambda) = j_k(A,2-\lambda).$$

A partir del teorema anterior se establece el *lema de simetría*, el cual será muy utilizado para demostrar los resultados principales de la monografía.

Lema 4.1.3. *(Lema de Simetría) Sea $\mathbf{F}$ un cuerpo y $A \in M_n(\mathbf{F})$ una matriz suma de dos matrices idempotentes. Entonces, para cada $\lambda \in \mathbf{F}\setminus\{0,1_{\mathbf{F}},2\cdot 1_{\mathbf{F}}\}$ los escalares λ y $2\cdot 1_{\mathbf{F}}-\lambda$ tienen la misma multiplicidad algebraica como eigenvalores de A.*

El próximo teorema será importante para demostrar el Lema 4.2.5, para detalles sobre la demotración consultar el *Teorema 4, página 3* de [2].

[1] Robert E Hartwig y Mohan S Putcha. «When is a matrix a difference of two idempotents». En: *Linear and Multilinear Algebra* 26.4 (1990), págs. 267-277.

[2] G. Song y Xue-Jün Guo. «Diagonability of idempotent matrices over noncommutative rings». En: *Linear Algebra and its Applications* 297.1-3 (1999). ISSN: 0024-3795, págs. 1-7. DOI: 10.1016/S0024-3795(99)00059-2.

Teorema 4.1.4. *Sea A una matriz idempotente sobre un anillo R. Si A es similar a una matriz en bloques diagonal $B = \operatorname{diag}\{B_1, B_2, \ldots, B_m\}$, entonces para todo $1 \leq i \leq m$, existen matrices S_{ii} tales que $A \sim D = \operatorname{diag}\{B_1S_{11}, B_2S_{22}, \ldots, B_mS_{mm}\}$. Además:*

1. $B_i \neq 0 \iff B_iS_{ii} \neq 0, \quad i = 1, 2, \ldots, m.$
2. *Si $B_i^2 = B_i$, se puede elegir a S_{ii} como la matriz identidad.*

Teorema 4.1.5. *Supongamos que $\operatorname{car}(\mathbf{F}) = 2$, y sea $A \in M_n(\mathbf{F})$. Entonces A es un $(1, -1)$-compuesto si y solo si para todo $\lambda \in \mathbf{F} \setminus \{0, 1\}$, todos los bloques en la reducción de Jordan de A respecto de λ tienen tamaño par.*

Dado $n \in \mathbb{N}^*$ y $\lambda \in \mathbf{F}$, se define la matriz $J := (\delta_{i,j+1})_{1 \leq i,j \leq n}$, i.e,

$$J = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 1 \\ 0 & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

Proposición 4.1.6. *Asuma $\#\mathbf{F} \leq 3$. Entonces, para cada $n \in N^*$ cada matriz de $M_n(\mathbf{F})$ es suma de tres idempotentes.*

Demostración. Por reducción a la forma canónica racional, basta con probar que toda matriz cíclica de $M_n(\mathbf{F})$ es suma de tres idempotentes. Sean $P \in \mathbf{F}[X]$ un polinomio irreducible mónico de grado m , $J := (\delta_{i,j+1})_{1 \leq i,j \leq n}$ y escriba $C(P) = \begin{bmatrix} J & C \\ H_{1,n-1} & \operatorname{tr} P \end{bmatrix}$ con $C \in M_{n-1,1}(\mathbf{F})$.

Defina $P_1 := (X-1)^{m-1}(X - \operatorname{tr} P + m \cdot 1_{\mathbf{F}})$, entonces

$$C(P_1) = \begin{bmatrix} J & C_1 \\ H_{1,n-1} & \operatorname{tr} P - 1 \end{bmatrix} \quad \text{para alguna } C_1 \in M_{n-1,1}(\mathbf{F}),$$

y $C(P_1)$ es suma de dos idempotentes por los Teoremas 4.1.2 y 4.1.5, ya que $\#\mathbf{F} \leq 3$. Finalmente

$$C(P) - C(P_1) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},$$

es una matriz idempotente, por lo tanto $C(P)$ es suma de tres idempotentes. □

La siguiente definición será fundamental para abordar los Teoremas 2 y 4.

Definición 4.1.7. *Si $\{R_i : i \in \Lambda\}$ es una colección arbitraria de anillos, el* **producto directo** *de estos anillos es el anillo de todos los símbolos $\prod_{i \in \Lambda} R_i = \{a = (a_1, a_2, \cdots) : a_i \in R_i\}$, donde la suma y el producto vienen dadas, respectivamente, por:*

$$(a_i)_{i \in I} + (b_i)_{i \in \Lambda} = (a_i + b_i)_{i \in \Lambda} \quad \textit{y} \quad (a_i)_{i \in I} \cdot (b_i)_{i \in \Lambda} = (a_i \cdot b_i)_{i \in \Lambda}.$$

Observación 9.

