Transformada de Fourier finita (transformada de Fourier sobre el grupo $\mathbb{Z}_n$)

Problemas para examen

Divisibilidad de los números reales

1. Divisibilidad de los números reales. Escriba la definición de la divisibilidad de los números reales.

2. Propiedad transitiva de la divisibilidad de los números reales. Demuestre que la divisibilidad de los números reales tiene propiedad transitiva.

3. Propiedades aritméticas de la divisibilidad de los números reales. Sean $\alpha, \beta \in \mathbb{R}$ tales que $\alpha \mid \beta$, y sea $m \in \mathbb{Z}$. Demuestre las siguientes propiedades:

$$\alpha \mid (\beta + \gamma), \qquad \alpha \mid (m\beta), \qquad (m\alpha) \mid (m\beta).$$

4. Divisibilidad de los números reales y multiplicación por -1. Sean $\alpha, \beta \in \mathbb{R}$. Demuestre que las siguientes cuatro afirmaciones son equivalentes:

$$\alpha \mid \beta, \qquad \alpha \mid (-\beta), \qquad (-\alpha) \mid \beta, \qquad (-\alpha) \mid (-\beta).$$

5. La divisibilidad y la comparación de los valores absolutos. Sean $\alpha, \beta \in \mathbb{R}$ tales que $\alpha \mid \beta$ y $\beta \neq 0$. Demuestre que $|\alpha| \leqslant |\beta|$. Se recomienda usar el hecho que si $k \in \mathbb{Z}$ y $k \neq 0$, entonces $|k| \geqslant 1$.

6. Sobre la divisibilidad mútua de números reales. Sean $\alpha, \beta \in \mathbb{R}$ tales que $\alpha \mid \beta$ y $\beta \mid \alpha$. Demuestre que $\alpha = \beta$ o $\alpha = -\beta$.

Raíces de la unidad

En este tema se supone que $n \in \mathbb{Z}$, $n \geqslant 1$. Usamos la notación

$$\omega_n = \exp\left(-\frac{2\pi\,\mathrm{i}}{n}\right).$$

7. Demuestre que $\omega_n^k = 1$ is y sólo si $n \mid k$.

8. Sean $p, q \in \mathbb{Z}$. Demuestre que $\omega_n^p = \omega_n^q$ si y sólo si $n \mid (p - q)$.

9. Sean $p, q \in \{0, \ldots, n-1\}$. Demuestre que $\omega_n^p = \omega_n^q$ si y sólo si $p = q$.

10. Descripción explícita de las raíces de la unidad. Demuestre que

$$\{z \in \mathbb{C} \colon\ z^n = 1\} = \{\omega_n^k \colon\ k \in \mathbb{Z}\} = \{\omega_n^k \colon\ k \in \{0, \ldots, n-1\}\},$$

y que el último conjunto tiene exactamente n elementos.

El grupo cociente de un grupo conmutativo sobre un subgrupo

En estos ejercicios suponemos que G es un grupo conmutativo, para el cual utilizamos la notación aditiva, y H es un subgrupo de G.

11. La suma de dos conjuntos del grupo. Sean $A, G \subseteq G$. Recuerde la definición del conjunto $A + B$.

12. La suma de un elemento del grupo con un subconjunto del grupo. Sean $a \in G$, $B \subseteq G$. Entonces $a + B$, por definición, es lo mismo que $\{a\} + B$. Muestre que

$$a + B = \{x \in G\colon\ x - a \in B\}.$$

13. Definimos en G un relación binaria mediante la siguiente regla:

$$a \overset{H}{\equiv} b \quad \Longleftrightarrow \quad a - b \in H.$$

Demuestre que $\overset{H}{\equiv}$ es una relación de equivalencia en G.

14. Sea $a \in G$. Demuestre que

$$\{x \in G\colon\ x \overset{H}{\equiv} a\} = a + H.$$

15. Sean $a_1, a_2, b_1, b_2 \in G$ tales que $a_1 \overset{H}{\equiv} a_2$, $b_1 \overset{H}{\equiv} b_2$. Muestre que

$$a_1 + b_1 \overset{H}{\equiv} a_2 + b_2.$$

16. Denotemos por G/H al conjunto de las clases de equivalencia de G respecto la relación $\overset{H}{\equiv}$:

$$G/H := \{a + H\colon\ a \in G\}.$$

Definimos la suma de dos clases de equivalencia mediante la siguiente regla:

$$(a + H) \oplus (b + H) := (a + b) + H.$$

Muestre que esta definición es consistente. Muestre que $(a + H) \oplus (b + H)$ coincide con la suma de los conjuntos $a + H$ y $b + H$. En lo que sigue usamos el símbolo $+$ para esta operación.

17. Muestre que G/H es un grupo.

El grupo $\mathbb{Z}_n$

18. La suma de dos conjuntos de números enteros. Sean $A, B \subseteq \mathbb{Z}$. Recuerde la definición del conjunto $A + B$.

