



Universidad Autónoma Metropolitana

Unidad Iztapalapa
DIVISIÓN DE CIENCIAS BÁSICAS E
INGENIERÍA
DEPARTAMENTO DE MATEMÁTICAS

Una generalización de la transformada de Fourier discreta

Tesis que presenta:

**KARLA ADRIANA ORTEGA
GALLEGOS**

Matrícula: 2193801751

para obtener el grado de: Maestra en Ciencias
(Matemáticas)

DIRECTOR: DR. ROBERTO QUEZADA BATALLA

JURADOS:

DR. RICARDO MARCELIN JIMENEZ

DR. JORGE RICARDO BOLANOS SERVIN

DR. CRISPIN HERRERA YANEZ

IZTAPALAPA, CIUDAD DE MÉXICO, 24 DE FEBRERO DE 2022

ADRI.MATE3017@GMAIL.COM

Índice general

Resumen	9
AGRADECIMIENTOS	9
Introducción	9
1. Preliminares	1
1.1. Espacios de Hilbert de dimensión finita	1
1.2. Operadores lineales	3
1.3. El teorema espectral para operadores normales	7
2. La transformada de Fourier discreta	11
2.1. Introducción	11
2.2. Propiedades básicas	12
2.3. La identidad de Parseval	13
2.4. Fórmulas de convolución, traslación y dilatación	14
2.5. La gaussiana discreta (función propia de la TFD)	16
2.6. Ejemplos	19
3. La transformada de Fourier discreta generalizada	23
3.1. Definición y propiedades básicas	23
3.2. El Teorema de Parseval	25
3.3. Fórmulas de convolución, traslación y dilatación	28
3.4. Ejemplos	29
4. Aplicaciones	33
4.1. El álgebra de matrices circulantes	33
4.2. El espectro de Gelfand del álgebra circulante	34
4.3. La transformada de Gelfand del álgebra circulante	36
4.4. Diagonalización de matrices circulantes	37

Agradecimientos

Antes que nada, quiero agradecer a Dios, porque con su gracia e infinito poder, me ayuda a salir adelante en cada momento de mi vida.

A mi mamá mi super heroína Graciela, por ser el pilar que me sostiene y mi motivación para no desistir del ámbito profesional. A mis sobrinos que siempre me motivaron con su alegría, amor y travesuras. A mis hermanos por apoyarme en cada decisión que tomo por muy descabellada que sea.

A todas aquellas personas que de alguna forma me han apoyado durante mis estudios, amigos, compañeros y maestros, de manera especial a mi asesor de tesis, Dr. Roberto Quezada Batalla, por guiarme durante el trabajo de investigación.

Finalmente, agradezco al Conacyt por el apoyo económico que recibí para realizar mis estudios de maestría y a la UAM-Iztapalapa por todas las oportunidades que me dio durante este período para crecer profesionalmente.

Resumen

En este trabajo desarrollamos una presentación autocontenida de la transformada de Fourier discreta (TFD). Demostramos sus propiedades básicas de convolución, traslación, dilatación e identidad de Parseval y estudiamos una de sus eigenfunciones definida en términos del símbolo de Legendre (Gaussiana discreta). Siguiendo la referencia [1], revisamos una generalización de esta transformada al caso de dos subespacios de Hilbert de dimensiones diferentes (TFDG), identificando sus correspondientes propiedades de convolución, traslación, dilatación e identidad de Parseval. Finalmente, siguiendo la referencia [5], mostramos cómo la TFD diagonaliza simultáneamente a todos los elementos del álgebra circulante y determinamos el espectro de Gelfand de esta álgebra conmutativa.

No puede existir un lenguaje más universal y simple,
más carente de errores y oscuridades, y por lo tanto más
apto para expresar las relaciones invariables de
las cosas naturales. Las matemáticas parecen constituir
una facultad de la mente humana destinada a compensar
la brevedad de la vida y la imperfección de los sentidos.

Joseph Fourier

Introducción

La transformada de Fourier discreta (TFD) es una aplicación lineal del espacio de Hilbert complejo \mathbb{C}^N en sí mismo. Como su análoga de dimensión infinita o variable continua, la TFD tiene una gran cantidad de aplicaciones en ingeniería, física y matemáticas. Se puede considerar como una aplicación del espacio de funciones complejas cuadrado sumables definidas sobre un grupo cíclico (o solo conmutativo) discreto, en esta forma junto con sus generalizaciones al caso no conmutativo, es la base del análisis de Fourier discreto.

Recientemente en [1] se utilizó una generalización de la TFD al caso de dos subespacios de dimensiones diferentes para estudiar un modelo cuántico de transporte de energía relacionado con el fenómeno de la fotosíntesis. El propósito principal de este trabajo es identificar las correspondientes fórmulas de convolución, traslación y dilatación de esta generalización de la transformada de Fourier discreta (TFDG) e ilustrarlas con algunos ejemplos, véase la Sección 3.3. Así, $\frac{1}{2}$ mismo, identificamos la correspondiente propiedad de Parseval, Teorema 3.2.4, y para completar el trabajo estudiamos una eigenfunción de la TFD y algunas aplicaciones en el álgebra de matrices circulantes.

Después de revisar algunos de conceptos del Álgebra Lineal, en el capítulo 2 desarrollamos una brevíssima introducción a la transformada de Fourier discreta, demostrando sus propiedades básicas de convolución, traslación, dilatación y la identidad de Parseval. También estudiamos una eigenfunción de la TFD definida en términos del símbolo de Legendre, cuyo eigenvalor está dado por una suma de Gauss.

En el capítulo 3 introducimos la TFDG, demostramos sus correspondientes propiedades básicas y las ilustramos con algunos ejemplos.

El capítulo 4 contiene un breve análisis, basado en la referencia [5], de la relación que existe entre la TFD y el álgebra circulante. Demostramos que la TFD diagonaliza simultáneamente a todos los elementos circulantes, calculamos el correspondiente espectro de Gelfand y mostramos cómo la TFD coincide con la transformada de Gelfand asociada con esta álgebra conmutativa.

Capítulo 1

Preliminares

1.1. Espacios de Hilbert de dimensión finita

Definición 1.1.1 *Un espacio con producto interno es un espacio vectorial complejo H con una aplicación $\langle \cdot, \cdot \rangle : H \times H \rightarrow \mathbb{C}$ que satisface las siguientes propiedades:*

- i) $\langle u, v \rangle = \overline{\langle v, u \rangle}$, para cada $u, v \in H$,*
- ii) $\langle u, v + \lambda w \rangle = \langle u, v \rangle + \lambda \langle u, w \rangle$ para cada $u, v, w \in H$ y $\lambda \in \mathbb{C}$,*
- iii) $\langle u, u \rangle \geq 0$, para cada $u \in H$,*
- iv) Si $\langle u, u \rangle = 0$, entonces $u = 0$.*

Como consecuencia de estas propiedades se obtiene lo siguiente.

Proposición 1.1.2 *El producto interno satisface:*

- i) Es lineal conjugado en la primera variable, es decir,*

$$\langle u + \lambda v, w \rangle = \overline{\langle w, u + \lambda v \rangle} = \langle u, w \rangle + \bar{\lambda} \langle v, w \rangle. \quad (1.1)$$

- ii) Se tiene que $\langle u, u \rangle = 0$ si y sólo si $u = 0$.*

Demostración. El inciso i) se sigue de iv) de la definición. Por otra parte, si $u = 0$ entonces $\langle u, v \rangle = 0$, para cada $v \in H$, pues:

$$\lambda \langle u, v \rangle = \langle u, v \rangle = \mu \langle u, v \rangle \quad (1.2)$$

para cada $\lambda, \mu \in \mathbb{C}$, entonces $\langle u, v \rangle = 0$. ■

La norma inducida por el producto interno está definida por $\|u\|^2 = \langle u, u \rangle$.

Lema 1.1.3 (Desigualdad de Cauchy Schwarz) *Para cada $u, v \in H$ se tiene que*

$$\langle u, v \rangle \leq \|u\| \|v\|. \quad (1.3)$$

La igualdad se cumple si y sólo si u es un múltiplo escalar de v .

Demostración. Sean $a = \|u\|^2$, $b = |\langle u, v \rangle|$, $c = \|v\|^2$ y un ángulo $\alpha = \frac{\langle u, v \rangle}{|\langle u, v \rangle|}$ si $\langle v, u \rangle \neq 0$ entonces $\alpha = 1$, el número complejo α tiene módulo uno y además $\alpha \langle v, u \rangle = |\langle v, u \rangle|$. Para cualquier real λ tenemos que

$$\begin{aligned} 0 \leq \langle u - \lambda v, u - \lambda v \rangle &= \|u\|^2 - 2\lambda \operatorname{Re}(\alpha \langle v, u \rangle) + \lambda^2 \|v\|^2 \\ &= \|u\|^2 - 2\lambda |\langle u, v \rangle| + \lambda^2 \|v\|^2 \end{aligned} \quad (1.4)$$

Entonces $a - 2b\lambda + c\lambda^2 \geq 0$, para cualquier real λ . Si $c = 0$ debemos tener que $b = 0$, pues en caso contrario la desigualdad es falsa para λ positivo grande. Si $c > 0$, tomando $\lambda = \frac{b}{c}$ se obtiene que $b^2 \leq ac$. Por la propiedad *ii*) del producto interno se sigue $\|u\|^2 - 2\lambda |\langle u, v \rangle| + \lambda^2 \|v\|^2 = 0$ si y sólo si $u = \theta v$ para algún $\theta \in \mathbb{C}$. ■

Proposición 1.1.4 *Para todo $u, v \in H$ se tiene que*

$$\|u + v\| \leq \|u\| + \|v\|. \quad (1.5)$$

Demostración. Usando la desigualdad de Schwarz obtenemos que

$$\|u + v\|^2 = \langle u + v, u + v \rangle = \|u\|^2 + 2\operatorname{Re}\langle u, v \rangle + \|v\|^2 \leq \|u\|^2 + 2|\langle u, v \rangle| + \|v\|^2 \leq (\|u\| + \|v\|)^2 \quad (1.6)$$

para toda $u, v \in H$. ■

Con esta norma el espacio H resulta ser un espacio vectorial normado. Si la dimensión de H es finita entonces el par $(H, \langle \cdot, \cdot \rangle)$ es un espacio de Hilbert. Si la dimensión de H no es finita, pueden existir sucesiones de Cauchy sin límites en H , el espacio vectorial normado $(H, \|\cdot\|)$ puede no ser completo. Un espacio de Hilbert de dimensión infinita es un espacio con producto interno que es completo bajo la norma $\|\cdot\|$. De ahora en adelante, trabajaremos sólo con espacios de Hilbert complejos de dimensión finita.

Definición 1.1.5 *Un conjunto $\{e_1, e_2, \dots, e_n\}$ de n vectores en H es ortonormal si cada uno de ellos es unitario y cada par es ortogonal, de manera breve esta propiedad se describe como $\langle e_j, e_i \rangle = \delta_{ij}$, para $1 \leq i, j \leq n$.*

Proposición 1.1.6 *En un espacio de Hilbert de dimensión n , un conjunto de n vectores ortonormales $\{e_1, \dots, e_n\}$ forman una base del espacio*

Demostración. Si

$$\sum_{j=1}^n \lambda_j e_j = 0 \quad (1.7)$$

así para cada $k = 1, 2, \dots, n$

$$0 = \langle e_k, \sum_{j=1}^n \lambda_j e_j \rangle = \sum_{j=1}^n \lambda_j \delta_{kj} = \lambda_k \quad (1.8)$$

lo cual demuestra que los n vectores son linealmente independientes y, por lo tanto, una base ortonormal. ■

1.2. Operadores lineales

Usaremos el símbolo $B(H_1, H_2)$ o simplemente $B(H)$ si $H_1 = H = H_2$, para denotar al conjunto de los operadores lineales de H_1 en H_2 . Este conjunto tiene una estructura natural de espacio vectorial, también tiene una norma que definiremos más adelante.

Dadas bases ortonormales $\{e_i\}$ $1 \leq i \leq n$ de H_1 y $\{f_j\}$ $1 \leq j \leq m$ de H_2 . Cada operador $x \in B(H_1, H_2)$ tiene una representación matricial (x_{ij}) , $1 \leq i \leq n$, $1 \leq j \leq m$, donde $x_{ij} = \langle f_i, xe_j \rangle$; tal que para cada $1 \leq j \leq n$, $xe_j = \sum_i \langle f_i, xe_j \rangle f_i = \sum_{i=1}^m x_{i,j} f_i$. Y para un vector arbitrario $u \in H_1$, $u = \sum_{j=1}^n u_j e_j$ se tiene que

$$xu = \sum_{j=1}^n u_j xe_j = \sum_{j=1}^n u_j \sum_{i=1}^m x_{ij} f_i = \sum_{i=1}^m \left(\sum_{j=1}^n x_{ij} u_j \right) f_i, \quad (1.9)$$

es decir, la i -ésima componente de xu está dada por $(xu)_i = \sum_j x_{ij} u_j$. En otras palabras el vector renglón xu se obtiene multiplicando la matriz $x = (x_{i,j})$ por el vector columna u .