1. *Si $S \leq_{sub} \prod_{i\in\Lambda} R_i$ entonces la correspondencia*

$$a \to a_i, \tag{4.1}$$

define un homomorfismo de S con un subanillo de S_i. Si, para cada $i \in \Lambda$, todo elemento de S_i es imagen de algún elemento de S o, en otras palabras, si el homomorfismo (4.1) es un epimorfismo de S en todo el anillo S_i se dice que S es el **subproducto directo** *de los anillos S_i.*

2. *Si R es isomorfo a un subproducto directo de anillos S_i cada proyección $R \to S_i$ es un epimorfismo y $S_i \cong R/I_i$ donde I_i es el ideal donde sus elementos son elementos de R a los que les corresponde el elemento cero en S_i. Como se asume que R es isomofro al subproducto directo de anillos S_i, elementos diferentes de R deben corresponder elementos diferentes en el producto directo, por lo tanto*

$$\bigcap_{i\in\Lambda} I_i = \{0\}.$$

3. *Es un resultado conocido que, si existe un conjunto de ideales $I_i \in R$ con intersección vacía, R es isomorfo al subproducto directo de anillos R/I_i, $i \in \Lambda$ (ver [3], Teorema 1, pág. 488).*

Ejemplo 4.1.8. *Considere el anillo $\mathbb{Z}_n$, con $n > 1$ tal que n no es primo. Por el Teorema Fundamental de la Aritmética n se puede expresar como $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, donde para cada $i \in \{1, 2 \cdots, k\}$, $n_i \in N$, p_i es primo y $p_1 < p_2 < \cdots < p_k$. Del Teorema Fundamental de los Grupos Abelianos Finitos (ver [1] , Teorema 11.1, pág. 212), sigue que:*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}.$$

Tambíen, si el anillo R es isomorfo a un subproducto directo T de anillos $S_i,\ i \in \lambda$, T será llamado una **representación** de R como subproducto directo de anillos S_i.

Siguiendo a Birkhoff [4], se dice que el anillo R es **subdirectamente irreducible** si en cualquier representación de R como un subproducto directo de anillos S_i, el homomorfismo de R con S_i es en realidad un isomorfismo para al menos un índice i. Así, R es subdirectamente irreducible si, y sólo si, la intersección de todos los ideales propios es en sí misma un ideal propio en R.

El siguiente resultado corresponde a un caso particular del teorema clásico de representación por subproductos directos, enunciado originalmente por Birkhoff [5] en el *Teorema 2, página 765*, adaptado al contexto de los anillos.

[3] Neal H. McCoy. «Subrings of infinite direct sums». En: *Duke Mathematical Journal* 4.3 (1938), págs. 486-494. DOI: 10.1215/S0012-7094-38-00441-7.

[4] Garrett Birkhoff. «Subdirect unions in universal algebra». En: *Bulletin of the American Mathematical Society* 50.10 (1944), págs. 764-768. DOI: 10.1090/S0002-9904-1944-08255-4.

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

Teorema 4.1.9 (Teorema de Birkhoff)**.** *Cada anillo R es isomorfo a una suma subdirecta de anillos subdirectamente irreducibles $\{R_i\}$, $i \in \lambda$.*

Para una profundización en los *productos y subproductos directos* se recomienda consultar los aportes presentados en [4], donde el concepto se desarrolla en un contexto más general a través de la teoría de álgebras universales, así como en [3], donde se aborda la caracterización de los anillos subdirectamente irreducibles en el contexto conmutativo.

4.2. Resultados Principales

En esta sección se expondrán los resultados fundamentales de Tang [1]. Estos teoremas se fundamentan en hallazgos previos presentados a lo largo de este trabajo y que que actuarán como base para afrontar los problemas propuestos.

Lema 4.2.1. *Si -1 es suma de tres idempotentes en un anillo R, entonces $2^2 \cdot 3 \cdot 5 = 0$ en R.*

Demostración. Escriba $-1 = e + f + g$ donde e, f, g son idempotentes en R. Entonces se verifica que $1 + 3e = (-1 - e)^2 = (f + g)^2 = f + g + fg + gf = (-1 - e) + fg + gf$, por lo tanto $2 + 4e = fg + gf$. Se sigue que $2 + 4(-1 - f - g) = fg + gf$, i.e,

$$-2 - 4f - 4g = fg + gf.$$

Multiplicando por f a la izquierda $f(-2-4f-4g) = f(fg+gf)$, i.e, $-6f-5fg = fgf$.
Asimismo, multiplicando por f a la derecha $(2 - 4f - 4g)f = (fg + gf)f$, i.e, $-6f - 5gf = fgf$.. De lo anterior sigue que

$$5fg = 5gf.$$

Entonces $5(-6f-5fg) = 5fgf = f(5gf) = f(5fg) = 5fg$, por lo tanto $-30fg = 30fg$, así $60fg = 0$. Se concluye que $60f = 0$. De forma similar, $60e = 0$ y $60g = 0$. Por tanto $60 = -60(e + f + g) = 0$.

□

Lema 4.2.2. *Sea $n \geq 1$ y $\mathbf{F}$ un cuerpo. Si cada matriz invertible en $M_n(\mathbf{F})$ es suma de tres idempotentes, entonces $\mathbf{F} \cong Z_p$, donde $p = 2, 3$ ó 5.*

Demostración. Por el Lema 4.2.1 y la Observación 1, la característica de $\mathbf{F}$ es p, donde $p = 2, 3$ o 5. Para cualquier $0 \neq a \in \mathbf{F}$, se define la matriz $A := \begin{bmatrix} a & 0 \\ 0 & I_{n-1} \end{bmatrix}$ la cual es invertible en $M_n(\mathbf{F})$, así que $A = E_1 + E_2 + E_3$, donde E_1, E_2, E_3 son matrices idempotentes sobre $\mathbf{F}$. Del Lema 4.2.5 sigue que $tr(A) = tr(E_1) + tr(E_2) + tr(E_3) = ran(E_1) \cdot 1_{\mathbf{F}} + ran(E_2) \cdot 1_{\mathbf{F}} + ran(E_3) \cdot 1_{\mathbf{F}} \in \mathbb{Z} \cdot 1_{\mathbf{F}} = \mathbb{Z}_p$. De lo anterior $a \in \mathbb{Z}_p$ y , por tanto, $\mathbf{F} \cong \mathbb{Z}_p$.

