Anillo de funciones aritméticas

José Luis Juanico

Julio 11, 2025

ESFM-IPN

Convolución de Dirichlet

Funciones aritméticas

Dedekind (1857): si $F(n) = \sum f(d)$, donde d recorre todos los divisores positivos de n, entonces

$$f(n) = F(n) - \sum F\left(\frac{n}{a}\right) + \sum F\left(\frac{n}{ab}\right) - \sum F\left(\frac{n}{abc}\right) + \cdots,$$

donde las sumas recorre las combinaciones de primos $a, b, \ldots$ de n.

Funciones aritméticas

Laguerre (1863) expresó esto en la notación

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$$

y fue el primero en usarla. Donde $\mu(1) = 1$, $\mu(p_1 p_2 \cdots p_k) = (-1)^k$ y $\mu(n) = 0$ si n es divisible por algún cuadrado (Möbius).

Formalización algebraica

$$\sum_{d|n} \mu(d) = 0, \text{si } n > 1 \qquad \text{(Mertens, 1874)}$$

$$\sum_{d|n} \varphi(d) = n \qquad \text{(Gauss, 1801)}$$

$$\sum_{d|n} \mu(d) \frac{n}{d} = \varphi(d) \qquad \text{(Laguerre, 1863).}$$

Formalización algebraica

Liouville, J. *Sur quelque functions numeriques*.

Bell, E. T. *Outline of a theory of arithmetical functions in their algebraic aspects*.

Convolución de Dirichlet

$$\sum_{d|n} f(d)g\left(\frac{n}{d}\right) := (f * g)(n)$$

Convolución de Dirichlet

$$\sum_{d|n} f(d)g\left(\frac{n}{d}\right) := (f * g)(n)$$

$$f(n) + g(n) := (f + g)(n)$$

Anillo de funciones aritméticas

- $(\mathcal{A}, +, *)$ es un álgebra conmutativa con identidad sobre el campo $\mathbb{C}$ (o $\mathbb{C}$-álgebra).
- $(\mathcal{A}, +)$ es un espacio vectorial sobre $\mathbb{C}$.
- $(\mathcal{A}, +, *)$ es un dominio entero.

Elementos irreducibles y primos

- $f \in \mathcal{A}$ es invertible si y sólo si $f(1) \neq 0$.
- $\mathcal{N}(f) = p$ primo implica que f es irreducible en $\mathcal{A}$.

Anillo de funciones aritméticas

- $\mathcal{A}$ es un dominio de factorización.
- $\mathcal{A}$ es un dominio de factorización única (DFU).
- $\mathcal{A}$ es un anillo local.

Elementos irreducibles y primos

Corolario:

- f es primo en $\mathcal{A}$ si y sólo si f es irreducible en $\mathcal{A}$.

Podríamos haber ahorrado trabajo probando que $\mathcal{A}$ es un dominio de ideales principales, pues todo DIP es un DFU. Este no es el caso.

Condición de la cadena ascendente

$\mathcal{A}$ cumple una versión débil de la cadena ascendente: si $(f_1) \subset (f_2) \subset (f_3) \subset \cdots$ y $f_i \nsim f_{i+1}, \forall i \in \mathbb{N}$ (no son asociados), entonces existe $n \in \mathbb{N}$ tal que $(f_i) = (f_n), \forall i \geq n$.

Condición de la cadena descendente

A propósito de cadenas descendentes, $\mathcal{A}$ no es Artiniano, como lo muestra la sucesión de ideales $I_n = \{f \in \mathcal{A} \mid \mathcal{N}(f) \geq n\} \cup \{\mathbf{0}\}$.

Isomorfismos

Isomorfismos

$$(\mathcal{A}_{\mathbb{R}}, +) \cong (P, *)$$

$$P = \{f \in \mathcal{A} \mid f(1) > 0\}$$

Isomorfismos

$$(\mathcal{M}, *) \cong (\mathcal{A}', +)$$

$$\mathcal{A}' = \{f \in \mathcal{A}_{\mathbb{R}} \mid f(n) = 0, \forall n \neq p^{\alpha}, p \text{ primo y } \alpha \in \mathbb{N}\}$$

Isomorfismos

$$(\mathcal{A}_{\mathbb{R}}, +) \cong (\mathcal{A}', +)$$

Isomorfismos

$$(\mathcal{A}_{\mathbb{R}}, +) \cong (\mathcal{A}_1, +)$$

$$\mathcal{A}_1 = \{f \in \mathcal{A} \mid f(1) \in \mathbb{R}\}$$

Isomorfismos

$$(\mathcal{A}_{\mathbb{R}}, +) \cong (\mathcal{A}, +)$$

Isomorfismos

$$(\mathcal{A}_{\mathbb{R}}, +) \cong (P, *) \cong (\mathcal{M}, *) \cong (\mathcal{A}', +) \cong (\mathcal{A}_1, +) \cong (\mathcal{A}, +)$$

Funciones pares

Funciones pares módulo r

$$f(n) = f((n, r)), \forall n \in \mathbb{N}$$

Sumas de Ramanujan

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6}\left(1 + \frac{(-1)^n}{2^2} + \frac{2\cos\left(\frac{2}{3}\pi n\right)}{3^2} + \frac{2\cos\left(\frac{1}{2}\pi n\right)}{4^2} + \frac{2\left[\cos\left(\frac{2}{5}\pi n\right) + \cos\left(\frac{4}{5}\pi n\right)\right]}{5^2} + \frac{2\cos\left(\frac{1}{3}\pi n\right)}{6^2} + \cdots\right)$$