Lema 1.2.1 *La composición $z = yx$ de dos operadores $x \in B(H, K)$ y $y \in B(K, L)$ tiene asociada la matriz producto yx con respecto a tres bases ortonormales fijas $\{e_j\} \subset H$, $\{f_i\} \subset K$ y $\{g_k\} \subset L$.*

Demostración. De lo anterior obtenemos

$$z_{kl} = \langle g_k, ze_l \rangle = \langle g_k, yxe_l \rangle = \langle g_k, y \sum_{i=1}^m x_{i,l} f_i \rangle = \sum_{i=1}^m x_{i,l} \langle g_k, y f_i \rangle = \sum_{i=1}^m y_{ki} x_{i,l} = (yx)_{kl} \quad (1.10)$$

■

Definición 1.2.2 *El adjunto de un operador $x \in B(H, K)$ es el único operador $x^* \in B(K, H)$ que satisface la relación*

$$\langle u, xv \rangle_K = \langle x^* u, v \rangle_H \quad (1.11)$$

Ejemplo 1.2.3 *Dadas dos bases ortonormales fijas en H y K , entonces la matriz de x^* es la transpuesta conjugada de la matriz de x .*

Demostración. Dadas bases ortonormales $\{e_i\}$ $1 \leq i \leq n$ de H y $\{f_j\}$ $1 \leq j \leq m$ de K . Cada operador $x \in B(H, K)$ tiene una representación matricial (x_{ij}) , $1 \leq i \leq n$, $1 \leq j \leq m$, donde $x_{ij} = \langle f_i, xe_j \rangle$; tal que para cada $1 \leq j \leq n$, $xe_j = \sum_i \langle f_i, xe_j \rangle f_i = \sum_{i=1}^m x_{i,j} f_i$. Y para un vector arbitrario $u \in H_1$, $u = \sum_{j=1}^n u_j e_j$. Pero

$$x^* f_i = \sum_j \langle x^* f_i, e_j \rangle e_j = \sum_i \langle f_i, xe_j \rangle e_j = \sum_{i=1}^m x_{i,j} f_i \quad (1.12)$$

y por otro lado

$$x^* f_i = \sum_j \langle x^* f_i, e_j \rangle e_j = \sum_{j=1}^n x_{i,j}^* e_j \quad (1.13)$$

observemos que $\overline{x_{ji}} = \langle x e_i, f_j \rangle$ por lo tanto $x^* = \overline{x}^T$ ■

Definición 1.2.4 Un operador $x \in B(H)$, es hermitiano o autoadjunto si satisface la condición $x^* = x$.

Definición 1.2.5 Un operador $x \in B(H)$ es positivo si satisface la condición $\langle u, xu \rangle \geq 0$ para todo vector $u \in H$.

Teorema 1.2.6 Dados un operador $x \in B(H)$ y los vectores $u, v \in H$, se cumple la siguiente identidad de polarización

$$\langle u, xv \rangle = \frac{1}{4} \{ \langle u+v, x(u+v) \rangle - \langle u-v, x(u-v) \rangle + i \langle u+iv, x(u+iv) \rangle - i \langle u-iv, x(u-iv) \rangle \} \quad (1.14)$$

Demostración.

$$\begin{aligned} & \frac{1}{4} \{ \langle u+v, x(u+v) \rangle - \langle u-v, x(u-v) \rangle + i \langle u+iv, x(u+iv) \rangle - i \langle u-iv, x(u-iv) \rangle \} \\ &= \frac{1}{4} \{ \langle u, x(u+v) \rangle + \langle v, x(u+v) \rangle - \langle u, x(u-v) \rangle + \langle v, x(u-v) \rangle \\ &+ i \langle u, x(u+iv) \rangle + i \langle iv, x(u+iv) \rangle - i \langle u, x(u-iv) \rangle + i \langle iv, x(u-iv) \rangle \} \\ &= \frac{1}{4} \{ \langle u, xu \rangle + \langle u, xv \rangle + \langle v, xu \rangle + \langle v, xv \rangle - \langle u, xu \rangle + \langle u, xv \rangle + \langle v, xu \rangle - \langle v, xv \rangle \\ &+ i \langle u, xu \rangle + i \langle u, xiv \rangle + i \langle iv, xu \rangle + i \langle iv, xiv \rangle - i \langle u, xu \rangle + i \langle u, xiv \rangle + i \langle iv, xu \rangle - i \langle iv, xiv \rangle \} \\ &= \frac{1}{4} \{ \langle u, xu \rangle + \langle u, xv \rangle + \langle v, xu \rangle + \langle v, xv \rangle - \langle u, xu \rangle + \langle u, xv \rangle + \langle v, xu \rangle - \langle v, xv \rangle + i \langle u, xu \rangle \\ &+ i(-i) \langle u, xv \rangle + ii \langle v, xu \rangle + i(-i)i \langle v, xv \rangle - i \langle u, xu \rangle + i(-i) \langle u, xv \rangle + ii \langle v, xu \rangle - i(-i)i \langle v, xv \rangle \} \\ &= \frac{1}{4} \{ 4 \langle u, xv \rangle \} = \langle u, xv \rangle \end{aligned} \quad (1.15)$$

■

El espacio vectorial $B(H)$ se convierte en un espacio de Banach cuando se le equipa con la norma

$$\|x\| = \sup_{u \neq 0} \frac{\|xu\|}{\|u\|}. \quad (1.16)$$

Se tiene que $\|x\| = \sup_{\|u\|=1} \|xu\| = \sup_{\|u\| \leq 1} \|xu\| < \infty$. En dimensión finita esta norma es equivalente con la norma Euclídeana de la matriz que representa al operador x .

Teorema 1.2.7 Si $X, Y \in B(H)$ y $\lambda \in \mathbb{C}$ se tienen las siguientes propiedades:

$$i) (\lambda X + Y)^* = \bar{\lambda}X^* + Y^*$$

$$ii) (XY)^* = Y^*X^*$$

$$iii) (X^*)^* = X$$

$$iv) \|X^*\| = \|X\|$$

Demostración.

$$\begin{aligned} i) \langle z, (\lambda X + Y)^*w \rangle &= \langle (\lambda X + Y)z, w \rangle = \bar{\lambda}\langle Xz, w \rangle + \langle Yz, w \rangle \\ &= \bar{\lambda}\langle z, X^*(w) \rangle + \langle z, Y^*(w) \rangle = \langle z, \bar{\lambda}X^*(w) \rangle + \langle z, Y^*(w) \rangle \\ &= \langle z, (\bar{\lambda}X^* + Y^*)(w) \rangle \end{aligned} \quad (1.17)$$

$$ii) \langle XY(z), w \rangle = \langle Y(z), X^*(w) \rangle = \langle z, Y^*X^*(w) \rangle \quad (1.18)$$

$$iii) \langle z, (X^*)^*(w) \rangle = \langle X^*(z), w \rangle = \overline{\langle w, (X^*)z \rangle} = \overline{\langle X(w), z \rangle} = \langle w, X(z) \rangle \quad (1.19)$$

■

Definición 1.2.8 Dado un operador x , se dice

$$i) x \text{ es normal si } xx^* = x^*x.$$

ii) Un operador $x \in B(H)$ es unitario si es un isomorfismo, o isométrico ($\|xu\| = \|u\|$) de H en sí mismo. Equivalentemente si $x^*x = I = xx^*$.

iii) $V \in B(H_1, H_2)$ es una isometría parcial, si para $h \in (\ker V)^\perp$, $\|Vh\| = \|h\|$. El espacio $(\ker V)^\perp$ se llama espacio inicial de V y el espacio $\text{ran } V$ es llamado espacio final de V .

Definición 1.2.9 Sea v un vector de H_1 y u un vector de H_2 , definimos el operador lineal $|u\rangle\langle v|$ de H_1 en H_2 mediante la correspondencia

$$|u\rangle\langle v|w = \langle v, w \rangle u, \quad \forall w \in H_1. \quad (1.20)$$

Teorema 1.2.10 La función $(v, u) \mapsto |u\rangle\langle v|$ de $H \times H$ a $B(H)$ satisface lo siguiente:

i) $|u\rangle\langle v|$ es lineal en u y lineal conjugada en v .

ii) $(|v\rangle\langle u|)^* = |u\rangle\langle v|$ en particular $|u\rangle\langle u|$ es auto-adjunto.

iii) $|u\rangle\langle v||\psi\rangle\langle\phi| = \langle v, \psi \rangle |u\rangle\langle\phi|$.

$$iv) \quad \| |u\rangle\langle v| \| = \|u\| \|v\|.$$

$$v) \quad \text{Para todo } A \in B(H), \quad A|u\rangle\langle v| = |Au\rangle\langle v| \text{ y } |u\rangle\langle v|A = |u\rangle\langle A^*v|.$$

Demostración. Sea $u, v, w \in H$ y $\alpha, \beta \in \mathbb{C}$

$$i) \quad |u\rangle\langle \alpha v|w = \langle \alpha v, w \rangle u = \bar{\alpha} \langle v, w \rangle u \quad (1.21)$$

$$ii) \quad |\beta u\rangle\langle v| = \langle v, w \rangle \beta u = \beta \langle v, w \rangle u \quad (1.22)$$

$$iii) \quad |u\rangle\langle v||\psi\rangle\langle \phi| = |u\rangle\langle v, \psi \rangle \langle \phi| \text{ como } \langle v, \psi \rangle \text{ es un número complejo tenemos que } \langle v, \psi \rangle |u\rangle\langle \phi| = |u\rangle\langle v||\psi\rangle\langle \phi|$$

$$iv) \quad \| |u\rangle\langle v|w \| = \| \langle v, w \rangle u \| = \| (\|v\| \|w\|) u \| = \|v\| \|w\| \|u\| \implies \| |u\rangle\langle v| \| = \|u\| \|v\| \quad (1.23)$$

$$v) \quad A|u\rangle\langle v|w = \langle v, w \rangle A(u) = |Au\rangle\langle v|w \quad (1.24)$$

■

Podemos apreciar la utilidad de la notación anterior en la siguiente propiedad llamada la relación de completez para bases ortonormales. Si $\{|i\rangle\}$ es una base ortonormal de H todo vector se escribe como $v = \sum_i \alpha_i |i\rangle$, donde $\alpha_i = \langle i, v \rangle$ y por tanto

$$\begin{aligned} \left(\sum_j |j\rangle\langle j| \right) v &= \left(\sum_j |j\rangle\langle j| \right) \left(\sum_i \alpha_i |i\rangle \right) = \sum_j \sum_i \alpha_i |i\rangle\langle j|i\rangle \\ &= \sum_j \sum_i \alpha_i \langle j, i \rangle |j\rangle = \sum_j \alpha_j |j\rangle = v \end{aligned} \quad (1.25)$$

Podemos concluir que

$$\sum_i |i\rangle\langle i| = I \quad (1.26)$$

Los valores propios de un operador A son las raíces del polinomio $p_A(\lambda) = \det(\lambda I - A)$ llamado polinomio característico de A . Puesto que nuestros espacios de Hilbert son complejos, el teorema fundamental del álgebra garantiza que todo operador tiene al menos un valor propio y su correspondiente vector propio.

El conjunto de vectores propios correspondientes a un valor propio λ es el espacio propio asociado a λ ; el conjunto de valores propios de un operador es su espectro

Definición 1.2.11 *Se dice que un operador $A \in B(H)$ es diagonalizable si existe una base ortonormal de vectores propios suyos $\{w_i\}$ con valores propios $\{\lambda_i\}$ respectivamente tales que $A = \sum_i \lambda_i |w_i\rangle\langle w_i|$. También se dice que A se diagonaliza con respecto a la base $\{w_i\}$*

Proposición 1.2.12 *Si N es operador normal, entonces*

$$i) \quad \ker N = \ker N^*$$

$$ii) \quad \text{Si } v \text{ es un elemento tal que } Nv = \lambda v, \text{ entonces } N^*v = \bar{\lambda}v.$$

iii) Si v es un vector propio de N tal que $Nv = \lambda v$ y v, w son vectores ortogonales, entonces también Nw y v son ortogonales.

Demostración. i) Como

$$\|N^*u\|^2 = \langle N^*u, N^*u \rangle = \langle NN^*u, u \rangle = \langle N^*Nu, u \rangle = \|Nu\|^2 \quad (1.27)$$

entonces $\|N^*x\| = 0$ si y sólo si $\|Nx\| = 0$.

ii) Tenemos que el operador $(N - \lambda I)$ es normal y por la propiedad i), $(N - \lambda I)x = 0$, si y sólo si $(N - \lambda I)^*x = 0$.

iii) Tenemos que

$$\langle v, Nw \rangle = \langle N^*v, w \rangle = \lambda \langle v, w \rangle = 0$$

■

1.3. El teorema espectral para operadores normales

Teorema 1.3.1 *Cualquier operador normal N en un espacio de Hilbert H de dimensión finita, es diagonal con respecto a alguna base ortonormal de H .*

Demostración. Realizaremos inducción sobre $d = \dim H$.

