

Capítulo 1

Espacios vectoriales

1.1. Espacio vectorial

Definición 1.1 *Un espacio vectorial es una terna $(V, +, \cdot)$, donde V es un conjunto no vacío y $+, \cdot$ son dos operaciones del tipo $+: V \times V \rightarrow V$, $\cdot: \mathbb{R} \times V \rightarrow V$ a las que llamaremos "suma de vectores" y "producto por escalares" respectivamente y con las siguientes propiedades: denotando $+(u, v) = u + v$ y $\cdot(\lambda, v) = \lambda v$,*

1. $u + (v + w) = (u + v) + w$, $\forall u, v, w \in V$ (asociativa).
2. $u + v = v + u$, $\forall u, v \in V$ (conmutativa).
3. Existe $e \in V$ tal que $e + v = v + e = v$, $\forall v \in V$ (elemento neutro).
4. Para cada $v \in V$ existe $w \in V$ tal que $v + w = w + v = e$ (elemento opuesto).
5. $\lambda(\mu v) = (\lambda\mu)v$, $\forall v \in V$, $\forall \lambda, \mu \in \mathbb{R}$ (pseudo-asociativa).
6. $\lambda(u + v) = \lambda u + \lambda v$ y $(\lambda + \mu)v = \lambda v + \mu v$, $\forall u, v \in V$ y $\forall \lambda, \mu \in \mathbb{R}$ (distributiva).
7. $1v = v$, $\forall v \in V$ (unimodular).

De forma abreviada, diremos que V es un espacio vectorial. A los elementos de V lo llamamos vectores y a los de \mathbb{R} , escalares.

Proposición 1.1 *En un espacio vectorial V ,*

1. El elemento neutro es único. Se denotará por $\mathbf{0}$.
2. El elemento opuesto de un vector es único. Si v es un vector, su opuesto lo denotamos por $-v$.

Demostración:

1) Sea $e \in V$ el elemento neutro de V y supongamos que existe otro elemento $e' \in V$ el cual también cumple que:

$\forall v \in V, v + e' = e' + v = v$, pero también tenemos que $v + e = e + v = v, \forall v \in V$.

Entonces:

$e + e' = e$ y $e + e' = e'$, por lo tanto $e = e'$. Por lo cual e es único y lo denotamos por $\mathbf{0}$.

2) Sea $v \in V$ y $a \in V$ su opuesto tal que: $a + v = v + a = e$, y supongamos que existe otro elemento opuesto $b \in V$ de v tal que: $v + b = b + v = e$, entonces:

$v + b = v + a$, ya que $v + a = e = v + b$, luego como $+$ es función tenemos:

$b + v + b = b + v + a$, luego

$(b + v) + b = (b + v) + a$; por propiedad asociativa.

$e + b = e + a$, lo que implica que $b = a$ y por lo tanto el opuesto de v es único. Ahora denotamos el opuesto de v como $-v$.

Dada la definición de espacio vectorial para siguiente proposición no es necesaria su demostración.

Proposición 1.2 En un espacio vectorial se tiene las siguientes propiedades:

1. $\lambda \mathbf{0} = \mathbf{0}, \lambda \in \mathbb{R}$.
2. $0v = \mathbf{0}, v \in V$.
3. $(-\lambda)v = -(\lambda v), \lambda \in \mathbb{R}, v \in V$.
4. Si $\lambda v = \mathbf{0}$, entonces $\lambda = 0$ o $v = \mathbf{0}$.

Demostración:

1) Sea $v \in V$ y $\lambda \in \mathbb{R}$, entonces $\lambda \mathbf{0} = \lambda(\mathbf{10}) = (\lambda \mathbf{1}) \cdot \mathbf{0}$

A continuación, damos algunos ejemplos de espacios vectoriales:

1. Si n es un número positivo, se considera el espacio euclídeo $\mathbb{R}^n = \{(x_1, x_2, \dots, x_n); x_i \in \mathbb{R}\}$ con las misma suma y producto por escalares siguientes:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n)$$

$$\lambda(x_1, \dots, x_n) = (\lambda x_1, \dots, \lambda x_n)$$

Siempre se supondrá que \mathbb{R}^n tiene esta estructura vectorial y que llamaremos *usual*.

2. Sea $V = \{(x, y) \in \mathbb{R}^2; x - y = 0\}$ con la suma y producto por escalares como antes.
3. Sea $V = \{p\}$ un conjunto con un único elemento y con $p + p = p$ y $\lambda p = p$.
4. Sea $V = \{f : \mathbb{R} \rightarrow \mathbb{R} ; f \text{ es aplicación } \}$ y para $x \in \mathbb{R}$ se define

$$(f + g)(x) = f(x) + g(x)$$

$$(\lambda f)(x) = \lambda f(x)$$

5. $W = \{f : \mathbb{R} \rightarrow \mathbb{R}; f \text{ es una función diferenciable}\}$ y la suma y el producto por escalares está definido de forma análoga a la del ejemplo anterior.

A continuación definimos estructuras de espacio vectorial a partir de la teoría de conjuntos. Concretamente, a partir del producto cartesiano, aplicaciones biyectivas, espacios cocientes y subconjuntos.

