Facultad de Matematicas

Región: Xalapa

Licenciatura en Matemáticas

Álgebras de dimensión finita

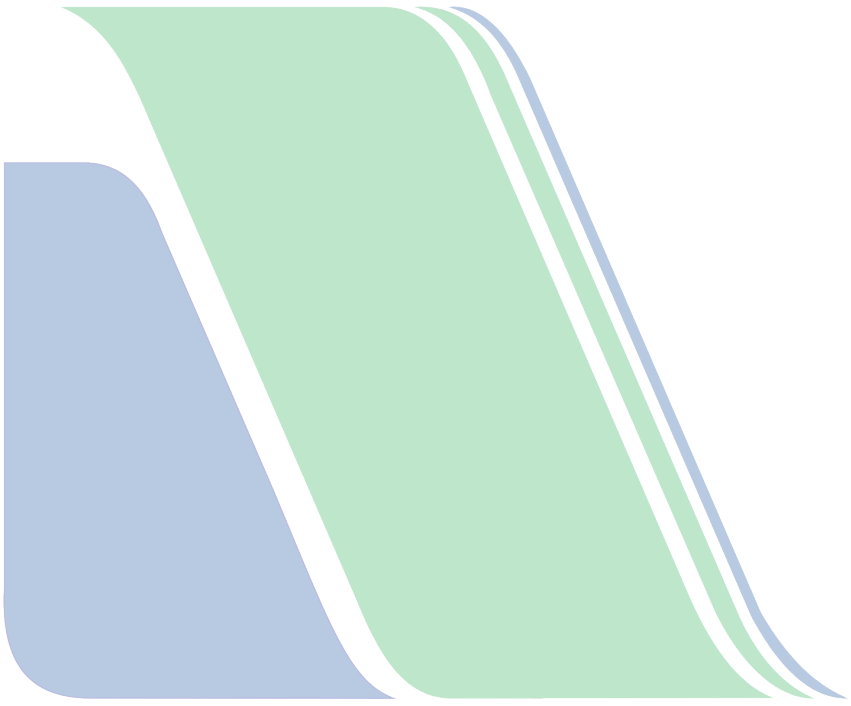
Tesis para acreditar la Experiencia recepcional

Presenta:
Roberto García Antonio

Directores:
Dr.Josué Rámirez Ortega
Dra. Yessica Hernández Eliseo

9 de junio de 2023

"Lis de Veracruz: Arte, Ciencia, Luz"



Universidad Veracruzana

Facultad de Matematicas
Región: Xalapa

Licenciatura en Matemáticas

Álgebras de dimensión finita

Tesis para acreditar la Experiencia recepcional

Presenta:
Roberto García Antonio

Directores:
Dr.Josué Rámirez Ortega
Dra. Yessica Hernández Eliseo

Asesores:
Dr. Luis Antonio Montero Ladron de Guevara

Agradecimientos

Agradezco al Doctor Josué por compartir su tiempo y conocimientos conmigo. Por las correcciones pertinentes y por permitirme trabajar con él.

A mi tutor el Doctor Porfirio Toledo Hernández por guiarme y aconsejare durante todo mi tiempo en la licenciatura. Y por inspirarme a seguir esforzándome y ser un mejor estudiante.

A mis amigos Iván, José Juan, Ulises, Abril y Víctor. Por siempre apoyarme a resolver mis dudas, por motivarme a seguir estudiando y permitirme compartir mi tiempo con ustedes.

A mi hermana Ingrid, a mi tía Anaberta y a mis padres Guillermina y Roberto. Por siempre brindarme su apoyo y acompañarme durante todo mi periodo como estudiante.

Un especial agradecimiento a los doctores Carlos Alberto Hernández Linares y Francisco Gabriel Hernández Zamora por tomarse el tiempo de evaluar este trabajo.

Finalmente, a mis abuelos Estela y Octavio por ser mi mayor motivación en la vida.

Dedicatoria

Dedico este trabajo mi familia, amigos y conocidos de la universidad.

Contents

Resumen

Un álgebra es un espacio vectorial V sobre un campo $\mathbf{F}$ en el cual se define un producto entre vectores $\odot : V \times V :\to V$, el cual es bilineal. Y en caso de ser conmutativa decimos que el álgebra es una álgebra conmutativa. Esta estructura algebraica aparece en áreas como el análisis funcional y la geometría diferencial.

En la presente proyecto se busca presentar los conceptos básicos de esta estructura centrándonos en el caso cuando el espacio vectorial es de dimensión finita. Tambien se busca dar una descripción hasta isomorfismo del álgebra generada por un operador lineal arbitrario en un espacio de dimensión finita. Esta álgebra es isomorfa a la suma directa de álgebras generada por una matriz nilpotente especial. Para logra esto expondremos la teoria necesaria para llevar a cabo las demostraciones de los teoremas de la descomposción prima y la descomposición de Jordan.

Comenzaremos exponiendo algunos preliminares algebraicos de teoría de anillos, ideales y polinomios. Posteriormente estudiaremos los temas de operadores proyección y suma directa de subespacios. Todos estos resultados seran necesarios necesarios para llevar acabo la demostración del teorema de la descomposicón prima y el teorema de la descomposicón de Jordan. Continuaremso dando la definición de una suma directa externa. En el siguiente capítulo daremos la definición formal de álgebra, presentaremos algunos ejemplos de álgebras y daremos el concepto de álgebra generada. Analizaremos con cierto detalle el álgebra generada por una matriz, una matriz elemental de Jordan y su transpuesta, un operador lineal y un operador proyección. Finalmente expondremos algunos ejemplos de álgebras generadas por ciertas matrices que nos ayudaran a dar una descripción mas precisa del álgebra generada por un operador lineal en un espacio vectorial de dimensión finita arbitrario.

Abstract

An algebra is a vector space V over a field $\mathbf{F}$ equipped with a bilinear product $\odot : V \times V \to V$. If this product is commutative, the algebra is called a commutative algebra. This algebraic structure appears in areas such as functional analysis and differential geometry.

The objective of this project is to present the basic concepts of this structure, focusing on the case where the vector space is finite-dimensional. We also aim to provide a description, up to isomorphism, of the algebra generated by an arbitrary linear operator on a finite-dimensional space. This algebra is isomorphic to the direct sum of algebras generated by a special nilpotent matrix. To achieve this, we will present the theory necessary to prove the Primary Decomposition Theorem and the Jordan Decomposition Theorem.

We begin by presenting some algebraic preliminaries regarding ring theory, ideals, and polynomials. Subsequently, we study projection operators and direct sums of subspaces. These results are necessary to carry out the proofs of the Primary Decomposition and Jordan Decomposition theorems. We continue by defining the external direct sum. In the following chapter, we provide the formal definition of an algebra, present examples, and introduce the concept of a generated algebra. We analyze in detail the algebra generated by a matrix, an elementary Jordan matrix and its transpose, a linear operator, and a projection operator. Finally, we present examples of algebras generated by specific matrices that allow for a more precise description of the algebra generated by a linear operator on an arbitrary finite-dimensional vector space.

Introducción

A finales del siglo XIX algunos matemáticos notaron que era posible hallar las soluciones de ecuaciones diferenciale y ecuaciones integrales centrándose en analizar un conjunto de funciones cuyo argumento eran funciones sobre un conjunto X y cuya imagen era nuevamente una función con domnio el mismo conjunto X. Estas funciones fueron llamadas operadores. Se estudio como interactuaban conjuntos de operadores con una determinada propiedad. En este estudio se buscaba que el conjunto de operadores tuvieran una estructura que les permitiera hacer "álgebra", dicho de otra forma que les permitiera realizar multiplicaciión de operadores. La estructura que se obtuvo fue nombrada álgebra.

Un álgebra es un espacio vectorial V sobre un campo $\mathbf{F}$ en el cual se define un producto entre vectores $\odot : V \times V :\rightarrow V$, el cual es bilineal y asosiativo. En caso de que este producto sea conmutativo diremos que el álgebra es una álgebra conmutativa y si $DimV < +\infty$ diremos que es un álgebra finita. En el área de análisis funcional se estudian distintos tipos de álgebras: Álgebras de operadores, álgebras C^*, álgebras de Banach, álgebras de Von Neumann entre otras.

En la presente proyecto se busca presentar los conceptos básicos de esta estructura centrándonos en el caso cuando el espacio vectorial es de dimensión finita. Ya que en este caso se puede estudiar la estructura sin la necesidad de cocnceptos topologicos.

Nuestro segundo objetivo principal es describir de una manera detallada el álgebra generada por un operador lineal. El álgebra generada por un operador resulta ser isomorfa a la suma directa de álgebras generadas por bloques de Jordan con valor propio 0. Estas álgebras son bastante sencillas de visualizar. Siendo un subconjunto de las matrices triangulares superiores. Con este propósito presentaremos los elementos necesarios para realizar las pruebas de los teoremas de la descomposición prima y la descomposición de Jordan. El teorema de la descomposición primaria nos permite obtener ciertas proyecciones que resultan ser polinomios de un operador T y por lo tanto pertenecen al álgebra generada por T que nos permitirán en cierto sentido separar la información de la representación matricial del operador. El teorema de la descomposición de Jordan nos permitirá probar que el álgebra generada por un operador T es isomorfa a cualquier representación matricial de este operador. En particular a la forma de Jordan de la matriz que lo representa. Una vez probado esto veremos que es posible limitarnos a estudiar el álgebra generada por matrices de Jordan.

Como ya se mencionó nos limitaremos al caso de un álgebra finita con el propósito de evitar introducir conceptos topológicos. De esta manera es posible leer el presente trabajo contando únicamente con cierta familiaridad con las nociones básicas de teoría de grupos. Conociendo los teoremas de homomorfismo. Y habiendo cursado los primeros cursos de álgebra lineal, o en su defecto, contando con los conocimientos de vectores y valores propios.

Preliminares

El propósito general de este trabajo es describir el álgebra generada por un operador lineal, en este sentido la forma canónica de Jordan permite hacer la descripción. Para poder realizar la prueba del Teorema de la descomposición de Jordan requerimos de ciertos resultados de operadores de proyección y suma directa de subespacios. Estos conceptos también nos ayudaran a entender el tema de álgebras. Por este motivo expondremos los conceptos que consideramos esenciales para entender las demostraciones que realizaremos en este trabajo.

4.1 Anillo de polinomios.

Los polinomios aparecen constantemente al momento de probar el teorema de la descomposición prima, y al momento de describir el álgebra generada una matriz. Por esta razón decidimos dedicar esta breve sección a recordar los conceptos que nos parecen esenciales para poder comprender los temas que expondremos en los siguientes capítulos.

Definición 1 (**Anillo**). *Un anillo R es un conjunto junto con 2 operaciones binarias $+$ y $\cdot$, llamadas suma y producto, que satisfacen:*

1) $(R, +)$ *es un grupo abeliano.*

2) $\cdot$ *es asociativo:* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *para todo* $a, b, c \in R$.

3) La ley distributiva se cumple en R: para todo $a, b, c \in R$

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c) \quad y \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

Si además R tiene un elemento I tal que

$$Ia = aI \quad \forall a \in R,$$

entonces se dice que R es un anillo con unidad (unidad multiplicativa). Se dice que R es un anillo conmutativo si $a \cdot b = b \cdot a$.

Definición 2 (**Espacio de polinomios**). *Sea* $\mathbb{F}$ *un campo. El espacio de polinomios en x de grado a lo más n y con coeficientes en* $\mathbb{F}$ *se denota por* $\mathbb{F}_n[x]$*:*

$$\mathbb{F}_n[x] = \{a_0 + a_1 x + ... + a_n x^n | \, a_j \in \mathbb{F}, j = 1, ..., n\}.$$

El conjunto de polinomios en x sobre $\mathbb{F}$ *se denota por* $\mathbb{F}[x]$*:*

$$\mathbb{F}[x] = \bigcup_{n=0}^{\infty} \mathbb{F}_n[x].$$

Las constantes distintas de cero son polinomios de grado cero. Dos polinomios $f(x) = f_0 + f_1 x + \cdots + f_n x^n$ *y* $g(x) = g_0 + g_1 x + \cdots + g_k x^k$ *son iguales si* $n = k$ *y* $f_i = g_i$ *para todo i.*

Se pueden definir operaciones de suma y producto en $\mathbb{F}[X]$ de tal manera que $\mathbb{F}[x]$ con la suma y producto sea un anillo. Para los polinomios

$$f(x) = f_n x^n + \cdots + f_0$$

y

$$g(x) = g_n x^n + \cdots + g_0,$$

la suma de f y g se define como

$$f(x) + g(x) = \sum_{i=0}^{n} (f_i + g_i) x^i.$$

Aquí los coeficientes f_n o g_n pueden ser cero, los polinomios se expresan así para sumar polinomios de distintos grados indicando que la suma se realiza coeficiente a coeficiente. El producto de los polinomios $f(x), h(x)$ se define como

$$f(x)g(x) = \left(\sum_{i=0}^{n} f_i x^i\right)\left(\sum_{i=0}^{m} h_i x^i\right) = \sum_{k=0}^{n+m}\left(\sum_{i=0}^{k} f_i h_{k-i}\right) x^k.$$

Proposición 1. *El conjunto $\mathbb{F}[x]$ es un anillo conmutativo con unidad con las operaciones de suma, producto y multiplicación por escalares anteriormente definidas.*

Demostración 1. *Sólo se realizarán las pruebas para el producto, pues las propiedades de la suma se siguen inmediatamente de la definición de suma de polinomios. Sean p, q, s polinomios con coeficientes $p_0, \cdots, p_n, q_0, \cdots, q_m, s_0, \cdots, s_k$. Para probar la asociatividad del producto veamos que el coeficiente de la potencia x^k del polinomio $(pq)s$ es*

$$\sum_{i=0}^{k}\left(\sum_{j=o}^{i} p_j q_{i-j}\right) s_{k-i} = \sum_{i=0}^{k}\sum_{j=0}^{i} p_j q_{i-j} s_{k-i} = \sum_{j=0}^{k} p_j \sum_{i=0}^{k-j} q_i s_{k-i-j}.$$

Notemos que el coeficiente de la potencia x^k del polinomio $p(qs)$ es precisamente $\sum_{i=0}^{k} p_i(\sum_{j=0}^{k-i} q_j s_{k-j-i})$, de donde se sigue que $p(qs) = (pq)s$.

***Distribuitividad por la izquierda**. El k-ésimo coeficiente del polinomio $p(q + s)$ es*

$$\sum_{i=0}^{k} p_i(q+s)_{k-i} = \sum_{i=0}^{k} p_i(q_{k-i} + s_{k-i}) = \sum_{i=0}^{k} p_i q_{k-i} + \sum_{i=0}^{k} p_i s_{k-i}.$$

La última suma es el k-ésimo coeficiente de $pq + ps$. La conmutativiad se sigue de la siguiente igualdad

$$\sum_{i=0}^{k} p_i q_{k-i} = \sum_{i=0}^{k} p_{k-i} q_i,$$

y finalmente la identidad en $\mathbb{F}[x]$ es la identidad de $\mathbb{F}$. ■.

Más aun, $\mathbb{F}[x]$ es un anillo entero, es decir, no tiene divisores propios del cero:

$$p(x)q(x) = 0 \implies p(x) = 0 \quad \text{o} \quad q(x) = 0,$$

donde se entiende que $a_0 + a_1 x + ... + a_n x^n = 0$ si, y solo si $a_i = 0$ para todo $i \in \{1, 2, ..., n\}$.

Proposición 2 (**Algoritmo de la división**). *Sea* $\mathbb{F}$ *un cuerpo. Si* $f, d \in \mathbb{F}[x]$ *y* $d \neq 0$*, entonces existen polinomios* $q, r \in \mathbb{F}[x]$ *tales que*

1. $f = dq + r$.

2. $r = 0$ *ó* $grad(r) < grad(d)$.

Definición 3 (**Subanillo**). *Un subconjunto* $\mathbb{K} \subset \mathbb{F}[x]$ *es un subanillo si* $\mathbb{K}$ *es un anillo con las operaciones de* $\mathbb{F}[x]$*, es decir,* $\mathbb{K}$ *satisface los 7 axiomas de anillo con la suma y producto definidas en* $\mathbb{F}[x]$.

La siguiente caracterización de subanillo es muy útil.

Lema 1. *Sea* $\mathbb{K} \subset \mathbb{F}[x]$ *distinto del vacío. Entonces* $\mathbb{K}$ *es un subanillo si, y sólo si se cumplen las siguientes condiciones*

1. $p, q \in \mathbb{K} \implies p - q \in \mathbb{K}$,

2. $p, q \in \mathbb{K} \implies p \cdot q \in \mathbb{K}$.

Es decir que sea cerrado bajo diferencias y productos.