□

Lema 4.2.3. *Sea p un número primo mayor que 3 y n un entero positivo. Si $-I_n$ es suma de tres matrices idempotentes en $M_n(\mathbb{Z}_p)$ entonces $p = 5$ y n es par.*

Demostración. Suponga que $-I_n = E_1 + E_2 + E_3$, para algunos idempotentes E_1, E_2, E_3. Defina $A := -I_n - E_1$, la cual es suma de dos idempotentes. Por otro lado, A es diagonalizable con valores propios en $\{-\bar{2}, -\bar{1}\}$; Ninguno de esos valores propios pertenece a $\{\bar{0}, \bar{1}, \bar{2}\}$ y por el *Lema de simetría*, para cada valor propio λ se tiene que $\bar{2} - \lambda$ también es un valor propio de A. De esto se deduce fácilmente que $p = 5$.

Ahora, suponga que n es impar. Entonces la aplicación $\lambda \mapsto \bar{2} - \lambda$ intercambia los dos elementos de $\{-\bar{2}, -\bar{1}\}$, por lo tanto $-\bar{2}$ y $-\bar{1}$ tienen la misma multiplicidad como valores propios de A, y se concluye que n es par. □

Lema 4.2.4. *Sea $n = 2m$ un entero positivo. Entonces $\begin{bmatrix} 1 & 0 \\ 0 & -I_{n-1} \end{bmatrix}$ no es suma de tres idempotentes en $M_n(\mathbb{Z}_5)$.*

Demostración. Sea $A := \begin{bmatrix} 1 & 0 \\ 0 & -I_{n-1} \end{bmatrix}$ y suponga que $A = E_1 + E_2 + E_3$ para algunas matrices idempotentes E_1, E_2, E_3 en $M_n(\mathbb{Z}_5)$. Si todas las E_i tuvieran rango m, entonces

$$tr(A) = 3m = -2m = -\bar{n},$$

lo cual es falso. Por tanto, una de las E_i, por ejemplo, E_1, tiene un valor propio α con multiplicidad r mayor que m.

Por la fórmula clásica de Grassmann, se tiene que $\dim(\ker(A + I_n) \cap \ker(E_1 - \alpha I_n)) \geq r - 1$, y se deduce que la multiplicidad geométrica de $-1 - \alpha$ como valor propio de $M := A - E_1$ es al menos $r - 1$. Por el *Lema de Simetría* sigue que $2(r-1) \leq n$, por tanto $r = m + 1$, y así M tiene polinomio característico $(x + \bar{1})^m (x + \bar{2})^m$. De lo anterior, para algún $\epsilon \in \{-1, 1\}$, se cumple que:

$$tr(A) = tr(E_1) + tr(M) = (m + \epsilon)\bar{1} - m\bar{1} - m\bar{2} = \bar{\epsilon} - \bar{n},$$

Lo cual contradice el hecho de que $tr(A) = -\bar{n} + \bar{2}$. □

Lema 4.2.5. *Sea R un anillo conmutativo local y $n \geq 1$. Si $E^2 = E \in M_n(R)$ entonces $tr(E) = ran(E) \cdot 1_R \in \mathbb{Z} \cdot 1_R$.*

Demostración. La afirmación es verdadera para $n = 1$. Suponga que $n > 1$. Por hipótesis $E(E - I_n) = 0$ luego si $E = [\overline{e_{ij}}] \in M_n(J(R))$ seguiría que E=0 ó, para algunos i, j, $a_{ij} = 1 \in J(R)$ pero $J(R)$ es un ideal maximal, por tanto E=0. Suponga entonces que $E = [\overline{e_{ij}}] \notin M_n(J(R))$, así que existen índices i, j tales que $\overline{e_{ij}} \in U(R)$. Entonces E es similar a $\begin{bmatrix} \overline{e_{ij}} & \cdots \\ \vdots & \ddots \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & E_1 \end{bmatrix}$, donde E_1 es una matriz de tamaño $(n-1) \times (n-1)$. Por el Teorema 4.1.4, E es similar a una matriz diagonal por bloques de la forma $\begin{bmatrix} a & 0 \\ 0 & E_2 \end{bmatrix}$, donde $a^2 = a$ y E_2 es una matriz idempotente de tamaño $(n-1) \times (n-1)$. Por lo tanto, $a = 0$ ó 1 y $\mathrm{tr}(E_2) = \mathrm{rank}(E_2) \cdot 1_R \in \mathbb{Z} \cdot 1_R$ por hipótesis de inducción. Como

la similitud preserva la traza y el rango de matrices sobre anillos locales conmutativos (Observación 6), sigue que

$$\begin{aligned}\operatorname{tr}(E) = \operatorname{tr}\begin{bmatrix} a & 0 \\ 0 & E_2 \end{bmatrix} = a + \operatorname{tr}(E_2) &= a + \operatorname{rank}(E_2)\cdot 1_R \\ &= \operatorname{rank}\begin{bmatrix} a & 0 \\ 0 & E_2 \end{bmatrix}\cdot 1_R \\ &= \operatorname{rank}(E)\cdot 1_R \in \mathbb{Z}\cdot 1_R.\end{aligned}$$

□

Teorema 1. *Sea* $\mathbf{F}$ *un cuerpo y* $n \geq 1$*. Las siguientes son equivalentes*

1. *Cada matriz en* $M_n(\mathbf{F})$ *es suma de tres idempotentes.*
2. *Cada matriz invertible en* $M_n(\mathbf{F})$ *es suma de tres idempotentes.*
3. $\mathbf{F} \cong \mathbb{Z}_2$ *o* $\mathbf{F} \cong \mathbb{Z}_3$.

Demostración. La implicación $(1) \Rightarrow (2)$ es clara.

