Journal homepage http://revistas.unitru.edu.pe/index.php/SSMM

SELECCIONES MATEMÁTICAS
Universidad Nacional de Trujillo
ISSN: 2411-1783 (Online)
2021; Vol. 8(2): 326-332.

A proof of the Cayley-Hamilton theorem using algebraic geometry

Una prueba del teorema de Cayley-Hamilton utilizando geometría algebraica

Carlos Mejía Alemán, Irene Edith Núñez Rodriguez, Rodolfo José Gálvez Pérez and Neisser Pino Romero

Received, Oct. 20, 2021 *Accepted, Dec. 10, 2021*

How to cite this article:
Megía C, Núñez I, Gálvez R, Pino N. *A proof of the Cayley-Hamilton theorem using algebraic geometry*. Selecciones Matemáticas. 2021;8(2):326–332. http://dx.doi.org/10.17268/sel.mat.2021.02.09

Abstract

In this work, we will prove the Cayley-Hamilton theorem using algebraic geometry. We will see a different proof than the one seen in a linear algebra course, in this case we will use the Zariski topology, then we will take advantage of the fact that every square matrix of order $n \times n$, with entries in a field $\mathbb{K}$, denoted by $(a_{ij})_{n\times n}$ can be seen as an element of the affine space of dimension $n \times n$ over the field $\mathbb{K}$ and thanks to this, we can resort to algebraic sets and algebraic varieties in order to obtain some results seen in an algebraic geometry and to get a proof of the Cayley-Hamilton theorem.

Keywords . Affine space, algebraic set, algebraic manifold, Zariski topology.

Resumen

En este trabajo, probaremos el teorema de Cayley-Hamilton utilizando geometría algebraica. Veremos una prueba diferente a la que se ve en un curso de álgebra lineal, en este caso utilizaremos la topología de Zariski, luego nos aprovecharemos de que toda matriz cuadrada de orden $n \times n$, con entradas en un cuerpo $\mathbb{K}$, denotada por $(a_{ij})_{n\times n}$ puede ser vista como un elemento del espacio afín de dimensión $n \times n$ sobre el cuerpo $\mathbb{K}$ y gracias a esto podemos recurrir a los conjuntos algebraicos y a las variedades algebraicas para así obtener algunos resultados vistos en un curso de geometría algebraica y conseguir una prueba del teorema de Cayley-Hamilton.

Palabras clave. Espacio afín, conjunto algebraico, variedad algebraica, topología de Zariski.

1. Introducción. Este artículo está inspirado por el trabajo que publicaron Jeffrey A. Rosoff y Gustavus Adolphus College, que tiene por nombre **A topological proof of the Cayley-Hamilton theorem**, ver [8].

En este artículo veremos algunas propiedades de la geometría algebraica clásica. Como primera definición veremos lo que es un espacio afín sobre un cuerpo $\mathbb{K}$, luego veremos lo que es un conjunto algebraico y enunciaremos algunas propiedades y ejemplos relacionadas con dicho conjunto. Veremos quienes son los conjuntos cerrados de la topología de Zariski, luego definiremos el ideal de un conjunto algebraico y daremos algunas propiedades. Definiremos un espacio topológico irreducible y luego daremos una caracterización de dicho espacio topológico, también daremos una caracterización de un conjunto algebraico irreducible y conseguiremos el Corolario 2.1 que será herramienta importante en la prueba central.

Definiremos lo que es una variadad algebraica, función polinomial y luego veremos lo que es una aplicación polinomial y daremos algunos ejemplos que serán importantes para el resultado central.

*Programa de Estudios Generales, Universidad de Lima. Lima, Perú. (camejia@ulima.edu.pe).
†Programa de Estudios Generales, Universidad de Lima. Lima, Perú.(inunez@ulima.edu.pe).
‡Facultad de Ciencias Matemáticas , Universidad Nacional Mayor de San Marcos. Lima, Perú. (rgalvezp@unmsm.edu.pe).
§Facultad de Ciencias y Filosofía, Universidad Peruana Cayetano Heredia. Lima, Perú. (neisser.pino@upch.pe).

Por último veremos algunos resultados, el primero dice lo siguiente: si el polinomio característico de la matriz $A \in M_{n\times n}(\mathbb{K})$ es $P_A(x)$ entonces existen polinomios $P_0, P_1, ..., P_{n-1} \in \mathbb{K}[X_{ij}]$ con $i, j = 1, 2, ..., n$ tales que $P_A(x) = x^n + P_{n-1}(A)x^{n-1} + ... + P_0(A)$. El segundo resultado afirma que el conjunto $\mathcal{R} = \{A \in \mathbf{A}_{\mathbb{K}}^{n^2} \mid P_A(A) = det(AI_n - A) = 0\}$ es un cerrado en la topología de Zariski y en su prueba utilizaremos el primer resultado. El tercer resultado dice que el conjunto

$$\mathcal{U} := \{A \in \mathbf{A}_{\mathbb{K}}^{n^2} \mid A \text{ tiene } n \text{ autovalores distinos}\}.$$

es un abierto no vacío de la topología de Zariski con $\mathcal{U} \subseteq \mathcal{R}$ donde $\mathbb{K}$ es un cuerpo algebraicamente cerrado. En los resultados anteriores vamos a considerar la clausura algebraica $\overline{\mathbb{K}}$ en vez $\mathbb{K}$ y así el teorema central quedará demostrado.