El caso 1 es trivial. Sea $d = n$, como estamos trabajando con espacios complejos, toda matriz tiene n valores propios. Por las propiedades mencionadas arriba, N y N^* tienen un vector propio común w_1 , que se puede suponer con norma 1. Sea $W = \{w_1\}^\perp = \{u \in H : \langle u, w_1 \rangle = 0\}$. Por la propiedad iii) la restricción de N a W está bien definida y por la Hipótesis de inducción, existe $\{w_2, w_3, \dots, w_n\}$ una base ortonormal de W constituida por vectores propios de N . Es claro que $\{w_1, w_2, \dots, w_n\}$ es una base ortonormal del espacio de Hilbert, por ende todo $v \in H$ se expresa como $v = \sum_i a_i w_i$ entonces

$$\left(\sum_i \lambda_i |w_i\rangle \langle w_i| \right) v = \sum_i \lambda_i a_i w_i = N \left(\sum_i a_i w_i \right) \quad (1.28)$$

por lo que podemos concluir que para cualquier operador normal, existe una base ortonormal en el espacio de Hilbert $\{w_i\}$ formada por los vectores propios de N y con valores propios asociados λ_i , tal que

$$N = \sum_i \lambda_i |w_i\rangle \langle w_i| \quad (1.29)$$

Por lo que se puede observar que la expresión anterior equivale a decir que $N = \sum_i \lambda_i P_i$, con p_i la proyección sobre el espacio propio asociado ■

Teorema 1.3.2 *Los operadores Hermitianos $A, B \in B(H)$ conmutan si y sólo si existe una base ortonormal de H con respecto a la cual A y B son diagonalizables simultáneamente*

Demostración. Sea $A = \sum_a aP_a$ considerando los valores propios $\{a\}$ distintos entre si y P_a es la proyección sobre el espacio propio E_a asociado con a . Se observa que $(E_a) \subset E_a$ porque $x \in E_a$ y se cumple $ABx = BAx = Bax = aBx$, así la restricción $Ba \equiv PaBP_a$ de B a E_a está bien definida y es Hermitiana, por ende E_a tiene una base ortonormal de vectores propios de B_a (se ve que también son vectores propios de A). Ahora veamos que cada vector propio $u \in E_a$ de B_a también lo es de B , en efecto, si $B_a u = bu$ tenemos que $bu = B_a u = P_a B P_a u = P_a B u = B u$ pues $B u \in E_a$ por la primera observación. Así, por cada E_a hay una base ortonormal de vectores propios de A y B . La base buscada para H es la unión de dichas bases. ■

Definición 1.3.3 Sea P un operador positivo, i.e., $P \geq 0$. Si además $\langle Pu, u \rangle = 0$ sólo es posible con $u = 0$ diremos que P es un operador positivo-definido ó estrictamente positivo y escribiremos $P > 0$. También definiremos $A \geq B$ si $A - B \geq 0$

Proposición 1.3.4 Se tienen las siguientes propiedades:

i) $\forall u \in H, |u\rangle\langle u|$ es positivo.

ii) $\forall T \in B(H), T^*T$ y TT^* son positivos y $T \geq 0 \iff T^* \geq 0$.

iii) Si $T, S \in B(H)$ son operadores positivos, entonces $\lambda S + T$ es un operador positivo si λ es un real no negativo.

Demostración. $\langle T^*T u, u \rangle = \langle u, TT^* u \rangle \quad \langle TT^* u, u \rangle = \langle Tu, Tu \rangle$

Si $T, S \in B(H)$ son operadores positivos, y $\lambda \in \mathbb{C}$

$$\langle (\lambda T + S)u, u \rangle = \bar{\lambda} \langle Tu, u \rangle + \langle Su, u \rangle \quad (1.30)$$

pero $\langle Su, u \rangle > 0$ y $\langle Tu, u \rangle > 0$, entonces $\lambda \langle Tu, u \rangle \geq 0$ y $\langle \lambda Tu, u \rangle \geq 0$ entonces $\bar{\lambda} \geq 0$ y $\lambda \geq 0$. Por lo tanto λ es real. ■

Proposición 1.3.5 Si $P \geq 0$, entonces P es hermitiano.

Demostración. Todo operador es combinación lineal de dos operadores hermitianos, su parte real y su parte imaginaria, de hecho tomando $A = \frac{1}{2}(P + P^*)$ y $B = \frac{1}{2i}(P - P^*)$, entonces $P = A + Bi$. Pero como P es positivo, tiene parte imaginaria $B = 0$, es decir,

$$0 \leq \langle u, Pu \rangle = \langle u, Au \rangle - i \langle u, Bu \rangle, \quad \forall u \in H \quad (1.31)$$

con $\langle u, Au \rangle, \langle u, Bu \rangle \in \mathbb{R}$ para todo $u \in H$, entonces $B = \frac{1}{2i}(P - P^*) = 0$ lo cual implica que $P = P^*$ ■

Teorema 1.3.6 (*Descomposición espectral para operadores positivos*). Para todo operador positivo $P \in B(H)$ existe una base ortonormal de H formada con vectores propios de P , $\{w_i\}$ con valores propios correspondientes $\{\lambda_i\}$ tales que

$$P = \sum_i \lambda_i |w_i\rangle\langle w_i| \quad \text{con } \lambda_i \geq 0. \quad (1.32)$$

Demostración. Como P es autoajunto, $PP^* = P^2 = P^*P$, entonces P es normal. Por el teorema 1.3.1 existe una base ortonormal tal que $P = \sum_i \lambda_i |w_i\rangle\langle w_i|$. Resta demostrar que cada $\lambda_i \geq 0$ pero por la positividad de P se tiene para cada i que

$$0 \leq \langle u_i, Pu_i \rangle = \lambda_i \langle u_i, u_i \rangle = \lambda_i \quad (1.33)$$

Esto finaliza la demostración. ■

Capítulo 2

La transformada de Fourier discreta

2.1. Introducción

Sea $N \geq 1$ un número natural y \mathbb{C}^N el espacio de Hilbert complejo de dimensión N . Sea $\{e_n : 0 \leq n \leq N-1\}$ la base ortonormal canónica de \mathbb{C}^N .

Definición 2.1.1 La **Transformada de Fourier Discreta (TFD)** es una transformación lineal de \mathbb{C}^N en sí mismo que se define mediante

$$F := \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n| \quad (2.1)$$

donde ζ_N es una raíz N -ésima primitiva de la unidad, por ejemplo $\zeta_N = e^{2\pi i \frac{1}{N}}$, y $|e_{n'}\rangle \langle e_n|$ denota al operador de rango uno de \mathbb{C}^N en sí mismo definido mediante $|e_{n'}\rangle \langle e_n| u = \langle e_n, u \rangle e_{n'}$.

Sea $x \in \mathbb{C}^N$, podemos suponer que $x = \sum_{n=0}^{N-1} x_n e_n$. Nótese que $\langle e_n, x \rangle = \langle e_n, \sum_{n'=0}^{N-1} x_{n'} e_{n'} \rangle = \sum_{n'=0}^{N-1} x_{n'} \langle e_n, e_{n'} \rangle = x_n$. Entonces la acción de F sobre un vector $x \in \mathbb{C}^N$ está dada explícitamente por la fórmula

$$\begin{aligned} Fx &= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n| x = \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} x_n e_{n'} \\ &= \frac{1}{\sqrt{N}} \sum_{n'=0}^{N-1} \left(\sum_{n=0}^{N-1} \zeta_N^{nn'} x_n \right) e_{n'} \end{aligned} \quad (2.2)$$

lo cual implica que la coordenada n -ésima de Fx es

$$(Fx)_n = \sum_{k=0}^{N-1} \zeta_N^{kn} x_k \quad (2.3)$$

Por esta razón también se puede definir la transformada de Fourier discreta mediante su acción sobre vectores de \mathbb{C}^N de la siguiente manera:

$$(Fx)_n = \sum_{k=0}^{N-1} x_k e^{2\pi i \frac{kn}{N}}, \quad 0 \leq n \leq N-1 \quad (2.4)$$

Los vectores $x \in \mathbb{C}^N$ también se pueden considerar como funciones de los enteros módulo N , \mathbb{Z}_N , en \mathbb{C} , i.e., $x : \mathbb{Z}_N \mapsto \mathbb{C}$. En este caso la n -ésima coordenada de x corresponde con el valor de la función x en n , i.e., $x_n = x(n)$. Así, la transformada de Fourier discreta transforma cada función $x : \mathbb{Z}_N \mapsto \mathbb{C}$ en la función $F(x) : \mathbb{Z}_N \mapsto \mathbb{C}$, definida mediante la relación

$$F(x)(n) = \sum_{k=0}^{N-1} x(k) e^{2\pi i \frac{kn}{N}}, \quad 0 \leq n \leq N-1 \quad (2.5)$$

2.2. Propiedades básicas

Proposición 2.2.1 *La TFD es una transformación lineal de \mathbb{C}^N en si mismo.*

Demostración.

$$\begin{aligned} F(\alpha x + y) &= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n| (\alpha x + y) = \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} (\alpha |e_{n'}\rangle \langle e_n|x + |e_{n'}\rangle \langle e_n|y) \\ &= \frac{1}{\sqrt{N}} \alpha \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n|x + \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n|y = \alpha F(x) + F(y) \end{aligned} \quad (2.6)$$

■

Lema 2.2.2 *Los coeficientes $\zeta_N^{nn'} = e^{2\pi i \frac{nn'}{N}}$ satisfacen la relación*

$$\sum_{n=0}^{N-1} \zeta_N^{(j-k)n} = N \delta_{jk}, \quad j = 0, 1, 2, \dots \quad (2.7)$$

donde δ_{ij} denota la función delta de Kronecker.

Demostración. Claramente, si $j = k$ se tiene $\sum_{n=0}^{N-1} \zeta_N^{(j-k)n} = N$. Ahora si $j \neq k$, entonces

$$\sum_{n=0}^{N-1} \zeta_N^{(j-k)n} = \frac{\zeta_N^{N(j-k)} - 1}{\zeta_N^{(j-k)} - 1} = 0$$

■

Proposición 2.2.3 *La TFD satisface*

$$F(F(x))(n) = x(-n), \quad n \in \mathbb{Z}_N \quad (2.8)$$

Demostración. Nótese que $-n + N \cong -n, \pmod{N}$ por lo que

$$\begin{aligned} F(F(x)) &= \frac{1}{\sqrt{N}} \sum_{m,m'=0}^{N-1} \zeta_N^{mm'} |e_{m'}\rangle \langle e_m| \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n|x \\ &= \frac{1}{N} \sum_{n,n',m,m'=0}^{N-1} \zeta_N^{mm'} \zeta_N^{nn'} \delta_{mn'} x(n) e_{m'} = \frac{1}{N} \sum_{n,m'=0}^{N-1} \left(\sum_{m=0}^{N-1} \zeta_N^{m(n+m')} \right) x(n) e_{m'} e_{m'} \quad (2.9) \\ &= \frac{1}{N} \sum_{n,m'=0}^{N-1} N \delta_{(m'+n),0} x(n) = \sum_{n=0}^{N-1} x(n) e_{N-n} = \sum_{k=0}^{N-1} x(N-k) e_k \end{aligned}$$

hemos usado que $\sum_{m=0}^{N-1} \zeta_N^{m(n+m')} = N \delta_{(m'+n),0}$, lo cual se demuestra como el lemma anterior. Después de tomar el producto interno con e_n obtenemos

$$F(F(x))(n) = x(N-n) = x(-n), \quad n \in \mathbb{Z}_N$$

con lo cual concluimos la demostración. ■

2.3. La identidad de Parseval

Teorema 2.3.1 (*Identidad de Parseval*)

Dados $x, y \in \mathbb{C}^N$, la TFD es una isometría en \mathbb{C}^N , i.e.,

$$\langle F(x), F(y) \rangle = \langle x, y \rangle \quad (2.10)$$

donde $\langle \cdot, \cdot \rangle$ es el producto interno en \mathbb{C}^N , lineal en la segunda coordenada y conjugado lineal en la primera.

