Polinomios

Lornar the Breton

Contents

Definición de Grupo

Un **grupo** G es un **conjunto** dotado de una **operación binaria** entre sus elementos, digamos $*$, tal que si $a, b \in G \implies a * b \in G$ y satisface:

1) **Asociatividad**
$$(a * b) * c = a * (b * c)$$
2) **Existencia del Neutro**
$$\forall a \in G,$$
$$a * e = a$$
$$e * a = a$$

3) **Existencia del Inverso**

$$\forall a \in G \exists a^{-1} \in G :$$
$$a * a^{-1} = e$$
$$a^{-1} * a = e$$

Definición de Grupo Abeliano

Un un **grupo** G se le llama **Abeliano** si cumple con:

$$\forall a, b \in G$$
$$a * b = b * a$$

Definición de Anillo

Sea A un **conjunto** con **dos operaciones binarias**, $+$, $*$. Decimos que A es un **anillo** $\iff$

1) $(A, +)$ es un **grupo abeliano**
2) $(a * b) * c = a * (b * c) \forall a, b, c \in A$
3) $a * (b + c) = a * b + a * c \land (b + c) * a = a * b + a * c$

Anillo con unidad

$$\exists 1 \in A : \forall a \in A$$
$$a * 1 = a$$
$$1 * a = a$$

Anillo conmutativo

$$\forall a \in A$$
$$a * b = b * a$$

Definición de Dominio Entero

Si A es un **anillo**, decimos que A es un **dominio entero** $\iff$

$$a * b = 0 \iff a = 0 \vee b = 0$$

Definición de Campo

Sea K un **conjunto** con $+$ y $*$. K es un **campo** $\iff$

1) $(K, +, *)$ es **anillo conmutativo con unidad**
2) $(K, 0, +, *)$ es un **grupo**

Observación

Si K es un **campo** $\implies$ K es **dominio entero**
Z_n es un **campo**, con $+$ y $* \pmod{n} \iff n$ es **primo**

Definición de Polinomio

Sea A un **anillo conmutativo con unidad**. Un **polinomio con coeficientes en** A es una expresión del tipo

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_2 x^2 + a_1 x + a_0$$

donde $a_i \in A$ y $n \in \mathbb{N}_0$.

Nota

$$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$$

Polinomio Cero

Si $a_j = 0 \forall j$, el **polinomio**

$$0x^n + 0x^{n-1} + ... + 0x + 0$$

se llama el **polinomio cero**. Se denota por 0.

Conjunto de todos los polinomios

El **conjunto de todos los polinomios** se denota como $A[x]$.

Igualdad de polinomios

Dos **polinomios** son **iguales** $\iff$ sus **coeficientes correspondientes** son iguales.

Ejemplo

En $\mathbb{Z}_{[4]}$

$$x^5 + 3 = x^2 + 2 = x^5 + 3x^2 + 4x - 2$$

pues en $\mathbb{Z}_{[4]}$, $0 = 4$ y $2 = -2$.

Definición del Grado de un polinomio

Sea $f \in A_{[x]}$ tal que:

$$f = a_n x^n + a_{n-1} x^{n-a} + ... + a_1 x + a_0$$

Decimos que f tiene **grado** m si

$$\forall k > m$$

$$a_k = 0 \wedge a_m \neq 0$$

En otras palabras, m es el **coeficiente máximo**.
El **grado** de f se denota como

$$gr(f) = m$$

Definición de mónico

Sea $f \in A_{[x]}$. Si $gr(f) = n$ y $a_n = 1$, entonces f es **mónico**.