19. La suma de un entero y un conjunto de números enteros. Sean $a \in \mathbb{Z}$, $B \subseteq \mathbb{Z}$. Entonces $a + B$, por definición, es lo mismo que $\{a\} + B$. Aplique la definición anterior y simplifíquela para este caso particular.

20. Subgrupo $n\mathbb{Z}$ del grupo $\mathbb{Z}$. Demuestre que el conjunto $n\mathbb{Z}$ es un subgrupo del grupo $\mathbb{Z}$.

21. Congruencia módulo n. Defina la relación de congruencia módulo n en $\mathbb{Z}$ y demuestre que es una relación de equivalencia.

22. La clase de congruencia módulo n de un número entero. Sea $j \in \mathbb{Z}$. Verifique que la clase de congruencia módulo n del número j es el conjunto

$$j + n\mathbb{Z}.$$

23. El conjunto de las clases de congruencia módulo n. Denotamos por $\mathbb{Z}_n$ el conjunto de las clases de equivalencia considerada en el problema anterior. Demuestre que $\mathbb{Z}_n$ tiene exactamente n elementos.

24. Adición en $\mathbb{Z}_n$. Sean $j, k \in \mathbb{Z}_n$. Demuestre que

$$(j + n\mathbb{Z}) + (k + n\mathbb{Z}) = (j + k) + n\mathbb{Z}.$$

25. $\mathbb{Z}_n$ como un grupo. Explique cómo se define la operación de adición en $\mathbb{Z}_n$ y demuestre que $\mathbb{Z}_n$ es un grupo abeliano.

26. Múltiplos enteros de un elemento de un grupo conmutativo. Explique cómo se definen los múltiplos enteros de un elemento en un grupo conmutativo (con notación aditiva). ¿Cuándo un elemento del grupo se llama su generador? ¿Cuándo un grupo se llama cíclico?

27. $\mathbb{Z}_n$ es un grupo cíclico. Demuestre que $\mathbb{Z}_n$ es un grupo cíclico.

28. Demuestre que el grupo $\mathbb{Z}_n$ es isomorfo al grupo de las raíces de 1 de orden n.

29. Caracteres del grupo $\mathbb{Z}_n$. Sea $p \in \mathbb{Z}$. Definimos $\varphi_{p+n\mathbb{Z}} \colon \mathbb{Z}_n \to \mathbb{T}$, mediante la regla

$$\varphi_{p+n\mathbb{Z}}(q + n\mathbb{Z}) := \omega_n^{-pq}.$$

Muestre que esta definición es consistente y que $\varphi_{p+n\mathbb{Z}}$ es un caracter de grupo $\mathbb{Z}_n$.

30. Caracteres del grupo $\mathbb{Z}_n$, continuación. Muestre que cada caracter del grupo $\mathbb{Z}_n$ es de la forma φ_A, donde $A \in \mathbb{Z}_n$.

La transformada finita de Fourier y sus propiedades principales

31. Escriba la definición de la matriz F_n.

32. Sobre sumas de las potencias de ω_n. Sea $m \in \mathbb{Z}$. Demuestre que

$$\frac{1}{n}\sum_{k=0}^{n-1} \omega_n^{mk} = \begin{cases} 1, & n \mid m; \\ 0, & n \nmid m. \end{cases}$$

33. Ortogonalidad de las raíces de la unidad. Sean $p, q \in \{0, \ldots, n-1\}$. Demuestre que

$$\frac{1}{n}\sum_{k=0}^{n-1} \omega_n^{-pk}\, \omega_n^{qk} = \delta_{p,q}.$$

34. Teorema sobre la inversa de la matriz de Fourier. Demuestre que

$$\frac{1}{n} F_n^* F_n = I_n.$$

Escriba una fórmula para F_n^{-1} y muestre que la matriz $\frac{1}{\sqrt{n}} F_n$ es unitaria.

35. La base finita de Fourier. Escriba la definición de la base finita de Fourier y muestre que $\frac{1}{\sqrt{n}} F_n x$ es el vector de las coordenadas del vector x respecto a la base finita de Fourier.

36. Matrices de Vandermonde y su sentido principal. Muestre cómo se expresan los valores de un polinomio en puntos dados en términos de la matriz de Vandermonde.

37. La matriz de Fourier como una matriz de Vandermonde. Muestre que la matriz de Fourier F_n es una matriz de Vandermonde y explique el sentido de la transformada discreta de Fourier en términos de coeficientes y valores de polinomios.

La transformada rápida de Fourier

38. Fórmula de Danielson y Lanczos. Enuncie y demuestre la fórmula de Danielson–Lanczos que expresa las componentes del vector $F_n x$ a través de las componentes de la transformada finita de Fourier aplicada a ciertos vectores de longitud $n/2$.

39. Algoritmo de la transformada rápida de Fourier. Sea n una potencia de 2. En algún lenguaje de programación escriba una función que calcule $F_n x$ usando la fórmula recursiva de Danielson y Lanczos. Se recomienda programar la función de manera recursiva.

