Matrices circulantes

Objetivos. Definir el concepto de matrices circulantes. Demostrar que el producto de una matriz circulante por un vector se escribe como la convolución discreta cíclica de dos vectores.

Requisitos. El grupo $\mathbb{Z}_n$ y su identificación con $[\![0,n[\![$, convolución discreta cíclica (sobre el grupo $\mathbb{Z}_n$), la matriz asociada a un operador lineal respecto a una base.

Suponemos que $n \in \mathbb{N}$. En estos apuntes denotamos $\operatorname{mod}(p+q,n)$ por $p \oplus q$ y la convolución discreta cíclica de dos vectores a, b por $a * b$.

Definición 1. Sea $a \in \mathbb{C}^n$. La *matriz circulante*, asociada al vector a, se define como

$$\operatorname{circ}(a) \coloneqq \left[a_{j\ominus k}\right]_{j,k=0}^{n-1}.$$

En otras palabras, $\operatorname{circ} a \in \mathcal{M}_n(\mathbb{C})$ y para cada j, k en $[\![0,n[\![$

$$\operatorname{circ}(a) = a_{j\ominus k} = \begin{cases} a_{j-k}, & k \le j; \\ a_{j-k+n}, & k > j. \end{cases}$$

Ejemplo 2. Si $n = 4$, entonces

$$\operatorname{circ}(a) = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix}.$$

Proposición 3. *Sean $a, b \in \mathbb{C}^n$. Entonces*

$$\operatorname{circ}(a)b = a * b.$$

Demostración. Notamos que $\operatorname{circ}(a)b$ y $a * b$ son vectores del espacio $\mathbb{C}^n$. Mostremos que estos vectores tienen las mismas componentes. Sea $j \in [\![0,n[\![$. Entonces

$$(\operatorname{circ}(a)b)_j = \sum_{k=0}^{n-1} \operatorname{circ}(a)_{j,k} b_k = \sum_{k=0}^{n-1} a_{j\ominus k} b_k = (a * b)_j.$$

Podemos escribir la demostración de otra manera, evitando la operación $\ominus$ y dividiendo la suma en dos partes:

$$(\operatorname{circ}(a)b)_j = \sum_{k=0}^{n-1} \operatorname{circ}(a)_{j,k} b_k = \sum_{k=0}^{j} a_{j-k} b_k + \sum_{k=j+1}^{n-1} a_{j-k+n} b_k = (a * b)_j. \qquad \square$$

Proposición 4 (repaso: el criterio de igualdad de matrices en términos de multiplicación por vectores)**.** *Sean* $A, B \in \mathcal{M}_n(\mathbb{C})$ *tales que* $Ax = Bx$ *para cada* x *en* $\mathbb{C}^n$*. Entonces* $A = B$*.*

Idea de demostración. En efecto, para cada k en $[\![0, n[\![$ ponemos $x = e_k$ y obtenemos que $A_{*,k} = B_{*,k}$, es decir, la k-ésima columna de A coincide con la k-ésima columna de B. □

Proposición 5. *Sean* $a, b \in \mathbb{C}^n$*. Entonces*

$$\operatorname{circ}(a) \operatorname{circ}(b) = \operatorname{circ}(a * b). \tag{1}$$

Demostración. Ya sabemos que la convolución discreta cíclica es asociativa. Entonces, para cualquier x en $\mathbb{C}^n$,

$$(a * b) * x = a * (b * x).$$

Transformamos ambos lados de esta igualdad usando la Proposición 3:

$$\operatorname{circ}(a * b)x = \operatorname{circ}(a)(\operatorname{circ}(b)x).$$

En el lado derecho aplicamos la propiedad asociativa de la multiplicación de matrices:

$$\operatorname{circ}(a * b)x = \big(\operatorname{circ}(a) \operatorname{circ}(b)\big)x.$$

Como x es arbitrario, por el criterio de igualdad de matrices en términos de multiplicación por vectores concluimos que se cumple (1). □

En el siguiente tema estudiaremos la diagonalización de las matrices circulantes (en otras palabras, la descomposición espectral de las matrices circulantes), usando el teorema de convolución para la convolución discreta cíclica.