2. Preliminares.

En este trabajo $\mathbb{K}$ denota un cuerpo y $\overline{\mathbb{K}}$ su clausura algebraica.

Definición 2.1. *Sea $n \in \mathbb{Z}$ tal que $n \geq 1$. El **espacio afín de dimensión n** sobre el cuerpo $\mathbb{K}$ se define como*

$$\mathbf{A}_{\mathbb{K}}^n := \{(a_1, a_2, ..., a_n) \mid a_i \in \mathbb{K}, 1 \leq i \leq n\}.$$

Definición 2.2. *Un **cero o raíz** de un polinomio $q(x_1, x_2, ..., x_n) \in \mathbb{K}[x_1, x_2, ..., x_n]$ es un elemento $a = (a_1, a_2, ..., a_n) \in \mathbf{A}_{\mathbb{K}}^n$ tal que $q(a) = 0$.*

*Una **hipersuperficie** es el conjunto de todos los ceros de un polinomio no constante $q \in \mathbb{K}[x_1, x_2, ..., x_n]$, se denota por $\mathcal{Z}(q) := \{a \in \mathbf{A}_{\mathbb{K}}^n \mid q(a) = 0\}$.* Para más detalles ver [4], página 4.

Definición 2.3. *Un conjunto $T \subseteq \mathbf{A}_{\mathbb{K}}^n$ es **algebraico** si $T = \mathcal{Z}(S)$ para algún $S \subseteq \mathbb{K}[x_1, x_2, ..., x_n]$ donde $\mathcal{Z}(S) := \{a = (a_1, a_2, ..., a_n) \in \mathbf{A}_{\mathbb{K}}^n \mid q(a) = 0, \text{ para todo } q(x_1, x_2, ..., x_n) \in S\}$.*

Observaciones.

1. Si $S = \{q\} \subseteq \mathbb{K}[x_1, x_2, ..., x_n]$, entonces $\mathcal{Z}(\{q\})$ coincide con $\mathcal{Z}(q)$.
2. $\mathcal{Z}(S) = \bigcap_{q\in S} \mathcal{Z}(q)$.
3. Sea I un subconjunto de $\mathbb{K}[x_1, x_2, ..., x_n]$ generado por S entonces $\mathcal{Z}(S) = \mathcal{Z}(I)$.

Esto último quiere decir, que podemos definir sin pérdida de generalidad un conjunto algebraico $U = \mathcal{Z}(I)$ con I ideal de $\mathbb{K}[x_1, x_2, ..., x_n]$ y esto es lo que haremos de ahora en adelante, a menos que se diga lo contrario.

Proposición 2.1. *Se cumplen:*

1. *Sean I, J ideales de $\mathbb{K}[x_1, x_2, ..., x_n]$, si $I \subseteq J$ entonces $\mathcal{Z}(J) \subseteq \mathcal{Z}(I)$.*
2. *$\mathcal{Z}(0) = \mathbf{A}_{\mathbb{K}}^n$ y $\mathcal{Z}(1) = \emptyset$; es decir, los conjuntos $\mathbf{A}_{\mathbb{K}}^n, \emptyset$ son algebraicos.*
3. *Sea $\{I_\lambda\}_{\lambda\in\Lambda}$ una familia de ideales de $\mathbb{K}[x_1, x_2, ..., x_n]$ entonces $\bigcap_{\lambda\in\Lambda} \mathcal{Z}(I_\lambda) = \mathcal{Z}(\bigcup_{\lambda\in\Lambda} I_\lambda)$.*
4. *Sean I, J ideales de $\mathbb{K}[x_1, x_2, ..., x_n]$ entonces $\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$.*

Ver [2], página 56 y [5], página 10.

2.1. La topología de Zariski.

Si $\mathcal{F} := \{U \subseteq \mathbf{A}_{\mathbb{K}}^n \mid \mathbf{A}_{\mathbb{K}}^n \setminus U \text{ es un conjunto algebraico}\}$ entonces $(\mathbf{A}_{\mathbb{K}}^n, \mathcal{F})$ es un espacio topológico, pues por la Proposición 2.1 tenemos que $\mathcal{Z}(0) = \mathbf{A}_{\mathbb{K}}^n$, $\mathcal{Z}(1) = \emptyset$, si $\{I_\lambda\}_{\lambda\in\Lambda}$ una familia de ideales de $\mathbb{K}[x_1, x_2, ..., x_n]$ entonces $\bigcap_{\lambda\in\Lambda} \mathcal{Z}(I_\lambda) = \mathcal{Z}(\bigcup_{\lambda\in\Lambda} I_\lambda)$ y $\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$. La topología $\mathcal{F}$ es llamada la topología de Zariski y los $\mathcal{Z}(I)$ son los cerrados de dicha topología.