40. Algoritmo de la transformada rápida inversa de Fourier. Explique qué cambios hay que hacer en la función anterior para calcular $F_n^{-1} x$.

41. El número de multiplicaciones en el algoritmo de la transformada rápida de Fourier. Sea n una potencia de 2. Denotemos por $A(n)$ el número de las multiplicaciones (potencias de ω_n por números reales) en el algoritmo anterior. Enuncie y demuestre una fórmula para $A(n)$.

Matrices diagonales

42. El álgebra $\mathbb{C}^n$. Demuestre que el espacio vectorial $\mathbb{C}^n$ dotado con la multiplicación por componentes, es una álgebra compleja asociativa conmutativa con identidad. Describa el grupo de los elementos invertibles. Enuncie y demuestre la fórmula para el espectro de un elemento de $\mathbb{C}^n$.

43. Propiedades adicionales del álgebra $\mathbb{C}^n$. En el álgebra $\mathbb{C}^n$ describa los divisores de cero, los elementos involutivos, los elementos idempotentes, los generadores.

44. Matrices diagonales. Escriba la definición de la matriz diagonal. Muestre que el álgebra de las matrices diagonales es isomorfa al álgebra $\mathbb{C}^n$. Describa las propiedades del álgebra de las matrices diagonales.

45. Matrices que conmutan con una matriz diagonal cuyas entradas diagonales son diferentes a pares. Sea $a \in \mathbb{C}^n$ tal que $a_j \neq a_k$ para cualesquiera j, k en $\{0, 1, \ldots, n-1\}$ con $j \neq k$, y sea $X \in \mathcal{M}_n(\mathbb{C})$ tal que

$$X \operatorname{diag}(a) = \operatorname{diag}(a) X.$$

Demuestre que X es una matriz diagonal.

Matrices circulantes y su diagonalización

46. Convolución discreta cíclica y las matrices circulantes. Sean $a, b \in \mathbb{C}^n$. Escriba la definición de $a * b$, escriba la definición de la matriz circulante $C(a)$, y demuestre que

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

47. Programación de la convolución discreta cíclica. En algún lenguaje de programación escriba una función de dos argumentos vectoriales a, b (se supone que a y b son de la misma longitud) que calcule y devuelva el vector $a * b$.

48. Construcción de matrices circulantes. En algún lenguaje de programación escriba una función de un argumento vectorial a que construya y devuelva la matriz circulante $C(a)$.

49. Teorema de convolución para el grupo $\mathbb{Z}_n$. Sean $a, b \in \mathbb{C}^n$. Demuestre que

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

50. Expresión de la convolución discreta cíclica en términos de la transformada finita de Fourier. De la fórmula del problema anterior despeje $a * b$.

51. Álgebra de convolución. Muestre que el álgebra compleja $(\mathbb{C}^n, *)$ es isomorfa al álgebra compleja $(\mathbb{C}^n, \odot)$. Demuestre que el corolario que el álgebra $(\mathbb{C}^n, *)$ es asociativa y conmutativa. Encuentre la identidad del álgebra $(\mathbb{C}^n, *)$.

52. El cálculo de la convolución discreta cíclica usando la transformada rápida de Fourier. En algún lenguaje de programación escriba una función de dos argumentos vectoriales a, b (se supone que $a, b \in \mathbb{C}^n$ y n es una potencia de 2) que utilice la fórmula del Problema 50 y las funciones programadas en los Problemas 39 y Problemas 40.

53. Diagonalización de las matrices circulantes. Sea $a \in \mathbb{C}^n$. Demuestre que

$$\left(\frac{1}{\sqrt{n}}F_n\right) C(a) \left(\frac{1}{\sqrt{n}}F_n\right)^* = \operatorname{diag}(F_n a).$$

Haga conclusiones sobre los valores y vectores propios de la matriz $C(a)$.

54. Criterio de matriz circulante en términos de la matriz de Fourier. Sea $A \in \mathcal{M}_n(\mathbb{C})$ tal que la siguiente matriz es diagonal:

$$\left(\frac{1}{\sqrt{n}}F_n\right) A \left(\frac{1}{\sqrt{n}}F_n\right)^*.$$

Demuestre que A es una matriz circulante.

55. El álgebra de las matrices circulantes. Muestre que las matrices circulantes forman una álgebra compleja isomorfa a $\mathbb{C}^n$. En particular, explique por qué las matrices circulantes conmutan entre si.

56. El operador del desplazamiento cíclico. Escriba las entradas de la matriz $C(e_1)$. Dado x en $\mathbb{C}^n$, calcule $C(e_1)x$.

57. Las matrices diagonales conmutan con la matriz del desplazamiento cíclico. Explique por qué $C(e_1)$ conmuta con cualquier matriz circulante.

58. Descripción de las matrices que conmutan con la matriz del desplazamiento cíclico. Sea $A \in \mathcal{M}_n(\mathbb{C})$ tal que $AC(e_1) = C(e_1)A$. Demuestre que A es una matriz circulante.