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.

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