Divisores de cero, idempotentes y generadores del álgebra compleja $\mathbb{C}^n$

Objetivos. Seguir estudiando las propiedades multiplicativas de $\mathbb{C}^n$ y deducir descripciones explícitas de varios objetos mencionados en el título.

Prerrequisitos. Álgebra compleja $\mathbb{C}^n$.

Divisores de cero

1 Definición (divisor de cero)**.** Sea $\mathcal{A}$ una álgebra compleja conmutativa. Denotemos por $0_\mathcal{A}$ su elemento cero (el elemento neutro bajo la adición). Un elemento de a de $\mathcal{A}$ se llama *divisor de cero* si $a \neq 0_\mathcal{A}$ y existe un elemento b en $\mathcal{A} \setminus \{0_\mathcal{A}\}$ tal que

$$ab = 0_\mathcal{A}.$$

En el álgebra $\mathbb{C}^n$, esta definición toma la siguiente forma: un elemento a de $\mathbb{C}^n$ se llama *divisor de cero* si $a \neq 0_n$ y existe un elemento b en $\mathbb{C}^n \setminus \{0_n\}$ tal que

$$a \odot b = 0_n.$$

2 Ejemplo. Igual que antes, denotamos e_p al vector canónico básico cuya p-ésima componente es 1 y las demás son 0:

$$e_p = \big[\delta_{p,j}\big]_{j=1}^{n}.$$

Si $n > 1$, entonces $e_1 \odot e_2 = 0_n$, por eso e_1 es un divisor de cero. De hecho, si $n > 1$, entonces todos los vectores $e_1, \ldots, e_n$ son divisores de cero.

3 Proposición (descripción de los divisores de cero en $\mathbb{C}^n$)**.** *El conjunto de los divisores de cero de $\mathbb{C}^n$ es $\mathbb{C}^n \setminus \big(\{0_n\} \cup \operatorname{Inv}(\mathbb{C}^n)\big)$. En otras palabras, un elemento a de $\mathbb{C}^n$ es un divisor de cero si alguna de las componentes de a es cero, pero no todas las componentes de a son cero.*

Demostración. Sea a un divisor de cero de $\mathbb{C}^n$. Supongamos que $b \in \mathbb{C}^n \setminus \{0_n\}$ y $a \odot b = 0_n$. Usando la condición que $b \neq 0_n$, encontramos j en $\{1, \ldots, n\}$ tal que $b_j \neq 0$. Por otro lado,

$$a_j b_j = (a \odot b)_j = (0_n)_j = 0.$$

De allí concluimos que $a_j = 0$.

Ahora suponemos que $a \neq 0_n$ y existe un j en $\{1, \ldots, n\}$ tal que $a_j = 0$. Entonces

$$(a \odot e_j)_j = a_j (e_j)_j = a_j \cdot 1 = a_j = 0.$$

Como $e_j \neq 0_n$, concluimos que a es un divisor de cero. $\square$

Si J es un subconjunto propio y no vacío de $\{1,\ldots,n\}$, $a_j \neq 0$ para cada j en J y $a_j = 0$ para cada j en $\{1,\ldots,n\} \setminus J$, entonces a es un divisor de cero del álgebra $\mathbb{C}^n$. Más aún, la Proposición 3 implica que cualquier divisor de ceron de $\mathbb{C}^n$ es de esta forma.

Elementos idempotentes

4 Definición. Sea $\mathcal{A}$ una álgebra compleja (o, más general, un anillo asociativo). Un elemento a de $\mathcal{A}$ se llama *idempotente* si $a^2 = a$.

Notamos que si $a^2 = a$, entonces *todas* las potencias enteras positivas de a coinciden con a.

En el caso del álgebra $\mathbb{C}^n$, la propiedad idempotente se puede escribir en la forma $a \odot a = a$.

5 Ejemplo. Cada uno de los vectores básicos $e_1,\ldots,e_n$ es idempotente. Más aún, e_1+e_2 también es idempotente:

$$(e_1 + e_2)^2 = e_1^2 + 2e_1 \odot e_2 + e_2^2 = e_1 + e_2.$$

Notamos que en el campo $\mathbb{C}$ hay dos elementos idempotentes: 0 y 1.

6 Proposición (descripción de los elementos idempotentes en $\mathbb{C}^n$)**.** *Sea $a \in \mathbb{C}^n$. Entonces a es un elemento idempodente de $\mathbb{C}^n$ si y sólo si existe un subconjunto J de $\{1,\ldots,n\}$ tal que $a_j = 1$ para cada j en J y $a_j = 0$ para cada j en $\{1,\ldots,n\} \setminus J$.*

Demostración. Sea a un elemento idempotente de $\mathbb{C}^n$. Definimos J como el conjunto de los índices j en $\{1,\ldots,n\}$ tales que $a_j \neq 0$. Tenemos por demostrar que $a_j = 1$ para cada j en $\{1,\ldots,n\}$. La propiedad idempotente significa que $a_j^2 = a_j$ para cada j, y si $a_j \neq 0$, entonces $a_j = 1$.