Demostración. Sean $x, y \in \mathbb{C}^N$. Por definición de producto escalar y el lema 2.2.2 tenemos que

$$\begin{aligned} \langle F(x), F(y) \rangle &= \left\langle \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n|x, \frac{1}{\sqrt{N}} \sum_{l,l'=0}^{N-1} \zeta_N^{ll'} |e_{l'}\rangle \langle e_l|y \right\rangle \\ &= \frac{1}{N} \sum_{n,n',l,l'=0}^{N-1} \zeta_N^{-nn'} \zeta_N^{ll'} \overline{\langle e_n, x \rangle} \langle e_l, y \rangle \langle e_{n'}, e_{l'} \rangle = \frac{1}{N} \sum_{n,n',l,l'=0}^{N-1} \zeta_N^{-nn'} \zeta_N^{ll'} \overline{x_n} y_l \langle e_{n'}, e_{l'} \rangle \\ &= \frac{1}{N} \sum_{n,n',l=0}^{N-1} \zeta_N^{(l-n)n'} \overline{x_n} y_l = \frac{1}{N} \sum_{n,l=0}^{N-1} N \delta_{nl} \overline{x_n} y_l \\ &= \sum_{n=0}^{N-1} \overline{x_n} y_n = \langle x, y \rangle \end{aligned} \quad (2.11)$$

Esta propiedad implica que F es un operador unitario. ■

Proposición 2.3.2 F es una transformación invertible cuya inversa F^* actúa, sobre funciones $x : \mathbb{Z}_N \mapsto \mathbb{C}$, mediante la fórmula

$$F^*(x) = \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{-nn'} |e_n\rangle \langle e_{n'}| x \quad (2.12)$$

Demostración. Como F es un operador unitario, F es biyectivo. En efecto, si $F(x) = 0$, entonces $0 = \langle F(x), F(y) \rangle = \langle x, y \rangle$ para todo y , lo cual implica que $x = 0$, por lo tanto F es inyectivo. Ahora, para cada $y \in \mathbb{C}^N$, sea $x = F^*y$ dado por (2.12). Entonces,

$$\begin{aligned} F(x) &= F(F^*(y)) = F\left(\frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{-nn'} |e_{n'}\rangle \langle e_n| y\right) \\ &= \frac{1}{\sqrt{N}} \sum_{m,m'=0}^{N-1} \zeta_N^{mm'} |e_m\rangle \langle e_{m'}| \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{-nn'} |e_n\rangle \langle e_{n'}| y \\ &= \frac{1}{N} \sum_{n,n',m,m'=0}^{N-1} \delta_{mn} \zeta_N^{mm'-nn'} |e_{m'}\rangle \langle e_{n'}| y = \frac{1}{N} \sum_{n,n',m'=0}^{N-1} \zeta_N^{n(m'-n')} |e_{m'}\rangle \langle e_{n'}| y \\ &= \frac{1}{N} \sum_{n',m'=0}^{N-1} N \delta_{n'm'} |e_{m'}\rangle \langle e_{n'}| y = \sum_{n'=0}^{N-1} \langle e_{n'}, y \rangle e_{n'} = \sum_{n'=0}^{N-1} y_{n'} e_{n'} = y \end{aligned} \quad (2.13)$$

Esto demuestra que F es suprayectiva y además que $FF^* = I$. De manera análoga se demuestra que $F^*F = I$. ■

2.4. Fórmulas de convolución, traslación y dilatación

Definición 2.4.1 Sean x y y funciones, $x, y : \mathbb{Z}_N \mapsto \mathbb{C}$, entonces se define:

i) La convolución $x * y$ de x con y como la función cuyo valor en $k \in \mathbb{Z}_N$ está dado por

$$(x * y)(k) = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} x(l)y(k-l) \quad (2.14)$$

Consecuentemente, $x * y = \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} x(l)y(k-l) \right) e_k$.

ii) El producto xy de x con y como la función cuyo valor en $k \in \mathbb{Z}_N$ es

$$(xy)(k) = x(k)y(k).$$

Teorema 2.4.2 *La transformada de Fourier discreta satisface la propiedad de convolución*

$$F(x * y) = F(x) F(y) \quad (2.15)$$

donde el producto en el lado derecho es el producto de funciones.

Demostración.

$$\begin{aligned}
F(x * y) &= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_n\rangle \langle e_{n'} | (x * y) \\
&= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_n\rangle \langle e_{n'} | \left(\sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} x(l)y(k-l) \right) e_k \right) \\
&= \frac{1}{N} \sum_{n,n'=0}^{N-1} \sum_{k=0}^{N-1} \zeta_N^{nn'} \left(\sum_{l=0}^{N-1} x(l)y(k-l) \right) |e_n\rangle \langle e_{n'}, e_k\rangle \\
&= \frac{1}{N} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} \left(\sum_{l=0}^{N-1} x(l)y(n'-l) \right) e_n = \frac{1}{\sqrt{N}} \sum_{n,m=0}^{N-1} \sum_{l=0}^{N-1} \zeta_N^{n(m+l)} x(l)y(m) e_n \\
&= \frac{1}{N} \sum_{n=0}^{N-1} \sum_{l=0}^{N-1} \zeta_N^{nl} x(l) \sum_{m=0}^{N-1} \zeta_N^{nm} y(m) e_n = \sum_{n=0}^{N-1} F(x)(n) F(y)(n) e_n
\end{aligned} \quad (2.16)$$

Entonces, $F(x * y)(n) = (F(x) F(y))(n)$ para cada $n \in \mathbb{Z}_N$.

Esto termina la demostración. ■

Proposición 2.4.3 *La TFD satisface las siguientes fórmulas de traslación y dilatación, respectivamente*

(i) **(Traslación)** *Si para cada $x \in \mathbb{C}^N$ definimos su trasladado por $a \in \mathbb{Z}_N$ mediante $T_a(x)(k) = x(k-a)$, $k \in \mathbb{Z}_N$, entonces*

$$F(T_a(x))(n) = e^{\frac{2\pi i a n}{N}} F(x)(n)$$

(ii) **(Dilatación)** *Si para cada $x \in \mathbb{C}^N$ definimos su dilatación por $a \in \mathbb{Z}_N$ mediante $D_a(x)(k) = x(ak)$, $k \in \mathbb{Z}_N$, donde el producto ak es en \mathbb{Z}_N , entonces*

$$F(D_a(x))(n) = D_{a^{-1}} F(x)(n)$$

Demostración.

$$\begin{aligned}
F(T_a(x))(n) &= \sum_{k=0}^{N-1} x_{k-a} e^{2\pi i \frac{kn}{N}} = \sum_{k=0}^{N-1} x_k e^{2\pi i \frac{(k+a)n}{N}} \\
&= e^{\frac{2\pi i a n}{N}} \sum_{k=0}^{N-1} x_k e^{2\pi i \frac{kn}{N}} = e^{\frac{2\pi i a n}{N}} F(x)(n)
\end{aligned} \quad (2.17)$$

$$F(D_a(x))(n) = \sum_{k=0}^{N-1} x(ak)e^{2\pi i \frac{kn}{N}} = \sum_{k=0}^{N-1} x_k e^{-\frac{2\pi i n a^{-1} k}{N}} = F(x)(a^{-1}n) = D_{a^{-1}}F(x)(n) \quad (2.18)$$

■

2.5. La gaussiana discreta (función propia de la TFD)

Es bien conocido que la función gaussiana $\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}$ es una función propia de la transformada de Fourier usual. En esta sección discutiremos su análoga discreta $h_N(k)$.

Definición 2.5.1 Para cualquier entero a , no divisible por un primo impar N , el símbolo de Legendre $\left(\frac{a}{N}\right)$ se define como

$$\left(\frac{a}{N}\right) = \begin{cases} 1 & \text{si } b^2 = a \text{ modulo } N, \text{ para algún } b \in \mathbb{Z}_N \\ -1 & \text{en otro caso} \end{cases} \quad (2.19)$$

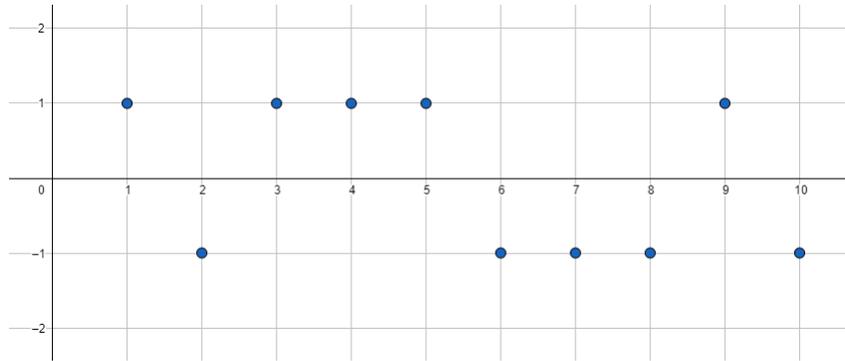


Figura 2.1: Símbolo de Legendre N=11

Proposición 2.5.2 (Criterio de Euler, ver [2]) Sean $a \in \mathbb{N}$ y N un primo impar que no es divisor de a , entonces

$$\left(\frac{a}{N}\right) = a^{\frac{N-1}{2}} \quad (2.20)$$

Demostración. Como \mathbb{Z}_N es un campo, cada polinomio de grado k tiene a lo más k raíces. En particular la ecuación $x^2 = a \pmod{N}$ tiene a lo más dos soluciones para cada a . Entonces además de 0, hay a lo más $\frac{N-1}{2}$ residuos cuadráticos módulo N . Pues cada uno de los $N-1$ posibles valores de x puede ir acompañado sólo de un valor más, distinto de x , con el mismo residuo módulo N .

Nótese que $(N - x)^2 = x^2 \pmod{N}$, pues $(N - x)^2 - x^2 = N(N - 2x)$. Entonces los $\frac{N-1}{2}$ residuos cuadráticos son: $1^2, 2^2, \dots, \left(\frac{N-1}{2}\right)^2, \pmod{N}$.

Por el pequeño teorema de Fermat, como N es primo, $a^{N-1} = 1, \pmod{N}$, es decir,

$$\left(a^{\frac{N-1}{2}} - 1\right)\left(a^{\frac{N-1}{2}} + 1\right) = 0 \quad (2.21)$$

Si a es residuo cuadrático, digamos $a = b^2, \pmod{N}$, entonces $a^{\frac{N-1}{2}} = b^{N-1} = 1, \pmod{N}$, nuevamente por el pequeño teorema de Fermat. Es decir cada residuo cuadrático anula al primer factor en (2.21). El resto de los residuos deben anular al segundo factor, pues en otro caso no se cumpliría el pequeño teorema de Fermat, entonces $a^{\frac{N-1}{2}} = -1$ si a no es residuo cuadrático. Podemos concluir que

$$a^{\frac{N-1}{2}} = \left(\frac{a}{N}\right) \quad (2.22)$$

■

Demostremos ahora algunos resultados concernientes a la transformada de Fourier discreta del símbolo de Legendre como función de su numerador que llamaremos función gaussiana discreta. Iniciamos con una definición.

Definición 2.5.3 Sea N un primo impar, defínase para cada k entero,

$$h_N(k) = \begin{cases} \left(\frac{k}{N}\right) & \text{si } N \text{ no divide a } k \\ 0 & \text{si } N \text{ divide a } k \end{cases} \quad (2.23)$$

y el correspondiente vector h_N con coordenadas $h_N(k)$, mediante $h_N = \sum_{k=0}^{N-1} h_N(k)e_k$, con $(e_k)_{1 \leq k \leq N}$ la base canónica de \mathbb{C}^N .

Lema 2.5.4 Para cualquier $a, b \in \mathbb{Z}$, si N no es divisor de a ni de b , entonces se cumple que

$$\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right) \quad (2.24)$$

Demostración. Por el criterio de Euler tenemos que

$$\left(\frac{ab}{N}\right) = (ab)^{\frac{N-1}{2}} = (a)^{\frac{N-1}{2}}(b)^{\frac{N-1}{2}} = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right) \quad (2.25)$$

■

Lema 2.5.5 Para N primo impar y N, k primos relativos se cumple que

$$\left(\frac{k}{N}\right) = \left(\frac{k^{-1}}{N}\right) \quad (2.26)$$

modulo N

Demostración. Como k no es divisible por N , entonces k tiene inverso en \mathbb{Z}_N , i.e., existe $k^{-1} \in \mathbb{Z}_N$ y $kk^{-1} = 1$. Ahora si $b^2 = k \pmod N$ tenemos que

$$1 = \left(\frac{kk^{-1}}{N}\right) = \left(\frac{k}{N}\right)\left(\frac{k^{-1}}{N}\right) = 1\left(\frac{k^{-1}}{N}\right) = \left(\frac{k^{-1}}{N}\right) \quad (2.27)$$

Si k no es residuo cuadrático y no es divisible por N , tenemos que $\left(\frac{k}{N}\right) = -1$ y consecuentemente

$$1 = \left(\frac{kk^{-1}}{N}\right) = \left(\frac{k}{N}\right)\left(\frac{k^{-1}}{N}\right) = -1\left(\frac{k^{-1}}{N}\right) \quad (2.28)$$

Por lo tanto,

$$\left(\frac{k^{-1}}{N}\right) = -1$$

Esto demuestra el lema. ■

Lema 2.5.6

$$F(h_N)(-k) = h_N(k)F(h_N)(-1) \quad (2.29)$$

Demostración. Tenemos que

$$\begin{aligned} F(h_N) &= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_n\rangle \langle e_{n'}| \sum_{l=0}^{N-1} h_N(l) e_l \\ &= \frac{1}{\sqrt{N}} \sum_{n,n',l=0}^{N-1} \zeta_N^{nn'} h_N(l) \langle e_{n'}, e_l \rangle e_n = \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} h_N(n') e_n \end{aligned} \quad (2.30)$$

lo cual implica que $F(h_N)(n) = \frac{1}{\sqrt{N}} \sum_{n'=0}^{N-1} \zeta_N^{nn'} h_N(n')$ para cada $n \in \mathbb{Z}$. Entonces si N no divide a k , por el lema 2.5.5

$$\begin{aligned} F(h_N)(-k) &= \frac{1}{\sqrt{N}} \sum_{n'=0}^{N-1} \zeta_N^{-kn'} h_N(n') = \frac{1}{\sqrt{N}} \sum_{n'=0}^{N-1} \zeta_N^{-kn'} \left(\frac{n'}{N}\right), \text{ con } b = kn', \\ &= \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} \zeta_N^{-b} \left(\frac{bk^{-1}}{N}\right) = \left(\frac{k^{-1}}{N}\right) \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} \zeta_N^{-b} \left(\frac{b}{N}\right) \\ &= h_N(k)F(h_N)(-1) \end{aligned} \quad (2.31)$$

pues N no divide a n' ni a kn' si $0 \leq n' \leq N-1$. Ahora, si N divide a k

$$\begin{aligned} F(h_N)(-k) &= \frac{1}{\sqrt{N}} \sum_{n'=0}^{N-1} \zeta_N^{-kn'} h_N(n') \\ &= \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} \zeta_N^{-b} h_N(k^{-1}b) = 0 \end{aligned} \quad (2.32)$$

pues N divide a cada $b = kn'$. Esto completa la demostración. ■

Teorema 2.5.7 *La función h_N es una función propia de la transformada de Fourier discreta, de hecho,*

$$F(h_N) = g^{-1}h_N \quad (2.33)$$

donde g es la suma de Gauss $g = F(h_N)(-1) = \sum_{a=1}^{N-1} \left(\frac{a}{N}\right)\zeta_N^a$, que satisface $g^2 = (-1)^{\frac{N-1}{2}}$, i.e.,

$$g = \begin{cases} \pm 1 & \text{si } \frac{N-1}{2} \text{ es par} \\ \pm i & \text{si } \frac{N-1}{2} \text{ es impar} \end{cases} \quad (2.34)$$

Demostración. Tomando transformada de Fourier discreta en (2.29) y usando la fórmula de inversión en la Proposición 2.8 se obtiene que

$$h_N(k) = F(F(h_N))(-k) = F(h_N)(-1)F(h_N)(k) = gF(h_N)(k), \quad \forall k \quad (2.35)$$

Ahora, evaluando (2.35) en $k = -1$ se obtiene que $h_N(-1) = g^2$. Recordando que

$$h_N(-1) = \left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}$$

la última identidad es por el Criterio de Euler, se concluye que $g^2 = (-1)^{\frac{N-1}{2}}$ y termina la demostración. ■

Con un poco de más trabajo usando estas y otras propiedades de la gaussiana discreta h_N , se puede demostrar la bien conocida ley de reciprocidad cuadrática. Pero esto queda fuera de los objetivos de este trabajo. El lector interesado puede consultar la referencia [4].