Demostración 2.
$\Rightarrow$ *Se sigue de que* $\mathbb{F}[x]$ *es un anillo.*
$\Leftarrow$ *Tomando* $p \in \mathbb{K}$*, hacemos* $q = p$*, entonces* $0 = p - q \in \mathbb{K}$*, además* $-p = 0 - p \in \mathbb{K}$*. Ahora tomamos cualesquiera* $p, q \in \mathbb{K}$*, entonces* $-q \in \mathbb{K}$ *y* $p + q = p - (-q) \in \mathbb{K}$*. Luego* $(\mathbb{K}, +)$ *es un grupo Abeliano. Así* $\mathbb{K}$ *es un anillo porque el resto de propiedades se heredan.* ■

Nota 1. *Tanto la definición de subanillo, como la prueba del lema anterior siguen siendo válidas si* $\mathbb{F}[x]$ *se cambia por cualquier anillo.*

Ejemplo 1. *Sea* $\mathbb{K}$ *el conjunto de polinomios con potencias pares*

$$\mathbb{K} = \{a_0 + a_1 x^2 + ... + a_n x^{2n} | \, a_j \in \mathbb{F}\}.$$

Entonces $\mathbb{K}$ *es un subanillo de* $\mathbb{F}[x]$.

4.2 Ideales.

Los ideales surgen de manera natural como núcleos de homomorfismos de anillos y se utilizan para describir estructuras algebraicas mas sencillas obtenidos mediante cocientes.

Definición 4 (Ideal). *Un subanillo I de $\mathbb{F}[x]$ es un ideal si $pq \in I$ para todo $p \in I$ y para todo $q \in \mathbb{F}[x]$.*

Veamos algunos ejemplos.

Ejemplo 2. *El conjunto de polinomios que tienen a cero como raíz de multiplicad mayor o igual a 2*

$$I_{x^2} = \{a_2x^2 + a_3x^3 + ... + a_nx^n | \, a_j \in \mathbb{F}\}$$

es un ideal de $\mathbb{F}[x]$, puesto que dados $p \in \mathbb{F}[x]$ y $q \in I$ el producto pq tiene al cero como raíz de multiplicidad al menos 2.

Ejemplo 3. *De manera general los polinomios que tienen a cero como raíz de multiplicidad mayor o igual a n que denotamos como*

$$I_{x^n} = \{a_nx^n + a_{n+1}x^{n+1} + ... + a_{n+k}x^{n+k} | \, a_j \in \mathbb{F}\}$$

son un ideal en el anillo $\mathbb{F}[x]$.

Nota: $\mathbb{K}$ del Ejemplo 1 es un anillo pero no es un ideal. Dados $p(x) = 1 + x^2 \in \mathbb{K}$ y $q(x) = x$, el producto $p(x)q(x) = x + x^3$ no pertenece a $\mathbb{K}$.

Proposición 3. *Sea R un anillo y $\{I_\alpha\}_{\alpha\in\Lambda}$ una familia de ideales. Entonces*

$$\bigcap_{\alpha\in\Lambda} I_\alpha$$

es un ideal.

Demostración 3. *La prueba es análoga a la dada en en el Lema 27.*

Ejemplo 4. *Dado $p_0 \in \mathbb{F}[x]$, el conjunto de todos los múltiplos de p_0 es un ideal, es decir,*

$$I_{p_0} = \{r(x)p_0(x) | \, r(x) \in \mathbb{F}[x]\}$$

es un ideal. En efecto, tomemos $p, q \in I_{p_0}$, es decir, existen $r_1, r_2 \in \mathbb{F}[x]$ tal que

$$p = r_1p_0 \quad y \quad q = r_2p_0.$$

Así

$$p - q = r_1p_0 - r_2p_0 = (r_1 - r_2)p_0 \in I_{p_0},$$
$$p \cdot q = r_1r_2p_0^2 = (r_1r_2p_0)p_0 \in I_{p_0}.\blacksquare$$

Definición 5 (Ideal Principal generado por a). *Sea R un anillo conmutativo, y $a \in R$. El ideal*

$$I_a = \{x \in R | \, x = ra \quad para\ algún \quad r \in R\}$$

es llamado el ideal principal generado por a. Desde luego $a \in I_a$ si R tiene unidad.

Notación 1. *El ideal generado por a se denota por I_a o por Ra. Aunque preferimos usar la notación I_a.*

Proposición 4. *Sea R un anillo conmutativo con unidad y $a \in R$. El ideal principal generado por a es la intersección de todos los ideales que contienen a a.*

Demostración 4. *Por definición de intersección de conjuntos tenemos que*

$$\bigcap \{I : I \text{ sea un ideal que contiene a } a\} \subset I_a.$$

Ahora bien, todo ideal que contenga a a debe de contener a I_a, por definición de I_a. Como la intersección de ideales es a su vez un ideal tenemos que en particular $I_a \subset \bigcap \{I : I \text{ sea un ideal que contiene a } a\}$. De donde concluimos que el ideal generado por a es igual a la intersección de todos los ideales que contienen a a ■.

Lema 2. *Todo ideal I de $\mathbb{F}[x]$ es un ideal principal, es decir, existe un polinomio $p_0 \in \mathbb{F}[x]$ tal que $I = I_{p_0} = \{rp_0 | \ r \in \mathbb{F}[x]\}$.*

Demostración 5. *Sea I un ideal de $\mathbb{F}[x]$. Si $I = \{0\}$, entonces $I = I_0$. Supongamos que $I \neq \{0\}$. Sea $p_0 \in I$ un polinomio no nulo de grado mínimo. Veamos que $I = I_{p_0}$. Como I es un ideal tenemos que*

$$I_{p_0} = \{rp_0 | \ r \in \mathbb{F}[x]\} \subset I.$$

Veamos que $I \subset I_{p_0}$. Tomemos $p \in I$, debemos demostrar que $p \in I_{p_0}$, esto es, debemos probar que existe $r \in \mathbb{F}[x]$ tal que

$$p = rp_0.$$

Por el algoritmo de la división, existen polinomios $r, t \in \mathbb{F}[x]$ tales que

$$p = rp_0 + t,$$

donde $deg(t) < deg(p_0)$ si $t \neq 0$, o $t = 0$. Veamos que $t = 0$. En efecto, por contradicción supongamos que $t \neq 0$, entonces

$$t = p - rp_0 \in I,$$
$$deg(t) < deg(p_0).$$

Pero esto contradice que $p_0 \in I$ es un polinomio de grado mínimo. Así $t = 0$ y $p = rp_0 \in I_{p_0}$. ■

Ejemplo 5. *Tenemos los siguientes ideales*

1) I_x,

2) I_{x^2},

3) I_{x^4},

4) $I_{1+x} = \{r(x)(1+x) | \ r \in \mathbb{F}[x]\}$.

4.3 Máximo común divisor.

Algunos resultados útiles de divisibilidad se presentarán en esta sección. El máximo común puede utilizarse para identificar subespacios invariantes de transformaciones lineales.

Definición 6. *Sean $f, g \in \mathbb{F}[x]$, decimos que g divide a f si existe $q \in \mathbb{F}[x]$ tal que*

$$f = qg.$$

En este caso se escribe $g|f$.

Definición 7 (Máximo común divisor). *Dados dos polinomios $p, q \in \mathbb{F}[x]$, se dice que $t \in \mathbb{F}[x]$ es común divisor de p, q si*

$$t|p \quad y \quad t|q.$$

Se dice que $d \in \mathbb{F}[x]$ es el máximo común divisor de p y q si es divisor común de p y q; y si t es otro divisor común, entonces

$$t|d.$$

Ejemplo 6. *Si $p(x) = x^2 - 3x + 2$ y $q(x) = x^2 - 4x + 3$, entonces un común divisor de p y q es $t(x) = x - 1$, puesto que $p(x) = (x-1)(x-2)$ y $q(x) = (x-1)(x-3)$.*

Ejemplo 7. *Si $p(x) = (x-1)^3(x-2)^4$ y $q(x) = (x-1)^2(x-2)^3$, entonces un común divisor es $t(x) = (x-1)(x-2)$ pero el máximo común divisor es $d(x) = (x-1)^2(x-2)^3$.*

Existe una forma de calcular el máximo común divisor de los polinomios p y q en $\mathbb{C}[x]$ usando el teorema fundamental del álgebra. Sean $p, q \in \mathbb{C}[x]$. Por el teorema fundamental del álgebra, tenemos que los polinomios $p(x)$ y $q(x)$ se reducen a productos de factores lineales

$$p(x) = (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2}...(x - \alpha_j)^{n_j},$$
$$q(x) = (x - \beta_1)^{m_1}(x - \beta_2)^{m_2}...(x - \beta_k)^{m_k},$$

donde

$$n = \deg(p) = n_1 + n_2 + ... + n_j,$$
$$m = \deg(q) = m_1 + m_2 + ... + m_k,$$

$\alpha_1, \alpha_2, ..., \alpha_j$ son las raíces distintas de p, y $\beta_1, \beta_2, ..., \beta_k$ las raíces distintas de q.

Buscamos las raíces comunes y las nombramos $\zeta_1, \zeta_2, ..., \zeta_l$. Cada ζ_i es raíz múltiple de p y q, tomamos la multiplicidad mínima de cada raíz ζ_i y la denotamos por e_i. Entonces el máximo común divisor de p y q es

$$d(x) = (x - \zeta_1)^{e_1}(x - \zeta_2)^{e_2}...(x - \zeta_l)^{e_l}.$$

En el caso de $\mathbb{F} = \mathbb{R}$, p y q se reducen a factores lineales y cuadráticos, donde los factores cuadráticos son irreducibles en $\mathbb{R}$, es decir, aportan raíces complejas. Explicaremos el método de calcular el máximo común divisor con un ejemplo.

Ejemplo 8. *Tomemos*

$$p(x) = (x-1)^4(x^2+x+1)^3(x-2)^5$$
$$q(x) = (x-1)^2(x^2+x+1)^5(x-2)^7$$

En este caso el máximo común divisor es $d(x) = (x-1)^2(x^2+x+1)^3(x-2)^5$.

Este método consiste en hallar una factorización irreducible sobre $\mathbb{F}$ de los polinomios; sin embargo, podemos usar el algoritmo de la división para hallar el máximo común divisor. El cálculo del máximo común divisor con este método es como sigue. Dados p, q polinomios en $\mathbb{F}[x]$, tales que ninguno es múltiplo del otro, podemos aplicar iteradammente el algoritmo de la división para obtener una sucesión de polinomios tales que

$$\begin{aligned}
p &= qs_1 + r_1, \quad grad(r_1) < grad(q)\\
q &= r_1 s_2 + r_2, \quad grad(r_2) < grad(r_1)\\
r_1 &= r_2 s_3 + r_3, \quad grad(r_3) < grad(r_2)\\
&\vdots\\
r_{n-2} &= r_{n-1} s_n + r_n, \quad grad(r_n) < grad(r_{n-1})\\
r_{n-1} &= r_n s_{n+1}.
\end{aligned}$$

Aquí r_n resulta ser el máximo común divisor de p y q.

Teóricamente el m.c.d. se calcula tomando en cuenta un ideal de $\mathbb{F}[x]$. Tomemos $p, q \in \mathbb{F}[x]$ y formemos el conjunto

$$I = I_{p,q} = \{rp + sq |\ r, s \in \mathbb{F}[x]\}.$$

Veremos que esto es un ideal. Además, todo divisor de p y de q es divisor de los elementos de $I_{p,q}$ y como veremos el este ideal tiene un generador. Por lo cual ese generador debe de ser el máximo común divisor

Ejemplo 9. *Si* $p(x) = x^2$ *y* $q(x) = x + 1$, *entonces*

$$I_{p,q} = \{x^2 r(x) + (x+1)s(x) |\ r, s \in \mathbb{F}[x]\}.$$

Si $r(x) = x^2 + 2x$ *y* $s(x) = x^3$, *entonces*

$$x^2(x^2+2x) + (x+1)x^3 = 2x^4 + 3x^3 \in I_{p,q}.$$

Lema 3. *El conjunto* $I_{p,q}$ *es un ideal de* $\mathbb{F}[x]$.

Demostración 6. *Primero demostraremos que el conjunto* $I_{p,q}$ *es un subanillo. Dados* $u, w \in I_{p,q}$, *veamos que* $u - w, uw \in I_{p,q}$. *Por definición de* $I_{p,q}$ *existen polinomios* r_1, r_2, s_1 *y* s_2 *tales que*

$$u(x) = p(x)r_1(x) + q(x)s_1(x),$$
$$w(x) = p(x)r_2(x) + q(x)s_2(x).$$

Por lo cual

$$u(x) - w(x) = p(x)[r_1(x) - r_2(x)] + q(x)[s_1(x) - s_2(x)] \in I_{p,q},$$
$$u(x)w(x) = p(x)w(x)r_1(x) + q(x)w(x)s_1(x) \in I_{p,q}.$$

Esto demuestra que $I_{p.q}$ es un subanillo. Para ver que $I_{p,q}$ es un ideal. Sean $w \in \mathbb{F}[x]$ y $u(x) = p(x)r_1(x) + q(x)s_1(x) \in I_{p,q}$. Tenemos que

$$u(x)w(x) = p(x)w(x)r_1(x) + q(x)w(x)s_1(x) \in I_{p,q}.$$

Por lo $I_{p,q}$ es un ideal de $\mathbb{F}[x]$. ■

Lema 4. *Existe $p_0 \in \mathbb{F}[x]$ tal que*

$$I_{p,q} = I_{p_0}$$

.

Demostración 7. *Sea p_0 un polinomio de grado mínimo en $I_{p,q}$. Entonces*

$$I_{p,q} = I_{p_0}.\blacksquare$$

Ejemplo 10. *Tomemos $p(x) = x + 2$ y $q(x) = x - 4$. Entonces*

$$I_{p,q} = \{r(x)(x + 2) + s(x)(x - 4) |\ r, s \in \mathbb{F}[x]\}$$

es un anillo de polinomios, pero además notemos que los polinomios constantes están en $I_{p,q}$. En particular $1 \in I_{p,q}$. Para probar esto tomemos $r_1(x) = \frac{1}{6}$ y $s_1(x) = -\frac{1}{6}$, entonces

$$r_1(x)(x + 2) + s_1(x)(x - 4) = \frac{1}{6}(x + 2) - \frac{1}{6}(x - 4) = \frac{1}{3} + \frac{2}{3} = 1.$$

Por esta razón el ideal generado por p, q debe ser todo el espacio de polinomios, cualquier polinomio p se puede escribir en la forma

$$p(x) = p(x) \cdot 1 = r(x)(x + 2) + s(x)(x - 4),$$

donde $r(x) = p(x)/6$ y $s(x) = -p(x)/6$.

Lema 5. *Un máximo común divisor de p, q es el polinomio p_0 tal que*

$$I_{p,q} = I_{p_0}.$$

Si p_0 es mónico, entonces p_0 es único.

Demostración 8. *Primero probemos que $p_0|p$ y $p_0|q$. Tomando $r = 1$ y $s = 0$ se obtiene que*

$$p = rp + sq \in I_{p,q}.$$

De manera análoga, tomando $r = 0$ y $s = 1$ justificamos que $q \in I_{p,q}$. Ahora $I_{p,q} = I_{p_0} = \{tp_0 |\ t \in \mathbb{F}[x]\}$, así p y q son múltiplos de p_0, luego existen polinomios t_1 y t_2 tales que $p = t_1p_0$ y $q = t_2p_0$, esto es, $p_0|p$ y $p_0|q$.

Sea h un común divisor de p y q. Queremos demostrar que $h|p_0$. Ahora $p_0 = p_0 \cdot 1 \in I_{p_0} = I_{p,q}$, luego existe r y s tales que $p_0 = rp + sq$. Entonces h divide a p_0 porque divide a p y a q. ■

Definición 8. *Se dice que p, q son primos relativos, y se escribe $(p, q) = 1$, si el máximo común divisor es 1.*

Ejemplo 11. *Los polinomios $p(x) = x + 2$ y $q(x) = x - 4$ son primos relativos porque el máximo común divisor es el polinomio $d(x) = 1$.*

Definición 9 (Máximo común divisor.)**.** *Sean $p_1, p_2, ..., p_m$ polinomios distintos de cero. El máximo común divisor de $p_1, p_2, ..., p_m$ es el polinomio mónico d tal que*

$$d|p_j,\ \ j = 1, 2, ..., m$$
$$si\ h|p_j,\ \ j = 1, 2, ...m\ entonces\ h|d.$$

El máximo común divisor se denota por $d = m.c.d(p_1, p_2, ..., p_m)$.