$(2) \Rightarrow (3)$. Como $\mathbf{F}$ es cuerpo y cada matriz invertible en $M_n(\mathbf{F})$ es suma de tres idempotentes sigue del lema 4.2.2 que $F \cong \mathbb{Z}_p$, $p = 2, 3$ ó 5, por los lemas 4.2.3 y 4.2.4 se descarta el caso donde $F \cong \mathbb{Z}_5$, luego $\mathbf{F} \cong Z_p$ con $p = 2$ ó 3.

$(3) \Rightarrow (1)$ es resultado de la Proposición 4.1.6. □

Recuerde que un **anillo reducido** es un anillo sin elementos nilpotentes no cero. Es conocido que un anillo reducido es conmutativo y además, si Q es un ideal de un anillo R y R/Q es reducido, se dice que Q es un **ideal reducido**.

Ejemplo 4.2.6. *Si* R *un anillo conmutativo y* η_R *un ideal de* R*, entonces* R/η_R *es reducido. Sea* $\overline{x} = x + \eta_R \in R/\eta_R$ *y suponga que* $\overline{x}^t = 0$ *en el cociente, entonces* $x^t \in \eta_R$*. Por definición de* η_R*, existe* $s > 1$ *tal que* $(x^t)^s = x^{ts} = 0$*. Así* x *es nilpotente en* R*, de modo que* $\overline{x} = 0$*. En consecuencia* R/η_R *es reducido.*

Sea Q un ideal reducido de un anillo R, y sean $a, b \in R$ tales que $ab \in Q$ entonces $ba \in Q$. En efecto, note que $(ba)^2 = ba \cdot ba = b(ab)a \in Q$, por lo tanto, para $ba + Q \in R/Q$ satisface $(ba+Q)^2 = (ba)^2 + Q = Q$, como R/Q es reducido, se concluye que $ba + Q = Q$, i.e, $ba \in Q$.

Proposición 4.2.7. *Sea* $\{I_\alpha\}_{\alpha\in A}$ *una familia de ideales reducidos de un anillo* R*. Entonces la intersección* $I = \bigcap_{\alpha\in A} I_\alpha$ *es un ideal reducido de* R*.*

Demostración. Sea $\{I_\alpha\}_{\alpha\in A}$ una familia de ideales reducidos de un anillo R y sea $I = \bigcap_{\alpha\in A} I_\alpha$.

Si $x, y \in I$ entonces $x, y \in I_\alpha$ para todo α, luego $x - y \in I_\alpha$ para todo α y por tanto $x - y \in I$; y si $r \in R$ y $x \in I$ entonces $x \in I_\alpha$ para todo α, luego $rx \in I_\alpha$ y $xr \in I_\alpha$ para todo α, con lo que $rx, xr \in I$ y así I es un ideal.

Sea $r \in R$ tal que $r^2 \in I$. Entonces $r^2 \in I_\alpha$ para todo α. Como cada I_α es reducido, de $r^2 \in I_\alpha$ sigue que $r \in I_\alpha$ para cada α. Por lo tanto $r \in \bigcap_{\alpha \in A} I_\alpha = I$. Así I es un ideal reducido. □

Proposición 4.2.8. *Sea Q un ideal reducido de un anillo R. Si A es el anulador por izquierda (derecha) modulo Q de algún subconjunto $S \subseteq R$, entonces A es un ideal reducido.*

Demostración. Suponga que el conjunto S contiene solamente un elemento s, ya que la intersección de ideales reducidos es nuevamente un ideal reducido (Proposición 4.2.7) . Defina $A = \{ r \in R \mid rs \in Q \}$. Rápidamente A es un ideal a izquierda puesto que si $r \in A$ y $x \in R$, entonces $(xr)s = x(rs) \in Q$, por lo que $xr \in A$. Considere ahora $srx \in Q$; Nuevamente, como Q es reducido, de $srx \in Q$ se sigue que $rxs \in Q$, así $rx \in A$. Por tanto, A es un ideal de R.

Para probar que A es reducido, es suficiente probar que si $r^2 \in A$ entonces $r \in A$. Considere $r^2 s \in Q$, i.e, $r(sr) \in Q$, entonces $rsr \in Q$. Como Q es reducido, de $rsr \in Q$ se sigue que $(rs)^2 \in Q$. Nuevamente, como Q es reducido, $(rs)^2 \in Q$ implica $rs \in Q$ y por consiguiente $r \in A$ y A es reducido. □

Teorema 4.2.9. *Si R es un anillo reducido, entonces R es subproducto directo de dominios enteros*

Demostración. Basta probar que, dado $0 \neq x \in R$, existe un ideal Q que no contenga a x, tal que R/Q sea un dominio entero. Como el ideal cero es reducido, se aplica el Lema de Zorn al conjunto de ideales reducidos que no contienen a x obteniendo un ideal reducido maximal Q que no contiene a x. Ahora, R/Q es un dominio entero, puesto que, si existen $a, b \in R$ tales que $ab \in Q, \quad a \notin Q, \quad b \notin Q$ y se considera el anulador por izquieda módulo Q de b y el anulador por derecha modulo Q de a, denotados por A y B, respectivamente, sigue por la Proposición 4.2.8 que A y B son ideales reducidos. Además, se cumple que $A \supseteq Q, \quad B \supseteq Q, \quad AB \subseteq Q$. Note que $A \neq Q$ ya que $a \in A$ y $B \neq Q$ pues $b \in B$. De lo anterior $x \in A$ y $x \in B$, por lo que $x^2 \in AB \subseteq Q$. Dado que Q es reducido, de $x^2 \in Q$ se concluye $x \in Q$, lo cual contradice la elección de Q. Por lo tanto, R/Q es un dominio entero. □

A partir del *Teorema 16.6, página 269* de Galian [1] se dice que el *cuerpo de fracciones* de un dominio entero R es el cuerpo más pequeño que contiene a R. Este cuerpo se construye contruyendo incialmente el conjunto $Q(R) = \left\{ \frac{a}{b} : a, b \in R \text{ y } b \neq 0 \right\}$, definiendo la igualdad y las operaciones de manera análoga a las fracciones en los enteros. Este cuerpo será de gran ayuda porque permitirá extender las propiedades de R a un contexto donde todo elemento no nulo es invertible.

