

El teorema de convolución para el grupo cíclico finito \mathbb{Z}_n

Objetivos. Demostrar el teorema de convolución para el grupo \mathbb{Z}_n .

Requisitos. Varias formas equivalentes del grupo \mathbb{Z}_n , convolución discreta cíclica (sobre el grupo \mathbb{Z}_n), transformada finita de Fourier.

Repaso: identificamos \mathbb{Z}_n con $\llbracket 0, n \llbracket := \{0, 1, \dots, n-1\}$

Sea $n \in \mathbb{Z}$, $n \geq 2$. El grupo \mathbb{Z}_n se define como el grupo cociente $\mathbb{Z}/(n\mathbb{Z})$. En estos apuntes, en vez trabajar con clases de congruencia, preferimos trabajar con sus “representantes canónicos”. Usamos la notación

$$\llbracket 0, n \llbracket := \{k \in \mathbb{Z} : 0 \leq k < n\} = \{0, 1, \dots, n-1\}.$$

Dotamos $\llbracket 0, n \llbracket$ de la “adición módulo n ”:

$$a \oplus_n b := \text{mod}(a+b, n) = \begin{cases} a+b, & 0 \leq a, b < n, a+b < n; \\ a+b-n, & 0 \leq a, b < n, a+b \geq n. \end{cases}$$

Aquí $\text{mod}(a+b, n)$ es el resto al dividir $a+b$ entre n . Ya sabemos que el grupo $(\llbracket 0, n \llbracket, \oplus_n)$ es isomorfo a \mathbb{Z}_n . La sustracción en este grupo se calcula así:

$$a \ominus_n b = \text{mod}(a-b, n) = \begin{cases} a-b, & 0 \leq a, b < n, a-b \geq 0; \\ a-b+n, & 0 \leq a, b < n, a-b < 0. \end{cases}$$

En estos apuntes, por brevedad, escribimos \oplus y \ominus en vez de \oplus_n y \ominus_n , respectivamente.

Repaso: la multiplicación de vectores por componentes, la convolución de dos vectores y la transformada finita de Fourier

Identificamos las funciones $\llbracket 0, n \llbracket \rightarrow \mathbb{C}$ con los vectores del espacio \mathbb{C}^n . Denotamos por \odot su multiplicación por componentes. En otras palabras, si a, b en \mathbb{C}^n , entonces

$$a \odot b := [a_j b_j]_{j=0}^{n-1}.$$

Dados dos vectores a, b en \mathbb{C}^n , su *convolución* se define como el siguiente vector:

$$a * b := \left[\sum_{k=0}^{n-1} a_{j \ominus k} b_k \right]_{j=0}^{n-1}.$$

En otras palabras, $a * b \in \mathbb{C}^n$ y para cada $j \in \llbracket 0, n \llbracket$

$$(a * b)_j := \sum_{k=0}^{n-1} a_{j \ominus k} b_k = \sum_{k=0}^j a_{j-k} b_k + \sum_{k=j+1}^{n-1} a_{j-k+n} b_k.$$

Esta operación se conoce también como la *convolución discreta cíclica* y corresponde a la convolución sobre el grupo \mathbb{Z}_n .

Pongamos $\omega_n := \exp \frac{2\pi i}{n}$ y denotamos por F_n la *matriz de Fourier*:

$$F_n := \left[\omega_n^{jk} \right]_{j,k=0}^{n-1}.$$

Lema 1. Sean $j, p, q \in \llbracket 0, n \llbracket$. Entonces

$$\omega_n^{j(p \oplus q)} = \omega_n^{jp} \omega_n^{jq}.$$

Demostración. Si $p + q < n$, entonces $p \oplus q = p + q$, y el resultado es obvio.