Lema 6. *Consideremos tres polinomios p_1, p_2 y p_3. Sea $d_1 = m.c.d(p_1, p_2)$. Entonces*

$$d = m.c.d.(p_1, p_2, p_3) = m.c.d.(d_1, p_3).$$

Demostración 9. *Sea $t = m.c.d(d_1, p_3)$. Demostraremos que $t = d$, es decir, demostraremos que*

$$t|p_j,\ \ j = 1, 2, 3$$
$$si\ h|p_j,\ \ j = 1, 2, 3\ entonces\ h|t.$$

Por definición de t, este polinomio divide a d_1 y p_3. Como $d_1 = m.c.d(p_1, p_2)$, entonces d_1 divide a p_1 y p_2, luego t divide a p_1 y p_2. Así t divide a p_1, p_2 y p_3. Supongamos que $h|p_j,\ \ j = 1, 2, 3$. En particular h divide a p_1 y p_2, así

$$h|d_1.$$

Como h divide a p_3 , entonces $h|t$. ■

Antes de concluir esta sección recordemos un importante resultado llamado teorema de Cayley-Hamilton.

Consideremos una matriz A de dimensión $n \times n$, representando un operador $T_A : \mathbb{C}^n \to \mathbb{C}^n$, dado por $T_A(X) = AX$. Tomemos el polinomio característico

$$p(x) = \det(xI - A).$$

El teorema de Cayley-Hamilton dice que

$$p(A) = 0.$$

Sea

$$I = \{q \in \mathbb{C}[x] : q(A) = 0\}.$$

Desde luego $p \in I$. Notemos que el conjunto I es un ideal de $\mathbb{C}[x]$, ya que dados $q \in I$ y $r \in \mathbb{C}[x]$, entonces $q(A)r(A) = 0 \cdot r(A) = 0$, también si $q, r \in I$, entonces $q(A) - r(A) = 0 - 0 = 0$. Pero $\mathbb{C}[x]$ es un anillo de ideales principales, luego existe $p_m \in I$ mónico tal que

$$I = I_{p_m}.$$

El polinomio p_m es de grado mínimo que anula a A, es decir, p_m es el polinomio minimal de A.

Teorema 1. *El polinomio p_m divide a p. Además p_m tiene todas las raíces de p salvo multiplicidad.*

Por ejemplo si A es una matriz cuyo polinomio característico es

$$p(x) = (x-2)^3(x-3)^4(x-5),$$

entonces el polinomio minimal es alguno de los siguientes

$$(x-2)^i(x-3)^j(x-5)$$

con $1 \leq i \leq 3$ y $1 \leq j \leq 4$.

4.4 Proyecciones.

El teorema de la descomposición prima se prueba hallando ciertos operadores que nos aseguren que el espacio es suma directa de sus imágenes. Estos operadores son proyecciones sobre subespacios invariantes. En la presente sección daremos la definición de una proyección y algunos resultados que nos relacionan el kernel y la imagen de una proyección.

Definición 10 (Proyección). *Sea V un espacio vectorial sobre un campo $\mathbb{F}$ de dimensión finita. Una transformacion lineal $P : V \to V$se dice que es una proyección si es idempotente, es decir,*

$$P^2 = P.$$

Sea N el espacio nulo de P y R su imagen. Decimos que P es la proyección sobre R a lo largo o paralelamente a N.

Es fácil verificar que si P es proyección, entonces también lo es $I - P$. Este resultado sera útil en las siguientes demostraciones.

Ejemplo 12. *Sea $\mathbb{R}^n$. Considérese el operador lineal*

$$\pi_1 : \mathbb{R}^n \to \mathbb{R}^n$$
$$(x_1, \cdots, x_n) \mapsto (x_1, 0 \cdots, 0).$$

Es fácil probar que el operador π_1 es en efecto una proyección. Notemos que este operador es un caso especial del operador lineal en $\mathbb{R}^n$ cuyo efecto sobre la base canónica es el siguiente

$$\pi_i(e_j) = \delta_{ij} e_j.$$

Continuaremos enunciando las propiedades de los operadores proyección que vamos a utilizar.

Lema 7. *Sea P una proyección en un espacio vectorial V. Un vector v está en la imagen de P si, y sólo si $v = Pv$.*

Demostración 10.
$\Rightarrow$ *Sea* $v \in Im(P)$*. Existe* $w \in V$ *tal que* $v = Pw$*, entonces* $Pv = P^2w = Pw = v$*.*

$\Leftarrow$ *Si* $v = Pv$ *es obvio que* $v \in Im(P)$*.* ■

Lema 8. *Sea* P *un operador líneal sobre un espacio vectorial* V*. Si* P *es una proyección se cumple que*

$$\ker(P) = Im(I - P),$$
$$Im(P) = \ker(I - P).$$

Demostración 11. *Sea* $v \in Im(P)$*. Por el Lema 7 tenemos que* $v = Pv$*, así*

$$(I - P)v = v - Pv = v - v = 0,$$

de donde se sigue que $v \in \ker(I - P)$*. Si* $w \in \ker(I - P)$*, entonces* $w = Pw$*, por el Lema 7 se tiene que* $w \in Im(P)$*, por lo tanto* $Im(P) = \ker(I - P)$*. La prueba de la otra igualdad es análoga, sólo considerando* $I - P$ *en lugar de* P *en el lema 7.* ■

4.5 Suma directa de subespacios.

La suma directa nos permitirá obtener información del espacio, centrándonos en estudiar subespacios vectoriales que sean más pequeños. Además, cuando el espacio es suma directa de subespacios podemos formar una base del espacio uniendo bases de cada subespacio. Esto nos ayudara al momento de realizar la prueba del teorema de la descomposición de Jordan.

Definición 11. *Sean* $W_1, W_2, \cdots, W_k$ *subespacios vectoriales de un espacio vectorial* V*. Se dice que* $W_1, \cdots, W_k$ *son independientes si*

$$w_1 + \cdots + w_k = 0, \quad w_i \in W_i$$

implica que $w_i = 0$ *para todo* i*.*

Lema 9. *Sea* V *un espacio vectorial de dimensión finita y* W_1, W_2 *subespacios vectoriales de* V*. Entonces* W_1 *y* W_2 *son independientes si, y sólo si* $W_1 \cap W_2 = \{0\}$*.*

Demostración 12. $\Rightarrow$ *Sea* $v \in W_1 \cap W_2$*. Por ser* W_1 *y* W_2 *independientes tenemos que* $v + (-v) = 0$ *implica que* $v = 0$*.*
$\Leftarrow$ *Si existen* $v_1 \in W_1$ *y* $v_2 \in W_2$ *tales que* $v_1 + v_2 = 0$*, entonces* $-v_2 = v_1 \in W_1 \cap W_2$*, por lo tanto* $v_1 = 0$ *y* $v_2 = 0$*. Esto es,* W_1 *y* W_2 *son independientes.* ■

Definición 12 (Espacio suma). *Sean* $V_1, \cdots, V_n$ *subespacios vectoriales de un espacio vectorial* V*. Se define su suma como*

$$V_1 + \cdots + V_n = \{v_1 + \cdots + v_n : v_j \in V_j\}.$$

Proposición 5. *Sean $V_1, \cdots, V_n$ subespacios vectoriales de un espacio vectorial V. El conjunto $V_1 + \cdots + V_n$ es un subespacio vectorial de V.*

Demostración 13. *Sean $v, w \in V_1 + \cdots + V_n$ y $c \in \mathbb{F}$. Entonces*

$$cv + w = c(v_1 + \cdots + v_n) + (w_1 + \cdots + w_n) = (cv_1 + w_1) + \cdots + (cv_n + w_n)$$

con $v_i, w_i \in V_i$. Por ser V_i espacio vectorial tenemos que $cv_i + w_i \in V_i$, por lo tanto $cv + w \in V_1 + \cdots + V_n$. La suma de $V_1, \cdots, V_n$ es un subespacio vectorial. ■

Lema 10. *Sea V un espacio vectorial de dimensión finita y $V_1, \cdots, V_n$ subespacios de V. Entonces $V_1, \cdots, V_n$ son independientes si, y sólo si cada vector v en $V_1 + \cdots + V_n$ puede ser expresando de manera única como*

$$v = v_1 + \cdots + v_n, \quad v_i \in V_i.$$

Demostración 14. $\Rightarrow$ *Sea $v \in V_1 + \cdots + V_n$, entonces existen vectores $v_1, \cdots, v_n$ con $v_i \in V_i$ tales que*

$$v = v_1 + \cdots + v_n \quad v_i \in V_i$$

y si además

$$v = w_1 + \cdots + w_n \quad w_i \in V_i,$$

entonces $0 = (v_1 - w_1) + \cdots (v_n - w_n)$. Por hipótesis tenemos que $v_i - w_i = 0$, es decir, $v_i = w_i$ para todo $i = 1, \cdots, n$.
$\Leftarrow$ *Recíprocamente, si cada vector en $V_1 + \cdots + V_n$ puede ser expresado de manera única tenemos que $V_1, \cdots, V_n$ son independientes, pues si $v_1 + \cdots + v_n = 0$, entonces $0 = 0 + \cdots + 0$ implica que $v_i = 0$.* ■

Definición 13 (Suma directa de subespacios). *Se dice que V es suma directa de los subespacios $V_1, \cdots, V_m$, y se escribe*

$$V = V_1 \oplus \cdots \oplus V_m,$$

si $V = V_1 + \cdots + V_m$ y cada vector se representa de manera única como

$$v = v_1 + \cdots + v_m \quad v_j \in V_j,$$

o dicho de otra forma, V es la suma de espacios independientes $V_1, \cdots, V_m$.

Ejemplo 13. *Sean $V = \mathbb{R}^2$, $V_1 =< (1,0) >$, $V_2 =< (0,1) >$ y $V_3 =< (1,1) >$. Tenemos que $V = \mathbb{R}^2 = V_1 + V_2 + V_3$ pero la suma no es directa, puesto que $(1,2) = 2(1,0) + 3(0,1) - 1(1,1)$. Sin embargo, $V = V_1 \oplus V_2$.*

Ejemplo 14. *Sea n un entero positivo y $V = \mathbb{M}_n(\mathbb{C})$. Sea V_1 el espacio de todas las matirces simétricas, es decir, matrices A tales que $A^T = A$. Sea V_2 el subepsacio de todas las matrices antisimétricas, es decir,*

matrices A tales que $A^T = -A$. Entonces $V = V_1 \oplus V_2$. Si A es cualquier matriz de V, la expresión única para A como suma de matrices, una de V_1 y la otra de V_2, es

$$A = A_1 + A_2,$$
$$A_1 = \frac{1}{2}(A + A^T),$$
$$A_2 = \frac{1}{2}(A - A^T).$$

El siguiente Lema nos permite relacionar el concepto de operador proyección y de suma directa de subespacios.

Lema 11. *Sea P una proyección en un espacio vectorial V. Se cumple que*

$$V = Im(P) \oplus \ker(P).$$

Demostración 15.
Primero notemos que $V = Im(p) + \ker(p)$. En efecto, cualquier $v \in V$ se puede expresar como

$$v = Pv + (Iv - Pv),$$

con $pv \in Im(P)$ y $Iv - Pv \in \ker(P)$. Sólo falta probar que $Im(P)$ y $\ker(P)$ son independientes. Notemos que si $v \in (Im(P) \cap \ker(P))$, por el Lema 7 tenemos que $v = Pv = 0$, de donde se sigue que $(Im(P) \cap ker(P)) = \{0\}$. Por el Lema 9, $Im(P)$ y $ker(P)$ son independientes. Por lo tanto

$$V = Im(P) \oplus \ker(P).\blacksquare$$

Lema 12. *Sea V un espacio vectorial de dimensión finita y $W_1, \cdots, W_m$ subespacios de V. Sea $W = W_1 + \cdots + W_m$. Las siguientes afirmaciones son equivalentes:*

1) $W_1, \cdots, W_m$ son independientes.

2) Para todo j, $2 \leq j \leq m$, se tiene

$$W_j \cap (W_1 + \cdots + W_{j-1}) = \{0\}.$$

Demostración 16.
1) $\implies$ 2) *Tomemos $w \in W_j \cap (W_1 + \cdots + W_{j-1})$. Entonces existen $w_1, \cdots, w_{j-1}$, con $w_i \in W_i$ tal que $w = w_1 + \cdots + w_{j-1}$, de donde se sigue que*

$$0 = w_1 + \cdots + w_{j-1} - w.$$

Como $W_1, \cdots, W_m$ son independientes se sigue que $w_1, \cdots, w_{j-1}, w = 0$.
2) $\implies$ 1) *Supongamos que hay vectores $w_i \in W_i$ no todos nulos tales que*

$$0 = w_1 + \cdots + w_m.$$

Sea p el mayor índice tal que $w_p \neq 0$, entonces $-w_p = w_1 + \cdots + w_{p-1}$ es un vector no nulo en $W_p \cap (W_1 + \cdots + W_{p-1})$ lo cual es una contradicción. ■

Lema 13. *Sea V un espacio vectorial de dimensión finita. Sean $W_1, \cdots, W_m$ subespacios independientes de V y sea $W = W_1 \oplus \cdots \oplus W_m$. Si $\mathfrak{B}_i$ es una base ordenada de W_i, $1 \leq i \leq k$, entonces $\mathfrak{B} = (\mathfrak{B}_1, \cdots, \mathfrak{B}_k)$ es una base ordenada de V.*

Demostración 17. *Cualquier combinación lineal de vectores de $\mathfrak{B}$ se simplifica a una suma de la forma*

$$v_1 + \cdots + v_k, \text{ con } v_i \in W_i.$$

En particular si $v_1 + \cdots + v_k = 0$, entonces cada $v_i = 0$. Por la independencia lineal de los vectores de $\mathfrak{B}_i$ tenemos que la única combinación lineal que satisface la igualdad es la trivial. ■

El siguiente Lema es fundamental para realizar la prueba del teorema de la descomposición prima.

Lema 14. *Sea V un espacio vectorial de dimensión finita sobre el campo $\mathbb{F}$. Sean $W_1, \cdots, W_n$ subespacios tales que*

$$V = W_1 \oplus \cdots \oplus W_n.$$

Por cada i definimos $P_i : V \to V$ mediante $P_i v = v_i$, donde $v = v_1 + \cdots + v_n$ con $v_k \in W_k$. Entonces

1) $P_i^2 = P_i$,

2) $I = P_1 + \cdots + P_n$,

3) $P_i P_j = 0$ si $j \neq i$.

Recíprocamente, si $P_1, ..., P_n$ satisfacen 1)-3), entonces $V = W_1 \oplus \cdots \oplus W_n$, donde $W_i = Im\, P_i$.

Demostración 18. $\Rightarrow$) *Primero supóngase que*

$$V = W_1 \oplus \cdots \oplus W_n.$$

La suma directa garantiza que P_i está bien definido. Además, es fácil ver que P_i es lineal e idempotente. Notemos que para cada $v \in V$

$$v = \sum_{i=1}^{n} v_i = \sum_{i=1}^{n} P_i v = \left(\sum_{i=1}^{n} P_i \right) v,$$

de donde se sigue que $P_1 + \cdots + P_n = I$. Para $i \neq j$,

$$P_i P_j(v) = P_i P_j \left(\sum_{i=1}^{n} v_i \right) = P_i(0 + \cdots + v_j + \cdots 0) = 0,$$

por lo cual $P_i P_j = 0$.

$\Leftarrow$) *Sean $P_1, \cdots, P_n$ operadores lineales sobre V que satisfacen 1) − 3) y sea $W_i = Im\, P_i$. Entonces*

$$V = W_1 + \cdots + W_n.$$

En efecto, dado $v \in V$ por la propiedad 2) tenemos que

$$v = P_1 v + \cdots + P_n v$$

con $P_i v \in W_i$. Ahora para probar que la suma es directa sean $w_i \in W_i$ tales que

$$w_1 + \cdots + w_n = 0.$$

Así su imagen bajo P_j es

$$\begin{aligned} P_j(w_1 + \cdots + w_n) &= P_j 0 = 0 \\ P_j P_1 w_1 + \cdots + P_j P_n w_n &= 0 \\ P_j^2 w_j &= 0 \\ P_j w_j &= 0 \\ w_j &= 0. \end{aligned}$$

Por lo tanto $W_1, \cdots, W_n$ son subespacios separados y V es su suma directa. ■

4.6 Subespacios invariantes

Cuando se puede expresar un espacio vectorial como suma directa de subespacios invariantes la matriz que representa a el operador en esa base será una diagonal por bloques. Este hecho tendrá mucha importancia al momento realizar la prueba del teorema de la descomposición de Jordan.

Definición 14. *Sea V un espacio vectorial de dimensión finita y T un operador lineal sobre V. Decimos que un subespacio W es invariante bajo T si $\forall w \in W$ se cumple que*

$$Tw \in W$$

es decir, $TW \subset W$.

Ejemplo 15. *Tomemos $V = \mathbb{R}^2$ y $W =< e_1 >$. Si T es el operador*

$$T = \begin{pmatrix} 3 & 4 \\ 0 & 7 \end{pmatrix},$$

entonces W es invariante bajo T.