Definición 1.2 Sean V_1 y V_2 dos espacios vectoriales. Se define en $V_1 \times V_2 = \{(v_1, v_2); v_i \in V_i\}$ las siguientes operaciones:

$$(v_1, v_2) + (u_1, u_2) = (v_1 + u_1, v_2 + u_2)$$

$$\lambda(v_1, v_2) = (\lambda v_1, \lambda v_2).$$

Con esta suma y producto por escalares, $V_1 \times V_2$ es un espacio vectorial y se llama *espacio producto*.

Como caso particular, se tiene $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ y de la misma forma, se puede definir el espacio vectorial $\mathbb{R}^n \times \mathbb{R}^m$.

Definición 1.3 Se considera V un espacio vectorial y V' un conjunto biyectivo con V . Sea $f : V \rightarrow V'$ una biyección entre ambos. Se define en V' la siguiente estructura de espacio vectorial:

$$v' + u' = f(f^{-1}(v') + f^{-1}(u'))$$

$$\lambda v' = f(f^{-1}(v'))$$

Se dice V' tiene la estructura vectorial inducida de V por la biyección f .

La estructura vectorial inducida en un subconjunto de un espacio vectorial motiva el estudio de subespacio vectorial.

1.2. Subespacio vectorial

Definición 1.4 Sea V un espacio vectorial y U un subconjunto suyo. Se dice que U es un subespacio vectorial de V si satisface las siguientes propiedades:

1. Si $u, v \in U$, entonces $u + v \in U$.
2. Si $\lambda \in \mathbb{R}$ y $u \in U$, entonces $\lambda u \in U$.
3. Con la suma y producto por escalares de V , U es un espacio vectorial.

Proposición 1.3 Sea U un subconjunto de un espacio vectorial V . Entonces U es un subespacio vectorial si y sólo si

1. Si $u, v \in U$, entonces $u + v \in U$.
2. Si $\lambda \in \mathbb{R}$ y $u \in U$, entonces $\lambda u \in U$.

Demostración:

Observamos que la condición necesaria se cumple por la definición de subespacio vectorial, así que solo basta probar la condición suficiente.

Supongamos que U satisface las propiedades 1 y 2. Veamos que con éstas son suficientes para probar todas las propiedades de espacio vectorial. Todas éstas son ciertas de forma trivial, excepto dos: la existencia de elemento neutro y opuesto. Pero para ello basta con probar que el elemento neutro de V se encuentra en U y lo mismo sucede con el elemento opuesto de un vector de U .

Por hipótesis, si $u \in U$, $0u = 0 \in U$. De la misma forma, si $u \in U$, $-1u = -(1u) = -u \in U$. Por lo tanto U es un subespacio vectorial.

En particular, todo subespacio vectorial debe contener el elemento neutro del espacio ambiente, así como los elementos opuestos de todos los vectores del subespacio.

Proposición 1.4 1. Si U_1 y U_2 son subespacios vectoriales, entonces $U_1 \cap U_2$ también es subespacio vectorial.

2. Si U_1 y U_2 son subespacios vectoriales de V y $U_1 \subset U_2$, entonces U_1 es un subespacio vectorial de U_2 .

Ejemplos:

1. Si V es un espacio vectorial, $\{0\}$ y V son subespacios vectoriales, llamados subespacios vectoriales triviales.
2. $U = \{(x, y) \in \mathbb{R}^2; x - y = 0\}$ es un subespacio vectorial de \mathbb{R}^2 .
3. En general, si a_1, \dots, a_n son números reales, no todos nulos, el conjunto $U = \{(x_1, \dots, x_n) \in \mathbb{R}^n; a_1x_1 + \dots + a_nx_n = b\}$ es un subespacio vectorial de \mathbb{R}^n si y sólo si $b = 0$.
4. Si V_1 y V_2 son espacios vectoriales, entonces $V_1 \times \{0\}$ y $\{0\} \times V_2$ son subespacios vectoriales del espacio producto $V_1 \times V_2$.
5. Si V es un espacio vectorial, V' es un conjunto biyectivo con V con la estructura de espacio vectorial inducida por una biyección $f : V \rightarrow V'$, entonces $U \subset V$ es un subespacio vectorial si y sólo si $f(U)$ es un subespacio vectorial de V' .

Definición 1.5 Sean U y W subespacios vectoriales de V . Se define la suma de U con W como el conjunto.

$$U + W = \{u + w; u \in U, w \in W\}$$

Entonces $U + W$ es un subespacio vectorial. Además se tienen las siguientes propiedades:

1. $U + W = W + U$.
2. $U + U = U$.
3. $U \subset U + W$.
4. $U + W$ es el menor subespacio (con respecto a la inclusión de conjuntos) que contiene a U y a W .

Definición 1.6

Un espacio vectorial V es suma directa de dos subespacios vectoriales U y W suyo, y se denota por $V = U \oplus W$, si $V = U + W$ y $U \cap W = \{0\}$

Con el concepto de subespacio vectorial podemos definir una estructura de espacio vectorial en un conjunto cociente.