Ejemplo 2.1. *El conjunto $A = \{(a_1, a_2) \in \mathbf{A}_{\mathbb{K}}^2 \mid a_1 = a_2 \text{ o } a_2 = a_1^2\}$ es algebraico.*

Ejemplo 2.2. *El conjunto $X = \{(a, b) \in \mathbf{A}_{\mathbb{R}}^2 \mid sen(a) = b\}$ no es algebraico.*

Para el siguiente ejemplo, vamos a denotar al anillo de polinomios de n^2 variables como $\mathbb{K}[x_{ij}]$, luego $p \in \mathbb{K}[x_{ij}]$ es de la forma $p(x_{ij}) = p(x_{11}, x_{12}, ..., x_{1n}, x_{21}, x_{22}, ..., x_{2n}, ..., x_{n1}, x_{n2}, ..., x_{nn})$.

Ejemplo 2.3. *El conjunto $SL_n(\mathbb{K}) := \{A \in M_{n\times n}(\mathbb{K}) \mid det(A) = 1\}$ es algebraico. Basta considerar la biyección natural entre $M_{n\times n}(\mathbb{K})$ y $\mathbf{A}_{\mathbb{K}}^{n^2}$ y tomar el polinomio $p(x_{ij}) = det(x_{ij}) - 1 \in \mathbb{K}[x_{ij}]$ donde $det(x_{ij})$ es el determinante de la matriz $(x_{ij})_{n\times n}$, luego $SL_n(\mathbb{K}) = \mathcal{Z}(p(x_{ij}))$.*

Ver [2], página 55 para más ejemplos.

Definición 2.4. *Sea $X \subseteq \mathbf{A}_{\mathbb{K}}^n$. Definimos el **ideal** del conjunto X como*

$$\mathcal{I}(X) := \{p \in \mathbb{K}[x_1, x_2, ..., x_n] \mid p(a) = 0, \text{ para todo } a \in X\}.$$

Proposición 2.2. *Se cumplen:*
1. $\mathcal{I}(X)$ *es un ideal de* $\mathbb{K}[x_1, x_2, ..., x_n]$.
2. *Si* $X \subseteq Y \subseteq \mathbf{A}^n_{\mathbb{K}}$ *entonces* $\mathcal{I}(Y) \subseteq \mathcal{I}(X)$.
3. $\mathcal{I}(\emptyset) = \mathbb{K}[x_1, x_2, ..., x_n]$.
4. $\mathcal{I}(\mathbf{A}^n_{\mathbb{K}}) = \{0\}$ *sí y sólo si* $\mathbb{K}$ *es infinito.*
5. $I \subseteq \mathcal{I}(\mathcal{Z}(I))$.
6. $\mathcal{Z}(\mathcal{I}(\mathcal{Z}(I))) = \mathcal{Z}(I)$.

Ver [7] página 3 y [5] página 12.

Definición 2.5. *Sea* $(X, \mathcal{G})$ *un espacio topológico. Decimos que X es* ***reducible*** *si existen* X_1 *y* X_2 *conjuntos cerrados propios de X tales que* $X = X_1 \cup X_2$. *En caso contrario decimos que X es* ***irreducible***.

Observación 2.1. *En la Definición 2.5 si* $X = \mathbf{A}^n_{\mathbb{K}}$ *y* $\mathcal{G}$ *es la topología de Zariski, tenemos que un conjunto algebrico* $\mathcal{Z}$ *es reducible si existen conjuntos algebraicos propios* $\mathcal{Z}_1$, $\mathcal{Z}_2$ *de* $\mathcal{Z}$ *tales que* $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2$.

Ejemplo 2.4. *El conjunto algebraico* $\mathcal{Z}(y^2 - xy - x^2y + x^3) \subseteq \mathbf{A}^2_{\mathbb{R}}$ *es reducible pues* $\mathcal{Z}(y^2 - xy - x^2y + x^3) = \mathcal{Z}(y - x) \cup \mathcal{Z}(y - x^2)$, *con* $\mathcal{Z}(y - x), \mathcal{Z}(y - x^2) \subseteq \mathbf{A}^2_{\mathbb{R}}$ *conjuntos algebraicos propios de* $\mathcal{Z}(y^2 - xy - x^2y + x^3)$.

Proposición 2.3. *Sea* $(X, \mathcal{G})$ *un espacio topológico. X es irreducible si y sólo si todo conjunto abierto no vacío* $U \subseteq X$ *es denso, por tanto* $\overline{U} = X$.

Ver [1] página 7.

Ahora veamos una caracterización de los conjuntos algebraicos irreducibles.

Proposición 2.4. *Sea* $\mathcal{Z} = \mathcal{Z}(I) \subseteq \mathbf{A}^n_{\mathbb{K}}$ *un conjunto algebraico.* $\mathcal{Z}$ *es irreducible sí y sólo si* $\mathcal{I}(\mathcal{Z}) \subseteq \mathbb{K}[x_1, x_2, ..., x_n]$ *es un ideal primo.*

Demostración:

[⇒] Si $\mathcal{I}(\mathcal{Z})$ no es un ideal primo existen $p, q \in \mathbb{K}[x_1, x_2, ..., x_n]$ tales que $p \cdot q \in \mathcal{I}(\mathcal{Z})$ pero $p \notin \mathcal{I}(\mathcal{Z})$ y $q \notin \mathcal{I}(\mathcal{Z})$. Dado que $p \cdot q \in \mathcal{I}(\mathcal{Z})$ entonces $\{p \cdot q\} \subseteq \mathcal{I}(\mathcal{Z})$ luego $\mathcal{Z}(\{p \cdot q\}) \supseteq \mathcal{Z}(\mathcal{I}(\mathcal{Z})) = \mathcal{Z}$.