Corolario 4.2.10. *Sea R un dominio entero y $n \geq 1$. Entonces, toda matriz en $M_n(R)$ es suma de tres idempotentes si y sólo si $R \cong \mathbb{Z}_2$ o $R \cong \mathbb{Z}_3$.*

Demostración. $\Rightarrow$). Sea $Q(R)$ el cuerpo de fracciones R, y sea $E^2 = E \in M_n(R)$. Como E es idempotente, en $M_n(Q(R))$, E es diagonalizable y por tanto E es similar a una matriz diagonal. Así, existe una matriz invertible $U \in M_n(Q(R))$ tal que $U^{-1}EU =$

$\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix}$ donde $r = ran(E)$. Como la traza es invariante bajo semejanza (Observación 6), sigue que

$$tr(E) = ran(E) \cdot 1_Q = ran(E) \cdot 1_R \in \mathbb{Z} \cdot 1_R.$$

Sea $a \in R$ y escriba $\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} = E_1 + E_2 + E_3$ donde cada E_i es una matriz idempotente en $M_n(R)$. Entonces $a = tr(E_1 + E_2 + E_3) = tr(E_1) + tr(E_2) + tr(E_3) = ran(E_1) \cdot 1_R + ran(E_2) \cdot 1_R + ran(E_3) \cdot 1_R$. Así, $R = \mathbb{Z} \cdot 1_R$. Como R es un dominio y $2^2 \cdot 3 \cdot 5 = 60 = 0$ en R (Lema 4.2.1), $car(R) = p$ donde $p = 2, 3$ ó 5. De lo anterior $R \cong \mathbb{Z}_p$ donde $p = 2, 3$ o 5; Finalmente, por el Teorema 1, $R \cong \mathbb{Z}_2$ ó $R \cong \mathbb{Z}_3$.

$\Leftarrow$) Sigue del Teorema 1. □

Teorema 2. *Suponga que cada matriz en $M_n(R)$ es suma de tres idempotentes donde R es un anillo conmutativo y $n \geq 1$. Entonces $J(R)$ y $R/J(R)$ tiene identidad $x^3 = x$. Si en adición R es un anillo indescomponible entonces $R \cong \mathbb{Z}_n$ donde $n = 2, 3$ o 4.*

Demostración. Como R es conmutativo, η_R es un ideal de R y por el Ejemplo 4.2.6, R/η_R es reducido. Ahora, por el Teorema 4.2.9, R/η_R es subproducto directo de dominios enteros $\{R_\alpha\}$. Note que, como $M_n(R_\alpha)$ es imagen homomorfica de $M_n(R)$, cada matriz en $M_n(R_\alpha)$ es suma de tres idempotentes y por el Corolario 4.2.10, R_α es isomorfo a $\mathbb{Z}_2$ ó $\mathbb{Z}_3$. De lo anterior en cada R_α se vale la identidad $x^3 = x$, entonces para cada $x \in R/\eta_R$ también se verifica que $x^3 = x$. De lo anterior sigue que $J(R/\eta_R) = \{0\}$, luego $J(R) = \eta_R$.

Ahora, suponga que R es un anillo indescomponible. Sea $a \in R/J(R)$, entonces $\bar{a}^3 = \bar{a}$, entonces $a^4 - a^2 \in J(R)$. Como $J(R)$ es nil, los idempotentes se anulan modulo $J(R)$, por tanto $a^2 - e \in J(R)$ para algún $e^2 = e \in R$. Si $e = 0$, entonces $a = (a - a^2) + a^2 \in J(R)$, lo cual es una contradicción. Por lo tanto $e = 1$ y así $a^2 - 1 \in J(R)$. De lo anterior $a \in U(R)$. con esto R es anillo local. Como, por hipótesis, para cualquier $a \in R$, $\begin{bmatrix} a & 0 \\ 0 & I_{n-1} \end{bmatrix}$ es suma de tres idempotentes, del Lema 4.2.5 sigue que $\operatorname{tr}\left(\begin{bmatrix} a & 0 \\ 0 & I_{n-1} \end{bmatrix}\right) \in \mathbb{Z} \cdot 1_R$. Así, $a \in \mathbb{Z} \cdot 1_R$, y por lo tanto $R = \mathbb{Z} \cdot 1_R$. Como $2^2 \cdot 3 \cdot 5 = 0$ en R (por el Lema 4.2.1), del Teorema Chino del Residuo sigue que $R = A \times B \times C$ donde $2^2 = 0$ en A, $3 = 0$ en B y $5 = 0$ en C. Como R es indescomponible, $R = A$ ó $R = B$ ó $R = C$ y por tanto, $R \cong \mathbb{Z}_n$ donde $n = 2, 3, 4$ ó 5. Pero, por el Teorema 1, $n \neq 5$ y así $R \cong \mathbb{Z}_n$, $n = 2, 3$ ó 4.