Definición 1.7 Sea U un subespacio vectorial de V . En V se define la siguiente relación binaria R :

$$vRw \text{ si } v - w \in U$$

Entonces R es una relación de equivalencia en V . Al conjunto cociente se denota por V/U . Es evidente que la clase de equivalencia de un vector v es

$$[v] = v + U = \{v + u; u \in U\}.$$

En V/U se define la siguiente suma y producto por escalares:

$$(v + U) + (w + U) = (v + w) + U.$$

$$\lambda(v + U) = (\lambda v) + U.$$

Estas operaciones están bien definidas: por ejemplo, si $v + U = v' + U$ y $w + U = w' + U$, $v - v' \in U$, $w - w' \in U$ y por tanto, $(v + w) + U = (v' + w') + U$.

Proposición 1.5 V/U es un espacio vectorial. El elemento neutro es $0 + U$ y si $v + U \subset V/U$, su elemento opuesto es $(-v) + U$.

1.3. Sistema de generadores. Dependencia lineal

Definición 1.8 Sean $X = \{v_1, \dots, v_n\}$ un conjunto de vectores de un espacio vectorial V . Una combinación lineal de X es una suma del tipo

$$a_1 v_1 + \dots + a_n v_n, a_i \in \mathbb{R}$$

Se llama subespacio vectorial generados por X al conjunto de combinaciones lineales:

$$\langle X \rangle = \langle v_1, \dots, v_n \rangle = L(\{X\}) = L(\{v_1, \dots, v_n\}) = \left\{ \sum_{i=1}^n a_i v_i; a_i \in \mathbb{R} \right\}.$$

Proposición 1.6 Se tienen las siguientes propiedades:

1. $\langle X \rangle$ es un subespacio vectorial. Si el cardina de X es 1, se dice que $\langle v \rangle$ es la recta vectorial generada por v .
2. Si $X \cap U$, donde U es un subespacio vectorial, entonces $\langle X \rangle \subset U$.
3. Si $X \subset Y$, entonces $\langle X \rangle \subset \langle Y \rangle$.

Como ejemplos tenemos:

1. En \mathbb{R}^3 , $\langle (1, 0, 1), (0, 1, 1) \rangle = \{(x, y, z) \in \mathbb{R}^3; x - z = 0, y - z = 0\}$.
2. $\mathbb{R}^2 = \langle (1, 1), (0, 2) \rangle$.
3. $\mathbb{R}^n = \langle (1, 0, \dots, 0), \dots, (0, 0, \dots, 1) \rangle$.
4. Si X es Y son dos conjuntos finitos de vectores, entonces $\langle X \rangle + \langle Y \rangle = \langle X \cup Y \rangle$.

Definición 1.9 Un espacio vectorial V se llama finitamente generado si existe un conjunto finito de vectores X tal que $\langle X \rangle = V$. X se llama un sistema de generadores de V .

De esta forma, $\{1, X, \dots, X^n\}$ es un sistema de generadores de $\mathbb{P}_n[X]$.

Proposición 1.7 1. Si X es un sistema de generadores, y $X \subset Y$, entonces Y también es un sistema de generadores.

2. Si $\{v_1, \dots, v_n\}$ es un sistema de generadores y v_1 es combinación lineal de los demás, entonces $\{v_2, \dots, v_n\}$ es un sistema de generadores de V .
3. $\{v_1, \dots, v_n\}$ es un sistema de generadores y $v = \lambda_1 v_1 + \dots + \lambda_n v_n$, con $\lambda_1 \neq 0$. Entonces v, v_2, \dots, v_n es un sistema de generadores de V .
4. Un subespacio vectorial de un espacio vectorial finitamente generado, también es finitamente generado.

Definición 1.10 Un conjunto de vectores $\{v_1, \dots, v_n\}$ se dice que es linealmente independiente (o que forman un conjunto de vectores libre) si la única combinación lineal nula de ellos es la trivial, es decir, si siempre que se tenga $\sum_{i=1}^n \lambda_i v_i = 0$, entonces $\lambda_i = 0$ para cada i . En caso contrario, se dice que son linealmente dependientes.

Proposición 1.8 1. $\{v\}$ es linealmente independiente si y sólo si v es no nulo.

2. Dos vectores son linealmente independientes si no son proporcionales.
3. Todo subconjunto de un conjunto de vectores linealmente independiente, también es linealmente independiente.
4. Un conjunto de vectores es linealmente dependiente si alguno de ellos es combinación lineal de los demás.

1. $(1, 0, 1), (0, 1, 1) \in \mathbb{R}^3$ son linealmente independientes.

2. $(1, 0, \dots, 0), \dots, (0, 0, \dots, 1) \subset \mathbb{R}^n$ es linealmente independientes.
3. $\{1, 1 + X, 1 + X^2\} \subset \mathbb{P}_2[X]$ es linealmente independiente.

Definición 1.11 *Una base de un espacio vectorial es un sistema de generadores y linealmente independiente.*

1. $\{(1, 0, 1), (0, 1, 1)\} \subset \mathbb{R}^3$ no es base.
2. $\{(1, 0, \dots, 0), \dots, (0, 0, \dots, 1)\} \subset \mathbb{R}^n$ es base. Se llamará la base usual de \mathbb{R}^n .
3. $\{1, 1 + X, 1 + X^2\} \subset \mathbb{P}_2[X]$ es base.