2.6. Ejemplos

Ejemplo 2.6.1 *Sea $x : \mathbb{Z}_N \mapsto \mathbb{C}$ tal que $x_n = 1$, $0 \leq n \leq N$, entonces se cumple que $F(x) = \sqrt{N}e_0$*

$$F(x) = \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n | x = \sqrt{N}e_0 \quad (2.36)$$

Demostración. Tomemos $x_n = 1$ para toda $n = 0, 1, 2, \dots, N-1$

$$\begin{aligned} \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n | x &= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_{n'}\rangle \langle e_n, x \rangle \\ &= \frac{1}{\sqrt{N}} \sum_{n'=0}^{N-1} \left(\sum_{n=0}^{N-1} \zeta_N^{nn'} \right) e_{n'} = \frac{1}{\sqrt{N}} \sum_{n'=0}^{N-1} N \delta_{n',0} e_{n'} \\ &= \sqrt{N}e_0 \end{aligned} \quad (2.37)$$

■

Ejemplo 2.6.2 Si $a : \mathbb{Z}_N \mapsto \mathbb{C}$ tal que $a_k = e^{\frac{2\pi i a k}{N}} = \zeta_N^{ak}$, $a = 0, 1, \dots, (N-1)$ se cumple que $F(a) = \sqrt{N}e_a$

Demostración.

$$\begin{aligned} F(a) &= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_n\rangle \langle e_{n'}| a = \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_n\rangle \langle e_{n'}, a \rangle = \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} \zeta_N^{an'} \\ &= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{n'=0}^{N-1} \zeta_N^{(n-a)n'} e_n = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} N \delta_{n,a} e_n = \sqrt{N} e_a \end{aligned} \quad (2.38)$$

■

Ejemplo 2.6.3 Si $\delta_a : \mathbb{Z}_N \mapsto \mathbb{C}$ tal que $\delta_a(k) = \delta_{a,k}$, $a, k = 0, 1, \dots, (N-1)$ se cumple que $F(\delta_a) = \frac{1}{\sqrt{N}} \mathbf{a}$, con $\mathbf{a}_n = \zeta_N^{an}$, $k = 0, \dots, N-1$.

Demostración.

$$\begin{aligned} F(\delta_a) &= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_n\rangle \langle e_{n'}| \delta_a = \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_n\rangle \langle e_{n'}, \delta_a \rangle \\ &= \frac{1}{\sqrt{N}} \sum_{n,n'=0}^{N-1} \zeta_N^{nn'} |e_n\rangle \delta_{a,n'} = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \zeta_N^{na} e_n = \mathbf{a} \end{aligned} \quad (2.39)$$

■

Ejemplo 2.6.4 Si $x = \frac{1}{2}(\delta_1 + \delta_{-1}) : \mathbb{Z}_N \mapsto \mathbb{C}$, se cumple que $F(x)(k) = \frac{1}{\sqrt{N}} \cos \frac{2\pi k}{N}$.

Demostración.

$$\begin{aligned} F(x)(k) &= \frac{1}{2\sqrt{N}} (1 + (-1)^k) = \frac{1}{2\sqrt{N}} (\zeta_N^{1k} + \delta_N^{(-1)k}) \\ &= \frac{1}{2\sqrt{N}} (e^{\frac{2\pi i 1k}{N}} + e^{\frac{2\pi i (-1)k}{N}}) = \frac{1}{\sqrt{N}} \cos\left(\frac{2\pi k}{N}\right) \end{aligned} \quad (2.40)$$

■

Ejemplo 2.6.5 Si $x = \frac{1}{3}(\delta_1 + \delta_{-1} + \delta_0) : \mathbb{Z}_N \mapsto \mathbb{C}$, se cumple que $F(x)(k) = \frac{1}{3\sqrt{N}}(1 + 2 \cos \frac{2\pi k}{N})$.

Demostración.

$$\begin{aligned}
 F(x)(k) &= \frac{1}{3\sqrt{N}}(1 + (-1) + 0) = \frac{1}{3\sqrt{N}}(\zeta_N^{1k} + \zeta_N^{(-1)k} + \zeta_N^{(0)k}) \\
 &= \frac{1}{3\sqrt{N}}(e^{\frac{2\pi i 1k}{N}} + e^{\frac{2\pi i (-1)k}{N} + 1}) = \frac{1}{3\sqrt{N}}(1 + 2 \cos(\frac{2\pi k}{N}))
 \end{aligned} \tag{2.41}$$

■

Ejemplo 2.6.6 Si $x = \frac{1}{2}(\delta_1 + \delta_0) : \mathbb{Z}_N \mapsto \mathbb{C}$, se cumple que $F(x)(k) = \frac{1}{\sqrt{N}}e^{\frac{2\pi i k}{N}} \cos \frac{\pi k}{N}$.

Demostración.

$$\begin{aligned}
 F(x)(l) &= \frac{1}{2\sqrt{N}}(1 + 0) = \frac{1}{2\sqrt{N}}(\zeta_N^{1l} + \zeta_N^{(0)k}) \\
 &= \frac{1}{2\sqrt{N}}(e^{\frac{2\pi i 1l}{N}} + e^{\frac{2\pi i (-0)l}{N}}) = \frac{1}{\sqrt{N}}e^{\frac{2\pi i l}{N}} \cos \frac{2\pi l}{N}
 \end{aligned} \tag{2.42}$$

■

Capítulo 3

La transformada de Fourier discreta generalizada

Sean E_N, E_M subespacios mutuamente ortogonales del espacio de Hilbert \mathbb{C}^{N+M} , con dimensiones $\dim E_M = M \leq N = \dim E_N$. Sean $(e_n)_{n=0}^{N-1}$ y $(f_m)_{m=0}^{M-1}$ bases ortonormales de E_N y E_M , respectivamente.

Una proyección ortogonal es una transformación lineal P que es autoadjunta, i.e., $\langle x, Py \rangle = \langle Px, y \rangle$ que satisface la identidad $P^2 = P$.

Sea P una proyección ortogonal y sea $E = \text{Ran}P = \{Px : x \in \mathbb{C}^{N+M}\}$ su rango. E es un subespacio de \mathbb{C}^{N+M} , pues $0 = P0 \in E$ y $Px + \alpha Py = P(x + \alpha y) \in E$. El complemento ortogonal de un subespacio E es el subespacio E^\perp definido mediante

$$E^\perp := \{x \in \mathbb{C}^{N+M} : \langle x, y \rangle = 0, \forall y \in E\}$$

Si P es una proyección ortogonal y $E = \text{Ran}P$, para cada $x \in \mathbb{C}^{N+M}$, se tiene $Px \in E$ y $x - Px \in E^\perp$, pues para cada $y \in E$ tenemos que

$$\langle x - Px, y \rangle = \langle x, y \rangle - \langle x, Py \rangle = 0 \quad (3.1)$$

En particular los vectores Px y $x - Px$ son mutuamente ortogonales y se tiene la descomposición ortogonal $x = Px + (x - Px)$, i.e., podemos escribir $I = P + (I - P)$. De ahora en adelante, si P es una proyección ortogonal y $E = \text{Ran}P$ es su rango, la denotaremos mediante el símbolo P_E . Así por ejemplo, P_N y P_M , denotarán las proyecciones ortogonales de \mathbb{C}^{N+M} sobre los subespacios E_N y E_M , respectivamente, como $\mathbb{C}^{N+M} = E_N + E_M$ y $E_N \perp E_M$, tenemos que $E_M = I - E_N = E_{N^\perp}$.

3.1. Definición y propiedades básicas

Definición 3.1.1 La transformada de Fourier discreta generalizada (TFDG) se define como la transformación lineal $Z_{N,M} : E_N \rightarrow E_M$ dada por

$$Z_{N,M} = \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} |f_m\rangle \langle e_n| \quad (3.2)$$

donde, como en el capítulo anterior, $\zeta_N = e^{\frac{2i\pi}{N}}$.

Consecuentemente, si $x \in E_N$, $x = \sum_{n=0}^{N-1} x_n e_n$, entonces

$$\begin{aligned} Z_{N,M}(x) &= \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} |f_m\rangle \langle e_n | \sum_{n'=0}^{N-1} x_{n'} e_{n'} \\ &= \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n,n'=0}^{N-1} \zeta_N^{mn} x_{n'} \delta_{nn'} f_m = \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} x_n f_m \end{aligned} \quad (3.3)$$

Esto significa que

$$Z_{N,M}(x)(m) = \sum_{n=0}^{N-1} \zeta_N^{mn} x_n$$

Proposición 3.1.2 *La TFDG $Z_{N,M}$ es lineal*

Demostración. Usando (3.3) se ve que

$$\begin{aligned} Z_{N,M}(x + \alpha y) &= \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} (x_n + \alpha y_n) f_m \\ &= \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} x_n f_m + \alpha \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} y_n f_m \\ &= Z_{N,M}x + \alpha Z_{N,M}y \end{aligned} \quad (3.4)$$

■

Proposición 3.1.3 *Se cumplen las siguientes relaciones*

(i) $Z_{N,N} = F_N$

(ii) $Z_{N,M}^2 = 0$ y $Z_{N,M}^{*2} = 0$, donde $Z_{N,M}^* x = \sum_{n'=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{-mn'} x_m e_{n'}$

(iii) $P_M Z_{N,M} = Z_{N,M}$ y $Z_{N,M} P_N = Z_{N,M}$

Demostración. Inmediatamente de la definición de $Z_{N,M}$ se obtiene (i) tomando $N = M$.

Nótese que

$$\begin{aligned} \langle x, Z_{N,M} y \rangle &= \left\langle \sum_{n=0}^{N-1} x_n e_n + \sum_{m'=0}^{M-1} x_{m'} f_{m'}, \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n'=0}^{N-1} \zeta_N^{mn'} y_{n'} f_m \right\rangle \\ &= \sum_{n'=0}^{N-1} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn'} \bar{x}_n y_{n'} \langle e_n, f_m \rangle + \sum_{m=0}^{M-1} \sum_{m'=0}^{M-1} \sum_{n'=0}^{N-1} \zeta_N^{mn'} \bar{x}_{m'} y_{n'} \langle f_{m'}, f_m \rangle \\ &= \sum_{m=0}^{M-1} \sum_{n'=0}^{N-1} \zeta_N^{mn'} \bar{x}_m y_{n'} = \sum_{m=0}^{M-1} \sum_{n'=0}^{N-1} \zeta_N^{mn'} \bar{x}_m \langle e_{n'}, y \rangle = \left\langle \sum_{n'=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{-mn'} x_m e_{n'}, y \right\rangle \\ &= \langle Z_{N,M}^* x, y \rangle \end{aligned} \quad (3.5)$$

Podemos concluir que $Z_{N,M}^*x = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{-mn} x_m e_n$. Ahora, para cada $x \in \mathbb{C}^{N+M}$ tenemos que

$$Z_{N,M}^{*2}x = \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{-mn} x_m Z_{N,M}^* e_n = 0 \quad (3.6)$$

De manera similar se demuestra que $Z_{N,M}^2 = 0$. Eso demuestra (ii).