Ejemplo 16. *Sea T un operador lineal sobre V y U cualquier operador que conmute con T. Sea $W = Im(U)$ y $N = \ker(U)$. Ambos W y N son invariantes bajo T. En efecto, sea $w \in W$, de modo que $w = Uv$ para algún $v \in V$, entonces $Tw = TUv = UTv \in W$. Ahora bien, si $w \in N$, entonces $UTw = TUw = T0 = 0$.*

Cuando W es un subespacio invariante bajo T, el operaor T induce un operador lineal

$$T_W := T|_W : W \to W.$$

Ejemplo 17. *Sea* $V = \mathbb{R}^3$ *y* $T = \begin{pmatrix} 2 & 3 & 0 \\ 4 & 5 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. *Entonces*

$$W = \{(x, y, 0)^t : \ x, y \in \mathbb{R}\}$$

es un subespacio invariante bajo T *y* T_W *es una matriz* 2×2.

$$T_w = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}.$$

Definición 15. *Sea* V *un espacio vectorial de dimensión finita y* W *un subespacio de* V. *Un complemento directo de* W *es cualquier subespacio* Z *tal que*

$$W \oplus Z = V.$$

Proposición 6. *Sea* V *un espacio vectorial de dimensión finita y sea* W_1 *un subespacio de* V. *Existe* W_2 *tal que* $V = W_1 \oplus W_2$.

Demostración 19. *Sea* $\mathcal{B} = \{v_1, \cdots, v_k\}$ *una base de* W_1. *Completamos a una base* $\mathcal{B}' = \{v_1. \cdots .v_k, w_1, \cdots, w_l\}$ *de* V. *Afirmamos que* W_2, *el espacio generado por los vectores* $\{w_1, \cdots, w_l\}$, *es un complemento directo de* W_1. *En efecto, sea* v *un vector que esté en la intersección de* W_1 *y* W_2, *entonces*

$$v = \sum_{i=1}^{k} c_i v_i$$

y

$$v = \sum_{j=1}^{l} d_j w_j$$

de donde se sigue que

$$\sum_{i=1}^{k} c_i v_i + \sum_{j=1}^{l} (-d_j) w_j = 0.$$

Como los vectores son linealmente independientes, se sigue que $c_1 = \cdots = c_k = d_1 = \cdots = d_l = 0$. *Es decir,* $v = 0$. *Y evidentemente* $V = W_1 + W_2$. ■

Supongamos W es un subespacio invariante bajo $T : V \to V$. También supongamos que Z es un complemento directo de W, invariante bajo T. Podemos considerar $\mathfrak{B}_W = \{w_1, \cdots, w_k\}$ una base de W y $\mathfrak{B}_Z = \{z_1, \cdots, z_p\}$ una base de Z, entonces $\mathfrak{B} = \mathfrak{B}_W \cup \mathfrak{B}_Z$ es una base de V. Sea A la matriz asociada a T en la base $\mathfrak{B}$, tenemos que

$$Tw_j = \sum_{i=1}^{k} a_{ij} w_i$$

por ser W_i invariante bajo T. De manera análoga

$$Tz_j = \sum_{i=1}^{p} b_{ij} z_j.$$

Así

$$\begin{aligned} A = [T]_{\mathfrak{B}} &= ([Tw_1]_{\mathfrak{B}}, \cdots, [Tw_k]_{\mathfrak{B}}, [Tz_1]_{\mathfrak{B}}, \cdots, [Tz_p]_{\mathfrak{B}}) \\ &= \begin{pmatrix} a_{11} & \cdots & a_{1k} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{k1} & \cdots & a_{kk} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & b_{11} & \cdots & b_{1p} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{p1} & \cdots & b_{pp} \end{pmatrix}. \end{aligned}$$

Observemos que

$$\begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{k1} & \cdots & a_{kk} \end{pmatrix} = [T_W]_{\mathfrak{B}_W} \quad \text{y} \quad \begin{pmatrix} b_{11} & \cdots & b_{1p} \\ \vdots & & \vdots \\ b_{p1} & \cdots & b_{pp} \end{pmatrix} = [T_Z]_{\mathfrak{B}_Z},$$

de modo que

$$A = \begin{pmatrix} [T_W]_{\mathfrak{B}_W} & 0 \\ 0 & [T_Z]_{\mathfrak{B}_Z} \end{pmatrix}.$$

De manera general, supongamos que $V = V_1 \oplus \cdots \oplus V_N$, donde cada V_j es invariante bajo T. Tomando una base $\mathfrak{B}_j$ de V_j y considerando $T_{V_j} = T|_{V_j}$ tenemos que

$$[T]_{\mathfrak{B}} = \begin{pmatrix} [T_{V_1}]_{\mathfrak{B}_1} & 0 & \cdots & 0 \\ 0 & [T_{V_2}]_{\mathfrak{B}_2} & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & [T_{V_N}]_{\mathfrak{B}_N} \end{pmatrix},$$

donde

$$\mathfrak{B} = \bigcup_{i=1}^{N} \mathfrak{B}_i.$$

4.7 Suma directa externa.

Concluimos el capítulo dando la definición de suma directa externa. Este concepto es otra manera de llamar a la estructura algebraica que se genera en el producto cartesiano de espacios vectoriales.

Definición 16 (**Suma directa externa**). *Sea $\{V_i\}_{i=1}^n$ una familia de espacios vectoriales de dimensión finita sobre el campo $\mathbb{F}$. La suma directa exterior de $\{V_i\}_{i=1}^n$, denotada como $\bigoplus_{i=1}^n V_i$, es el conjunto de*

todas las n-tuplas $(v_1, \cdots, v_n)$*, con* $v_i \in V_i$*, donde la suma de vectores y el producto escalar se definen como sigue*

$$(v_1, \cdots, v_m) + (w_1, \cdots, w_m) = (v_1 + w_1, \cdots, v_m + w_m),$$
$$\lambda(v_1, \cdots, v_m) = (\lambda v_1, \cdots, \lambda v_m),$$

para todo $(v_1, v_2, \cdots, v_m)$*,* $(w_1, w_2, \cdots, w_m)$ *en* $V_1 \times \cdots \times V_n$ *y todo* $\lambda \in \mathbb{F}$*.*

Es inmediato notar que $\bigoplus_{i=1}^{n} V_i$ es un espacio vectorial sobre el campo $\mathbb{F}$. Además, existe un relación directa entre la suma directa externa de subespacios y la suma directa de subespacios.

Proposición 7. *Sea* V *un espacio vectorial de dimensión finita sobre el campo* $\mathbb{F}$*. Sean* $W_1, \cdots, W_n$ *subespacios linealmente independientes de* V*. Entonces*

$$W_1 \oplus \cdots \oplus W_n \cong \bigoplus_{i=1}^{n} W_i.$$

Demostración 20. *En efecto, considérese la transformación* $\phi : W_1 \oplus \cdots \oplus W_n \to \bigoplus_{i=1}^{n} W_i$ *dada por*

$$\phi(w_1 + \cdots + w_n) = (w_1, \cdots, w_n), \quad w_i \in W_i.$$

Como cada vector en $W_1 \oplus \cdots \oplus W_n$ *se expresa de manera única como suma de vectores* $w_i \in W_i$*, es decir, la transformación está bien definida. Por el mismo argumento se sigue que es una biyección. Y de la definición de las operaciones en* $\bigoplus_{i=1}^{n} W_i$ *se concluye que* ϕ *es lineal. Luego* ϕ *es un isomorfismo de espacios vectoriales.* ■

Definición 17 (**Suma directa externa de operadores**)**.** *Sea* $\{V_i\}_{i=1}^{n}$ *una familia de espacios vectoriales de dimensión finita sobre el campo* $\mathbb{F}$*, y sea* $\{L_i\}_{i=1}^{n}$ *una familia de operadores lineales tales que* $L_i \in \mathcal{L}(V_i)$*. La suma directa de* $\{L_i\}_{i=1}^{n}$ *es la transformación de* $\bigoplus_{i=1}^{n} V_i$ *en sí misma, definida como*

$$\left(\bigoplus_{i=1}^{n} L_i\right)(v_1, \cdots, v_n) = (L_1 v_1, \cdots, L_n v_n)$$

para cada $(v_1, \cdots .v_n) \in \bigoplus_{i=1}^{n} V_i$*.*

Proposición 8. *Sea* $\{V_i\}_{i=1}^{n}$ *una familia de espacios vectoriales de dimensión finita sobre el campo* $\mathbb{F}$ *y* $L_i \in \mathcal{L}(V_i)$*. Entonces* $\bigoplus_{i=1}^{n} L_i$ *es un operador lineal en* $\bigoplus_{i=1}^{n} V_i$*.*

Sea T un operador en un espacio vectorial V, con polinomio minimal

$$p_M = p_1^{r_1} \cdots p_k^{r_k}.$$

De acuerdo al teorema de la descomposición prima,

$$V = V_1 \oplus \cdots \oplus V_k \cong \bigoplus_{i=1}^{k} V_i,$$

donde cada V_i es invariante bajo T. Considerando $T_i = T|_{V_i}$, la restricción de T a V_i, se tiene

$$T = \bigoplus_{i=1}^{k} T_i.$$

Forma canonica de Jordan.

El teorema de la descomposición de Jordan nos va a permitir describir el álgebra generada por un operador. Para realizar la prueba primero se prueba el Teorema de la descomposición prima. Este teorema nos asegura que el espacio se va a descomponer como suma directa de espacios invariantes bajo T. Lo cual nos va a permitir hacer la prueba del Teorema de la descomposición de Jordan solo para operadores nilpotentes.

5.1 Espacios cíclicos y descomposición prima.

El teorema de la descomposición primaria nos dice que dado un espacio vectorial y un operador lineal T sobre él, es posible expresar el espacio como suma directa de subespacios invariantes bajo T. Además, nos asegura la existencia de unos polinomios de T que son proyecciones. Y cuya imagen es invariante bajo T. Para poder llevar a cabo la prueba daremos algunos resultados que nos ayudar a saber si un subespacio es invariante bajo T.

Definición 18. *Sea V un espacio vectorial de dimensión finita. Si v es un vector de V, el subespacio T-cíclico generado por v es el subespacio $Z(v;T)$ de vectores de la forma $g(T)v$, con $g \in \mathbb{F}[x]$.*

Definición 19. *Sea V un espacio vectorial de dimensión finita. Si v es un vector de V, el T-anulador de v es el ideal $M(v;T)$ en $\mathbb{F}[x]$ que consta de todos los polinomios $g \in \mathbb{F}[x]$ de modo que $g(T)v = 0$. Al polinomio mónico p_v que genera este ideal se la llamará también el T-anulador de v.*

Lema 15. *Sea v un vector no nulo en V y sea p_v el T-anulador de v. Si el grado de p_v es k, entonces los vectores $v, Tv, T^2v, \cdots, T^{k-1}v$ forman una base de $Z(v;T)$.*

Demostración 21. *Sea g un polinomio sobre el cuerpo $\mathbb{F}$. Se puede escribir como*

$$g = p_v q + r,$$

donde $r = 0$ ó $grad(r) < k$. El polinomio $p_v q$ está en el T-anulador de v, por lo tanto

$$g(T)v = r(T)v.$$

Como $r = 0$ ó $grad(r) < k$, el vector $r(T)v$ es combinación lineal de los vectores $v, Tv, T^2v, \cdots, T^{k-1}v$. Como $g(T)v$ es un vector arbitrario de $Z(v;T)$, los vectores $v, Tv, T^2v, \cdots, T^{k-1}v$ generan a $Z(v;T)$. Ahora bien, son linealmente independientes, pues si existiera una combinación lineal

$$c_0 v + c_1 Tv + \cdots + c_{k-1}T^{k-1}v = 0$$

con algún $c_i \neq 0$, entonces existiría un polinomio $g \neq 0$, de grado menor a k, tal que

$$g(T)v = 0,$$

lo cual es una contradicción. ■

Lema 16. *Sea $T : V \to V$ una transformación líneal y $q(T)$ un polinomio cualquiera en T. Entonces* $\ker q(T)$ *e* $\operatorname{Im} q(T)$ *son subespacios invariantes bajo T.*

Demostración 22. *Sabemos que el operador $q(T)$ conmuta con T. En virtud del Ejemplo 16, los subespacios* $\ker q(T)$ *e* $\operatorname{Im} q(T)$ *son subespacios invariantes bajo T.* ■

Lema 17. *Sea v un vector no nulo de V. El espacio $Z(v;T)$ es invariante bajo T.*

Demostración 23. *Sea $w \in Z(v;T)$. Entonces $w = g(T)v$, para algún $g \in \mathbb{F}[x]$. Luego $Tw = h(T)v \in Z(v;T)$, donde $h(x) = xg(x)$.* ■

Lema 18. *Sea $P : V \to V$ una proyección y $W = \operatorname{Im} P$. Entonces W es invariante bajo T si y sólo si*

$$PTP = TP$$

Demostración 24. *Primero supongamos que W es invariante bajo T. Sea $v \in V$. Entonces $w := Pv$ y Tw están en W. Según el Lema 7, tenemos que*

$$PTPv = TPv.$$

Recíprocamente, supongamos que se cumple que $PTP = TP$. Sea $w \in W$ entonces

$$Tw = TPw.$$

Por hipótesis,

$$Tw = PTPw = Pu, \quad u = TPw \in V,$$

de donde $Tw \in W$, luego W es invariante bajo T. ■

Lema 19. *Sea $P : V \to V$ una proyección y T un operador lineal. Los subespacios* $\operatorname{Im} P$ *y* $\ker P$ *son invariantes bajo T si y sólo si $TP = PT$.*

Demostración 25. *Por el Lema 18 sabemos que* $\ker P = Im(I - P)$ *es invariante bajo T si y sólo si*

$$(I - P)T(I - P) = T(I - P),$$

de donde $\ker P$ *es invariante bajo T si y sólo si*

$$PTP = PT.$$

Por el Lema 18, $Im(P)$ es invariante bajo T si y sólo si

$$TPT = TP.$$

Luego $\operatorname{Im} P$ *y* $\ker P$ *son invariantes bajo T si y sólo si*

$$TP = PT.$$■

Lema 20. *Sean $T, F : V \to V$ operadores lineales. Entonces* $\ker T \subset \ker FT$.

Ahora que hemos desarrollado la suficiente teoía nos encontramos en las condicones de llevar a cabo la demostración del primer teorema importante del trabajo.

Teorema 2 (**Teorema de la descomposición prima**). *Sea T un operador lineal sobre el espacio vectorial V de dimensión finita sobre el cuerpo $\mathbb{F}$. Sea p_M el polinomio minimal de T,*

$$p_M = p_1^{r_1} \cdots p_k^{r_k}$$

donde $p_1, \cdots, p_k$ son polinomios irreducibles sobre el cuerpo $\mathbb{F}$, distintos entre sí. Entonces cada subespacio $V_i = \ker p_i^{r_i}(T)$ es invariante bajo T y

$$V = V_1 \oplus \cdots \oplus V_k.$$

Además, si $T_i : V_i \to V_i$ es la restricción de T a V_i, entonces el polinomio minimal de T_i es $p_i^{r_i}$.

Demostración 26. *Para cada i definimos*

$$q_i = \frac{p_M}{p_i^{r_i}} = \prod_{j \neq i} p_j^{r_j}.$$

Como no hay factor irreducible común en los polinomios $q_1, ..., q_k$, entonces existen polinomios $a_1, \cdots, a_k$ tales que

$$a_1(x)q_1(x) + \cdots + a_k(x)q_k(x) = 1. \tag{5.1}$$

Hacemos $t_i(x) = a_i(x)q_i(x)$ para $i = 1, \cdots, k$. Definimos

$$P_i = t_i(T).$$

Veamos que

$$\begin{aligned} P_1 + \cdots + P_k &= I, \\ P_i^2 &= P_i, \quad i = 1, ..., k, \\ P_i P_j &= 0, \quad i \neq j. \end{aligned} \tag{5.2}$$

Evaluando (5.1) en T obtenemos $t_1(T) + \cdots + t_k(T) = I$, esto justifica (5.2). Para $i \neq j$,

$$\begin{aligned} P_i P_j &= a_i(T)q_i(T)a_j(T)q_j(T) \\ &= a_i(T)a_j(T)q_i(T)q_j(T), \end{aligned}$$

donde $q_i(x)q_j(x)$ es un polinomio divisible por $p_M(x)$. Esto implica que $P_i P_j = 0$. Ahora multiplicamos (5.2) con P_i por la izquierda,

$$P_i P_1 + \cdots P_i P_k = P_i,$$

de donde se infiere que $P_i^2 = P_i$. Por el Lema 14 tenemos que

$$V = ImP_1 \oplus \cdots \oplus ImP_k.$$

Ahora veamos que $Im\, P_i = \ker p_i^{r_i}(T)$. *Sin pérdida de generalidad veamos que* $V_1 = W_1$, *donde* $W_i = Im\, P_i$. *Tenemos que*

$$q_1(T)p_1^{r_1}(T) = p_M(T) = 0.$$

Multiplicando por $a_1(T)$ *obtenemos*

$$P_1 p_1^{r_1}(T) = 0.$$

Si $v \in Im\, P_1$, *entonces*

$$p_1^{r_1}(T)v = p_1^{r_1}(T)P_1 v = 0.$$

Luego $Im\, P_1 \subset \ker p_1^{r_1}(T)$.