Se tiene la siguiente caracterización de base.

Proposición 1.9 *Sea $B = \{v_1, \dots, v_n\}$ un conjunto de vectores de un espacio vectorial. Entonces este conjunto es una base si y sólo si para cada $v \in V$, existen únicos $\lambda_i \in \mathbb{R}$ tales que $v = \sum_{i=1}^n \lambda_i v_i$. A estos números se le llaman coordenadas de v respecto de la base B y se escribirá $(\lambda_1, \dots, \lambda_n)$.*

A partir de ahora vamos a demostrar que en un espacio vectorial dado, el cardinal de las bases de dicho espacio es siempre el mismo. Primero resolvemos el problema de la existencia de bases en un espacio finitamente generado.

Proposición 1.10 *Sean X e Y dos conjuntos finitos de un espacio vectorial, tales que $X \subset Y$, X es linealmente independiente e Y es un sistema de generadores. Entonces existe una base B de V tal que $X \subset B \subset Y$.*

Como consecuencia

Corolario 1.1 *Si v es un vector no nulo, v pertenece a una base.*

Corolario 1.2 *Dado un conjunto de vectores linealmente independientes, siempre es posible añadir vectores hasta tener una base (completación).*

Corolario 1.3 *En todo sistema de generadores, existe un subconjunto suyo que es base.*

Lema 1.1 Sea $B = \{e_1, \dots, e_n\}$ una base de un espacio vectorial. Sea $v \in V$ y $v = \sum_{i=1}^n \lambda_i v_i$. Si $\lambda_1 = 0$, entonces $\{v, e_2, \dots, e_n\}$ es una base de V .

Teorema 1.1 (de la base) Sea V un espacio vectorial finitamente generado. Entonces todas las bases de V tienen el mismo cardinal, al que se llamará *dimensión* de V .

Corolario 1.4 Sea V un espacio vectorial de dimensión n . Sea $X = e_1, \dots, e_m$ un conjunto de vectores linealmente independiente (resp. sistema de generadores). Entonces $m \leq n$ (resp. $m \geq n$). Además se tiene la igualdad si y sólo si X es base.

Corolario 1.5 Si U es un subespacio vectorial de un espacio vectorial V , entonces $\dim(U) \leq \dim(V)$ y la igualdad se tiene si y sólo si $U = V$.

Se tiene los siguiente ejemplos de dimensiones de espacios vectoriales:

1. Por definición $\dim(0) = 0$.
2. La dimensión de \mathbb{R}^n es n .
3. La dimensión de $\mathbb{P}_n[X]$ es $n + 1$.

Teorema 1.2 1. Si V y V' son dos espacios vectoriales, entonces $\dim(V \times V') = \dim(V) + \dim(V')$.

2. Si V es un espacio vectorial y V' es un conjunto biyectivo con V , entonces $\dim(V') = \dim(V)$, considerando en V' la estructura vectorial inducida por la biyección.

3. Si U y W son dos subespacios vectoriales, entonces $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$. Como caso particular, si $V = U \oplus W$, entonces $\dim(V) = \dim(U) + \dim(W)$.

4. Si U es un subespacio vectorial, entonces $\dim(V/U) = \dim(V) - \dim(U)$.

Demostración:

1. Si $\{e_1, \dots, e_n\}$ y $\{e'_1, \dots, e'_m\}$ son bases de V y V' respectivamente, entonces una base de $V \times V'$ es $\{(e_1, 0), \dots, (e_n, 0), (0, e'_1), \dots, (0, e'_m)\}$.

2. Sea $f : V \rightarrow V'$ la biyección. Si $\{e_1, \dots, e_n\}$ es una base de V , entonces $f(e_1), \dots, f(e_n)$ es una base de V' .
3. Si $\{e_1, \dots, e_k\}$ es una base de $U \cap W$, $\{e_1, \dots, e_k, u_1, \dots, u_m\}$ es base de U y $\{e_1, \dots, e_k, w_1, \dots, w_r\}$ es base de W , entonces una base de $U + W$ es $\{e_1, \dots, e_k, u_1, \dots, u_m, w_1, \dots, w_r\}$. En particular, $V = U \oplus W$ si y sólo si la unión de una base de U y otra de W es una base de V .
4. Si $\{e_1, \dots, e_m\}$ es una base de U y $\{e_1, \dots, e_m, e_{m+1}, \dots, e_n\}$ es una base de V , entonces $\{e_{m+1} + U, \dots, e_n + U\}$ es una base de V/U .

Capítulo 2

Formas Canónicas

2.1. Introducción a los Polinomios

En general los polinomios se presenta como expresiones formales en una o en varias variables con coeficiente en algún cuerpos \mathbb{K} , en esta sección daremos una definición no tan conocida de dichos polinomios para así poder definir las formas canónicas que conoceremos en este capítulo y así tener una noción para poder entender lo que es el Álgebra Multilineal.

Definición 2.1 Sea $f : \mathbb{N}_0 \rightarrow \mathbb{K}$ una función.