Ahora supongamos que J es un subconjunto de J, $a_j = 1$ para cada j en J y $a_j = 0$ para cada j en $\{1,\ldots,n\} \setminus J$. Entonces para cada j en $\{1,\ldots,n\}$ tenemos $a_j^2 = a_j$, lo cual significa que $a \odot a = a$. $\square$

7 Definición. Sea $\mathcal{A}$ una álgebra compleja asociativa. Denotamos su elemento cero por $0_{\mathcal{A}}$. Un elemento a de $\mathcal{A}$ se llama *nilpotente* si si existe un número entero positivo p tal que $a^p = 0_{\mathcal{A}}$.

8 Ejercicio. Encuentre todos los elementos nilpotentes del álgebra $\mathbb{C}^n$.

9 Definición. Sea $\mathcal{A}$ una álgebra compleja asociativa con identidad $1_{\mathcal{A}}$, y sea a un elemento de $\mathcal{A}$. Se dice que a tiene *propiedad involutiva* si $a^2 = 1_{\mathcal{A}}$.

10 Ejercicio. Encuentre la forma general de los elementos involutivos del álgebra $\mathbb{C}^n$.

Generadores de $\mathbb{C}^n$

11 Definición (polinomio de un elemento de una álgebra compleja asociativa con identidad)**.** Sean $\mathcal{A}$ una álgebra compleja asociativa con identidad $1_{\mathcal{A}}$, a un elemento de $\mathcal{A}$ y f un polinomio con coeficientes complejos:

$$f(t) = \sum_{k=0}^{m} f_k t^k.$$

Entonces $f(a)$ se define como

$$f(a) \coloneqq \sum_{k=0}^{m} f_k a^k,$$

donde, por definición, $a^0 \coloneqq 1_{\mathcal{A}}$.

12 Proposición. *Sea $\mathcal{A}$ una álgebra compleja asociativa con identidad $1_{\mathcal{A}}$ y sea a un elemento de $\mathcal{A}$. Denotemos por $\mathcal{B}$ al conjunto de los elementos b de $\mathcal{A}$ tales que existe un polinomio f con la propiedad $f(a) = b$. Entonces $\mathcal{B}$ es una subálgebra con identidad de $\mathcal{A}$ y $a \in \mathcal{B}$. Más aún, $\mathcal{B}$ es la mínima entre todas las subálgebras de $\mathcal{A}$ que contienen al elemento a.*

Idea de demostración. Es fácil ver que si f y g son dos polinomios, entonces $(fg)(a) = f(a)g(a)$, donde fg es el producto común de los polinomios. Las operaciones lineales con elementos de $\mathcal{B}$ también producen elementos de $\mathcal{B}$. Si f es el polinomio uno, es decir, $f(t) = 1t^0$, entonces $f(a) = 1_{\mathcal{A}}$. Por lo tanto, $\mathcal{B}$ es una subálgebra de $\mathcal{A}$ con la misma identidad $1_{\mathcal{A}}$.

Si $\mathcal{C}$ es alguna subálgebra del álgebra compleja $\mathcal{A}$ tal que $1_{\mathcal{A}} \in \mathcal{C}$ y $a \in \mathcal{C}$. entonces cualquier elemento de $\mathcal{A}$ de la forma $f(a)$, donde f es un polinomio, pertenece a $\mathcal{C}$. Luego $\mathcal{B} \subseteq \mathcal{C}$. $\square$

13 Definición. Sea $\mathcal{A}$ una álgebra compleja asociativa con identidad $1_{\mathcal{A}}$. Entonces el conjunto de los elementos de la forma $f(a)$, donde f es un polinomio con coeficientes complejos, se llama el *subálgebra con identidad generada* por a. La denotemos por $\operatorname{alg}(a)$.

14 Ejemplo. Sea $n = 3$ y sea

$$a = \begin{bmatrix} 4 \\ 5 \\ 5 \end{bmatrix}.$$

Entonces para cualquier polinomio f tenemos

$$f(a) = \begin{bmatrix} f(4) \\ f(5) \\ f(5) \end{bmatrix}.$$

El conjunto de los elementos de esta forma no coincide con $\mathbb{C}^3$: por ejemplo, e_3 no es de esta forma. Por eso $\operatorname{alg}(a) \neq \mathbb{C}^3$.

15 Proposición (descripción de los generadores del álgebra $\mathbb{C}^n$)**.** *Sea* $a \in \mathbb{C}^n$*. Entonces* $\operatorname{alg}(a) = \mathbb{C}^n$ *si y sólo si todas las componentes de* a *son diferentes entre si.*

Demostración. Necesidad. Supongamos que $\operatorname{alg}(a) = \mathbb{C}^n$. Sean $p, q \in \{1, \ldots, n\}$ tales que $p \neq q$. Por la hipótesis, $e_p \in \operatorname{alg}(a)$, luego existe un polinomio f tal que $f(a) = e_p$. Como

$$f(a_p) = ((f(a))_p = (e_p)_p = 1 \neq 0 = (e_p)_q = ((f(a))_q = f(a_q),$$

concluimos que $a_p \neq a_q$.

Suficiencia. Supongamos que todas las componentes de a son diferentes entre si. Sea $b \in \mathbb{C}^n$. Por el teorema sobre la interpolación polinomial, existe un polinomio f de grado $\leq n - 1$ tal que

$$f(a_j) = b_j \qquad (j \in \{1, \ldots, n\}). \tag{1}$$

La condición (1) significa que $f(a) = b$, así que $b \in \operatorname{alg}(a)$. $\square$