Tenemos

$$\mathcal{Z} = \mathcal{Z} \cap \mathcal{Z}(p \cdot q) = \mathcal{Z} \cap [\mathcal{Z}(p) \cup \mathcal{Z}(q)] = [\mathcal{Z} \cap \mathcal{Z}(p)] \cup [\mathcal{Z} \cap \mathcal{Z}(q)].$$

Como $p \notin \mathcal{I}(\mathcal{Z})$ entonces $p(a) \neq 0$, para algún $a \in \mathcal{Z}$, es decir $a \notin \mathcal{Z}(p)$ luego $\mathcal{Z}(p)$ es un subconjunto propio de $\mathcal{Z}$ entonces $\mathcal{Z} \cap \mathcal{Z}(p)$ es un subconjunto propio de $\mathcal{Z}$. De forma similar $\mathcal{Z} \cap \mathcal{Z}(q)$ es un subconjunto propio de $\mathcal{Z}$. Por tanto $\mathcal{Z}$ es reducible.

[⇐] Supongamos que $\mathcal{Z}$ es reducible entonces existen $\mathcal{Z}_1 = \mathcal{Z}_1(I_1), \mathcal{Z}_2 = \mathcal{Z}_2(I_2) \subseteq \mathbf{A}^n_{\mathbb{K}}$ conjuntos algebraicos propios de $\mathcal{Z}$ tales que $\mathcal{Z} = \mathcal{Z}_1 \cup \mathcal{Z}_2$, luego $\mathcal{Z}_1 \subseteq \mathcal{Z}$ y $\mathcal{Z}_2 \subseteq \mathcal{Z}$ entonces $\mathcal{I}(\mathcal{Z}_1) \supseteq \mathcal{I}(\mathcal{Z})$ e $\mathcal{I}(\mathcal{Z}_2) \supseteq \mathcal{I}(\mathcal{Z})$. Es fácil ver que existen $f_1 \in \mathcal{I}(\mathcal{Z}_1)$, $f_2 \in \mathcal{I}(\mathcal{Z}_2)$ tales que $f_1, f_2 \notin \mathcal{I}(\mathcal{Z})$.

Ahora si $a \in \mathcal{Z}$ entonces $a \in \mathcal{Z}_1$ ó $a \in \mathcal{Z}_2$. Tenemos dos casos:
Si $a \in \mathcal{Z}_1$ entonces $f_1(a) = 0$ luego $(f_1 \cdot f_2)(a) = 0$ esto quiere decir que $f_1 \cdot f_2 \in \mathcal{I}(\mathcal{Z})$.
Si $a \in \mathcal{Z}_2$ entonces $f_2(a) = 0$ luego $(f_1 \cdot f_2)(a) = 0$ esto quiere decir que $f_1 \cdot f_2 \in \mathcal{I}(\mathcal{Z})$.

Por tanto $\mathcal{I}(\mathcal{Z})$ no es ideal primo.

Corolario 2.1. *Si* $\mathbb{K}$ *es infinito entonces* $\mathbf{A}^n_{\mathbb{K}}$ *es irreducible.*

Demostración: Como $\mathbb{K}$ es infinito entonces $\mathcal{I}(\mathbf{A}^n_{\mathbb{K}}) = \{0\}$ y dado que $\{0\} \subseteq \mathbb{K}[x_1, x_2, ..., x_n]$ es ideal primo entonces por Proposición 2.4 $\mathbf{A}^n_{\mathbb{K}}$ es irreducible.

Definición 2.6. *Una* ***variedad algebraica*** *de* $\mathbf{A}^n_{\mathbb{K}}$ *es un conjunto algebraico irreducible de* $\mathbf{A}^n_{\mathbb{K}}$.

Definición 2.7. *Sea* $\mathcal{Z}$ *una variedad algebraica no vacía de* $\mathbf{A}^n_{\mathbb{K}}$. *La función* $F : \mathcal{Z} \longrightarrow \mathbb{K}$ *es llamada una* ***función polinomial*** *sobre* $\mathcal{Z}$ *si existe un polinomio* $p \in \mathbb{K}[x_1, x_2, ..., x_n]$ *tal que* $F(a_1, a_2, ..., a_n) = p(a_1, a_2, ..., a_n)$ *para cada* $(a_1, a_2, ..., a_n) \in \mathcal{Z}$.

Definición 2.8. *Sean* $\mathcal{Z}_1 \subseteq \mathbf{A}^n_{\mathbb{K}}$ *y* $\mathcal{Z}_2 \subseteq \mathbf{A}^m_{\mathbb{K}}$ *variedades algebraicas no vacías. Una función* $\varphi : \mathcal{Z}_1 \longrightarrow \mathcal{Z}_2$ *es llamada* ***aplicación polinómica*** *si existen polinomios* $p_1, p_2, ..., p_m \in \mathbb{K}[x_1, x_2, ..., x_n]$ *tales que* $\varphi(a_1, a_2, ..., a_n) = (p_1(a_1, a_2, ..., a_n), p_2(a_1, a_2, ..., a_n), ..., p_m(a_1, a_2, ..., a_n))$ *para cada* $(a_1, a_2, ..., a_n) \in \mathcal{Z}_1$.