Se dice que f tiene soporte finito, si y solo si el conjunto

$$f^{-1}(\mathbb{K} - \{0\}) = \{n \in \mathbb{N}_0 : f(n) \in \mathbb{K} - \{0\}\}$$

es finito.

Definición 2.2 El conjunto de los polinomios se denota por

$$\mathbb{K}[x] = \{f : \mathbb{N}_0 \rightarrow \mathbb{K} \mid f \text{ tiene soporte finito}\}$$

Las operaciones suma y el producto en $\mathbb{K}[x]$ está dadas por:

Suma: Sea $f, g \in \mathbb{K}[x]$, luego $f + g : \mathbb{N}_0 \rightarrow \mathbb{K}$ definido por

$$(f + g)(i) := f(i) + g(i)$$

Producto: $f, g \in \mathbb{K}[x]$, luego $fg : \mathbb{N}_0 \rightarrow \mathbb{K}$ definido por

$$(fg)(i) = \sum_{t=0}^i f(i-t) \cdot g(t)$$

Propiedad 2.1 $\mathbb{K}[x]$ con esta suma y con este producto es un anillo conmutativo con unidad. Es decir,

1. $(\mathbb{K}[x], +)$ es un grupo abeliano.
2. $(\mathbb{K}[x], \cdot)$ es un monoide conmutativo.
3. Distributividad del producto sobre la suma.

Definición 2.3 Sea f un polinomio no nulo, se dice que n es el grado de f si y sólo si

$$n = gr(f) = deg(f) = \max\{f^{-1}(\mathbb{K} - \{0\})\}$$

Teorema 2.1 Sean f y g dos polinomios en $\mathbb{K}[x]$ entonces:

1. $f \cdot g = 0$ si y solo si $f = 0$ o $g = 0$.
2. Si f, g son no nulos, entonces

$$gr(fg) = gr(f) + gr(g).$$

Función Polinomial: Sea $f \in \mathbb{K}[x]$

1. Si $f : \mathbb{K} \rightarrow \mathbb{K}$, si $a \in \mathbb{K}$, entonces

$$f(a) = \sum_{i=0}^{gr(f)} f(i)a^i = f(0) + \sum_{i=1}^{gr(f)} f(i)a^i$$

2. Si $f : M_n(\mathbb{K}) \rightarrow M_n(\mathbb{K})$, si $A \in M_n(\mathbb{K})$, entonces

$$f(A) = \sum_{i=0}^{gr(f)} f(i)A^i = f(0)Id + \sum_{i=1}^{gr(f)} f(i)A^i$$

3. Si $f : End(V) \rightarrow End(V)$, si $T \in End(V)$, entonces

$$f(T) = \sum_{i=0}^{gr(f)} f(i)T^i = f(0)Id + \sum_{i=1}^{gr(f)} f(i)T^i$$

Notación: Sea $f \in \mathbb{K}[x]$ no nulo, entonces denotamos:

$$f = \sum_{i=0}^{gr(f)} f(i)x^i$$

Ejemplo 2.1 Sea $f = 1 + 3x + x^2$, donde si $f : \mathbb{N}_0 \rightarrow \mathbb{K}$, tenemos:

$$f(i) = \begin{cases} 1 & i \in \{0, 2\} \\ 3 & i = 1 \\ 0 & i \notin \{0, 1, 2\} \end{cases}$$

1. Sea $A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, luego

$$f(A) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 3 \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} 3 & 8 \\ 4 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 14 \\ 7 & 21 \end{pmatrix}$$

2. Si $T(x, y) = (3x + y, 4x + 3y)$, luego

$$\begin{aligned} T^2(x, y) &= T(T(x, y)) \\ &= T(3x + y, 4x + 3y) \\ &= (3(3x + y) + (4x + 3y), 4(3x + y) + 3(4x + 3y)) \\ &= (13x + 6y, 24x + 3y). \end{aligned}$$

Ahora

$$\begin{aligned} f(T) &= Id + 3T + T^2 \\ f(T(x, y)) &= Id(x, y) + 3T(x, y) + T^2(x, y) \\ &= (x, y) + 3(3x + y, 4x + 3y) + (13x + 6y, 24x + 3y) \\ &= (23x + 9y, 23y + 36x) \end{aligned}$$

Propiedad 2.2 Si $\dim_{\mathbb{K}}(V) = n$, entonces

$$End(V) \simeq M_n(\mathbb{K})$$

.

Definición 2.4 Sea f un polinomio y $\alpha \in \mathbb{K}$, decimos que α es una raíz de f si y sólo si $f(\alpha) = 0$.

Con la definición utilizada es fácil probar el siguiente teorema.

Teorema 2.2 Sea $A \in M_n(\mathbb{K})$, $T \in \text{End}(V)$ y $f, g \in \mathbb{K}[x]$, entonces

1. $(f + g)(A) = f(A) + g(A)$, $(f + g)(T) = f(T) + g(T)$
2. $(fg)(A) = f(A) \cdot g(A)$, $(fg)(T) = f(T) \cdot g(T)$

Ahora presentamos un importante teorema en esta teoría.