Finalmente,

$$\begin{aligned} P_M Z_{N,M} &= \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} x_n P_M f_m = \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n,n'=0}^{N-1} \zeta_N^{mn} x_{n'} \delta_{nn'} f_m \\ &= \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} x_n f_m = Z_{N,M} \end{aligned} \quad (3.7)$$

De manera similar se demuestra la segunda identidad en (iii). Esto concluye la demostración. ■

3.2. El Teorema de Parseval

Una isometría parcial U_D actuando en \mathbb{C}^{N+M} es un operador lineal singular, cuyo kernel $K = K(U_D)$ coincide con el complemento ortogonal de su rango, i.e. $K = U_D(\mathbb{C}^{N+M})^\perp$. La TFDG $Z_{N,M}$ se puede extender a una transformación lineal de \mathbb{C}^{N+M} en sí mismo definiéndola como cero en $E_N^\perp = E_M$. Abusando de la notación pero sin causar confusión, denotaremos con el mismo símbolo a esta extensión de $Z_{N,M}$.

Recordemos que la adjunta de una transformación lineal T de \mathbb{C}^{N+M} en sí mismo, es la transformación lineal T^* definida mediante la relación

$$\langle x, Ty \rangle = \langle T^*x, y \rangle, \quad \forall x, y \in \mathbb{C}^{N+M}$$

Denotaremos mediante $|Z_{N,M}|$ al operador $|Z_{N,M}| = Z_{N,M}^* Z_{N,M}$.

Proposición 3.2.1 (i) $Z_{N,M} Z_{N,M}^* = P_M$ la proyección ortogonal de \mathbb{C}^{N+M} sobre E_M .

(ii) $|Z_{N,M}|$ es una proyección ortogonal y $|Z_{N,M}| \leq P_N$ con igualdad si y sólo si $N = M$, i.e., $|Z_{N,M}|$ es una subproyección de P_N .

Demostración.

$$\begin{aligned}
 Z_{N,M}Z_{N,M}^* &= \frac{1}{N} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{mn} |f_m\rangle \langle e_n| \sum_{n'=0}^{N-1} \sum_{m'=0}^{M-1} \zeta_N^{-m'n'} |e_{n'}\rangle \langle f_{m'}| \\
 &= \frac{1}{N} \sum_{n,n'=0}^{N-1} \sum_{m,m'=0}^{M-1} \zeta_N^{mn-m'n'} \delta_{nn'} |f_m\rangle \langle f_{m'}| \\
 &= \frac{1}{N} \sum_{n=0}^{N-1} \sum_{m,m'=0}^{M-1} \zeta_N^{(m-m')n} |f_m\rangle \langle f_{m'}| = \frac{1}{N} \sum_{m,m'=0}^{M-1} N \delta_{m,m'} \\
 &= \sum_{m=0}^{M-1} |f_m\rangle \langle f_m| = P_M
 \end{aligned} \tag{3.8}$$

Esto demuestra el inciso (i).

Ahora, $|Z_{N,M}|^* = (Z_{N,M}^* Z_{N,M})^* = Z_{N,M}^* Z_{N,M} = |Z_{N,M}|$, entonces $|Z_{N,M}|$ es autoadjunto. Por otra parte,

$$\begin{aligned}
 |Z_{N,M}|^2 &= (Z_{N,M}^* Z_{N,M})^2 = Z_{N,M}^* Z_{N,M} Z_{N,M}^* Z_{N,M} = Z_{N,M}^* P_M Z_{N,M} = Z_{N,M}^* Z_{N,M} \\
 &= |Z_{N,M}|
 \end{aligned} \tag{3.9}$$

Entonces $|Z_{N,M}|$ es una proyección ortogonal. Pero $P_N - |Z_{N,M}|$ es autoadjunto y además

$$\begin{aligned}
 (P_N - |Z_{N,M}|)^2 &= (P_N - Z_{N,M}^* Z_{N,M})^2 \\
 &= P_N^2 + (Z_{N,M}^* Z_{N,M})^2 - P_N Z_{N,M}^* Z_{N,M} - Z_{N,M}^* Z_{N,M} P_N \\
 &= P_N + Z_{N,M}^* Z_{N,M} - (Z_{N,M} P_N)^* Z_{N,M} - Z_{N,M}^* Z_{N,M} \\
 &= P_N + Z_{N,M}^* Z_{N,M} - 2Z_{N,M}^* Z_{N,M} \\
 &= P_N - Z_{N,M}^* Z_{N,M} = P_N - |Z_{N,M}| \geq 0
 \end{aligned} \tag{3.10}$$

Entonces $|Z_{N,M}|$ es una subproyección de P_N . Esto concluye la demostración. \blacksquare

Demostraremos un resultado que generaliza al teorema de Parseval 2.3.1. Para esto necesitamos definir una base ortonormal distinguida, llamada base ortonormal de vectores de máximo entrelazamiento y demostrar un lema.

Definición 3.2.2 *Los vectores de máximo entrelazamiento $\varphi_n \in E_N$ se obtienen como la transformada inversa de Fourier de los vectores básicos, i.e.,*

$$\varphi_n = F_N^* e_n = \frac{1}{\sqrt{N}} \sum_{n'=0}^{N-1} \zeta_N^{-nn'} e_{n'} \tag{3.11}$$

Lema 3.2.3 (i) *El conjunto de vectores de máximo entrelazamiento es una base ortonormal de E_N .*

(ii) $\ker |Z_{N,M}| = \ker Z_{N,M} = \text{Span}\{\varphi_n : M \leq n \leq N-1\}$

Demostración. Como la transformada de Fourier es un operador unitario, el inciso (i) se sigue inmediatamente de esta propiedad.

Ahora, mediante cálculos directos se obtiene que

$$\begin{aligned}
Z_{N,M}F_N^* &= Z_{N,M} = \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} |f_m\rangle \langle e_n| \frac{1}{\sqrt{N}} \sum_{n',n''=0}^{N-1} \zeta_N^{-n'n''} |e_{n''}\rangle \langle e_{n'}| \\
&= \frac{1}{N} \sum_{m=0}^{M-1} \sum_{n,n',n''=0}^{N-1} \zeta_N^{mn-n'n''} \delta_{nn''} |f_m\rangle \langle e_{n'}| = \frac{1}{N} \sum_{m=0}^{M-1} \sum_{n,n'=0}^{N-1} \zeta_N^{n(m-n')} |f_m\rangle \langle e_{n'}| \quad (3.12) \\
&= \sum_{m=0}^{M-1} \sum_{n'=0}^{N-1} \delta_{m,n'} |f_m\rangle \langle e_{n'}| = \sum_{m=0}^{M-1} |f_m\rangle \langle e_m|
\end{aligned}$$

Consecuentemente,

$$Z_{N,M}\varphi_n = Z_{N,M}F_N^*e_n = \sum_{m=0}^{M-1} |f_m\rangle \langle e_m|e_n = \begin{cases} f_n & \text{si } 0 \leq n \leq M-1 \\ 0 & \text{si } M \leq n \leq N-1 \end{cases} \quad (3.13)$$

Esto demuestra la segunda identidad del inciso (ii). Por otra parte, la desigualdad $\ker Z_{N,M} \subset \ker |Z_{N,M}|$ es inmediata y por el inciso (ii) de la proposición 3.2.1 junto con el inciso (iii) de la Proposición 3.1.3, si $u \in \ker |Z_{N,M}|$ entonces

$$0 = Z_{N,M}Z_{N,M}^*Z_{N,M}u = P_M Z_{N,M}u = Z_{N,M}u$$

Esto completa la demostración del lema. ■

Teorema 3.2.4 (*Parseval generalizado*)

Los operadores $Z_{N,M}$ y $Z_{N,M}^*$ son isomorfismos isométricos que preservan el producto interno entre los subespacios $\text{Ran}|Z_{N,M}| \subset E_N$ y E_M .

Demostración. De la ecuación (3.13) se obtiene que $Z_{N,M}\varphi_n = f_n$ si $0 \leq n \leq M-1$. Multiplicando en ambos lados por $Z_{N,M}^*$ se obtiene que

$$Z_{N,M}^*f_n = Z_{N,M}^*Z_{N,M}\varphi_n = |Z_{N,M}|\varphi_n = \varphi_n$$

pues $|Z_{N,M}|$ es una proyección. Esto demuestra que la base ortonormal de E_M es enviada por $Z_{N,M}^*$ en una base ortonormal de $\text{Ran}|Z_{N,M}| = \text{Span}\{\varphi_n : 0 \leq n \leq M-1\}$, i.e., $Z_{N,M}^*$ es una isometría que preserva el producto interno entre estos subespacios. ■

Salvo isomorfismo, el teorema anterior se reduce al teorema de Parseval 2.3.1 en el caso cuando $N = M$.

Proposición 3.2.5 *La transformada de Fourier generalizada cumple con*

$$\begin{aligned}
 |Z_{N,M}| &= \sum_{b=0}^{M-1} |\varphi_{bN}\rangle \langle \varphi_{bN}| \\
 |Z_{N,M}|^\perp &= \sum_{n=M}^{N-1} |\varphi_{bN}\rangle \langle \varphi_{bN}|
 \end{aligned} \tag{3.14}$$

Demostración. Por la proposición (3.2.1) y la ecuación (3.2.3) tenemos que

$$\begin{aligned}
 |Z_{N,M}|^\perp &= \frac{1}{N} \sum_{a,a'=0}^{N-1} \sum_{b=k}^{N-1} \zeta_N^{b(a-a')} |a'_N\rangle \langle a_N| = \frac{1}{N} \sum_{a,a'=0}^{N-1} \sum_{b=k}^{N-1} \zeta_N^{ba} \zeta_N^{-ba'} |a'_N\rangle \langle a_N| \\
 &= \frac{1}{N} \sum_{b=k}^{N-1} \left| \sum_{a'=0}^{N-1} \zeta_N^{-ba'} a'_N \right\rangle \left\langle \sum_{a=0}^{N-1} \zeta_N^{-ba} a_N \right| = \sum_{b=k}^{M-1} |\varphi_{bN}\rangle \langle \varphi_{bN}|
 \end{aligned} \tag{3.15}$$

Así

$$|Z_{N,M}| = P_N - |Z_{N,M}|^\perp = \sum_{b=0}^{k-1} |\varphi_{bN}\rangle \langle \varphi_{bN}| \tag{3.16}$$

■

3.3. Fórmulas de convolución, traslación y dilatación

Teorema 3.3.1 *La TFDG satisface la propiedad de convolución*

$$Z_{N,M}(x * y) = Z_{N,M}(x) Z_{N,M}(y) \tag{3.17}$$

Demostración.

$$\begin{aligned}
 Z_{N,M}(x * y) &= \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} |f_m\rangle \langle e_n| \left(\sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} x(l)y(k-l) \right) e_k \right) \\
 &= \frac{1}{N} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} \zeta_N^{mn} \left(\sum_{l=0}^{N-1} x(l)y(k-l) \right) \delta_{nk} f_m \\
 &= \frac{1}{N} \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \zeta_N^{mn} \left(\sum_{l=0}^{N-1} x(l)y(n-l) \right) f_m = \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \sum_{n'=0}^{N-1} \sum_{l=0}^{N-1} \zeta_N^{m(n'+l)} x(l)y(n') f_m \\
 &= \frac{1}{N} \sum_{m=0}^{M-1} \sum_{l=0}^{N-1} \zeta_N^{ml} x(l) \sum_{n'=0}^{N-1} \zeta_N^{mn'} y(n') f_m = \sum_{m=0}^{M-1} Z_{N,M}(x)(m) Z_{N,M}(y)(m) f_m
 \end{aligned} \tag{3.18}$$

Entonces, $Z_{N,M}(x * y)(m) = (Z_{N,M}(x) Z_{N,M}(y))(m)$ para cada $0 \leq m \leq M-1$. Esto termina la demostración. ■

Proposición 3.3.2 *La transformada satisface las siguientes fórmulas de traslación y dilatación, respectivamente*

(i) **(Traslación)** *Si para cada $x \in \mathbb{C}^N$ definimos su trasladado por $a \in \mathbb{Z}_N$ mediante $T_a(x)(k) = x(k - a)$, $k \in \mathbb{Z}_N$, entonces*

$$Z_{N,M}(T_a(x))(m) = e^{\frac{2\pi i a m}{N}} Z_{N,M}(x)(m)$$

(ii) **(Dilatación)** *Si para cada $x \in \mathbb{C}^N$ definimos su dilatación por $a \in \mathbb{Z}_N$ mediante $D_a(x)(k) = x(ak)$, $k \in \mathbb{Z}_N$, entonces*

$$Z_{N,M}(D_a(x))(m) = D_{a^{-1}}(Z_{N,M}x)(m)$$

Demostración.

$$\begin{aligned} Z_{N,M}T_a(x)(m) &= \sum_{n=0}^{N-1} e^{\frac{2i\pi mn}{N}} T_a(x)_n = \sum_{n=0}^{N-1} e^{\frac{2i\pi mn}{N}} x_{n-a} \\ &= \sum_{n'=0}^{N-1} e^{\frac{2i\pi m(n'+a)}{N}} x_{n'} = e^{\frac{2i\pi a m}{N}} Z_{N,M}(x)(m) \end{aligned} \quad (3.19)$$

$$Z_{N,M}(D_a(x))(m) = \sum_{n=0}^{N-1} e^{\frac{2i\pi mn}{N}} x_{an} = \sum_{n'=0}^{N-1} e^{\frac{2i\pi a^{-1} m n'}{N}} x_{n'} = D_{a^{-1}}(Z_{N,M}x)(m) \quad (3.20)$$

■

3.4. Ejemplos

Ejemplo 3.4.1 *Sea $x : E_N \rightarrow \mathbb{C}$ tal que $x_n = 1$, $0 \leq n \leq N$, entonces se cumple que $Z_{N,M}(x) = \sqrt{N} f_0$*

Demostración. Tomemos $x_n = 1$ para toda $n = 0, 1, 2, \dots, N - 1$

$$\begin{aligned} \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{nm} |f_m\rangle \langle e_n | x &= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{nm} |f_m\rangle \langle e_n, x \rangle \\ &= \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \left(\sum_{n=0}^{N-1} \zeta_N^{nm} \right) f_m = \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} N \delta_{m,0} f_m \\ &= \sqrt{N} f_0 \end{aligned} \quad (3.21)$$

■

Ejemplo 3.4.2 Si $a : E_N \mapsto \mathbb{C}$ tal que $a_k = e^{\frac{2\pi i a k}{N}} = \zeta_N^{ak}$, $k = 0, 1, \dots, (N-1)$ se cumple que $Z_{N,M}(a) = \sqrt{N} f_a$

Demostración.

$$\begin{aligned} Z_{N,M} &= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{nm} |f_m\rangle \langle e_n | a = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{nm} |f_m\rangle \langle e_n, a \rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{nm} \zeta_N^{an} f_m \\ &= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{(m-a)n} f_m = \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} N \delta_{m,a} f_m = \sqrt{N} f_a \end{aligned} \quad (3.22)$$

■

Ejemplo 3.4.3 Si $\delta_a : E_N \mapsto \mathbb{C}$ tal que $\delta_a(k) = \delta_{a,k}$, $a, k = 0, 1, \dots, (N-1)$ se cumple que $Z_{N,M}(\delta_a) = \mathbf{a}$, con $\mathbf{a}_m = \frac{1}{\sqrt{N}} \zeta_N^{am}$, $m = 0, \dots, M-1$.