□

Lema 4.2.11. *Sea R un anillo y $n \geq 1$. Entonces, cada elemento de $M_n(R)$ es suma de tres idempotentes si y sólo si cada elemento de $M_n(R/I)$ es suma de tres idempotentes para todo anillo cociente indescomponible R/I.*

Demostración. La necesidad es clara. Para la suficiencia suponga, por el contrario, que existe $[a_{ij}] \in M_n(R)$ que no es suma de tres idempotentes. Considere el conjunto

$$\mathcal{F} = \{\, I \lhd R : \ [\overline{a_{ij}}] \in M_n(R/I) \text{ no es suma de tres idempotentes} \,\}.$$

Por hipótesis $\mathcal{F} \neq \varnothing$. Sea $\{I_\lambda\}$ una cadena en $\mathcal{F}$ y sea $I = \bigcup_\lambda I_\lambda$. No es difícil ver que I es un ideal de R y suponga que $[\overline{a_{ij}}] \in M(R/I)]$ sí es suma de tres idempotentes.

Así, existen matrices $[\overline{e_{ij}}], [\overline{f_{ij}}], [\overline{g_{ij}}] \in M_n(R/I)$ tales que

$$[\overline{a_{ij}}] = [\overline{e_{ij}}] + [\overline{f_{ij}}] + [\overline{g_{ij}}], \quad [\overline{e_{ij}}]^2 = [\overline{e_{ij}}], \quad [\overline{f_{ij}}]^2 = [\overline{f_{ij}}], \quad [\overline{g_{ij}}]^2 = [\overline{g_{ij}}].$$

Así, los siguientes elementos pertenecen a $M_n(I)$:

$$[a_{ij}] - [e_{ij}] - [f_{ij}] - [g_{ij}], \quad [e_{ij}] - [e_{ij}]^2, \quad [f_{ij}] - [f_{ij}]^2, \quad [g_{ij}] - [g_{ij}]^2,$$

Como $\{I_\lambda\}$ es cadena, existe algún I_λ tal que todas esas diferencias pertenecen a $M_n(I_\lambda)$. Por tanto, las ecuaciones anteriores ya valen en $M_n(R/I_\lambda)$ y esto implica que $[\overline{a_{ij}}]$ es suma de tres idempotentes, lo cual es una contradicción con $I_\lambda \in \mathcal{F}$. De lo anterior, $I \in \mathcal{F}$, y por lo tanto $\mathcal{F}$ es un conjunto inductivo y por el Lema de Zorn, $\mathcal{F}$ contiene un ideal maximal I.

Se afirma que R/I es indescomponible. En efecto, si R/I fuera descomponible, existirian ideales I_1, I_2 de R con $I \subsetneq I_k \subsetneq R$ $(k = 1, 2)$ tales que $R = I_1 + I_2$ y $I_1 \cap I_2 = I$. Entonces

$$R/I \cong R/I_1 \times R/I_2, \text{ por medio de la asignación } (r + I) \longmapsto (r + I_1, r + I_2).$$

lo que induce un isomorfismo

$$M_n(R/I) \cong M_n(R/I_1) \times M_n(R/I_2),$$

por medio de la asignación:

$$[r_{ij} + I] \longmapsto ([r_{ij} + I_1], [r_{ij} + I_2]).$$

Por maximalidad de I, $[\overline{a_{ij}}] \in M_n(R/I_k)$ es suma de tres idempotentes para $k = 1, 2$. De lo anterior seguiría que $[\overline{a_{ij}}] \in M(R/I)$ es suma de tres idempotentes, lo cual es una contradicción. Lo anterior muestra que R/I es indescomponible. Sin embargo, por hipótesis cada matriz en $M_n(R/I)$ es suma de tres idempotentes, contradiciendo que $I \in \mathcal{F}$.

□

Teorema 3. *Sea R un anillo conmutativo con $\eta_R = 0$ (por ejemplo $J(R) = 0$) y $n \geq 1$. Las siguientes son equivalentes:*

1. *Cada matriz en $M_n(R)$ es suma de tres idempotentes.*
2. *$R \cong A \times B$ donde A es anillo booleano y B es cero o subproducto directo de $\mathbb{Z}_3$.*
3. *R tiene identidad $x^3 = x$.*

Demostración. La implicación $(1) \Rightarrow (3)$ se deduce del Teorema 2. La equivalencia $(2) \Leftrightarrow (3)$ es evidente.

$(3) \Rightarrow (1)$. Sea R' un anillo cociente indescomponible de R. Entonces R' tiene identidad $x^3 = x$. Para todo $0 \neq a \in R'$, de esto se tiene que a^2 es un idempotente no nulo en R', por tanto $a^2 = 1$. Así, R' es un cuerpo, y se deduce que R' es isomorfo a $\mathbb{Z}_2$ ó $\mathbb{Z}_3$. Por lo tanto, por el Lema 4.2.11 y el Teorema 1, toda matriz en $M_n(R)$ es suma de tres idempotentes. □

Recuerde que, un elemento $a \in R$ es una *involución si* $a^2 = 1_R$. *Más aún, si* $k \in R$ *y si* $a^2 = k$, *se dirá que* a *es una* k-involución. . Al conjunto de elementos involutivos de R se le denotará inv(R).

Observación 10. *No es dificíl ver que todo elemento no nulo de un anillo* R *es una involución si y sólo si* $R \cong \mathbb{Z}_2$ *o* $R \cong \mathbb{Z}_3$.

A continuación un lema auxiliar necesario para demostrar el Teorema 4.