Sumas de Ramanujan

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6} \sum_{r=1}^{\infty} \frac{c_r(n)}{r^2},$$

$$c_r(n) = \sum_{\substack{a=1 \\ (a,r)=1}}^{r} \cos\left(\frac{2\pi}{r} an\right)$$

Sumas de Ramanujan

$$c_r(n) = \sum_{d|(n,r)} \mu\left(\frac{r}{d}\right) d$$

Funciones pares

- Cualquier función constante
- (n, r)
- El número de divisores de (n, r)
- $f((n, r))$, donde f es cualquier función aritmética
- $\sum_{d|(n,r)} g(d)$

Expansión de "Fourier"

f par módulo r implica

$$f(n) = \sum_{d|r} \alpha(d) c_d(n), \forall n \in \mathbb{N}$$

para algunos coeficientes α.

Sumas de Ramanujan

$\mathcal{B}_r = \{c_d\}_{d|r}$ es una base de $\mathcal{A}_r$

¡$\mathcal{A}_r$ tiene dimensión $\tau(r)$!

$\mathcal{A}_r$ también tiene producto interno

$$\langle f, g\rangle = \sum_{d|r} \varphi(d) f\left(\frac{r}{d}\right) \overline{g\left(\frac{r}{d}\right)}$$

y

$$\mathcal{B}'_r = \left\{ \frac{1}{\sqrt{r\varphi(d)}} c_d \right\}$$

es una base ortonormal de $\mathcal{A}_r$.

Aplicaciones

Señal

$$x : \mathbb{Z} \longrightarrow \mathbb{C}$$

Señal periódica con periodo r

$$x[n] = x[n + kr], \forall n, k \in \mathbb{Z}$$

Señal simética módulo r

$$x[n] = x[n-r], \forall n \in \mathbb{Z}$$

Señal par módulo r

$$x[n] = x[(n, r)], \forall n \in \mathbb{Z}$$

Implicaciones

Toda señal par módulo r es simétrica módulo r y también periódica módulo r.

Transformada Discreta de Fourier

$$X[k] = \sum_{n=1}^{r} x[n] W_r^{nk}, k = 1, \ldots, r,$$

$$x[n] = \frac{1}{r} \sum_{k=1}^{r} X[k] W_r^{-nk}, n \in \mathbb{Z},$$

con $W_r = e^{-j(2\pi/r)}$ y x periódica con periodo r.

Sistemas de residuos

Si d es un divisor positivio de r, se define

$$S_d = \left\{ \left(\frac{r}{d}\right) \alpha \mid (\alpha, d) = 1, 1 \leq \alpha \leq d \right\}.$$

Sistemas de residuos

$$\bigcup_{d|r} S_d = \{1, 2, \ldots, r\} \qquad \text{(Gauss, 1801)}$$

Funciones indicadoras

Se define

$$h_{r,d}[n] = \begin{cases} 1 & \text{si } n \in S_d \\ 0 & \text{en otro caso.} \end{cases}$$

Para $n \in \{1, \dots, r\}$. Se puede extender a todo $\mathbb{Z}$ haciendo n módulo r y la señal $h_{r,d}$ se vuelve par.

Funciones indicadoras

Los coeficientes de Fourier clásicos para las funciones $h_{r,d}$, para d divisor de r fijo, están dados por:

$$H_{r,d}[k] = c_d[k], k = 1, \ldots, r.$$

¡Sus coeficientes son las sumas de Ramanujan módulo d! Conexión entre Gauss y Ramanujan.

Corolarios

Si x es par módulo r, entonces sus coeficientes de Fourier clásicos están dados por:

$$X[k] = \sum_{d|r} x\left[\frac{r}{d}\right] c_d[k], k = 1, \ldots, r.$$

Más aún,

$$x[n] = \frac{1}{r} \sum_{d|r} X\left[\frac{r}{d}\right] c_d[n], \forall n \in \mathbb{Z}.$$

Ejemplo

Si por ejemplo, supóngase que se tiene una señal par módulo 10 y se quiere calcular sus Transformada Discreta Fourier. Se tiene que los sistemas de residuos de 10 son:

$$
\begin{aligned}
S_1 &= \{10\} \\
S_2 &= \{5\} \\
S_5 &= \{2, 4, 6, 8\} \\
S_{10} &= \{1, 3, 5, 7\}
\end{aligned}
$$

Ejemplo

Luego

$$X[1] = X[3] = X[5] = X[7] = \sum_{d|10} x\left[\frac{10}{d}\right] c_d[1] = x[10] - x[5] - x[2] + x[1]$$

$$X[2] = X[4] = X[6] = X[8] = \sum_{d|10} x\left[\frac{10}{d}\right] c_d[2] = x[10] + x[5] - x[2] - x[1]$$

$$X[5] = \sum_{d|10} x\left[\frac{10}{d}\right] c_d[5] = x[10] - x[5] + 4x[2] - 4x[1]$$

$$X[10] = \sum_{d|10} x\left[\frac{10}{d}\right] c_d[10] = x[10] + x[5] + 4x[2] + 4x[1]$$

Entonces, para obtener el valor de su transformada en cualquier entero basta conocer los valores de $X[1], X[2], X[5], X[10]$.

Ejemplo

$$\begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 4 & -4 \\ 1 & 1 & 4 & 4 \end{bmatrix}$$

¡Gracias!