Demostración.

$$\begin{aligned} Z_{N,M}(\delta_a) &= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{nm} |f_m\rangle \langle e_n | \delta_a = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{nm} |f_m\rangle \langle e_n, \delta_a \rangle \\ &= \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{m=0}^{M-1} \zeta_N^{nm} |f_m\rangle \delta_{a,n} = \frac{1}{\sqrt{N}} \sum_{m=0}^{M-1} \zeta_N^{ma} f_m = \mathbf{a} \end{aligned} \quad (3.23)$$

■

Ejemplo 3.4.4 Si $x = \frac{1}{2}(\delta_1 + \delta_{-1}) : E_N \mapsto \mathbb{C}$, se cumple que

$$Z_{N,M}(x)(l) = \frac{1}{\sqrt{N}} \cos \frac{2\pi l}{N}, \quad 0 \leq l \leq M-1. \quad (3.24)$$

Demostración. Si $0 \leq l \leq M-1$ entonces (3.23) implica

$$\begin{aligned} Z_{N,M}(x)(l) &= \frac{1}{2\sqrt{N}} (\zeta_N^l + \zeta_N^{-l}) \\ &= \frac{1}{2\sqrt{N}} (e^{\frac{2\pi i l}{N}} + e^{-\frac{2\pi i l}{N}}) = \frac{1}{\sqrt{N}} \cos\left(\frac{2\pi l}{N}\right) \end{aligned} \quad (3.25)$$

■

Ejemplo 3.4.5 Si $x = \frac{1}{3}(\delta_1 + \delta_{-1} + \delta_0) : E_N \mapsto \mathbb{C}$, se cumple que

$$Z_{N,M}(x)(l) = \frac{1}{3\sqrt{N}} (1 + 2 \cos \frac{2\pi l}{N}), \quad 0 \leq l \leq M-1. \quad (3.26)$$

Demostración. Si $0 \leq l \leq M - 1$ entonces (3.23) implica

$$\begin{aligned} Z_{N,M}(x)(l) &= \frac{1}{3\sqrt{N}} (\zeta_N^l + \zeta_N^{-l} + \zeta_N^{(0)l}) \\ &= \frac{1}{3\sqrt{N}} (e^{\frac{2\pi il}{N}} + e^{-\frac{2\pi il}{N}} + 1) = \frac{1}{3\sqrt{N}} (1 + 2 \cos(\frac{2\pi l}{N})) \end{aligned} \quad (3.27)$$

■

Ejemplo 3.4.6 Si $x = \frac{1}{2}(\delta_1 + \delta_0) : E_N \mapsto \mathbb{C}$, se cumple que

$$Z_{N,M}(x)(l) = \frac{1}{\sqrt{N}} e^{\frac{2\pi il}{N}} f_1 + f_0, \quad 0 \leq l \leq M - 1. \quad (3.28)$$

Demostración. Si $0 \leq l \leq M - 1$ entonces (3.23) implica

$$\begin{aligned} Z_{N,M}(x)(l) &= \frac{1}{2\sqrt{N}} (1 + 0) = \frac{1}{2\sqrt{N}} (\zeta_N^{1l} + \zeta_N^{(0)l}) \\ &= \frac{1}{2\sqrt{N}} (e^{\frac{2\pi il}{N}} + e^{\frac{2\pi i(-0)l}{N}}) = \frac{1}{\sqrt{N}} e^{\frac{2\pi il}{N}} \cos \frac{2\pi l}{N} \end{aligned} \quad (3.29)$$

■

Capítulo 4

Aplicaciones

En este capítulo seguimos la referencia [5] para mostrar la estrecha relación entre la TFD y el álgebra de las matrices circulantes. Nuestra aportación consistió en completar las demostraciones que los autores dejaron en manos del lector.

4.1. El álgebra de matrices circulantes

Definición 4.1.1 Una matriz compleja de tamaño $p \times p$, $c = (c_{ij})_{0 \leq i, j \leq p-1}$, es circulante si y sólo si $c_{ij} = c_{j-i}$, para cada $0 \leq i, j \leq p-1$, donde (c_0, \dots, c_{p-1}) es un vector en \mathbb{C}^p y las operaciones en los subíndices son módulo p , $(c_{(j-i) \bmod p})$. Es decir,

$$c = \begin{pmatrix} c_0 & c_1 & \cdots & c_{p-1} \\ c_{p-1} & c_0 & \cdots & c_{p-2} \\ \vdots & \vdots & \vdots & \vdots \\ c_1 & c_2 & \cdots & c_0 \end{pmatrix} \quad (4.1)$$

Usualmente, una matriz circulante c se denota por $c = \text{circ}(c_0, c_1, \dots, c_{p-1})$ o también mediante $c = (c_0, c_1, \dots, c_{p-1})$. Cada matriz circulante c es una combinación lineal de potencias de la matriz de permutación primaria J

$$c = \sum_{k=0}^{p-1} c_k J^k \quad (4.2)$$

con $J = \text{circ}(0, 1, 0, \dots, 0)$. Así mismo J es una combinación lineal de proyecciones de rango uno

$$J = \sum_{k=0}^{p-1} |e_k\rangle\langle e_{k+1}| \quad (4.3)$$

con $\{e_i\}_{i=0}^{p-1}$ es la base canónica de \mathbb{C}^p , con operaciones en los subíndices módulo p . El conjunto de matrices circulantes de tamaño $p \times p$, \mathcal{C}_p , tiene estructura de álgebra conmutativa sobre los complejos con las operaciones de suma y multiplicación de matrices y multiplicación por

escalares; de hecho, es un álgebra de von Neumann con la operación de involución definida como la toma de adjuntos. Mostraremos que la aplicación $c \mapsto (c_0, c_1, \dots, c_{p-1})$ define un isomorfismo del álgebra de von Neumann de las matrices circulantes en el álgebra de von Neumann $(\mathbb{C}^p, *)$, donde \mathbb{C}^p se provee con su estructura natural de espacio vectorial junto con la operación de involución consistente en inversión del orden de las coordenadas seguida de conjugación, $(c_0, c_1, \dots, c_{p-1})^* := (\overline{c_0}, \overline{c_{p-1}}, \dots, \overline{c_1})$, y la multiplicación de vectores definida mediante la convolución:

$$c * c' := ((c * c')_0, (c * c')_1, \dots, (c * c')_{p-1}) \quad (4.4)$$

con $(c * c')_i = \sum_{j=0}^{p-1} c_j c'_{i-j}$, con operaciones módulo p en los subíndices.

Proposición 4.1.2 *La aplicación ι de \mathcal{C}_p en $(\mathbb{C}^p, *)$ definida por $\iota(c) = (c_0, c_1, \dots, c_{p-1})$ es un $*$ -isomorfismo de álgebras.*

Demostración. Es claro que ι es lineal, pues si $c = (c_0, \dots, c_{p-1})$ y $d = (d_0, \dots, d_{p-1})$ son dos matrices circulantes, entonces $\iota(c + \lambda d) = (c_0 + \lambda d_0, \dots, c_{p-1} + \lambda d_{p-1}) = (c_0, \dots, c_{p-1}) + \lambda(d_0, \dots, d_{p-1}) = \iota(c) + \lambda \iota(d)$. Además

$$c^* = \left(\sum_k c_k J^k \right)^* = \sum_k \overline{c_k} J^{k*} = \sum_k \overline{c_k} J^{p-k} = \sum_k \overline{c_{p-k}} J^k = \text{circ}(\overline{c_p}, \overline{c_{p-1}}, \dots, \overline{c_1}),$$

entonces $\iota(c^*) = (\overline{c_0}, \overline{c_{p-1}}, \dots, \overline{c_1}) = \iota(c)^*$. Por otra parte, como $cd = \sum_k \left(\sum_l c_l d_{k-l} \right) J^k$, tenemos que $\iota(cd) = \left((\iota(c) * \iota(d))_0, \dots, (\iota(c) * \iota(d))_{p-1} \right) = \iota(c) * \iota(d)$. Es inyectiva pues $\iota(c) = 0$ implica que $c = \text{circ}(\iota(c)) = 0$ y es sobreyectiva por el teorema de la dimensión. Podemos concluir que es un $*$ -isomorfismo. ■

4.2. El espectro de Gelfand del álgebra circulante

Si A es un álgebra de Banach conmutativa con unidad e , se denota por $\text{hom}(A, \mathbb{C})$ al conjunto de todos los homomorfismos $w : A \mapsto \mathbb{C}$ de A en los complejos, es decir, $w \in \text{hom}(A, \mathbb{C})$ si w es un funcional lineal complejo tal que

$$w(xy) = w(x)w(y), \text{ para cada } x, y \in A. \quad (4.5)$$

El espectro de Gelfand de A se define como el conjunto

$$\text{sp}(A) = \{w \in \text{hom}(A, \mathbb{C}) : w \neq 0\} \quad (4.6)$$

de todos los homomorfismos complejos no triviales de A . En ocasiones también se le llama espacio de ideales máximos de A .

Proposición 4.2.1 *El espectro de Gelfand satisface lo siguiente:*

- i) Cada $w \in sp(A)$ satisface $w(e) = 1$.
- ii) Cada $w \in sp(A)$ es continuo, mejor aún, $\|w\| = 1$.
- iii) Para cada $w \in sp(A)$, $\ker(w)$ es un ideal de A .

Demostración. Para cada $w \in sp(A)$ tenemos que

$$w(x) = w(xe) = w(x)w(e) \quad \forall x \in A \iff w(e) = 1 \quad (4.7)$$

Sea $w \in sp(A)$ y sea $M = \ker(w)$, esto es, $M = \{x \in A : w(x) = 0\}$. Como $w(x - w(x)e) = 0$ para todo x en A , entonces cada elemento en A se puede escribir de la forma $\alpha e + x$ para algún $\alpha \in \mathbb{C}$ y $x \in M$. Entonces

$$\begin{aligned} \|w\| &= \sup_{y \neq 0} \frac{|w(y)|}{\|y\|} = \sup_{x \in M, \alpha \neq 0} \frac{|w(\alpha e + x)|}{\|\alpha e + x\|} \\ &= \sup_{x \in M, \alpha \neq 0} \frac{|\alpha e|}{\|\alpha e + x\|} = \sup_{h \in M} \frac{1}{\|e + h\|} = 1, \end{aligned} \quad (4.8)$$

lo anterior se cumple porque $\|e + h\| \geq 1$ para $h = \frac{x}{\alpha}$, pues la desigualdad $\|e + h\| < 1$ implica que h es invertible, por lo cual $h \notin M$. Por lo tanto $\|w\| = 1$ y por ende w es continua. Finalmente $\ker(w)$ es cerrado bajo sumas y producto por escalares. ■

Teorema 4.2.2 *Existe una biyección entre los subconjuntos $sp(\mathcal{C}_p)$ y $\{\xi^0, \xi, \dots, \xi^{p-1}\}$, donde ξ es una raíz primitiva de la unidad de orden p*