Notemos que $p_1^{r_1}(T)$ *es factor de* P_j *para* $j = 2, \cdots, k$. *Luego* $\ker p_1^{r_1}(T) \subset \ker P_j$. *Así*

$$V_1 \in \bigcap_{j=2}^{k} \ker P_j \subset \ker(P_2 + \cdots + P_k).$$

Pero $P_2 + \cdots + P_k = I - P_1$, *así*

$$V_1 \subset \ker(I - P_1) = Im\, P_1 = W_1.$$

Ahora veamos que el polinomio minimal del operador inducido $T_i : V_i \to V_i$ *es* $p_i^{r_i}$. *Sea* m_{T_i} *el polinomio minimal de* T_i. *Como* $p_i^{r_i}(T)$ *es la transformación idénticamente cero en* V_i, *entonces* $p_i^{r_i}(T_i)$ *también lo es. Por lo tanto, tenemos que* $m_{T_i} | p_i^{r_i}$. *Así* $m_{T_i} | p_m$ *para cada i. Además* $m_{T_1}, ..., m_{T_k}$ *son primos relativos. Supongamos que* $g \in \mathbb{F}[x]$ *es un múltiplo de* m_{T_i} *para cada i. Entonces* $g(T_i) = 0$ *en* V_i. *Para cada* $v \in V$,

$$v = v_1 + \cdots + v_k, \quad con\ v_i \in V_i.$$

Así que

$$g(T)(v) = \sum_{i=1}^{k} g(T)(v_i) = \sum_{i=1}^{k} g(T_i)(v_i) = 0.$$

Por lo tanto $g(T) = 0$, *en consecuencia* $p_m | g$. *Por lo tanto* p_m *es el mínimo común multiplo de los polinomios* $m_{T_1}, ..., m_{T_k}$. *Como los polinomios son primos relativos, tenemos que* $p_m = \prod_{i=1}^{k} m_{T_i}$. *Pero sabemos que* $p_m = \prod_{i=1}^{k} p_i^{r_i}$ *y que* $m_{T_i} | p_i^{r_i}$. *Como cada polinomio es mónico, se sigue que* $p_i^{r_i} = m_{T_i}$ *como se deseaba probar.* ■

Más adelante veremos que el operador proyección

$$P_i = a_i(T)q_i(T)$$

es un elemento del álgebra generada por el operador T para cada i. Además, como estos operadores son polinomios en T, conmutan con T.

Otro resultados que ahora podemos probar es el siguiente.

Proposición 9. *Sea T operador lineal sobre el espacio vectorial V de dimensión finita con polinomio característico*

$$p_c(x) = (x - \lambda_1)^{d_1} \cdots (x - \lambda_k)^{d_k}$$

y polinomio minimal

$$p_m(x) = (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}.$$

Sea $V_i = \ker(T - \lambda_i I)^{r_i}$. Entonces el espacio de vectores propios generalizados

$$W_i = \{v \in V | \ (T - \lambda_i I)^m v = 0 \quad \textit{para algún m positivo}\}.$$

coincide con V_i.

Demostración 27. *Sólo se demostrará la contensión*

$$\{v \in V | (T - \lambda_i I)^m v = 0 \quad \textit{para algún m positivo}\} \subseteq V_i$$

pues la otra contensión es trivial.

Sea $v \in V$ y m tal que $(T - \lambda_i I)^m v = 0$. Si $m \leq r_i$, entonces $v \in V_i$. En caso contrario, existen enteros p, r tales que $m = pr_i + r$ con $p > 0$ y $0 \leq r < r_i$. El vector $(T - \lambda_i I)^{m-r_i} v \in V_i = Im\ P_i$, donde $P_i : V_i \to V_i$ es la proyección descrita por el Teorema 2. El lema 8 nos dice que $Im(P_i) = \ker(I - P_i)$. Luego

$$(T - \lambda_i I)^{m-r_i}(I - P_i)v = (I - P_i)(T - \lambda_i I)^{m-r_i} v = 0.$$

De donde $(T - \lambda_i I)^{m-2r_i}(v - P_i v) \in V_i = \ker(I - P_i)$. Aplicando la transformación $I - P_i$ al vector $(T - \lambda_i I)^{m-2r_i}(I - P_i)v$ se sigue que

$$(T - \lambda_i I)^{m-2r_i}(I - P_i)v = 0,$$

y por lo tanto $(T - \lambda_i I)^{m-3r_i}(I - P_i)v \in V_i$. Procediendo de este modo se sigue que

$$(T - \lambda_i I)^{m-pr_i}(I - P_i)v \in V_i$$

y en consecuencia $(I - P_i)v \in V_i = \ker(I - P_i)$. De donde $P_i v = v$ y $v \in V$.■

5.2 Operadores nilpotentes

En la prueba del teorema de la descomposición de Jordan veremos que cuando restringimos cierto operador lineal a uno de los subespacios vectoriales que nos da el teorema de la descomposición prima este operador es nilpotente. Lo cual nos va a permitir solo realizar la prueba de este teorema para el caso cuando el operador es nilpotente.

Definición 20 (Operadores nilpotentes). *Sea V un espacio vectorial sobre el campo $\mathbb{F}$ y $T : V \to V$ un operador lineal. Decimos que T es un operador lineal nilpotente si existe un $k \in \mathbb{N}$ tal que*

$$T^k = 0.$$

Dado un operador lineal nilpotente, definimos su índice de nilpotencia como el minimo entero k tal que $T^k = 0$.

Nota 2. *La definición de una matriz nilpotente $A \in \mathbb{M}_n(\mathbb{F})$ es análoga.*

Antes de proceder enunciaremos un resultado técnico que usaremos con frecuencia.

Proposición 10. *Sea $T : V \to V$ un operador lineal. Para cada entero positivo i se cumple que*

1) $\ker T^i \subseteq \ker T^{i+1}$,

2) si $v \in \ker T^{i+1}$ entonces $T(v) \in \ker T^i$.

Demostración 28. *El inciso* 1) *se sigue del Lema 20. Para probar* 2)*, sea $v \in \ker T^{i+1}$. Entonces*

$$T^i T v = T^{i+1} v = 0,$$

así $T(v) \in \ker T^i$ como se deseaba demostrar. ■

El siguiente Lema nos dice que el kernel de un operador nilpotente va a ir incrementando de tamaño hasta llegar a ser el mismo espacio.

Lema 21. *Sea V un espacio vectorial de dimensión finita sobre el campo $\mathbb{F}$ y $T : V \to V$ un operador lineal nilpotente, con índice de nilpotencia k. Entonces*

$$\{0\} = \ker(I) \subsetneq \ker(T) \subsetneq \ker(T^2) \subsetneq \cdots \subsetneq \ker(T^{k-1}) \subsetneq \ker(T^k) = V.$$

Demostración 29. *En virtud de la Proposición 10 basta probar que dado $i \in \mathbb{N}$ tal que*

$$\ker T^i = \ker T^{i+1}$$

entonces $\ker T^i = \ker T^j$*, $\forall\, j \geq i$. Sea $v \in \ker T^{i+2}$. Por la Proposición 10 tenemos que $Tv \in \ker T^{i+1} = \ker T^i$, de donde $T^{i+1}v = 0$, por lo tanto $v \in \ker T^i$. Ahora bien supongamos que para $n \in \mathbb{N}$, tenemos que* $\ker T^i = \ker T^{i+1} = \ker T^{i+n}$*. Sea $v \in \ker T^{i+n+1}$, entonces $Tv \in \ker T^{i+n} = \ker T^i$, por lo tanto $v \in \ker T^{i+1} = \ker T^i$. Desde luego* $\ker T^k = \ker T^{k+1}$*. Si $i < k$, entonces se contradice que k es el índice de nilpotencia.* ■

Lema 22. *Sea V un espacio vectorial de dimensión finita sobre el campo $\mathbb{F}$ y $T : V \to V$ un operador lineal tal que*

$$\ker(T^i) \subsetneq \ker(T^{i+1})$$

para algun $i \in \mathbb{N}$. Si $\{v_1, \cdots, v_n\}$ es una base de $\ker(T^i)$ *que se extiende a una base $\{v_1, \cdots, v_n, w_1, \cdots, w_m\}$ de* $\ker(T^{i+1})$*, entonces*

$$\{T(w_1), \cdots, T(w_m)\}$$

es linealmente independiente en $\ker(T^i)$*.*

Demostración 30. *En virtud de la Proposición 10 tenemos que* $Tw_j \in \ker T^i$ *para* $j = 1, \cdots, m$. *Además, según la demostración de la Proposición 6 tenemos que*

$$\ker T^{i+1} = \ker T^i \oplus Gen\{w_1, \cdots, w_m\}.$$

Sean $c_1, \cdots, c_m \in \mathbb{F}$ *tales que*

$$\sum_{l=1}^{m} c_l T w_l = 0.$$

Por la linealidad de T *tenemos que*

$$\sum_{l=1}^{m} c_l w_l \in \ker T \subset \ker T^i.$$

Evidentemente $\sum_{l=1}^{m} c_l w_l \in Gen\{w_1, \cdots, w_m\}$. *Por lo tanto tenemos que*

$$\sum_{l=1}^{m} c_l w_l = 0.$$

Por ser $\{w_1, \cdots, w_m\}$ *un conjunto linealmente independiente de vectores tenemos que* $c_1 = \cdots = c_m = 0$. *Por lo tanto* $\{Tw_1, \cdots, Tw_m\}$ *es un conjunto linealmente independiente en* $\ker T^i$. ■

Lema 23. *Sea* $T : V \to V$ *un operador lineal nilpotente con índice de nilpotencia* k. *Para* $1 \leq j \leq k$ *sea* $\{v_1, \cdots, v_m\}$ *un conjunto de vectores linealmente independientes tales que*

$$\ker T^j = \ker T^{j-1} \oplus Gen\{v_1, \cdots, v_m\}.$$

Si $w_0, ..., w_{j-1} \in Gen\{v_1, \cdots, v_m\}$ *satisfacen*

$$w_0 + Tw_1 + \cdots + T^{j-1} w_{j-1} = 0,$$

entonces $w_0 = \cdots = w_{j-1} = 0$.

Demostración 31. *En efecto, sean* $w_0, \cdots, w_{j-1}$ *como en la hipótesis, la imagen de*

$$w_0 + Tw_1 + \cdots + T^{j-1} w_{j-1},$$

bajo T^{j-1} *es*

$$0 = T^{j-1}(w_0 + Tw_1 + \cdots + T^{j-1} w_{j-1}) = T^{j-1} w_0.$$

La descomposición en suma directa implica que $w_0 = 0$ *y por lo tanto*

$$Tw_1 + \cdots + T^{j-1} w_{j-1} = 0.$$

Ahora bien la imagen de $Tw_1 + \cdots + T^{j-1} w_{j-1}$ *bajo* T^{j-2} *es*

$$0 = T^{j-2}(Tw_1 + \cdots + T^{j-1} w_{j-1}) = T^{j-1} w_1,$$

y nuevamente por la descomposición en suma directa se concluye que $w_1 = 0$. *Y de manera similar se prueba que* $w_2 = \cdots = w_{j-1} = 0$. ■

Lema 24. *Sea V un espacio vectorial de dimensión finita y $T : V \to V$ un operador lineal nilpotente con índice de nilpotencia k. Para $1 \leq j \leq k$ sea $\{v_1, \cdots, v_m\}$ un conjunto de vectores linealmente independientes tales que*

$$\ker T^j = \ker T^{j-1} \oplus Gen\{v_1, \cdots, v_m\}.$$

El conjunto

$$\{v_{il} = T^{j-i}v_l : i = 1, \cdots, j;\ l = 1, \cdots, m\}$$

es linealmente independiente en $\ker T^j$.

Demostración 32. *Se tiene que* $\ker T^{j-1} \subsetneq \ker T^j$. *Supongamos que*

$$\sum_{i=1}^{j}\sum_{l=1}^{m} a_{il}v_{il} = 0.$$

Primero notemos que

$$w_j := \sum_{l=1}^{m} a_{jl}v_{jl} = \sum_{l=1}^{m} a_{jl}v_l \in Gen\{v_1, \cdots, v_m\}$$

mientras que $\sum_{i=1}^{j-1}\sum_{l=1}^{m} a_{il}v_{il} \in \ker(T^{j-1})$. *La descomposición en suma directa implica que* $w_j = 0$. *De la independencia lineal de los* v_i *se sigue que*

$$a_{j1} = \cdots = a_{jm} = 0.$$

Así

$$\sum_{i=1}^{j-1}\sum_{l=1}^{m} a_{il}v_{il} = 0.$$

Definimos

$$w_{j-i} := \sum_{l=1}^{m} a_{(i)l}v_l \in Gen\{v_1, \cdots, v_m\}.$$

Entonces

$$\sum_{l=1}^{m} a_{il}v_{il} = T^{j-i}\left(\sum_{l=1}^{m} a_{il}v_l\right) = T^{j-i}w_{j-i}$$

y

$$\sum_{i=1}^{j-1} T^{j-i}w_{j-i} = \sum_{p=1}^{j-1} T^p w_p = 0.$$

Por el Lema 23 se concluye que $w_0 = \cdots = w_{j-1} = 0$ *y por la independencencia lineal del conjunto* $\{v_1, \cdots, v_m\}$ *se sigue que*

$$a_{11} = \cdots = a_{21} = \cdots = a_{jm} = 0.\blacksquare$$

5.3 Forma de Jordan

En esta sección llevaremos a cabo la prueba del teorema de la descomposición de Jordan. Este teorema nos dice que todo operador tiene una base en cuya representación matricial es bastante sencilla.

Primero se probará esto en el caso particular cuando el operador es nilpotente y posteriormente usando el Teorema de la descomposición prima se hará la prueba para el caso general. La prueba consiste en hallar ciertos vectores linealmente independientes, tales que al considerar sus imágenes bajo T estas siguen siendo linealmente independientes al unirlos con los primeros vectores.

Antes de empezar con las pruebas definamos lo que es una matriz elemental de Jordan.

Definición 21. *Sea $\mathbb{F}$ un campo. Se dice que $J_n(c) \in \mathbb{M}_n(\mathbb{F})$ es una matriz elemental de Jordan con valor propio c si es de la forma*

$$J_n(c) = \begin{pmatrix} c & 1 & \cdots & 0 & 0 \\ 0 & c & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & c & 1 \\ 0 & 0 & \cdots & 0 & c \end{pmatrix}.$$

Ahora se demostrara que todo operador nilpotente puede ser representado por una matriz diagonal por bloques, donde cada bloque es una matriz elemental de Jordan.