Teorema 2.3 Sea $A \in M_n(\mathbb{K})$, entonces existe un polinomio f en $\mathbb{K}[x]$ no nulo tal que

$$f(A) = 0$$

.

Demostración:

Si A es la matriz nula solo tomamos el polinomio $f = x$, ahora si A no es la matriz nula, sabemos que la dimensión de las matrices $M_n(\mathbb{K})$ es n^2 , luego el conjunto $\{Id, A, A^2, \dots, A^{n^2}\}$ es linealmente dependiente(ya que tiene $n^2 + 1$ elementos), es decir existen algún $\alpha_i \neq 0$ en \mathbb{K} tal que

$$\alpha_0 + \alpha_1 A + \dots + \alpha_{n^2} A^{n^2} = 0$$

luego definimos

$$f = \alpha_0 + \alpha_1 x + \dots + \alpha_{n^2} x^{n^2} \in \mathbb{K}[x]$$

y por lo que tenemos $f(A) = 0$. \square

Luego tenemos que por la propiedad 2.2, también se cumple el corolario siguiente.

Corolario 2.1 Sean V un espacio vectorial de dimensión finita sobre \mathbb{K} y $T \in \text{End}(V)$, entonces existe un polinomio f en $\mathbb{K}[x]$ no nulo tal que

$$f(T) = 0.$$

Propiedad 2.3 Sean $f \in \mathbb{R}[x]$, $\alpha \in \mathbb{R}$ una raíz de f y $n \in \mathbb{Z}^+$ es la multiplicidad de α en f si y sólo si

$$\left(\frac{d^j f}{dx^j} \right) (\alpha) = f^{(j)}(\alpha) = 0, \quad \text{si } j < n$$

$$f^{(n)}(\alpha) \neq 0$$

Observación: La demostración se obtiene usando la siguiente propiedad, tomamos un polinomio $f : \mathbb{N}_0 \rightarrow \mathbb{R}$ y un polinomio $\acute{f} = f^{(1)} \rightarrow \mathbb{R}$ tal que $f(i) = (i+1)f(i+1)$, de modo otro modo tenemos que si $f = \sum_{i=0}^n f(i)x^i$, entonces

$$\acute{f} = \sum_{i=1}^n i f(i) x^{i-1} = \sum_{j=0}^{n-1} (j+1) f(j+1) x^j$$

Si $f, g \in \mathbb{R}[x]$ entonces

$$(fg)^{(n)} = \sum_{i=0}^n \binom{n}{i} f^{(i)} g^{(n-i)}$$

En la teoría de números se tenemos el teorema de la división euclídea, no obstante en esta teoría también podemos tener algo similar utilizando el grado de los polinomios.

Teorema 2.4 Sean $f, g \in \mathbb{K}[x]$, $\alpha \in \mathbb{K}$, entonces existen $h, r \in \mathbb{K}[x]$ únicos tales que

$$f = g \cdot h + r,$$

con $r = 0$ ó $gr(g) > gr(r)$.

Corolario 2.2 Sean $f \in \mathbb{K}[x]$ y $\alpha \in \mathbb{K}$ entonces α es una raíz de f si y sólo si existe $h \in \mathbb{K}[x]$ tal que $f = (x - \alpha) \cdot h$

Demostración:

Como $f, x - \alpha \in \mathbb{K}[x]$, entonces por teorema de la división tenemos que existen $h, r \in \mathbb{K}[x]$ tal que

$$f = (x - \alpha) \cdot h + r,$$

luego como α es una raíz de f tenemos que $0 = f(\alpha) = (\alpha - \alpha) \cdot h + r = r$, por lo tanto $f = (x - \alpha) \cdot h$.

Desde ahora en adelante usaremos la notación fg para indicar $f \cdot g$.

Definición 2.5 Sea A un anillo conmutativo. Se dice que I es un ideal de A si y sólo si

1. Si $f, g \in I$, entonces $f + g \in I$.
2. Si $g \in I$, $h \in A$, entonces $gh \in I$.

Ejemplo 2.2 Sea \mathbb{K} un cuerpo y $g \in \mathbb{K}[x]$, entonces

$$\langle g \rangle = \{g \cdot h \mid h \in \mathbb{K}[x]\}$$

es un ideal de $\mathbb{K}[x]$, llamado ideal generado por g .

Solución:

Llamemos I al ideal $\langle g \rangle$, luego sean $f_1, f_2 \in I$, entonces existen $h_1, h_2 \in \mathbb{K}[x]$ tal que $f_1 = gh_1$ y $f_2 = gh_2$, entonces $f_1 + f_2 = g(h_1 + h_2) = g(h)$ con $h = h_1 + h_2 \in \mathbb{K}[x]$, por lo que $f_1 + f_2 \in I$.

Ahora sea $f \in I$ y $k \in \mathbb{K}[x]$, como $f \in I$, entonces existe $h \in \mathbb{K}[x]$ tal que $f = gh$, luego $fk = (gh)k = g(hk)$ y como $hk \in \mathbb{K}[x]$ tenemos que $fk \in I$, así que por lo tanto $I = \langle g \rangle$ es un ideal de $\mathbb{K}[x]$. \square

Teorema 2.5 Sea \mathbb{K} un cuerpo, entonces todo los ideales de $\mathbb{K}[x]$ están generados por un elemento, es decir

Si el ideal I es no nulo, entonces existe un único polinomio mónico que lo genera.