Demostración. Sean $w \in sp(\mathcal{C}_p)$ y J la matriz de permutación primaria. Como w es un homomorfismo, tenemos que

$$w(J^k) = w(J)^k \in \mathbb{C} \quad (4.9)$$

para todo $k \leq 0$. En particular, $w(J^p) = w(I) = 1$ y en consecuencia $w(J)^p = 1$, por lo que $w(J)$ es una raíz de la unidad de orden p . Si ξ es una raíz primitiva de orden p , existe un único $\lambda = \lambda(w)$ con $0 \leq \lambda \leq 1$ tal que $w(J) = \xi^\lambda$. Defínase $\phi : sp(\mathcal{C}_p) \mapsto \{\xi^0, \xi, \dots, \xi^{p-1}\}$, mediante $\phi(w) = \xi^\lambda$ para $w \in sp(\mathcal{C}_p)$ con $w(J) = \xi^\lambda$. La aplicación ϕ es una biyección entre $sp(\mathcal{C}_p)$ y $\{\xi^0, \xi, \dots, \xi^{p-1}\}$. Para demostrar esto nótese primero que es inyectiva. En efecto, si para $w_1, w_2 \in sp(\mathcal{C}_p)$, $\phi(w_1) = \phi(w_2)$, entonces existen únicos $0 \leq \lambda_1, \lambda_2 \leq 1$ tales que $\phi(w_1) = \xi^{\lambda_1}$, $\phi(w_2) = \xi^{\lambda_2}$ y así

$$\xi^{\lambda_1} = \xi^{\lambda_2} \iff \lambda_1 - \lambda_2 = 0 \text{ mod } p \iff \lambda_1 = \lambda_2 \iff w_1 = w_2 \quad (4.10)$$

donde hemos usado que cada λ_j , $j = 1, 2$, está asociado de manera biunívoca con su respectivo w_j . Y es sobreyectiva, ya que para cada $\xi^k \in \{\xi^0, \xi, \dots, \xi^{p-1}\}$, la aplicación $w_k : \mathcal{C}_p \mapsto \mathbb{C}$ definida para toda $c = \sum_{j=0}^{p-1} c_j J^j$ mediante $w_k(c) = \sum_{j=0}^{p-1} c_j \xi^{kj}$ define un elemento $w_k \in hom(\mathcal{C}_p, \mathbb{C})$. En efecto, sean $\alpha \in \mathbb{C}$,

$$c = \sum_{j=0}^{p-1} c_j J^j, \quad d = \sum_{j=0}^{p-1} d_j J^j \in \mathcal{C}_p \quad (4.11)$$

para la matriz circulante

$$\alpha c + d = \sum_{j=0}^{p-1} (\alpha c_j + d_j) J^j \quad (4.12)$$

se tiene que

$$w_k(\alpha c + d) = \sum_{j=0}^{p-1} (\alpha c_j + d_j) \xi^{kj} = \alpha \sum_{j=0}^{p-1} c_j \xi^{kj} + \sum_{j=0}^{p-1} d_j \xi^{kj} = \alpha w_k(c) + w_k(d) \quad (4.13)$$

Entonces w_k es un funcional. Además se observa que

$$w_k(I) = w_k(J^0) = \xi^{k0} = 1 \quad (4.14)$$

Ahora, la multiplicación de dos matrices circulantes $c, d \in \mathcal{C}_p$ es la matriz circulante

$$cd = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} c_j d_{(p-j+i)} J^i \quad (4.15)$$

Por lo tanto, como $\xi^{kp} = 1$, haciendo $m + j \cong i \pmod{p}$, equivalentemente, $m = (p - j + i) \pmod{p}$, se obtiene

$$w_k(c)w_k(d) = \sum_{m=0}^{p-1} \sum_{j=0}^{p-1} c_j d_m \xi^{k(m+j)} = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} c_j d_{(p-j+i)} \xi^{ki} = w_k(cd) \quad (4.16)$$

Lo cual demuestra que w_k es un homomorfismo no trivial, y $w_k \in \text{sp}(\mathcal{C}_p)$. Esto concluye la demostración. ■

4.3. La transformada de Gelfand del álgebra circulante

De ahora en adelante identificaremos al conjunto $\text{sp}(\mathcal{C}_p)$ con las raíces de la unidad $\{\xi^0, \xi, \dots, \xi^{p-1}\}$. Cada elemento $c \in \mathcal{C}_p$ da lugar a una función

$$\hat{c} : \{\xi^0, \xi, \dots, \xi^{p-1}\} \rightarrow \mathbb{C} \quad (4.17)$$

definida por

$$\hat{c}(\xi^k) = \sum_{j=0}^{p-1} c_j \xi^{jk}, \quad 0 \leq k \leq p-1 \quad (4.18)$$

La función \hat{c} se llama la transformada de Gelfand de c y la aplicación $c \mapsto \hat{c}$ es la transformada de Gelfand. Nótese que cada función \hat{c} se puede identificar con el vector de todos sus

valores: $\hat{c} = (\hat{c}(\xi^0), \hat{c}(\xi), \dots, \hat{c}(\xi^{p-1}))$. Esta identificación nos permite escribir a la transformada de Gelfand como una aplicación lineal $\hat{\cdot}$ que asocia con cada matriz (vector) circulante $c = (c_0, \dots, c_{p-1})$, la función (vector) $\hat{c} = (\hat{c}(\xi^0), \hat{c}(\xi), \dots, \hat{c}(\xi^{p-1}))$, de manera que

$$\hat{c} = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & \xi & \dots & \xi^{p-2} & \xi^{p-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \xi^{p-2} & \dots & \xi^{(p-2)(p-2)} & \xi^{(p-2)(p-1)} \\ 1 & \xi^{p-1} & \dots & \xi^{(p-1)(p-2)} & \xi^{(p-1)(p-1)} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{p-2} \\ c_{p-1} \end{pmatrix} \quad (4.19)$$

Es decir, la transformada de Gelfand es el operador

$$\hat{\cdot} = \sum_{0 \leq k, l \leq p-1} \xi^{kl} |e_k\rangle \langle e_l| \quad (4.20)$$

cuya matriz asociada aparece arriba. Nótese que esta transformación también es la transformada de Fourier discreta. De hecho el propósito de Gelfand al definir su transformada fue precisamente generalizar el concepto de transformada de Fourier, originalmente definida en $L_1(\mathbb{R}^n)$, al caso de álgebras conmutativas arbitrarias. Aquí observamos cómo la extensión de Gelfand se reduce al concepto original de Fourier.

4.4. Diagonalización de matrices circulantes

En esta sección demostraremos que la transformada de Fourier (2.1) diagonaliza a cualquier matriz circulante.

Proposición 4.4.1 $F^* J F = \text{diag}(\xi^0, \xi, \dots, \xi^{p-1})$ En particular, los valores propios de J son las coordenadas del vector $(\xi^0, \xi, \dots, \xi^{p-1})$. Consecuentemente, para cada matriz circulante c , $F^* c F$ es la matriz diagonal

$$F^* c F = \text{diag}(\hat{c}(\xi^0), \hat{c}(\xi), \dots, \hat{c}(\xi^{p-1})) \quad (4.21)$$

donde \hat{c} es la transformada de Gelfand de c dada por (4.18); los valores propios de c son las coordenadas del vector $\hat{c} = (\hat{c}(\xi^0), \hat{c}(\xi), \dots, \hat{c}(\xi^{p-1}))$.

Demostración. Tenemos que

$$\begin{aligned} F^* J &= \frac{1}{p} \sum_{i,j=0}^{p-1} \xi^{-ij} |e_j\rangle \langle e_i| \sum_k |e_k\rangle \langle e_{k+1}| = \frac{1}{p} \sum_{i,j,k=0}^{p-1} \xi^{-ij} \delta_{ik} |e_j\rangle \langle e_{k+1}| \\ &= \frac{1}{p} \sum_{i,j=0}^{p-1} \xi^{-ij} |e_j\rangle \langle e_{i+1}| \end{aligned} \quad (4.22)$$

de manera que

$$\begin{aligned}
F^* J F &= \frac{1}{p^2} \sum_{i,j=0}^{p-1} \xi^{-ij} |e_j\rangle \langle e_i| \sum_{i',j'=0}^{p-1} \xi^{-i'j'} |e_{j'}\rangle \langle e_{i'}| = \frac{1}{p^2} \sum_{i,j,i',j'} \xi^{i'j'-ij} \delta_{i+1,i'} |e_j\rangle \langle e_{j'}| \\
&= \frac{1}{p^2} \sum_{i,j,j'} \xi^{(i+1)j'-ij} |e_j\rangle \langle e_{j'}| = \frac{1}{p^2} \sum_{j,j'} \left(\sum_{i=0}^{p-1} \xi^{i(j'-j)} \xi^{j'} |e_j\rangle \langle e_{j'}| \right) \\
&= \frac{1}{p^2} \sum_{j,j'} \xi^{(i(j'-j)} \xi^{j'} |e_j\rangle \langle e_{j'}| = \frac{1}{p^2} \sum_{j,j'} p \delta_{jj'} \xi^{j'} |e_j\rangle \langle e_{j'}| \\
&= \frac{1}{p} \sum_{j,j'} \xi^{j'} |e_j\rangle \langle e_{j'}| = \text{diag}(\xi^0, \xi, \dots, \xi^{p-1})
\end{aligned} \tag{4.23}$$

Esto demuestra la primera afirmación de la proposición, el resto es consecuencia de la identidad

$$c = \sum_{k=0}^{p-1} c_k J^k \tag{4.24}$$

■

De acuerdo con el resultado de la proposición anterior, los valores propios (espectro) de cada matriz circulante c , se obtienen mediante los valores $\{\xi^0, \xi, \dots, \xi^{p-1}\}$ de la transformada de Gelfand en cada elemento del espectro de Gelfand $\{\hat{c}(\xi^0), \hat{c}(\xi), \dots, \hat{c}(\xi^{p-1})\}$ del álgebra circulante. Esta es una propiedad general de la transformada de Gelfand en cualquier álgebra conmutativa.

Conclusiones y perspectivas

En este trabajo hemos desarrollado una introducción a la transformada de Fourier discreta (TFD). Demostramos sus propiedades básicas de convolución, traslación, dilatación e identidad de Parseval y estudiamos una de sus eigenfunciones (Gaussiana discreta). Revisamos una generalización de esta transformada al caso de dos subespacios de Hilbert de dimensiones diferentes (TFDG), identificando sus correspondientes propiedades de convolución, traslación, dilatación e identidad de Parseval. Mostramos cómo la TFD diagonaliza simultáneamente a todos los elementos del álgebra circulante y determinamos el espectro de Gelfand de esta álgebra conmutativa.

En esta dirección se podría continuar estudiando:

1. Otras eigenfunciones de la TFD y más generalmente su teoría espectral.
2. Otras extensiones de la TFD, por ejemplo al caso de grupos no conmutativos.
3. Otras aplicaciones de la TFD y sus extensiones.

Bibliografía

- [1] Bolaños-Servín J.R., Rios-Cangas J.I. and Quezada R., *Transition Maps between Hilbert Subspaces and Quantum Energy Transport*, Open Systems & Information Dynamics Vol. 27, No. 3 (2020) 1950001 (22 pages) DOI:S1230161220500134
- [2] Dence Joseph B., Dence Thomas P., *Elements of the Theory of Numbers*. Harcourt Academic Press. p. 197, 1999, ISBN 9780122091308.
- [3] Euler Leonhard, *Theorematum quorundam ad numeros primos spectantium demonstratio*. *Commentarii academiae scientiarum Petropolitanae* 8, 1741, pp. 141-146, Reprinted in *Opera Omnia: Series 1, Volume 2*, pp. 33 - 37.
- [4] Terras Audry, *Fourier Analysis on Finite Groups and Applications*, Cambridge University Press, 1999.
- [5] Márquez-Martínez A.C. y Quezada R., *El espectro de Gelfand del álgebra circulante*, MIXBA'AL Rev. Met. de Mat., Vol. IX, 2018, 7-12.



Casa abierta al tiempo

UNIVERSIDAD AUTÓNOMA METROPOLITANA

ACTA DE EXAMEN DE GRADO

No. 00224

Matrícula: 2193801751

UNA GENERALIZACIÓN DE LA TRANSFORMADA DE FOURIER DISCRETA



KARLA ADRIANA ORTEGA GALLEGOS
ALUMNA

REVISÓ

MTRA. ROSALÍA SERRANO DE LA PAZ
DIRECTORA DE SISTEMAS ESCOLARES

Con base en la Legislación de la Universidad Autónoma Metropolitana, en la Ciudad de México se presentaron a las 18:00 horas del día 24 del mes de febrero del año 2022 POR VÍA REMOTA ELECTRÓNICA, los suscritos miembros del jurado designado por la Comisión del Posgrado:

DR. RICARDO MARCELIN JIMENEZ
DR. CRISPIN HERRERA YAÑEZ
DR. JORGE RICARDO BOLAÑOS SERVIN

Bajo la Presidencia del primero y con carácter de Secretario el último, se reunieron para proceder al Examen de Grado cuya denominación aparece al margen, para la obtención del grado de:

MAESTRA EN CIENCIAS (MATEMÁTICAS)

DE: KARLA ADRIANA ORTEGA GALLEGOS

y de acuerdo con el artículo 78 fracción III del Reglamento de Estudios Superiores de la Universidad Autónoma Metropolitana, los miembros del jurado resolvieron:

Aprobar

Acto continuo, el presidente del jurado comunicó a la interesada el resultado de la evaluación y, en caso aprobatorio, le fue tomada la protesta.

DIRECTOR DE LA DIVISIÓN DE CBI

DR. JESUS ALBERTO OCHOA TAPIA

PRESIDENTE

DR. RICARDO MARCELIN JIMENEZ

VOCAL

DR. CRISPIN HERRERA YAÑEZ

SECRETARIO

DR. JORGE RICARDO BOLAÑOS SERVIN