Para el siguiente ejemplo vamos a considerar que una matriz $A = (a_{ij})_{n \times n} \in M_{n \times n}(\mathbb{K})$ puede ser vista como un elemento de $\mathbf{A}^{n^2}_{\mathbb{K}}$ entonces $A = (a_{11}, a_{12}, ..., ..., a_{nn})$.

Ejemplo 2.5. *La función* $\varphi_1 : \mathbf{A}^{n^2}_{\mathbb{K}} \longrightarrow \mathbf{A}^{n^2}_{\mathbb{K}}$, $\varphi_1(A) := A = (a_{ij})_{n \times n}$ *es una aplicación polinómica pues existen polinomios* $p_{11}(x_{ij}) = x_{11}, p_{12}(x_{ij}) = x_{12}, ..., p_{nn}(x_{ij}) = x_{nn}$ *en* $\mathbb{K}[x_{ij}]$ *con* $i, j = 1, 2, ..., n$ *tales que* $\varphi(a_{11}, a_{12}, ..., a_{nn}) = \varphi(A) = A = (a_{11}, a_{12}, ..., a_{nn}) = (p_{11}(a_{ij}), p_{12}(a_{ij}), ..., p_{nn}(a_{ij}))$.

De forma similar se prueba que las funciones $\varphi_i : \mathbf{A}_{\mathbb{K}}^{n^2} \longrightarrow \mathbf{A}_{\mathbb{K}}^{n^2}$, $\varphi_i(A) := A^i$ *son aplicaciones polinómicas para* $i = 2, 3, ..., n$.

3. Resultado central. Antes de demostrar el teorema de Cayley-Hamilton, veremos algunos resultados.

Lema 3.1. *Sea* $P_A(x) := det(xI_n - A)$ *el polinomio característico de la matriz* $A \in M_{n\times n}(\mathbb{K}) \cong \mathbf{A}_{\mathbb{K}}^{n^2}$. *Para cada* $A \in M_{n\times n}(\mathbb{K})$ *existen* $P_0, P_1, ..., P_{n-1} \in \mathbb{K}[x_{ij}]$ *con* $i, j = 1, 2, ..., n$ *tales que* $P_A(x) = x^n + P_{n-1}(A)x^{n-1} + ... + P_1(A)x + P_0(A)$.

Demostración: Inducción sobre n.

Para $n = 2$. Si $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ entonces $P_A(x) = x^2 + (-a - d)x + (ad - bc)$, luego existen polinomios $P_1(x_1, x_2.x_3, x_4) = -x_1 - x_4, P_0(x_1, x_2.x_3, x_4) = x_1x_4 - x_2x_3$ en $\mathbb{K}[x_1, x_2, x_3, x_4]$ tales que $P_A(x) = x^2 + P_1(A)x + P_0(A)$.

Dada $A = (a_{ij})_{n\times n} \in M_{n\times n}(\mathbb{K})$ y sin pérdida de generalidad supongamos que n es impar.

Tenemos:

$$P_A(x) = det\begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & x - a_{22} & \cdots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \cdots & x - a_{nn} \end{pmatrix}$$

$$= det\begin{pmatrix} E_{n1} \end{pmatrix}(-a_{n1}) - det\begin{pmatrix} E_{n2} \end{pmatrix}(-a_{n2}) + ... - det\begin{pmatrix} E_{n(n-1)} \end{pmatrix}(-a_{n(n-1)})$$

$$+det\begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1(n-1)} \\ -a_{21} & x - a_{22} & \cdots & -a_{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{(n-1)1} & -a_{(n-1)2} & \cdots & x - a_{(n-1)(n-1)} \end{pmatrix}(x - a_{nn}),$$

donde E_{ni} es una submatriz de la matriz $xI_n - A$ obtenida de eliminar la n-sima fila y la i-ésima columna para cada $i = 1, 2, ..., n - 1$.

El determinante que está multiplicando a $(x - a_{nn})$ es el polinomio característico de alguna matriz $B \in M_{(n-1)(n-1)}(\mathbb{K})$; es decir,

$$P_B(x) = det\begin{pmatrix} x - a_{11} & -a_{12} & \cdots & -a_{1(n-1)} \\ -a_{21} & x - a_{22} & \cdots & -a_{2(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{(n-1)1} & -a_{(n-1)2} & \cdots & x - a_{(n-1)(n-1)} \end{pmatrix}.$$

Luego, por la hipótesis inductiva existen $P_0, P_1, ..., P_{n-2} \in \mathbb{K}[x_{ij}]$ para cada $i, j = 1, 2, ..., n-1$ tales que

$$P_B(x) = x^{n-1} + P_{n-2}(B)x^{n-2} + ... + P_1(B)x + P_0(B).$$

También observemos que $det(E_{n1}), det(E_{n2}), ..., det(E_{n(n-1)})$ son polinomios de grado $n - 2$.