Lema 25. *Sea V un espacio vectorial de dimensión finita y $T : V \to V$ un operador lineal nilpotente con índice de nilpotencia k. Entonces existe una base de V en la cual la matriz de T es una matriz diagonal por bloques de la forma*

$$\begin{pmatrix} J_{m_1}(0) & & \\ & \ddots & \\ & & J_{m_s}(0) \end{pmatrix}.$$

Demostración 33. *Consideremos vectores $v_1, \cdots, v_{m_0}$ linealmente independientes tales que*

$$\ker(T^k) = \ker(T^{k-1}) \oplus Gen\{v_1, ..., v_{m_0}\}.$$

En virtud del Lema 24 el conjunto $\{v_{il} = T^{k-i}v_l : i = 1, \cdots, k; l = 1, \cdots, m_0\}$ es linealmente independiente y forma parte de una base de V. Si $\{v_{il} = T^{k-i}v_l : i = 1, \cdots, k-1; l = 1, \cdots, m_0\}$ no es una base de $\ker(T^{k-1})$ notemos que $Tv_l \in \ker T^{k-1} \setminus \ker T^{k-2}$, para $l = 1, \cdots, m_0$. En caso contrario tendriamos que

$$0 = T^{j-2}(Tv_i) = T^{j-1}v_i$$

una contradicción. Por lo tanto el espacio

$$\ker T^{j-2} + Gen\{Tv_1, \cdots, Tv_{m_0}\}$$

es una suma directa y por lo tanto existen vectores $y_1, \cdots, y_{m_1}$ *tales que*

$$\{Tv_1, \cdots, Tv_{m_0}, y_1, \cdots, y_{m_1}\}$$

es un conjunto linealmente independinte y

$$\ker(T^{k-1}) = \ker(T^{k-2}) \oplus Gen\{T(v_1), \cdots, T(v_{m_0}), y_1, \cdots, y_{m_1}\}.$$

De acuerdo con el Lema 24 y usando la misma notación tenemos que

$$\{v_{il} : i = 1, \cdots, k-1; l = 1, \cdots, m_0\} \cup \{y_{il} : i = 2, \cdots, k; l = 1, \cdots, m_1\}$$

es un conjunto linealmente independiente en $\ker T^{k-1}$*. La descomposición en suma directa de* $\ker T^k$ *nos garantiza la independencia lineal del conjunto*

$$\{v_{il} : i = 1, \cdots, k; l = 1, \cdots, m_0\} \cup \{y_{il} : i = 2, \cdots, k; l = 1, \cdots, m_1\}.$$

En efecto, supongamos que

$$\sum_{l=1}^{m_0} \sum_{i=1}^{k} a_{ij} v_{ij} + \sum_{l=1}^{m_1} \sum_{i=2}^{k} b_{il} y_{il} = 0$$

en donde

$$\sum_{l=1}^{m_0} a_{kl} v_{kl} \in Gen\{v_1, \cdots, v_{m_0}\}$$

y el resto de los sumandos pertenecen a $\ker T^{k-1}$*, luego*

$$a_{k1} = \cdots = a_{km_0} = b_{12} = \cdots = b_{km_1} = 0.$$

Si el conjunto

$$\{v_{il} : i = 1, \cdots, k-2; l = 1, \cdots, m_0\} \cup \{y_{il} : i = 2, \cdots, k-1; l = 1, \cdots, m_1\}$$

no forma una base $\ker(T^{j-2})$ *volvemos a repetir el proceso. Continuando de estma manera es posible hallar una sucesión de vectores* $v_1, \cdots, v_{m_0}, y_1, \cdots, z_1 \cdots, z_{m_p}$ *tales que el conjunto*

$$\{v_{il}\} \cup \cdots \cup \{z_{il}\}$$

sea una base de V. Notemos que para $i = 1, \cdots, m_0$ *se tiene que*

$$\begin{aligned} TV_{1i} &= T(T^{k-1} v_i) = 0 \\ Tv_{2i} &= T(T^{k-2} V_i) = T^{k-1} v_i = v_{1i} \\ &\vdots \\ Tv_{(k-1),i} &= T(Tv_i) = v_{(k-2),i} \\ Tv_{ki} &= Tv_i = v_{(k-1),i}. \end{aligned}$$

El mismo resultado se cumple para los vectores

$$\{y_{il}\} \cup \cdots \cup \{z_{il}\}$$

de esta manera es posible acomodar los vectores como

$$\{v_{11}, \cdots, v_{k1}, v_{12}, \cdots v_{k2} \cdots, y_{21}, \cdots, y_{k1}, \cdots, z_{q1}, \cdots, z_{k1}, \cdots, z_{km_p}\}$$

la cual es la base deseada. ■

Procederemos a realizar la prueba para el caso general.

Teorema 3 (**Forma de Jordan**). *Sea v un espacio vectorial de dimensión finita sobre un campo $\mathbb{F}$ y sea $T : V \to V$ un operador lineal. Sean $c_1, \cdots, c_k$ los valores propios de T, si $c_i \in \mathbb{F}, \quad i = 1, \cdots k$ entonces hay una base de V respecto a la cual la matriz de T es una matriz diagonal por bloques, en la cual cada bloque es de la forma*

$$\begin{pmatrix} J_{n_1}(c_i) & & & \\ & J_{n_2}(c_i) & & \\ & & \ddots & \\ & & & J_{n_p}(c_i) \end{pmatrix}$$

Donde J_{n_i} es una matriz elemental de Jordan asociada al valor propio C_i.

Demostración 34. *Sea $P_c = (x - c_1)^{d_1} \cdots (x - c_k)^{d_k}$ el polinomio caracteristico de T. Por el Teorema de Cayley Hamilton el polinomio minimal deT es*

$$P_m = (x - c_1)^{r_1} \cdots (x - c_k)^{r_k} \quad 1 \leq r_i \leq d_i.$$

Por el teorema de la descomposición primaria

$$V = W_1 \oplus \cdots \oplus W_k \quad con \quad W_i = \ker(T - C_i I)^{r_i}.$$

Definiendo $N_i = T_i - c_i I$, con $T_i = T\big|_{W_i}$ tenemos que N_i es nilpotente en W_i, y por el Lema 25 tenenmos que hay una base $\mathcal{B}_{W_i}$ tal que

$$[N_i]_{W_i}$$

es una matriz diagonal por bloques, donde cada bloque es una matriz elemental de Jordan con valor propio cero. De aquí se sigue que

$$[T_i]_{\mathcal{B}_{W_i}} = [N_i]_{\mathcal{B}_{W_i}} + [C_i I]_{\mathcal{B}_{W_i}}$$

es decir que T_i sera representaa por una matriz diagonal por bloques donde cada bloque es una matriz elemental de Jordan con valor propio c_i. Ahora bien, según el Lema 13

$$\mathcal{B} = (\mathcal{B}_{w_1}, \cdots, \mathcal{B}_{w_k})$$

es una base de V. Además, como cada W_i es invariante bajo T la matriz de T en la base $\mathcal{B}$ es

$$\begin{pmatrix} [T_1]_{\mathcal{B}_{W_1}} & & \\ & \ddots & \\ & & [T_k]_{\mathcal{B}_{W_k}} \end{pmatrix}.\blacksquare$$

Álgebras.

En este capítulo vamos a presentar el tema central de este trabajo, el concepto de álgebra. También vamos a estudiar el álgebra generada por un operador lineal, pero antes veremos algunas álgebras que nos ayudaran a facilitar la descripción del álgebra generada por un operador lineal.

6.1 Álgebras.

En pocas palabras un álgebra es un espacio vectorial en el cual es posible realizar productos entre vectores. Este concepto d producto entre vectores aparece de manera natural en algunos espacios vectoriales tales como el de las matrices o el de las funciones continuas. Los conceptos que vamos a presentar en esta sección el de álgebra, una subálgebra y el de álgebra generada.

Definición 22 (Álgebra). *Sea $(\mathcal{A}, +, \cdot)$ un espacio vectorial sobre el campo sobre $\mathbb{F}$. Se define $\odot : \mathcal{A} \times \mathcal{A} \Rightarrow \mathcal{A}$, se dice que $\mathcal{A}$ es una álgebra sobre $\mathbb{F}$ si $\odot$ es bilineal y asociativa. Es decir, $\forall\ a, b, c \in \mathcal{A}$ y $\alpha \in \mathbb{F}$ se cumple que:*

1. $(\alpha \cdot a) \odot b = \alpha \cdot (a \odot b) = a \odot (\alpha \cdot b)$,
2. $(a + c) \odot b = a \odot b + c \odot b$,
3. $a \odot (b + c) = a \odot b + a \odot c$,
4. $(a \odot b) \odot c = a \odot (b \odot c)$.

Ejemplo 18. *El conjunto de las matrices $n \times n$ sobre $\mathbb{F}$, con el producto de matrices es una álgebra.*

Ejemplo 19. *Otro ejemplo sencillo de una álgebra es el espacio de todos los operadores lineales sobre un espacio vectorial, con la composición como producto. Además es una algebra con identidad.*

Ejemplo 20. *Los polinomios $\mathbb{F}[x]$ con las operaciones usuales son un álgebra.*

Definición 23 (Homomorfismo de álgebras). *Sean $\mathcal{A}_1$ y $\mathcal{A}_2$ álgebras sobre $\mathbb{F}$, y sea $\varphi : \mathcal{A}_1 \to \mathcal{A}_2$ una función. φ es un homomorfismo de álgebras si*

$$\begin{aligned} \varphi(a + b) &= \varphi(a) + \varphi(b), \\ \varphi(a \odot b) &= \varphi(a) \odot \varphi(b), \\ \varphi(\alpha \cdot a) &= \alpha \cdot \varphi(a). \end{aligned}$$

*En el caso de que la transformación sea biyectiva se dice que φ es un **isomorfismo de álgebras.***

Definición 24 (**Subalgebra**). *Sea $\mathcal{A}$ una álgebra. Un subconjunto $\mathcal{B} \subset \mathcal{A}$ es una subálgebra de $\mathcal{A}$ si $\mathcal{B}$ es una álgebra con las operaciones de $\mathcal{A}$.*

Lema 26. *Sea $\mathcal{B} \subset \mathcal{A}$. Entonces $\mathcal{B}$ es una subálgebra si, y sólo si $\mathcal{B}$ es un subespacio vectorial de $\mathcal{A}$ y el producto en $\mathcal{B}$ es cerrado.*

Demostración 35.
$\Rightarrow$ Sea $\mathcal{B}$ una subálgebra, en particular es un subespacio vectorial y un subanillo de $\mathcal{A}$. Por el Lema 1 sabemos que el producto en $\mathcal{B}$ es cerrado.
$\Leftarrow$ Basta probar que $\mathcal{B}$ es un subanillo, pues las propiedades de bilinealidad se heredan. Por ser $\mathcal{B}$ un subespacio vectorial, para todo $a, b \in \mathcal{B}$, se tiene que $a - b \in \mathcal{B}$. Por el Lema 1, $\mathcal{B}$ es un subanillo de $\mathcal{A}$. Por lo tanto $\mathcal{B}$ es una subálgebra de $\mathcal{A}$. ■

Ejemplo 21. *Sea $A \in \mathbb{M}_n(\mathbb{C})$ y $D = \{p(A) : p \in \mathbb{C}[x]\}$. Entonces D es una subálgebra de $\mathbb{M}_n(\mathbb{C})$. Primero notemos que D es un subespacio vectorial de $\mathbb{M}_n(\mathbb{C})$, ya que dados $p(A), q(A) \in D$ y $\lambda \in \mathbb{C}$ arbitrarios se cumple que*

$$p(A) + \lambda q(A) = (a_0 + \cdots + a_n A^n) + \lambda(b_0 + \cdots b_m A^m) \in D$$

Además si tomamos $p(A), q(A)$

$$p(A)q(A) = (pq)(A) = c_0 + c_1 A + \cdots + c_{n+m} A^{n+m} \in D.$$

Por lo tanto el producto es cerrado.

Lema 27. *Sea $\mathcal{A}$ una álgebra y $\{\mathcal{A}_\alpha\}_{\alpha \in \Lambda}$ una familia de subálgebras de $\mathcal{A}$, entonces*

$$\mathcal{B} = \bigcap_{\alpha \in \lambda} \mathcal{A}_\alpha$$

es una subálgebra de $\mathcal{A}$.

Demostración 36. *Por el Lema 26 basta probar que $\mathcal{B}$ es un subespacio vectorial de $\mathcal{A}$, y que el producto es cerrado. Tenemos que $\mathcal{A}_\alpha$ es un subespacio vectorial de $\mathcal{A}$ para cada $\alpha \in \Lambda$, luego $\mathcal{B}$ es un subespacio vectorial de $\mathcal{A}$. Ahora dados $a, b \in \mathcal{B}$, tenemos que $a, b \in \mathcal{A}_\alpha$ para todo $\alpha \in \Lambda$, por lo tanto $ab \in \mathcal{A}_\alpha$ para todo $\alpha \in \Lambda$, en consecuencia $ab \in \mathcal{B}$.* ■

Definición 25 (**Álgebra generada**). *Dada una álgebra $\mathcal{A}$ y $\mathcal{B} \subset \mathcal{A}$ no vacío, el álgebra generada por $\mathcal{B}$ es la intersección de todas las subálgebras de $\mathcal{A}$ que contienen a $\mathcal{B}$. Denotaremos al álgebra generada por $\mathcal{B}$ por $\mathcal{A}(\mathcal{B})$.*

En adelante asumiremos que las álgebras contienen a la Identidad multiplicativa. Si una familia $\mathcal{F} \subset \mathcal{A}$ no contiene a la identidad multiplicativa asumiremos que

$$\mathcal{A}(\mathcal{F}) = \mathcal{A}(\mathcal{F}, \{I\}).$$

Proposición 11. *El álgebra generada por $\mathcal{B}$ es el álgebra más pequeña que contiene a $\mathcal{B}$.*

Demostración 37. *Sea $\mathcal{A}_\lambda$ una álgebra que contiene a $\mathcal{B}$, por definición de álgebra generada tenemos que*

$$\mathcal{A}(\mathcal{B}) \subset \mathcal{A}_\lambda.$$

Por lo tanto$\mathcal{A}(\mathcal{B})$ es el álgebra más pequeña que contiene a $\mathcal{B}$. ■

El siguiente ejemplo sera utilizado varias veces en lo que resta del trabajo.

Ejemplo 22 (Álgebra generada por una matriz).
Sea $\mathcal{A} = \mathbb{M}_n(\mathbb{C})$ y $\mathcal{F} = \{A\}$, donde $A \in \mathbb{M}_n(\mathbb{C})$. Necesariamente $A^k \in \mathcal{A}(\mathcal{F})$ para cada $k \in \mathbb{N}$. Del hecho de que $\mathcal{A}(\mathcal{F})$ es un espacio vectorial se sigue que

$$\{p(A) : p \in \mathbb{C}[x]\} \subset \mathcal{A}(\mathcal{F}).$$

Probaremos que los únicos elementos de $\mathcal{A}(\mathcal{F})$ son polinomios en A. Para esto notemos que según el Ejemplo 21, $\{p(A) : p \in \mathbb{C}[x]\}$ es una subálgebra que contiene a A. Por la Proposición 11,

$$\mathcal{A}(\mathcal{F}) \subset \{p(A) : p \in \mathbb{C}[x]\}.$$

Así $\mathcal{A}(\mathcal{F}) = \{p(A) : p \in \mathbb{C}[x]\}$. Esta descripción del álgebra generada por A es buena pero no muy precisa.

Veamos un caso particular para entender mejor el problema. Consideremos un bloque de Jordan y la matriz identidad de dimensión $n \times n$:

$$J_n(0) = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & 1 \\ & & & 0 \end{pmatrix}, \qquad I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

¿Qué álgebra generan I y $J_n(0)$? es decir, ¿Qué matrices podemos formar con productos y combinaciones lineales de I y J? Por ejemplo, podemos formar las matrices

$$\alpha I + \beta J_n(0), (I + J_n(0))^2, \ \ J_n(0)^{n-1}.$$

En el caso de matrices 2×2 tenemos que $J^2 = 0$, por lo tanto todas las matrices que se pueden generar son de la forma

$$\alpha I + \beta J_2(0) = \begin{pmatrix} \alpha & \beta \\ 0 & \alpha \end{pmatrix}.$$

Ahora consideremos matrices 3×3, es decir,

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad J_3(0) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

¿Cuál es el álgebra generada por estas matrices? En este caso vale considerar $J_n(0)^2$, entonces el álgebra generada por I y $J_3(0)$ consiste de todas las matrices de la forma

$$\alpha I + \beta J_3(0) + \gamma J_3(0)^2 = \begin{pmatrix} \alpha & \beta & \gamma \\ 0 & \alpha & \beta \\ 0 & 0 & \alpha \end{pmatrix}.$$

De manera general, el álgebra generada por I y $J_n(0)$ consiste de todos los polinomios en J de grado a lo más $n-1$ porque $J_n(0)^n = 0$, tenemos entonces todas las matrices de la forma

$$\begin{aligned} p(J_n(0)) &= a_0 I + a_1 J_n(0) + a_2 J_n(0)^2 + \ldots + a_{n-1} J_n(0)^{n-1} \\ &= \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ 0 & a_0 & \ddots & \vdots \\ & & \ddots & a_1 \\ 0 & & 0 & a_0 \end{pmatrix}. \end{aligned}$$

También podemos describir explícitamente el álgebra generada por la matriz

$$A = \begin{pmatrix} \lambda & 1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & \lambda & 1 \\ 0 & \cdots & \cdots & 0 & 0 & \lambda \end{pmatrix}.$$

Esta es la misma álgebra que la generada por $J_n(0)$, puesto que $A = \lambda I - J_n(0)$, por lo cual $A \in \mathcal{A}(\{J_n(0)\})$, de manera similar $J_n(0) = \lambda I - A$, por lo cual $J_n(0) \in \mathcal{A}(\{A\})$. De esta manera tenemos que $\mathcal{A}(\{A\}) = \mathcal{A}(\{J_n(0)\})$.