Demostración:

Sea I un ideal no nulo de $\mathbb{K}[x]$, luego definamos la siguiente función $gr : I - \{0\} \rightarrow \mathbb{N}_0$ tal que a cada polinomio f de I le asigna su grado.

Como $Im(gr) \subseteq \mathbb{N}_0$ y es no vacío, luego existe el mínimo, sea $p \in I$, tal que p es mónico y $gr(p)$ es el mínimo de la $Im(gr)$.

Ahora demostraremos que $\langle p \rangle = I$.

La primera contención $\langle p \rangle \subset I$ es inmediata ya que $p \in I$ e I es un ideal.

En el otro sentido, sea $f \in I$, luego aplicando el teorema de la división, tenemos que existen $p, r \in \mathbb{K}[x]$ tal que:

$$f = pd + r$$

donde $r = 0$ ó $gr(p) > gr(r)$, luego

$$f = pd + r \iff f - pd = r,$$

donde $f \in I$ y $pd \in I$, luego $r \in I$.

Si $r \neq 0$ entonces $gr(p) > gr(r)$ lo cual es una contradicción ya que p es el polinomio de grado mínimo en I .

De este modo se tiene que $r = 0$ y

$$f = pd \in \langle p \rangle$$

por lo que $I = \langle p \rangle$.

Ahora probemos la unicidad

Supongamos que existen $p, q \in I$ tal que $I = \langle p \rangle = \langle q \rangle$, entonces existen $f, g \in \mathbb{K}[x]$ tales que $fp = q$ y $p = qg$, reemplazando y comparando los grados se obtiene la unicidad. \square

Propiedad 2.4 Sea $A \in M_n(\mathbb{K})$, entonces $I = \{f \in \mathbb{K}[x] | f(A) = 0\}$ es un ideal de $\mathbb{K}[x]$.

Demostración:

1. $I = \{f \in \mathbb{K}[x] | f(A) = 0\} \neq \emptyset$, por teorema 2.3.
2. Sean $f, g \in I$, luego

$$(f \pm g)(A) = f(A) \pm g(A) = 0 \pm 0 = 0.$$

3. Sean $f \in I$ y $h \in \mathbb{K}[x]$, luego

$$(fh)(A) = f(A)h(A) = 0h(A) = 0$$

Por lo tanto I es un ideal de $\mathbb{K}[x]$. \square

Corolario 2.3 Sea $A \in M_n(\mathbb{K}) - \{0\}$, entonces existe un único polinomio mónico φ_A tal que

$$\{f \in \mathbb{K}[x] | f(A) = 0\} = \langle \varphi_A \rangle.$$

Demostración:

Como $\{f \in \mathbb{K}[x] | f(A) = 0\}$ es un ideal de $\mathbb{K}[x]$ entonces por teorema 2.5, tenemos que existe un único polinomio $\varphi_A \in \mathbb{K}[x]$ tal que $\{f \in \mathbb{K}[x] | f(A) = 0\} = \langle \varphi_A \rangle$. \square

Propiedad 2.5 Sean V un espacio vectorial de dimensión finita sobre \mathbb{K} y $T \in \text{End}(V)$ no nulo, entonces existe un único polinomio mónico φ_A tal que

$$\{f \in \mathbb{K}[x] | f(T) = 0\} = \langle \varphi_T \rangle.$$

Sea $A \in M_n(\mathbb{K}) - \{0\}$, φ_A es llamado el **polinomio minimal** de A , es decir, φ_A es el polinomio de grado menor, con coeficiente principal igual a 1 que cumple con $\varphi_A(A) = 0$, y todo otro se puede factorizar, donde uno de los factores es el polinomio minimal.

Sean V un espacio vectorial de dimensión finita sobre \mathbb{K} y $T \in \text{End}(V)$ no nulo, φ_T es llamado el **polinomio minimal** asociado T , es decir, φ_T es el polinomio de grado menor, con coeficiente principal igual a 1 que cumple con $\varphi_T(T) = 0$, y todo otro se puede factorizar, donde uno de los factores es el polinomio minimal.

Ejemplo 2.3 Sea $\alpha \in \mathbb{R}$.

1. Sea $Id \in M_n(\mathbb{R})$, entonces $\varphi_{Id} = x - 1$
2. Sea $\alpha Id \in M_n(\mathbb{R})$, entonces $\varphi_{\alpha Id} = x - \alpha$
3. Sea $A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$, entonces $\varphi_A = (x - 1)(x - 2)$.

2.2. Diagonalización

Definición 2.6 1. α es un **valor propio** de A si y sólo si existe $v \in \mathbb{K}^n - \{0\}$ tal que $A \cdot v^t = \alpha v^t$

2. $v \in \mathbb{K}^n - \{0\}$ es un **vector propio** de A si y sólo si existe $\alpha \in \mathbb{K}$ tal que $A \cdot v^t = \alpha v^t$.