Lema 4.2.12. *Sea* R *un anillo con* $2 \in U(R)$ *y* $n \geq 1$. *Entonces:*

1. *La aplicación* $e \mapsto 1 - 2e$ *da una biyección de* $\mathrm{idem}(R)$ *a* $inv(R)$.
2. $a \in R$ *es una suma de* n *idempotentes si y sólo si* $n - 2a$ *es una suma de* n *involuciones.*
3. *Todo elemento de* R *es una suma de* n *idempotentes si y sólo si todo elemento de* R *es una suma de* n *involuciones.*

Teorema 4. *Sea* R *un anillo conmutativo y* $n \geq 1$. *Las siguientes son equivalentes:*

1. *Cada matriz en* $M_n(R)$ *es suma de tres matrices involutivas.*
2. *Cada anillo cociente indescomponible de* R *es isomorfo a* $\mathbb{Z}_3$.
3. *R es subproducto directo de Anillos* $\mathbb{Z}_3$.

Demostración. (1) $\Rightarrow$ (3). Sea R' un anillo cociente indescomponible de R y sea $\mathbf{F}$ un cuerpo que es un anillo cociente de R'. Primero se probará que $2 \neq 0$ en $\mathbf{F}$. Suponga que $2 = 0$ en $\mathbf{F}$. Sea A una matriz involutiva en $M_n(F)$. Es un resultado conocido (Proposición 3.1.10) que A es similar a una matriz racional en forma canónica

$$B = \begin{bmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_s \end{bmatrix},$$

donde $s \geq 1$ y cada B_i es una matriz compañera de tamaño n_i, y $n_1 + n_2 + \cdots + n_s = n$. Como A es involutiva, B también lo es, de modo que cada B_i es involutiva. Es fácil verificar que, si C es una matriz compañera involutiva sobre un cuerpo $\mathbf{F}$, entonces C tiene tamaño 1×1, o bien $C = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Así, cada $n_i = 1$ o $n_i = 2$. Entonces suponga que, para algún k, se cumple $n_i = 1$ para $i = 1, \ldots, k$ y $n_i = 2$ para $i = k+1, \ldots, s$. Además, $tr(A) = tr(B) = tr(B_1) + \cdots + tr(B_k) = k \cdot 1_F$. Si n es par, entonces k es par, así que $tr(A) = 0$; si n es impar, entonces k es impar, así que $tr(A) = 1_{\mathbf{F}}$. Por tanto, para n par, toda matriz involutiva en $M_n(\mathbf{F})$ tiene traza 0, y para n impar, toda matriz involutiva

en $M_n(\mathbf{F})$ tiene traza 1_F. De aquí se sigue que, para n par, E_{11} no es suma de (tres) matrices involutivas, y para n impar con $n > 1$, $E_{11} + E_{22}$ no es suma de tres matrices involutivas. Más aún, en el caso $n = 1$, $1 \in \mathbb{Z}_2$ no es suma de tres involuciones. Por lo anterior, $2 \neq 0$ en $\mathbf{F}$. omo toda matriz en $M_n(\mathbf{F})$ es suma de tres matrices involutivas, entonces toda matriz en $M_n(F)$ es suma de tres matrices idempotentes por el Lema 4.2.12. Así, $F \cong \mathbb{Z}_3$ por el Teorema 1. Luego, para todo ideal maximal M de R', se tiene $3 \in M$, y de allí que $3 \in J(R')$. Entonces $2 \in U(R')$. Como toda matriz en $M_n(R')$ es suma de tres matrices involutivas, toda matriz en $M_n(R')$ es suma de tres matrices idempotentes por el Lema 4.2.12. Por el Teorema 2, $R' \cong \mathbb{Z}_3$ (pues $2 \in U(R')$). Por el *Teorema de Birkhoff*, R es un subproducto subdirecto de anillos indescomponibles R_α donde, para cada α, R_α es indescomponible, así que $R_\alpha \cong \mathbb{Z}_3$. De ahí que R sea un subproducto subdirecto de copias de $\mathbb{Z}_3$.

(3) $\Rightarrow$ (2). Por (3), en R vale la identidad $x^3 = x$ y $2 \in U(R)$. Sea S un anillo cociente indescomponible de R. Entonces S vale la identidad $x^3 = x$ y $2 \in U(S)$. Para cualquier $0 \neq a \in S$, se cumple a^2 es un idempotente no trivial, de modo que $a^2 = 1$. Así, S es un cuerpo, y de ello sigue que $S \cong \mathbb{Z}_3$.

(2) $\Rightarrow$ (1). Suponga que (2) se cumple. Entonces $2 \in U(R)$ y, por el Teorema 2 y el Lema 4.2.11, toda matriz en $M_n(R)$ es suma de tres matrices idempotentes. Por tanto, por el Lema 4.2.12, toda matriz en $M_n(R)$ es suma de tres matrices involutivas.

□

5. Conclusiónes

El desarrollo de esta monografía ha permitido cumplir de manera satisfactoria los objetivos establecidos. En primer lugar, se examinó de forma exhaustiva los anillos de matrices sobre anillos conmutativos que pueden expresarse como la suma de tres idempotentes o tres involuciones, siguiendo el trabajo de Tang, Zhou y Su [1]. Este análisis llevó a una caracterización precisa de los anillos conmutativos que presentan esta propiedad, con énfasis en los anillos $\mathbb{Z}_2$, $\mathbb{Z}_3$, y $\mathbb{Z}_4$.

En segundo lugar, se detallaron y verificaron de manera clara las demostraciones de los resultados principales presentados en la referencia [1]. Se destacó cómo herramientas como la forma canónica racional y la reducción a cocientes indescomponibles facilitan la simplificación y el fortalecimiento de los argumentos. Este análisis riguroso aseguró que se cumpliera el objetivo de fundamentar teóricamente la investigación.

En conclusión, se lograron de manera integral los objetivos general y específicos planteados en esta monografía, ofreciendo una visión clara y sistemática sobre la descomposición especial de matrices en el contexto de los anillos conmutativos.