Pasamos a analizar el caso del álgebra genera por J y su transpuesta. Observe que

$$J_n(0)^T = J_n^T = \begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \\ & & & \\ 0 & & 1 & 0 \end{pmatrix}.$$

Algunas matrices del álgebra generada por I, $J_n(0)$ y J_n^T son suma de polinomios en $J_n(0)$ con polinomios en J_n^T, ambos polinomios de grado a los más $n-1$, esto es, algunas matrices del álgebra generada por $J_n(0)$ y J_n^T son

$$\begin{aligned} p(J_n(0)) + q(J_n^T) &= a_0 I + a_1 J_n(0) + \ldots + a_{n-1}(J_n(0))^{n-1} + b_1 J_n^T + b_2 (J_n^T)^2 + \ldots + b_{n-1}(J_n^T)^{n-1} \\ &= \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ b_1 & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 \\ b_{n-1} & \ldots & b_1 & a_0 \end{pmatrix}. \end{aligned}$$

Este tipo de matrices se llaman matrices de Toeplitz, pero no son todas las matrices que están en el álgebra generada por I, $J_n(0)$ y J_n^T pues tenemos por ejemplo la matriz $J_n(0)J_n^T$. Sea M^{jk} la matriz cuyas entradas son cero, excepto la entrada (j,k) la cual es 1. En el caso $n = 2$ verificamos fácilmente que

$$J_2(0)J_2^T = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = M_{11}.$$

De manera general tenemos que

$$(J_n(0))^{n-1}(J_n^T)^{n-1} = \begin{pmatrix} 0 & \cdots & 1 \\ \vdots & \ldots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ldots & \vdots \\ 1 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ldots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} = M^{11}.$$

De este modo conseguimos más matrices del álgebra generada por I, $J_n(0)$ y J_n^T:

$$M^{1j} = M^{11}J^{j-1} \in \mathcal{A}(\{J_n(0), J_n^T\}), \quad j = 2, ..., n,$$

pues la k-ésima fila de

$$M^{11}(J_n(0))^{j-1}$$

es el producto de la k-ésima fila de M^{11} por $(J_n(0))^{j-1}$. También

$$M^{j1} = (J_n^T)^{j-1}M^{11} \in \mathcal{A}(\{J_n(0), J_n^T\}), \quad j = 2, ..., n,$$

pues la k-ésima columna de

$$(J_n^T)^{j-1}M^{11}$$

es el producto de $(J_n^T)^{j-1}$ y la k-ésima columa de M^{11}. Por otra parte $M^{ik} = M^{ij}M^{jk}$, en efecto, por definición de producto de matrices tenemos que

$$(M^{ij}M^{jk})_{pq} = \sum_{s=1}^{n}(M^{ij})_{ps}(M^{jk})_{sq} = \sum_{s=1}^{n}(\delta_{ip}\delta_{js})(\delta_{kq}\delta_{js}) = \delta_{ip}\delta_{kq} = (M^{ik})_{pq}.$$

Entonces otras matrices en $\mathcal{A}(\{J_n(0), J_n^T\})$ son los productos $M^{jk} = M^{j1}M^{1k}$. De esta manera tenemos que el álgebra generada por $J_n(0)$, J_n^T es $\mathbb{M}_n(\mathbb{C})$ ya que para cualquier matriz A,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \cdots & \vdots & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}M^{ij}.$$

Notemos que podemos darle una expresión explícita a la matriz A en términos de $J_n(0)$ y J_n^T substituyendo

$$M^{j1} = (J_n^T)^{j-1}M^{11} = (J_n^T)^{j-1}(J_n(0))^{n-1}(J_n^T)^{n-1}$$
$$M^{1j} = M^{11}(J_n(0))^{j-1} = (J_n(0))^{n-1}(J_n^T)^{n-1}(J_n(0))^{j-1}.$$

6.2 Producto directo de álgebras.

De manera similar a grupos, podemos generar nuevas álgebras a partir de algunas ya conocidas por medio del producto cartesiano.

Definición 26 (**Producto directo de algebras.**). *Sea $\mathcal{A}_1, ..., \mathcal{A}_m$ una colección de álgebras sobre un cuerpo $\mathbb{F}$. Tomemos el producto cartesiano*

$$\mathcal{A} = \mathcal{A}_a \times \cdots \times \mathcal{A}_m.$$

Introducimos las siguientes operaciones en $\mathcal{A}$:

$$\begin{aligned}(a_1, a_2, \cdots, a_m) + (b_1, b_2, \cdots, b_m) &= (a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m),\\ \lambda(a_1, a_2, \cdots, a_m) &= (\lambda a_1, \lambda a_2, \cdots, \lambda a_m),\\ (a_1, a_2, \cdots, a_m) \cdot (b_1, b_2, \cdots, b_m) &= (a_1 b_1, a_2 b_2, \cdots, a_m b_m).\end{aligned}$$

$\mathcal{A}$ junto con estas operaciones recibe el nombre de producto directo de álgebras.

Proposición 12. *El producto directo de álgebras es una álgebra.*

Demostración 38. *Sean $\mathcal{A}_1, ..., \mathcal{A}_m$ álgebras y $\mathcal{A}$ su producto directo. Primeramente notemos que $\mathcal{A}$ con la suma y producto escalar es un espacio vectorial. La tercera operación es asociativa porque se define coordenada a coordenada y el producto en cada álgebra es asociativo. Finalmente dados $a, b, c \in \mathcal{A}$ y $\alpha \in \mathbb{F}$ tenemos que*

$$\begin{aligned}\alpha(a \cdot b) =& \alpha(a_1 b_1, a_2 b_2, \cdots, a_m b_m) = (a_1, \cdots, a_m)(\alpha b_1, \cdots, \alpha b_m) = (a) \cdot (\alpha b)\\ &= (\alpha a_1, \alpha a_2, \cdots, \alpha a_m) \cdot (b_1.b_2, \cdots, b_m) = (\alpha a) \cdot b\end{aligned}$$

y

$$\begin{aligned}a \cdot (b + c) =& (a_1, \cdots, a_m) \cdot (b_1 + c_1, \cdots, b_m + c_m)\\ =& (a_1 b_1 + a_1 c_1, \cdots, a_m b_m + a_m c_m) = a \cdot b + a \cdot c.\end{aligned}$$

La prueba de que $(a + b) \cdot c = a \cdot c + b \cdot c$ es análoga. Por lo tanto el producto directo de álgebras es una álgebra. ■

Ejemplo 23. *Sea $\mathcal{A} = \mathbb{M}_2(\mathbb{C}) \times \mathbb{M}_3(\mathbb{C})$. $\mathcal{A}$ es el álgebra de pares de matrices donde las operaciones se realizan coordenada a coordenada. Por ejemplo*

$$\left(\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{pmatrix}\right) \in \mathcal{A}.$$

En el álgebra $\mathcal{B}$ cuyos elementos tienen la forma

$$\begin{pmatrix}A_1 & 0\\ 0 & A_2\end{pmatrix} \in \mathbb{M}_5(\mathbb{C}), \quad A_1 \in \mathcal{A}_1 \quad y \quad A_2 \in \mathcal{A}_2,$$

las operaciones se realizan del mismo modo que en $\mathcal{A}$. En realidad $\mathcal{A}$ y $\mathcal{B}$ son isomorfas, con el ismorfismo $\phi : \mathcal{A} \to \mathcal{B}$, dado por $\phi(A_1, A_2) = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$.

Ejemplo 24. *Recordando que el álgebra generada por una matriz A es el conjunto de todos los polinomios en A, en particular tomemos $A = \begin{pmatrix} J_1 & 0 \\ 0 & J_2 \end{pmatrix} \in \mathbb{M}_5(\mathbb{C})$, donde J_1 es un bloque de Jordan de tamaño 2×2 y J_2 es un bloque de Jordan de tamaño 3×3. Tenemos que $\mathcal{A}(A)$ es el conjunto de polinomios de grado a lo sumo 2, y un elemento en $\mathcal{A}(A)$ debe de ser de la forma*

$$c_0 I + c_1 A + c_2 A^2 = \begin{pmatrix} c_0 & c_1 & 0 & 0 & 0 \\ 0 & c_0 & 0 & 0 & 0 \\ 0 & 0 & c_0 & c_1 & c_2 \\ 0 & 0 & 0 & c_0 & c_1 \\ 0 & 0 & 0 & 0 & c_0 \end{pmatrix}.$$

Si ahora consideramos $\mathcal{B} = \mathcal{A}(\{A, I_1, I_2\})$, donde

$$I_1 = \begin{pmatrix} I_{2\times 2} & 0 \\ 0 & 0 \end{pmatrix} \quad y \quad I_2 = \begin{pmatrix} 0 & 0 \\ 0 & I_{3\times 3} \end{pmatrix},$$

entonces $\mathcal{B}$ debe de contener a todas las matrices de la forma

$$\begin{pmatrix} c_0 & c_1 & 0 & 0 & 0 \\ 0 & c_0 & 0 & 0 & 0 \\ 0 & 0 & c_0 & c_1 & c_2 \\ 0 & 0 & 0 & c_0 & c_1 \\ 0 & 0 & 0 & 0 & c_0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} c_0 & c_1 & 0 & 0 & 0 \\ 0 & c_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

junto a las matrices de la forma

$$\begin{pmatrix} c_0 & c_1 & 0 & 0 & 0 \\ 0 & c_0 & 0 & 0 & 0 \\ 0 & 0 & c_0 & c_1 & c_2 \\ 0 & 0 & 0 & c_0 & c_1 \\ 0 & 0 & 0 & 0 & c_0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c_0 & c_1 & c_2 \\ 0 & 0 & 0 & c_0 & c_1 \\ 0 & 0 & 0 & 0 & c_0 \end{pmatrix}.$$

De esta manera generamos una álgebra que contiene a todas las matrices de la forma

$$\begin{pmatrix} c_0 & c_1 & 0 & 0 & 0 \\ 0 & c_0 & 0 & 0 & 0 \\ 0 & 0 & c_2 & c_3 & c_4 \\ 0 & 0 & 0 & c_2 & c_3 \\ 0 & 0 & 0 & 0 & c_2 \end{pmatrix}.$$

Notemos que $\mathcal{A}(A) \subset \mathcal{B}$, esta contención es propia pues

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

está en $\mathcal{B}$ pero no en $\mathcal{A}(A)$. Además, tenemos que $\mathcal{A}(J_1) \times \mathcal{A}(J_2) \subseteq \mathcal{B}$, y como $I_1, I_2, A \in \mathcal{A}(J_1) \times \mathcal{A}(J_2)$, tenemos que $\mathcal{A}(J_1) \times \mathcal{A}(J_2) = \mathcal{B}$.

La siguiente proposición nos dice que el álgebra generada por un operador proyección es isomorfa a un producto de álgebras.

Proposición 13 (**Álgebra generada por un operador proyección**). *Sea V un espacio vectorial de dimensión finita sobre el campo $\mathbb{F}$. El álgebra generada por un operador proyección es isomorfa al álgebra $\mathbb{F} \times \mathbb{F}$.*

Demostración 39. *Asumiendo que $P \neq I, 0$ entonces el álgebra generada por P es*

$$\mathcal{A}(P) = \{q(P) : q \in \mathbb{F}[x]\} = \{\alpha I + \beta P : \alpha, \beta \in \mathbb{F}\} = \{\gamma P + \delta(I - P) : \gamma, \delta \in \mathbb{F}\}.$$

De esto último tenemos que todas las operaciones sobre $\mathcal{A}(P)$ se realizan coordenada a coordenada en el siguiente sentido. Dados $a, b \in \mathcal{A}(P)$, con $a = \alpha_1 P + \beta_1(I - P)$, $b = \alpha_2 P + \beta_2(I - P)$ y $\lambda \in \mathbb{F}$. Tenemos que

1) $a + b = \alpha_1 P + \beta_1(I - P) + \alpha_2 P + \beta_2(I - P) = (\alpha_1 + \alpha_2)P + (\beta_1 + \beta_2)(I - P)$,

2) $\lambda a = \lambda[\alpha_1 P + \beta_1(I - P)] = \lambda\alpha_1 P + \lambda\beta_1(I - P)$,

3)
$$\begin{aligned} a \cdot b &= [\alpha_1 P + \beta_1(I - P)][\alpha_2 P + \beta_2(I - P)] \\ &= \alpha_1\alpha_2 P^2 + \alpha_1\beta_2 P(I - P) + \alpha_2\beta_1(I - P)P + \beta_1\beta_2(I - P)^2 \\ &= \alpha_1\alpha_2 P + \beta_1\beta_2(I - P) \end{aligned}$$

pues $P(I - P) = P - P^2 = 0$, $(I - P)P = 0$ y $(I - P)^2 = I - P$.

La función $\phi : \mathcal{A}(P) \to \mathbb{F} \times \mathbb{F}$ dada por

$$\phi(\alpha P + \beta(I - P)) = (\alpha, \beta)$$

es evidentemente biyectiva. Por lo comentado anteriormente también es un homomorfismo. y por lo tanto es un isomorfismo. ■

6.3 Álgebras generadas por matrices de Jordan.

En la presente sección daremos algunos ejemplos de álgebras generadas por matrices relativamente sencillas. Estos ejemplos nos ayudarán a dar una descripción detallada del álgebra generada por un operador lineal arbitrario. Estos ejemplos son álgebras generadas por matrices que son suma directa de matrices de Jordan de distintos tamaños.

Ejemplo 25. *En el Ejemplo 22 se analizó con cierto detalle el caso del álgebra generada por un bloque de Jordan $J_n(0)$. Ahora consideramos el caso del álgebra generada por una matriz J de la forma*

$$J = \begin{pmatrix} J_n(0) & & \\ & \ddots & \\ & & J_n(0) \end{pmatrix}.$$

Sabemos, por el mismo ejemplo 22, que el álgebra consiste de todas las matrices de la forma

$$\begin{pmatrix} p(J_n(0)) & & \\ & \ddots & \\ & & p(J_n(0)) \end{pmatrix}$$

con $p \in \mathbb{F}[x]$. Notemos que esta álgebra es esencialmente $\mathcal{A}(J_n(0))$. En efecto, consideremos la transformación $\varphi : \mathcal{A}(J_n(0)) \to \mathcal{A}(J)$ dada por

$$\varphi(p(J_n(0))) = \begin{pmatrix} p(J_n(0)) & & \\ & \ddots & \\ & & p(J_n(0)) \end{pmatrix}.$$

Es fácil ver que esta transformación es un isomorfismo de álgebras, por lo tanto $\mathcal{A}(J_n(0)) \cong \mathcal{A}(J)$.

Ejemplo 26. *Considérese la matriz*

$$J = \begin{pmatrix} J_n(0) & 0 \\ 0 & J_m(0) \end{pmatrix} \quad con \quad n \geq m.$$

Nuevamente el álgebra generada por J consiste de todos los polinomios en J con coeficientes complejos. Notemos que

$$J^m = \begin{pmatrix} J_n^m(0) & 0 \\ 0 & J_m^m(0) \end{pmatrix} = \begin{pmatrix} J_n^m(0) & 0 \\ 0 & 0 \end{pmatrix}.$$

A partir de la potencia m-ésima, la matriz $J_m(0)$ no aportará información, sólo cuentan las potencias de $J_n(0)$, por lo cual parecería que basta estudiar el álgebra generada por $J_n(0)$. En efecto, sea $\varphi : \mathbb{C}[x] \to \mathcal{A}(J)$ dada por

$$\varphi(p) = p(J).$$

Es fácil ver que φ es un homomorfismo de álgebras debido a las propiedades del producto de matrices. Ahora bien notemos que $Im\,\varphi = \mathcal{A}(J)$, afirmamos que $\ker\varphi = I_{x^n}$. En efecto, la contención

$$I_{x^n} \subset \ker\varphi$$

es trivial por lo cual sólo probaremos la contención

$$\ker\varphi \subset I_{x^n}.$$

Sea $p \in \ker\varphi$. Podemos escribir $p = q + r$, donde

$$q(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1},$$

$$r(x) = a_n x^n + \cdots + a_{n+k} x^{n+k},$$

donde los coeficientes $a_n, \cdots, a_{n+k}$ pueden ser cero. Note que $r \in \ker \varphi$. Tenemos que

$$0 = p(J) = q(J) = \begin{pmatrix} q(J_n(0)) & 0 \\ 0 & q(J_m(0)) \end{pmatrix}.$$

Entonces $q(J_n(0)) = 0$. Del Ejemplo 22 tenemos que $a = 0 = \cdots = a_{n-1} = 0$. Por lo tanto $p = r \in I_{x^n}$. Por el primer teorema de isomorfismos para álgebras tenemos que

$$\mathcal{A}(J) \cong \mathbb{C}[x]/I_{x^n}.$$

También

$$\mathcal{A}(J_n(0)) \cong \mathbb{C}[x]/I_{x^n}.$$

El ejemplo anterior tiene una generalización bastante natural y que se sigue de los mismos argumentos.