Tenemos:

$$det(E_{n1}) = r_1x^{n-2} + b_{n-3}^{(1)}x^{n-3} + ... + b_1^{(1)}x + b_0^{(1)},$$

$$det(E_{n2}) = r_2x^{n-2} + b_{n-3}^{(2)}x^{n-3} + ... + b_1^{(2)}x + b_0^{(2)},$$

$$\vdots$$

$$det(E_{n(n-1)}) = r_{n-1}x^{n-2} + b_{n-3}^{(n-1)}x^{n-3} + ... + b_1^{(n-1)}x + b_0^{(n-1)}.$$

Sea

$$\begin{aligned} L &= -a_{n1}det(E_{n1}) + a_{n2}det(E_{n2}) - ... + a_{n(n-1)}det(E_{n(n-1)}) \\ &= [-r_1a_{n1} + r_2a_{n2} - ... + r_{n-1}a_{n(n-1)}]x^{n-2} + \\ &+ [-a_{n1}b_{n-2}^{(1)} + a_{n2}b_{n-2}^{(2)} - ... + a_{n(n-1)}b_{n-2}^{(n-1)}]x^{n-3} + ... \\ &+ ... + [-a_{n1}b_1^{(1)} + a_{n2}b_1^{(2)} - ... + a_{n(n-1)}b_1^{(n-1)}]x + \\ &+ [-a_{n1}b_0^{(1)} + a_{n2}b_0^{(2)} - ... + a_{n(n-1)}b_0^{(n-1)}]. \end{aligned}$$

Tenemos

$$\begin{aligned} P_A(x) &= -a_{n1}det(E_{n1}) + a_{n2}det(E_{n2}) - ... + a_{n(n-1)}det(E_{n(n-1)}) + P_B(x)(x - a_{nn}) \\ &= L + [x^{n-1} + P_{n-2}(B)x^{n-2} + P_{n-3}(B)x^{n-3} + ... + P_1(B)x + P_0(B)](x - a_{nn}) \\ &= L + x^n + (P_{n-2}(B) - a_{nn})x^{n-1} + (P_{n-3}(B) - a_{nn}P_{n-2}(B))x^{n-2} + ... \\ &+ (P_0(B) - a_{nn}P_1(B))x - a_{nn}P_0(B) \\ &= x^n + [P_{n-2}(B) - a_{nn}]x^{n-1} + ... \\ &+ [P_{n-3}(B) - r_1a_{n1} + r_2a_{n2} - ... + r_{n-1}a_{n(n-1)} - P_{n-2}(B)a_{nn}]x^{n-2} \\ &+ ... + [P_0(B) - a_{n1}b_1^{(1)} + a_{n2}b_1^{(2)} - ... + a_{n(n-1)}b_1^{(n-1)} - a_{nn}P_1(B)]x \\ &- a_{n1}b_0^{(1)} + a_{n2}b_0^{(2)} - ... + a_{n(n-1)}b_0^{(n-1)} - a_{nn}P_0(B). \end{aligned}$$

Por tanto existen $\widetilde{P}_0(x_{ij}), \widetilde{P}_1(x_{ij}), ..., \widetilde{P}_{n-1}(x_{ij}) \in \mathbb{K}[x_{ij}]$ con $i, j = 1, 2, ..., n$ tales que $P_A(x) = x^n + \widetilde{P}_{n-1}(A)x^{n-1} + ... + \widetilde{P}_1(A)x + \widetilde{P}_0(A)$.

Lema 3.2. *El conjunto* $\mathcal{R} = \{A \in M_{n\times n}(\mathbb{K}) \mid P_A(A) := det(AI_n - A) = 0\}$ *es un cerrado en la topología de Zariski.*

Demostración: Por Lema 3.1, para cada $A \in M_{n\times n}(\mathbb{K})$ existen $P_0, P_1, ..., P_{n-1} \in \mathbb{K}[x_{ij}]$ con $i, j = 1, 2, ..., n$ tales que $P_A(x) = x^n + P_{n-1}(A)x^{n-1} + ... + P_1(A)x + P_0(A)$.

Sabemos que las funciones $\varphi_i : \mathbf{A}_{\mathbb{K}}^{n^2} \longrightarrow \mathbf{A}_{\mathbb{K}}^{n^2}$, $\varphi_i(A) := A^i$ son aplicaciones polinómicas para cada $i = 1, 2, ..., n$. Ahora definimos la función $\Psi : \mathbf{A}_{\mathbb{K}}^{n^2} \longrightarrow \mathbf{A}_{\mathbb{K}}^{n^2}$,

$$\Psi(A) := P_0(A) + P_1(A)\varphi_1(A) + P_{n-1}(A)\varphi_{n-1}(A) + \varphi_n(A) = P_A(A).$$

Es fácil ver que Ψ es una aplicación polinómica, luego existen $\Psi_{11}(x_{ij}), \Psi_{12}(x_{ij}), ..., \Psi_{nn}(x_{ij}) \in \mathbb{K}[x_{ij}]$ para cada $i, j = 1, 2, ..., n$ tales que

$$\Psi(A) = (\Psi_{11}(A), \Psi_{12}(A), ..., \Psi_{nn}(A)).$$

Afirmación: Sea $\mathcal{I} = \langle \Psi_{11}, \Psi_{12}, ..., \Psi_{nn} \rangle$ un ideal de $\mathbb{K}[x_{ij}]$ para cada $i, j = 1, 2, ..., n$. Se cumple que $\mathcal{R} = \mathcal{Z}(\mathcal{I})$. En efecto, $A \in \mathcal{R}$ si y sólo si $0 = P_A(A) = \Psi(A) = (\Psi_{11}(A), \Psi_{12}(A), ..., \Psi_{nn}(A))$ si y sólo si $\Psi_{11}(A) = \Psi_{12}(A) = ... = \Psi_{nn}(A) = 0$ si y sólo si $Q(A) = 0$ para cada $Q \in \mathcal{I}$ si y solo si $A \in \mathcal{Z}(\mathcal{I})$.