6. Trabajos Futuros

A partir de los resultados obtenidos en esta monografía, se identifican diversas posibles extensiones y desarrollos complementarios que pueden servir como punto de partida para futuras líneas de trabajo. A continuación, se destacan algunos de los más relevantes.

1. Una posible extensión de este trabajo consiste en analizar la descomposición de matrices como suma de un número arbitrario k de matrices idempotentes o involutivas, con $k > 3$. Este estudio permitiría identificar posibles cotas mínimas del número de idempotentes requeridos en distintos contextos algebraicos.

2. Otro posible trabajo a futuro consiste en formular procedimientos constructivos o algoritmos que permitan, dado un anillo conmutativo R y una matriz $A \in M_n(R)$, determinar explícitamente matrices idempotentes o involutivas cuya suma sea igual a A.

3. Un problema de interés que se desprende de este trabajo es la clasificación de los anillos que satisfacen la identidad $x^3 = x$. El estudio de estos anillos podría contribuir a comprender mejor la relación entre las propiedades polinómicas internas del anillo y el comportamiento de las matrices idempotentes definidas sobre él. Asimismo, examinar su estructura ideal, sus morfismos y sus posibles descomposiciones en subproductos directos permitiría establecer vínculos con otras clases de anillos especiales, tales como los anillos booleanos o los anillos von Neumann regulares.

Durante el desarrollo del presente trabajo se dejaron abiertos diversos problemas que, si bien están relacionados con los resultados obtenidos, no fueron tratados en detalle dentro del marco de esta investigación. A continuación, se presentan algunos de los más relevantes.

1. El presente trabajo se restringe al estudio de matrices sobre anillos conmutativos con unidad. Un problema que permanece abierto es determinar en qué medida los resultados obtenidos se mantienen válidos cuando el anillo de base no es conmutativo.

2. En el desarrollo del trabajo se establece que ciertas matrices pueden expresarse como suma de tres idempotentes o involutivas; sin embargo, no se aborda la cuestión de si dicho número es óptimo. Un problema pendiente consiste en determinar el mínimo número posible de idempotentes (o involutivas) que permitan representar una matriz dada, así como estudiar si dicho número depende de las propiedades del anillo R o del tamaño de la matriz.

3. Algunos de los resultados previos necesarios para entender las demostraciones principales del artículo principal suponen que el cuerpo base $\mathbf{F}$ tiene característica distinta de dos, lo cual excluye un conjunto importante de casos algebraicos. Un problema abierto consiste en extender los resultados al caso $\mathrm{car}(\mathbf{F}) = 2$, explorando cómo las demostraciones deben modificarse y qué nuevas condiciones son necesarias para mantener los resultados expuestos.

4. Si bien en este trabajo se demuestra la existencia de descomposiciones del tipo $A = E_1 + E_2 + E_3$, no se analiza la posible no unicidad de tales representaciones. Es decir, podrían existir distintas tríadas de idempotentes (o involutivas) que produzcan la misma matriz A. Resulta de interés estudiar bajo qué condiciones la descomposición es única, o describir el conjunto completo de todas las posibles descomposiciones equivalentes.

Bibliografía

Atiyah, Michael Francis y Ian Grant Macdonald. *Introducción al álgebra conmutativa*. Reverté, 1989 (vid. págs. 11, 12).

Bhattacharya, Phani Bhushan, Surender Kumar Jain y SR Nagpaul. *Basic abstract algebra*. Cambridge University Press, 1994 (vid. pág. 30).

Birkhoff, Garrett. «Subdirect unions in universal algebra». En: *Bulletin of the American Mathematical Society* 50.10 (1944), págs. 764-768. DOI: 10.1090/S0002-9904-1944-08255-4 (vid. págs. 30, 31).

Dummit, David Steven, Richard M Foote et al. *Abstract algebra*. Vol. 3. Wiley Hoboken, 2004 (vid. pág. 20).

Gallian, J. *Contemporary abstract algebra*. Chapman y Hall/CRC, 2021 (vid. págs. 10, 11, 30, 34).

Hartwig, Robert E y Mohan S Putcha. «When is a matrix a difference of two idempotents». En: *Linear and Multilinear Algebra* 26.4 (1990), págs. 267-277 (vid. pág. 28).

McCoy, Neal H. «Subrings of infinite direct sums». En: *Duke Mathematical Journal* 4.3 (1938), págs. 486-494. DOI: 10.1215/S0012-7094-38-00441-7 (vid. págs. 30, 31).

Oswaldo, Lezama Serrano José. *Álgebra lineal*. 2020 (vid. págs. 22, 23).

Seguins Pazzis, Clément de. «On decomposing any matrix as a linear combination of three idempotents». En: *Linear algebra and its applications* 433.4 (2010), págs. 843-855. DOI: 10.1016/j.laa.2010.04.017 (vid. págs. 17, 18).

– «On sums of idempotent matrices over a field of positive characteristic». En: *Linear algebra and its applications* 433.4 (2010), págs. 856-866. DOI: 10.1016/j.laa.2010.04.018 (vid. pág. 17).

Song, G. y Xue-Jün Guo. «Diagonability of idempotent matrices over noncommutative rings». En: *Linear Algebra and its Applications* 297.1-3 (1999). ISSN: 0024-3795, págs. 1-7. DOI: 10.1016/S0024-3795(99)00059-2 (vid. pág. 28).

Tang, Gaohua, Yiqiang Zhou y Huadong Su. «Matrices over a commutative ring as sums of three idempotents or three involutions». En: *Linear and Multilinear Algebra* 67.2 (2019), págs. 267-277. DOI: 10.1080/03081087.2017.1417969 (vid. págs. 8, 28, 31, 39).