AMPLIACIÓN DE MATEMÁTICAS

POLINOMIOS.

Sobre el conjunto de los **polinomios sobre un cuerpo**, $\mathbb{F}[x]$, se puede hacer una teoría de la **divisibilidad** análoga a la que tenemos para los números enteros. Así para polinomios, podremos dar un Teorema del Resto, una Identidad de Bezout, un Algoritmo de Euclides y un Teorema Chino del Resto. Respecto de sus propiedades algebraicas, tanto $\mathbb{Z}$ como $\mathbb{F}[x]$ son **dominios de ideales principales**.

Números y polinomios pueden ser descompuestos en productos de factores no descomponibles (números primos y polinomios **irreducibles**, respectivamente). Así como las propiedades de los números se usan en **Teoría de Códigos** y en **Criptografía**, por las mismas razones se usan los polinomios en estas mismas áreas.

En los próximos capítulos vamos a justificar lo que acabamos de afirmar.

En primer lugar vamos a dar la definición formal del conjunto de polinomios. **No es necesaria**. Las definiciones dadas en la Introducción a las Estructuras Algebraicas son suficientes para trabajar con los polinomios.

Definición 1. *Dado* $(\mathbb{A}, +, \times)$ *un anillo conmutativo con unidad se llama* ***conjunto de polinomios sobre*** $\mathbb{A}$*, o con coeficientes en* $\mathbb{A}$*, al conjunto de sucesiones*

$$\mathbb{A}[x] = \{\, (a_k)_{k=0}^{\infty} \in \mathbb{A}^{\mathbb{N}} \ : \ \exists n_0 \ \text{ de modo que } a_k = 0 \text{ si } k > n_0 \,\}$$

Sobre $\mathbb{A}[x]$ *se definen dos operaciones. Dados dos elementos* $p, q \in \mathbb{A}[x]$*,*

$$p = (a_0, a_1, ..., a_{n_0}, 0, 0...., 0, ...)$$

y

$$q = (b_0, b_1, ..., b_{m_0}, 0, 0...., 0, ...), \qquad \text{de modo que } n_0 \leq m_0$$

se definen

- ***la suma:***

$$p + q = (a_0 + b_0, a_1 + b_1, ..., a_{n_0} + b_{n_0}, b_{n_0+1}, ..., b_{m_0}, 0...., 0, ...)$$

  (la suma de sucesiones);
- ***el producto:*** $pq = (c_k)_{k=0}^{\infty}$ *donde*

$$c_k = \sum_{j=0}^{k} a_j b_{k-j}.$$

Proposición 1. *Si* $(\mathbb{A}, +, \times)$ *es un anillo conmutativo, entonces* $(\mathbb{A}[x], +, \times)$ *también es un anillo conmutativo.*

En adelante vamos a trabajar con polinomios con coeficientes en un cuerpo $\mathbb{F}$. En este caso ya hemos visto que que $\mathbb{F}[x]$ es un **dominio de integridad** (es decir, un anillo conmutativo, con unidad y sin divisores de cero).

POLINOMIOS SOBRE CUERPOS.

Definición 2. *Sea* $(\mathbb{F}, +, \times)$ *un cuerpo.*

A: *Sea* $\mathbb{F}[x] = \{a_0 + a_1x + ... + a_nx^n \ : \ n \in \mathbb{N} \ y \ a_0, a_1, ..., a_n \in \mathbb{F} \ \}$ *el conjunto de* ***polinomios*** *con* ***coeficientes*** *en el cuerpo* $\mathbb{F}$.

B: *Sean* $p, q \in \mathbb{F}[x]$, $p(x) = \sum_{k=0}^{n_0} a_k x^k$ *y* $q(x) = \sum_{k=0}^{m_0} b_k x^k$.

B_1**:** *Se llama* ***grado*** *del polinomio* p *al mayor* k *de modo que* $a_k \neq 0$ *(****Notación:*** $grad.p = n_0$*).*

B_2**:** *Se define la* ***suma:*** $(p+q)(x) = \sum_{k=0}^{\text{máx}\{n_0,m_0\}} (a_k + b_k)x^k$ *(****Observación****, el grado de la suma es menor o igual que el mayor de los grados de los polinomios:* $grad.(p+q) \leq \text{máx}\{n_0, m_0\}$.

B_3**:** *Se define el* ***producto:*** $pq(x) = \sum_{k=0}^{\text{máx}\{n_0+m_0\}} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k$ *(****Observación****, el grado del producto es la suma de grados:* $grad.(pq) = n_0 + m_0$*. Esto es así por ser* $\mathbb{F}$ *un cuerpo).*

C: *Un polinomio* $p(x) = \sum_{k=0}^{n_0} a_k x^k$ *se llama* ***mónico*** *si* $a_{n_0} = 1$*, si el coeficiente de la potencia de* x *de mayor grado es* 1.

D: *Dado un polinomio* $p(x) = \sum_{k=0}^{n_0} a_k x^k$ *se llama* ***función polinómica*** *asociada a* p *a la aplicación*

$$\begin{array}{rcccc} \overline{p} & : & \mathbb{F} & \to & \mathbb{F} \\ & & y & \to & \overline{p}(y) \ = \ \sum_{k=0}^{n_0} a_k y^k \end{array}$$

Observación: *las funciones polinómicas tienen las siguientes propiedades, si* $p, q \in \mathbb{F}[x]$

$$\begin{array}{rcl} - \ \overline{p+q} & = & \overline{p} + \overline{q} \\ - \ \overline{pq} & = & \overline{p} \ \overline{q} \\ - \ \overline{p \circ q} & = & \overline{p} \circ \overline{q}. \end{array}$$

E: *Se llama* ***raíz*** *de un polinomio* $p \in \mathbb{F}[x]$ *a todo* $\alpha \in \mathbb{F}$ *de modo que*

$$\overline{p}(\alpha) = \sum_{k=0}^{n_0} a_k (\alpha)^k = 0.$$

Al estudiar anillos vimos que

Proposición 2. *Si $\mathbb{F}$ es un cuerpo, entonces el anillo de polinomios $\mathbb{F}[x]$ es un* ***dominio de integridad****.*

Demostración: $p(x) = 1$, es la unidad del producto. Ahora si $p, q \in \mathbb{F}[x]$ con $p(x) = \sum_{k=0}^{n_0} a_k x^k$ y $q(x) = \sum_{k=0}^{m_0} b_k x^k$ se tiene que

$$pq(x) = \sum_{k=0}^{\text{máx}\{n_0+m_0\}} \left(\sum_{j=0}^{k} a_j b^{k-j} \right) x^k \neq 0$$

ya que $a_{n_0} b_{m_0} \neq 0$ □

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

Email address: Cesar_Ruiz@mat.ucm.es