De la afirmación tenemos que $\mathcal{R}$ es un conjunto algebraico y por tanto es un cerrado en la topología de Zariski.

Ahora veremos algunos resultados del Álgebra Lineal en una proposición y algunos resultados sobre el discriminante de polinomios.

Proposición 3.1. *Sea A una matriz en* $M_{n\times n}(\mathbb{K})$. *Entonces se cumplen:*

1. *Si A tiene n autovalores diferentes entonces sus autovectores asociados son linealmente independientes.*
2. *Si* $B \in M_{n\times n}(\mathbb{K})$ *es semejante a la matriz A entonces sus polinomios característicos son iguales.*
3. *A es diagonalizable si y solo si tiene n autovectores linealmente independientes. En tal caso la matriz diagonal D semejante a la matriz A está dada por*

$$D = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

donde los λ_i con $i = 1, 2, ..., n$ son los autovalores de A.

Ver [9], páginas 555 hasta 559.

Definición 3.1. *Sea $P(x) = a_n(x-r_1)(x-r_2)...(x-r_n)$ un polinomio de grado $n \geq 1$ con coeficientes en $\mathbb{K}$ y no necesariamente raices distintas $r_1, r_2, ..., r_n$ en $\overline{\mathbb{K}}$. Entonces el **discriminante** de $P(x)$ es*

$$Disc(P(x)) := a_n^{2n-2} \prod_{1 \leq i < j \leq n} (r_i - r_j)^2 \in \mathbb{K}.$$

Ver [6], página 179.

Observación 3.1. *$Disc(P(x)) \neq 0$ si y sólo si las raices $r_1, r_2, ..., r_n$ en $\overline{\mathbb{K}}$ son distintas.*

Lema 3.3. *Sea $\mathbb{K}$ un cuerpo algebraicamente cerrado y consideremos el conjunto*

$$\mathcal{U} := \{A \in M_{n\times n}(\mathbf{K}) \mid A \text{ tiene } n \text{ autovalores distinos}\}.$$

Entonces $\mathcal{U}$ es un abierto no vacío de la topología de Zariski y $\mathcal{U} \subseteq \mathcal{R}$.

Demostración: Primero veamos que $\mathcal{U} \subseteq \mathcal{R}$. En efecto, dado $A \in \mathcal{U}$ entonces A tiene n autovalores distintos a los cuales denotaremos por $\lambda_1, \lambda_2, ...\lambda_n \in \mathbb{K}$, luego A tiene n autovectores $v_1, v_2, ..., v_n$ linealmente independientes asociados a los λ_i con $i = 1, 2, ..., n$. ($Av_i = \lambda_i v_i$ para cada $i = 1, 2, ..., n$).

Tenemos que A es diagonalizable, es decir A es semejante a una matriz diagonal de la forma

$$D = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix},$$

entonces los polinomios característicos de las matrices A y D son iguales, es decir $P_A(x) = P_D(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_n)$. Es fácil ver que $P_A(A)v_i = 0$ para cada $i = 1, 2, ..., n$ y dado que $\beta = \{v_1, v_2, ..., v_n\}$ es una $\mathbb{K}$-base de $\mathbf{A}^n_{\mathbb{K}}$ entonces $P_A(A) = 0$. Por tanto $A \in \mathcal{R}$.

Ahora veamos que $\mathcal{U}$ es un abierto en la topología de Zariski. En efecto, definimos la función

$$F : \mathbf{A}^{n^2}_{\mathbb{K}} \longrightarrow \mathbb{K}, \quad F(A) := Disc(P_A(x)).$$

Es fácil ver que F es una función polinomial es decir existe un polinomio $P \in \mathbb{K}[x_{ij}]$ con $i, j = 1, 2..., n$ tal que $F(A) = P(A)$, para cada $A \in \mathbf{A}^{n^2}_{\mathbb{K}}$.

Tomemos $A \in \mathcal{U}$ entonces el polinomio caraterístico de A es de la forma

$$P_A(x) = (x - r_1)(x - r_2) \cdots (x - r_n),$$

donde los $r_i \in \mathbb{K}$ con $i = 1, 2, ..., n$ son los autovalores de A, luego

$$F(A) := Disc(P(x)) := a_n^{2n-2} \prod_{1 \leq i < j \leq n} (r_i - r_j)^2 \neq 0.$$

Por ser F una función polinomial existe un polinomio $p \in \mathbb{K}[x_{ij}]$ con $i, j = 1, 2..., n$ tal que $0 \neq F(A) = p(A)$, si y sólo si $A \notin \mathcal{Z}(p)$. Por tanto $\mathcal{U} = \mathbf{A}^{n^2}_{\mathbb{K}} - \mathcal{Z}(p)$.

Ahora ya tenemos las herramientas para probar el teorema central de este trabajo.

Teorema 3.1 (Teorema de Cayley-Hamilton).
Sean $A \in M_{n\times n}(\mathbb{K})$, $P_A(x) \in \mathbb{K}[x]$ *el polinomio característico de A. Entonces* $P_A(A) = 0$.