Si $p + q \geq n$, entonces $p \oplus q = p + q - n$, y el resultado se sigue de la igualdad $\omega_n^{jn} = 1$. \square

Teorema 2 (el teorema de convolución para el grupo discreto cíclico). Sean $a, b \in \mathbb{C}^n$. Entonces

$$F_n(a * b) = (F_n a) \odot (F_n b).$$

Primera demostración: usamos las operaciones \oplus y \ominus . Sea $j \in \llbracket 0, n \llbracket$. Aplicamos la definición de F_n , luego la definición de $a * b$:

$$(F_n(a * b))_j = \sum_{k=0}^{n-1} (F_n)_{j,k} (a * b)_k = \sum_{k=0}^{n-1} \omega_n^{jk} \sum_{p=0}^{n-1} a_{k \ominus p} b_p.$$

Aplicamos la propiedad distributiva y metemos el factor ω_n^{jk} adentro de la suma interior. Luego intercambiamos el orden de las sumas.

$$(F_n(a * b))_j = \sum_{p=0}^{n-1} \sum_{k=0}^{n-1} \omega_n^{jk} a_{k \ominus p} b_p.$$

Ahora en la suma interior hacemos el cambio de variable $q = k \ominus p$. En este cambio de variable tratamos p como un parámetro fijo. Utilizamos el hecho que la función $k \mapsto k \ominus p$ es una biyección $\llbracket 0, n \llbracket \rightarrow \llbracket 0, n \llbracket$. La inversa de esta función está dada por $q \mapsto q \oplus p$.

$$q = k \ominus p, \quad k = p \oplus q.$$

Obtenemos

$$(F_n(a * b))_j = \sum_{p=0}^{n-1} \sum_{q=0}^{n-1} \omega_n^{j(p \oplus q)} a_q b_p.$$

Ahora aplicamos el Lema 1, usamos la propiedad distributiva para las sumas y factorizamos la suma doble en un producto:

$$\begin{aligned} (F_n(a * b))_j &= \sum_{p=0}^{n-1} \sum_{q=0}^{n-1} \omega_n^{jp} \omega_n^{jq} a_q b_p = \sum_{p=0}^{n-1} \omega_n^{jp} b_p \sum_{q=0}^{n-1} \omega_n^{jq} a_q \\ &= (F_n a)_j (F_n a)_j = ((F_n a) \odot (F_n b))_j. \quad \square \end{aligned}$$

Segunda demostración: dividimos la suma en dos partes. Igual que en la primera demostración, llegamos a la expresión

$$(F_n(a * b))_j = \sum_{p=0}^{n-1} \sum_{k=0}^{n-1} \omega_n^{jk} a_{k \oplus p} b_p.$$

Ahora partimos la suma interior en dos partes:

$$(F_n(a * b))_j = \sum_{p=0}^{n-1} \sum_{k=0}^{p-1} \omega_n^{jk} a_{k-p+n} b_p + \sum_{p=0}^{n-1} \sum_{k=p}^{n-1} \omega_n^{jk} a_{k-p} b_p.$$

Dentro de la primera suma doble, en la suma interior hacemos el siguiente cambio (tratando p como parámetro):

$$q = k - p + n, \quad k = q + p - n.$$

Dentro de la segunda suma doble, en la suma interior hacemos el siguiente cambio (tratando p como parámetro):

$$q = k - p, \quad k = p + q.$$

Después de estos cambios,

$$(F_n(a * b))_j = \sum_{p=0}^{n-1} \sum_{q=n-p}^{n-1} \omega_n^{j(q+p-n)} a_q b_p + \sum_{p=0}^{n-1} \sum_{k=0}^{n-p-1} \omega_n^{j(p+q)} a_q b_p.$$

Aplicando la igualdad $\omega_n^{jn} = 1$, podemos juntar las sumas:

$$(F_n(a * b))_j = \sum_{p=0}^{n-1} \sum_{q=n-p}^{n-1} \omega_n^{j(p+q)} a_q b_p + \sum_{p=0}^{n-1} \sum_{q=0}^{n-p-1} \omega_n^{j(p+q)} a_q b_p = \sum_{p=0}^{n-1} \sum_{q=0}^{n-1} \omega_n^{j(p+q)} a_q b_p.$$

Finalmente, notamos que $\omega_n^{j(p+q)} = \omega_{jp} \omega_{jq}$ y separamos la última suma doble en un producto:

$$(F_n(a * b))_j = \left(\sum_{p=0}^{n-1} \omega_n^{jp} b_p \right) \left(\sum_{q=0}^{n-1} \omega_n^{jq} a_q \right) = (F_n a)_j (F_n a)_j = ((F_n a) \odot (F_n b))_j. \quad \square$$