3. El espacio propio asociado a α es el conjunto

$$V_\alpha = \{v \in \mathbb{K}^n | A \cdot v^t = \alpha v^t\}.$$

Análogamente la nociones para transformaciones lineales.

Definición 2.7 Sean V un espacio vectorial sobre \mathbb{K} y $T \in \text{End}(V)$, $\alpha \in \mathbb{K}$

1. α es un **valor propio** de T si y sólo si existe $v \in V - \{0\}$ tal que $T(v) = \alpha v$.

2. $v \in V - \{0\}$ es un **vector propio** de T si y sólo si existe $\alpha \in \mathbb{K}$ tal que $T(v) = \alpha v$.

3. El espacio propio asociado a α es el conjunto

$$V_\alpha = \{v \in V | T(v) = \alpha v\}.$$

Propiedad 2.6 Sea $A \in M_n(\mathbb{K})$, $\alpha \in \mathbb{K}$, entonces α es un valor propio de A si y sólo si α es una raíz de φ_A .

Demostración:

Como $A \cdot v = \alpha v$, notemos por inducción lo siguiente

$$A^2 v^t = A(Av^t) = A(\alpha v^t) = \alpha(Av^t) = \alpha^2 v^t.$$

Además se tiene que

$$A^{n+1}v^t = AA^n v^t = A(\alpha^n v^t) = \alpha^n (Av^t) = \alpha^{n+1} v^t$$

Por lo tanto $A^n v^t = \alpha^n v^t$, para todo $n \in \mathbb{N}$.

Sea

$$\varphi_A(x) = \sum_{i=0}^r a_i x^i.$$

Veamos ahora la demostración, para ello recordemos que $\varphi_A(A) = 0$, evaluando α tenemos $\varphi_A(\alpha) = \sum_{i=0}^r a_i \alpha^i$, además

$$\varphi_A(\alpha)(v^t) = \sum_{i=0}^r a_i (\alpha^i v^t) = \sum_{i=0}^r a_i (A^i v^t) = \left(\sum_{i=0}^r a_i (A^i) \right) v^t = \varphi_A(A) v^t = 0 v^t = 0$$

es decir,

$$\varphi_A(\alpha)(v^t) = 0$$

Como $v \neq 0$, luego $\varphi_A(\alpha) = 0$, de lo cual α es una raíz de φ_A .

El recíproco, sea α una raíz de φ_A , tenemos por corolario 2.2 que existe $h \in \mathbb{K}[x]$ tal que

$$\varphi_A = (x - \alpha)h,$$

y

$$\varphi_A(A) = (A - \alpha Id)h(A) = 0$$

1. Si $h(A)$ es invertible, entonces

$$A - \alpha Id = 0, \quad \varphi_A = x - \alpha,$$

de donde $A = \alpha Id$.

2. Si $h(A)$ no es invertible, notemos que $gr(\varphi_A) > gr(h)$ y $h(A) \neq 0$, ya que φ_A es el polinomio minimal de A (es decir el menor polinomio que anula a A).
Luego existe $w \in \mathbb{K}^n$ tal que

$$h(A)w^t = v^t \neq 0$$

Reemplazando se tiene que

$$\begin{aligned} \varphi_A(A)w^t &= 0 \\ (A - \alpha Id)(h(A)w^t) &= 0 \\ (A - \alpha Id)v^t &= 0 \\ Av^t - \alpha v^t &= 0 \\ Av^t &= \alpha v^t \end{aligned}$$

De este modo, α es un valor propio de A . \square

Un resultado análogo se tiene para transformaciones lineales, el cuál es un corolario del teorema anterior.

Corolario 2.4 Sean V un espacio vectorial sobre \mathbb{K} y $T \in \text{End}(V)$, $\alpha \in \mathbb{K}$, entonces α es un valor propio de T si y sólo si α es una raíz de φ_T .

Definición 2.8 Sea $A \in M_n(\mathbb{K})$,
Se define el **Polinomio característico** asociado a una matriz como

$$P_A = \det(A - xId) \in \mathbb{K}[x]$$

Ejemplo 2.4 Sea $A = \begin{bmatrix} 5 & -6 & -6 \\ -1 & 4 & 2 \\ 3 & -6 & -4 \end{bmatrix}$
Determinar $P_A(x)$ el polinomio característico.

Solución:

Reemplazando tenemos

$$\begin{aligned} P_A(x) &= \begin{vmatrix} 5-x & -6 & -6 \\ -1 & 4-x & 2 \\ 3 & -6 & -4-x \end{vmatrix} \\ &= -(x^3 - 5x^2 + 8x - 4) \\ &= -(x-1)(-x^2 + 4x - 4) = -(x-1)(x-2)^2. \end{aligned}$$

por lo tanto $P_A(x) = -(x-1)(x-2)^2$.

Observación: En caso de endomorfismo la definición es similar ya que

$$\begin{aligned} \det(A - xId) &= \det(A - xId)\det(P^{-1}P) \\ &= \det(P^{-1})\det(A - xId)\det(P) \\ &= \det(P^{-1}(A - xId)P) \\ &= \det(P^{-1}AP - xId) \end{aligned}$$

Luego el determinante, no depende de la base, de otro modo es invariante de la base.