Demostración: Sabemos que los conjuntos $\mathcal{R}_1 = \{B \in \mathbf{A}_{\mathbb{K}}^{n^2} \mid P_A(B) := det(BI_n - A) = 0\}$ es un cerrado de la topología de Zariski y $\mathcal{U}_1 := \{A \in \mathbf{A}_{\mathbb{K}}^{n^2} \mid A\ tiene\ n\ autovalores\ distinos\} \neq \emptyset$ es abierto con $\mathcal{U}_1 \subseteq \mathcal{R}_1$ por los Lemas 3.2 y 3.3 respectivamente.

Por otro lado $\overline{\mathbb{K}}$ es algebraicamente cerrado, luego es infinito, ver [5], entonces por Corolario 2.1 $\mathbf{A}_{\overline{\mathbb{K}}}^{n^2}$ es irreducible luego tenemos por Proposición 2.3 que $\overline{\mathcal{U}}_1 = \mathbf{A}_{\overline{\mathbb{K}}}^{n^2}$.

Ya que $\mathbb{K} \subseteq \overline{\mathbb{K}}$ entonces $\mathbf{A}_{\mathbb{K}}^{n^2} \subseteq \mathbf{A}_{\overline{\mathbb{K}}}^{n^2} = \overline{\mathcal{U}}_1 \subseteq \overline{\mathcal{R}}_1 = \mathcal{R}_1$ luego $\mathbf{A}_{\mathbb{K}}^{n^2} \subseteq \mathcal{R}_1$, esto quiere decir que para cada $A \in M_{n\times n}(\mathbb{K})$ se tiene que $A \in \mathcal{R}_1$, por tanto $P_A(A) = 0$.

4. Conclusiones. Este trabajo se desarrolló con la finalidad de desenvolver el artículo [8]. Hemos tratado de explicar con más detalles algunos resultados, como por ejemplo los Lemas 3.1, 3.2 y 3.3. Hemos demostrado algunos resultados de la geometría algebraica, como por ejemplo la Proposición 2.4 y el Corolario 2.1, que son utilizados en la demostración del teorema central. También es importante mencionar que las definiciones y resultados de este trabajo son la base para poder continuar con esta área tan bonita que es la geometría algebraica.

5. Agradecimientos. Se quiere expresar un especial agradecimiento a Aislan Leal, Victor Mielly y a Carlos Sáez Calvo más conocido como ”geómetracat”por las observaciones y sugerencias de este trabajo; como también al profesor Tomás Núñez Lay por la revisión de la redacción.

ORCID and License
Carlos Mejía Alemán https://orcid.org/0000-0002-5081-9175
Irene Edith Núñez Rodriguez https://orcid.org/0000-0001-7132-0501
Rodolfo José Gálvez Pérez https://orcid.org/0000-0002-6349-7793
Neisser Pino Romero https://orcid.org/0000-0002-9865-5974

Referencias

[1] Beshenov A. *Invitación a la teoría de esquemas. Apuntes de clase*. Universidad de El Salvador, 2019. Recuperado de https://cadadr.org/san-salvador/2019-esquemas/esquemas.pdf
[2] Borges H, Tengan E. *Álgebra comutativa em quatro movimentos*. Projeto Euclides, Instituto de Matemática Pura e Aplicada (IMPA), 2015. Recuperado de https://loja.sbm.org.br/index.php/algebra-comutativa-em-quatro-movimentos.html
[3] Cox D, Little J. O'Shea D. *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer, 2007. Recuperado de https://doc.lagout.org/science/0_Computer%20Science/2_Algorithms/Ideals%2C%20Varieties%2C%20and%20Algorithms%20%284th%20ed.%29%20%5BCox%2C%20Little%20%26%20O%27Shea%202015-06-14%5D.pdf
[4] Fulton W. *Algebraic curves: An introduction to algebraic geometry*. University of Michigan, 2008. Recuperado de http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf
[5] Gathmann A. *Algebraic Geometry-Notes*. University of Kaiserslautern, 2003. Recuperado de https://www.mathematik.uni-kl.de/~gathmann/class/alggeom-2002/alggeom-2002.pdf
[6] Grillet PA. *Abstract algebra.* Graduate Texts in Mathematics. Editorial Board, Springer, 2000. Recuperado de http://dobrochan.ru/src/pdf/1204/Grillet_P._A._-_Abstract_Algebra_(2007)(684).pdf
[7] Hartshorne R. *Algebraic Geometry.* Graduated Texts in Mathematics, Editorial Board, Springer-Verlag, 1977. Recuperado de http://userpage.fu-berlin.de/aconstant/Alg2/Bib/Hartshorne.pdf
[8] Jeffrey A, Rosoff G, College A. *A topological proof of the Cayley-Hamilton theorem.* Missouri Journal of Mathematical Sciences, 1995, 7(2):63-67. DOI: 10.35834/1995/0702063
[9] Stanley I, Grossman S. *Álgebra Lineal.* University of Montana, University College London. Editorial McGraw-Hill, 2007. Recuperado de http://up-rid2.up.ac.pa:8080/xmlui/bitstream/handle/123456789/1326/%C3%81lgebra%20lineal.pdf?sequence=1&isAllowed=y