Ejemplo 27. *Ahora consideramos la matriz*

$$J = \begin{pmatrix} J_{n_1}(0) & & & \\ & J_{n_2}(0) & & \\ & & \ddots & \\ & & & J_{n_m}(0) \end{pmatrix}$$

con $n_1 \geq n_2 \geq \cdots \geq n_m$. Por los mismos argumentos dados en el Ejemplo 26, tenemos que

$$\mathcal{A}(J) \cong \mathcal{A}(J_{n_1}(0)) \cong \mathbb{C}[x]/I_{x^{n_1}}.$$

Ahora consideramos el álgebra generada por una matriz diagonal por bloques y por su transpuesta, donde cada bloque es una matriz elemental de Jordan con valor propio cero. Primero consideremos el caso en que sólo hay 2 bloques.

Ejemplo 28 (Álgebra generada por un bloque de Jordan y su transpuesta). *Sea*

$$J = \begin{pmatrix} J_n(0) & 0 \\ 0 & J_m(0) \end{pmatrix} \quad con \quad n > m.$$

El álgebra generada por J y J^t debe contener a las matrices

$$J^{n-1}(J^t)^{n-1} = \begin{pmatrix} (J_n(0))^{n-1}(J_n^t(0))^{n-1} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} M^{11} & 0 \\ 0 & 0 \end{pmatrix}.$$

Los calculos hechos en el Ejemplo 22 nos permiten ver que todas las matrices de la forma

$$\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix} \quad A \in \mathbb{M}_n(\mathbb{C})$$

pertenecen a $\mathcal{A}(J, J^t)$. Este hecho justifica que la matriz

$$\begin{pmatrix} 0 & 0 \\ 0 & J_m(0) \end{pmatrix}$$

está en $\mathcal{A}(J, J^t)$. Entonces podemos garantizar que las matrices de la forma

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \quad A \in \mathbb{M}_n(\mathbb{C}), B \in \mathbb{M}_m(\mathbb{C})$$

pertenencen a $\mathcal{A}(J, J^t)$. Esto prueba que $\mathcal{A}(J, J^t) \cong \mathbb{M}_n(\mathbb{C}) \times \mathbb{M}_m(\mathbb{C})$.

Una generalización sencilla del ejemplo anterior es la siguiente.

Ejemplo 29. *Sea*

$$J = \begin{pmatrix} J_{n_1}(0) & & & \\ & J_{n_2}(0) & & \\ & & \ddots & \\ & & & J_{n_m}(0) \end{pmatrix}$$

con $n_1 > n_2 \cdots > n_m$. El álgebra generada por J y J^t es isomorfa a

$$\mathbb{M}_{n_1}(\mathbb{C}) \times \cdots \times \mathbb{M}_{n_m}(\mathbb{C}).$$

Ejemplo 30. *Si en el Ejemplo 28 consideremos $n = m$ tendremos que*

$$\mathcal{A}(J) \cong \mathbb{M}_n(\mathbb{C}).$$

Ejemplo 31. *Si en 29 consideramos que $n_1 \geq \cdots \geq n_m$, entonces sea el conjunto de indices $\{i_1, \cdots, i_p\}$ tales que*

$$n_{i_1} > \cdots > n_{i_p}.$$

Es decir que solo consideremos los índices tales que se obtenga la situación del ejemplo29, entonces

$$\mathcal{A}(J) \cong \mathbb{M}_{n_{i_1}}(\mathbb{C}) \times \cdots \times \mathbb{M}_{n_{i_p}}(\mathbb{C})$$

6.4 Álgebra generada por un operador lineal.

Ahora estamos en condiciones de considerar el caso del álgebra generada por un operador lineal sobre un espacio vectorial de dimensión finita arbitrario.

Ejemplo 32. *Sea $T : V \to V$ un operador lineal sobre un espacio vectorial de dimensión finita. Existe una base $\mathcal{B}$ tal que*

$$A = [T]_{\mathcal{B}} = \begin{pmatrix} J_{n_{1,1}}(\lambda_1) & & & & & & \\ & \ddots & & & & & \\ & & J_{n_{1,k_1}}(\lambda_1) & & & & \\ & & & \ddots & & & \\ & & & & J_{n_{m,1}}(\lambda_m) & & \\ & & & & & \ddots & \\ & & & & & & J_{n_{m,k_m}}(\lambda_m) \end{pmatrix}$$

donde $n_{j,k}$ es un entero que indica el tamaño del bloque de Jordan y $\lambda_1 \cdots, \lambda_m$ son los valores propios de T distintos entre sí. Desde luego k_j representa el número de bloques de Jordan asociados al valor propio λ_j. Consideremos el isomorfismo $\phi : V \to \mathbb{C}^n$ definido por

$$\phi(v) = [v]_{\mathcal{B}}.$$

La aplicación ϕ induce el siguiente isomorfismo de álgebras

$$\begin{aligned} \Phi : End(V) &\to End(\mathbb{C}^n) \\ S &\mapsto \phi S \phi^{-1} \end{aligned}$$

En realidad $\Phi(S)$ es la representación matricial de S en la base $\mathcal{B}$. La restrición de Φ a $\mathcal{A}(T) \subset End(V)$ es un isomorfismo de álgebras

$$\begin{array}{rccc} \Phi : & \mathcal{A}(T) & \to & \mathcal{A}(A) \\ & S = p(T) & \mapsto & p(A). \end{array}$$

Entonces el álgebra generada por T es isomorfa al álgebra generada por $A = [T]_{\mathcal{B}}$. Esto nos permite reducir nuestro estudio a álgebras generadas por matrices diagonales por bloques, donde cada bloque es un bloque de Jordan asociado a un valor propio λ. Ahora consideremos el polinomio minimal de T o de A:

$$p_m = (x - \lambda_1)^{n_1} \cdots (x - \lambda_m)^{n_m}.$$

Por el Teorema 2 se tiene la descomposición en subespacios invariantes

$$V = V_1 \oplus \cdots \oplus V_m, \quad V_i = \ker(T - \lambda_j)^{n_j}.$$

De manera equivalente

$$\mathbb{C}^n = W_1 \oplus \cdots \oplus W_m, \quad W_j = \ker(A - \lambda_j I)^{n_j}.$$

Tenemos las proyecciones $P_1, \cdots, P_m$ tales que

$$\begin{aligned} P_1 + \cdots + P_m &= I, \\ P_i P_j = 0 \quad si \quad i \neq j, \\ Im\, P_j &= V_j, \end{aligned}$$

para las cuales existen polinomios $q_1, \cdots, q_m$ tales que

$$P_j = q_j(T) \in \mathcal{A}(T).$$

Entonces $P_jTP_j \in \mathcal{A}(T)$. Observe que $\mathcal{A}(T)$ es una álgebra conmutativa. Se tiene que

$$\mathcal{A}(T) = \mathcal{A}(P_1TP_1, \cdots, P_mTP_m).$$

En efecto, por las propiedades de las proyecciones P_i tenemos que

$$T = ITI = (P_1 + \cdots + P_m)T(P_1 + \cdots + P_m) = P_1TP_1 + \cdots + P_mTP_m.$$

Ahora consideremos la subálgebra $\mathcal{A}(P_jTP_j)$. Para cualquier polinomio p se tiene que $p(P_jTP_j) = P_jp(T)P_j$. Entonces la aplicación $\Phi_j : \mathcal{A}(T) \to \mathcal{A}(P_jTP_j)$ definida por

$$\Phi_j(S) = P_jSP_j$$

es un homomorfismo de álgebras. Además, podemos definir la transformación

$$\psi : \mathcal{A}(T) \to \bigoplus_{i=1}^{m} \mathcal{A}(P_iTP_i)$$
$$S = p(T) \mapsto (P_1p(T)P_1, \cdots, P_mp(T)P_m).$$

Esta transformación es un homomorfismo, veamos que es un isomorfismo de álgebras, es decir,

$$\mathcal{A}(T) \cong \mathcal{A}(P_1TP_1) \oplus \cdots \oplus \mathcal{A}(P_mTP_m).$$

En efecto, sea $S = p(T) \in \ker\psi$. Dado que

$$p(T) = P_1p(T)P_1 + \cdots + P_mp(T)P_m,$$

entonces $S = p(T) = 0$. Ahora ψ es inyectivo porque si $\psi(q(T)) = \psi(p(T))$, entonces $\psi(p(T) - q(T)) = 0$, por lo tanto $p(T) = q(T)$. Veamos que ψ es sobreyectivo, sea

$$S = (P_1r_1(T)P_1, \cdots, P_mr_m(T)P_m) \in \bigoplus_{i=1}^{m} \mathcal{A}(p_iTp_i).$$

Sabemos que $P_j = q_j(T)$ es un polinomio en T. Definimos $p(x) = q_1(x)r_1(x)q_1(x) + \cdots + q_m(x)r_m(x)q_m(x)$. Entonces $p(T) = P_1r_1(T)P_1 + \cdots + P_mr_m(T)P_m \in \mathcal{A}(T)$ y

$$\psi(p(T)) = (P_1r_1(T)P_1, \cdots, P_mr_m(T)P_m) = S.$$

Recordando que $\mathcal{A}(T) \cong \mathcal{A}(A)$, de los mismos argumentos dados, se sigue que

$$\mathcal{A}(A) \cong \bigoplus_{i=1}^{m} \mathcal{A}([P_iTP_i]_{\mathcal{B}}).$$

Notemos que $[P_jTP_j]_{\mathcal{B}} \in \mathcal{A}(A)$. Además

$$[P_iTP_i]_{\mathcal{B}} = \begin{pmatrix} 0 & & & & & & \\ & \ddots & & & & & \\ & & J_{n_{i,1}}(\lambda_i) & & & & \\ & & & \ddots & & & \\ & & & & J_{n_{i,k_i}}(\lambda_i) & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{pmatrix}.$$

Cada una de las álgebras $\mathcal{A}([P_iTP_i]_{\mathcal{B}})$ es isomorfa al álgebra generada por un bloque de Jordan de la forma expuesta en el Ejemplo 27. Así

$$\mathcal{A}(T) \cong \mathcal{A}(A) \cong \bigoplus_{i=1}^{m} (\mathbb{C}[x]/I_{x^{n_{i,1}}}).$$

Ejemplo 33. *Ahora vamos a considerar el álgebra generada por un operador lineal y su adjunta. Asumimos que la base $\mathcal{B}$ lleva a T a la forma canónica de Jordan. En el espacio V se introduce un producto interno $\langle \cdot, \cdot \rangle$ de modo que $\mathcal{B}$ resulte una base ortonormal. Dado un operador $S \in End(V)$, el adjunto de S es el operador S^* tal que*

$$\langle Sv, w \rangle = \langle v, S^* w \rangle \quad \forall v, w.$$

Dado que $\mathcal{B}$ es base ortonormal, entonces

$$[S^*]_{\mathcal{B}} = [S]^*_{\mathcal{B}},$$

donde $[S]^*_{\mathcal{B}}$ significa la matriz transpuesta conjugada de $[S]_{\mathcal{B}}$. Respecto al producto interno indicado, los subespacios V_j son ortogonales entre sí. Esto implica que cada P_j es una proyección ortogonal, así P_j es auto-adjunta. Como en el ejemplo anterior, un punto clave de la demostración es que podamos probar que

$$\mathcal{A}(T, T^*) = \mathcal{A}(P_1TP_1, P_1T^*P_1, \cdots, P_mTP_m, P_mT^*P_m).$$

Dado que T conmuta con P_j se tiene que $P_jT^* = T^*P_j$, en particular esto significa que cada subespacio V_j es invariante bajo T^*. Además, de aquí se sigue que para todo polinomio p se cumple que

$$P(P_iTP_i, P_iT^*P_i) = P_ip(T, T^*)P_i.$$

La prueba para ver que

$$\mathcal{A}(T, T^*) \cong \bigoplus_{i=1}^{m} \mathcal{A}(P_iTP_i, P_iT^*P_i)$$

es la misma que la dada en el ejemplo anterior, ya que los elementos de $\mathcal{A}(P_iTP_i, P_iT^*P_i)$ son precisamente polinomios de $P_iTP_i, P_iT^*P_i$. Finalmente, sólo debemos ver que $\mathcal{A}(P_iTP_i, P_iT^*P_i)$ es isomorfa al álgebra generada por un bloque de Jordan y su transpuesta. Esto es

$$\mathcal{A}(P_iTP_i, P_iT^*P_i) \cong \mathbb{M}_{n_{i,1}}(\mathbb{C}) \times \cdots \times \mathbb{M}_{n_{i,k_i}}(\mathbb{C}).$$

Para esto, veamos primero que

$$\mathcal{A}(P_iTP_i, P_iT^*P_i) = \mathcal{A}(P_iTP_i - \lambda_iP_i, P_iT^*P_i - \overline{\lambda_i}P_i).$$

En efecto, para probar que $P_iTP_i \in \mathcal{A}(P_iTP_i - \lambda_iP_i, P_iT^*P_i - \overline{\lambda_i}P_i)$ probaremos primero que $P_i \in \mathcal{A}(P_iTP_i, P_iT^*P_i)$. Recordemos que existe $t_i(x) \in \mathbb{C}[x]$ para el cual

$$P_i = t_i(T),$$

de esta manera al evaluar P_iTP_i en $t_i(x)$ tenemos que

$$P_i = P_iP_iP_i = P_it_i(T)P_i = t_i(P_iTP_i) \in \mathcal{A}(P_iTP_i, P_iT^*P_i).$$

Y por lo tanto

$$P_iTP_i = P_iTP_i - \lambda_iP_i \in \mathcal{A}(P_iTP_i - \lambda_iP_i, P_iT^*P_i - \overline{\lambda_i}P_i)$$

de la misma manera se prueba que $P_iT^*P_i \in \mathcal{A}(P_iTP_i - \lambda_iP_i, P_iT^*P_i - \overline{\lambda_i}P_i)$ *y la otra contención es trivial porque los generadores del álgebra son polinomios de* P_iTP_i *y* $P_iT^*P_i$.

Ahora bien $\mathcal{A}(P_iTP_i - \lambda_iP_i, P_iT^*P_i - \overline{\lambda_i}P_i)$ *es isomorfa al álgebra generada por las representaciones matriciales en la base* $\mathcal{B}$ *de sus generadores, pero la representación matricial del primer generador es una matriz diagonal por bloques donde todos los bloques son cero salvo un bloque es una matriz de la forma vista en el ejemplo 27. Y la representación del segundo generador es la transpuesta del primero. De esta manera está algebra es isomorfa a la generada por un bloque de Jordan y su transpuesta.*

Conclusiones

El teorema de la descomposición de Jordan nos permitió probar que el álgebra generada por un solo operador lineal es isomorfa a un producto directo de álgebras más sencillas. Siendo estas las generadas por una matriz de Jordan.

Cuando se desea estudiar estructuras algebraicas se buscan subestructuras algebraicas que sean más simples de estudiar pero que nos sigan brindando información.

También logramos dar una descripción del álgebra generada por un operador y su adjunta. Se probó que para poder estudiar esta álgebra basta con estudiar el álgebra generada por un bloque de Jordan y su transpuesta.

Estas álgebras en general son distintas, puesto que al agregar la traspuesta podemos generar productos entre ellos y eso genera más elementos.

Apendice

A.1 Álgebras cociente

Si I es un ideal en una álgebra $\mathcal{A}$, entonces en particular I es un subespacio vectorial de V y podemos considerar las clases laterales $z + I = \{z + x : x \in I\}$ para $z \in \mathcal{A}$. Entonces el espacio cociente

$$\mathcal{A}/I = \{z + I : z \in V\}$$

es un espacio vectorial y se le puede dar la estructura de álgebra definiendo el producto como

$$(w + I) \odot (z + I) = (w \odot z + I).$$

Además se satisface lo siguiente

Lema 28. *La transformación $\pi : \mathcal{A} \to \mathcal{A}/I$ que manda $x \in \mathcal{A}$ a la clase lateral $x+I$ es un homomorfismo de álgebras.*

Teorema 4 (**Teorema de isomorfismo de álgebras**)**.** *Sea $\varphi : \mathcal{A}_1 \to \mathcal{A}_2$ un homomorfismo de álgebras. Entonces* $\ker\varphi$ *es un ideal de $\mathcal{A}_1$ y $Im\,\varphi$ es una subalgebra de $\mathcal{A}_2$, además*

$$\mathcal{A}_1 / \ker\varphi \cong Im\,\varphi.$$

Bibliography

[1] J. A. Beachy; W. D. Blair, *Abstract Algebra*. Fourth Edition, Waveland Press, Inc. Illinois, USA, 2019.

[2] T. S. Blyth; E. F. Robertson, *Further Linear Algebra*. Springer, London, 2006.

[3] K Hoffman; R. Kunzen, *Linear algebra*. Prentice Hall, New Jersey, 1971.

“Lis de Veracruz: Arte, Ciencia, Luz”

www.uv.mx