6. El anillo de polinomios $K[x]$.

Dado un cuerpo K, se llama **polinomio en la indeterminada x con coeficientes en el cuerpo** K a $p(x) = \sum_{i=0}^{m} a_i x^i$, siendo $a_i \in K, i = 0, \ldots, m, m \in \mathbb{N} \cup \{0\}$.

Por convenio, $x^0 = 1$ y si $a_i = 0$, entonces $a_i x^i = 0$. Esto nos permite denotar al polinomio $p(x) = \sum_{i=0}^{m} a_i x^i = a_m x^m + \ldots + a_0$ por $p(x) = \sum a_i x^i$, entendiendo que $a_i = 0$ si $i > m$.

Dos polinomios $p(x) = \sum a_i x^i$ y $q(x) = \sum b_i x^i$ son iguales si $a_i = b_i$, para todo i.

Definición. Sea $p(x) = \sum a_i x^i \neq 0$ un polinomio en x con coeficientes en el cuerpo K. Se llama **grado del polinomio** $p(x)$ y de denota por deg(p), al mayor exponente m al que aparece elevado la varible x, siendo $a_m \neq 0$, esto es,

$$\deg(\mathrm{p}) = \max\{\mathrm{i} \in \mathbb{N} \cup \{0\} \mid \mathrm{a_i} \neq 0\}.$$

Si $p(x) = 0$, entonces el grado de p es $-\infty$.

Obviamente, si $p(x) = \sum a_i x^i \neq 0$ es un polinomio de grado m, entonces $a_j = 0$, si $j > m$.

Definición. Sea $p(x) = \sum a_i x^i$ un polinomio de grado m. Se llama **coeficiente director** de $p(x)$ al coeficiente a_m. Si el coeficiente director de $p(x)$ es 1, se dice que $p(x)$ es un **polinomio mónico**.

El conjunto de todos los polinomios en x con coeficientes en K se denota por:

$$K[x] = \{\sum_{i=0}^{m} a_i x^i \mid a_i \in K, i = 0, \ldots, m, m \in \mathbb{N} \cup \{0\}\},$$

En $K[x]$ se definen dos operaciones: la suma y el producto de polinomios.

Definición. Sean $p(x) = \sum a_i x^i$ y $q(x) = \sum b_i x^i$ dos polinomios de $K[x]$. Se llama **suma de los polinomios** $p(x)$ **y** $q(x)$, y se denota por $p(x) + q(x)$ al polinomio

$$p(x) + q(x) = \sum (a_i + b_i) x^i.$$

Es fácil ver que $(K[x], +)$ tiene estructura de grupo abeliano siendo 0 el elemento neutro del mismo y dado $p(x) = \sum a_i x^i$, su elemento opuesto es $-p(x) = \sum (-a_i) x^i$.

Definición. Sean $p(x) = \sum a_i x^i$ y $q(x) = \sum b_i x^i$ dos polinomios de $K[x]$. Se llama **producto de los polinomios** $p(x)$ **y** $q(x)$, y se denota por $p(x) \cdot q(x)$ al polinomio

$$p(x) \cdot q(x) = \sum c_i x^i,$$

donde $c_i = \sum_{j=0}^{i} a_j b_{i-j}$, para todo i.

Se puede demostrar que $(K[x], \cdot)$ es un semigrupo conmutativo con elemento identidad, siendo éste 1. Además, $(K[x], +, \cdot)$ tiene estructura de anillo conmutativo con elemento identidad, que recibe el nombre de **anillo de los polinomios con coeficientes en** K **en la indeterminada** x.

Por otro lado, sabemos que dados $p(x), q(x) \in K[x]$, siendo $q(x) \neq 0$, existen unos únicos polinomios $c(x)$ y $r(x)$ tales que $p(x) = q(x)c(x) + r(x)$ y $deg(r) < deg(q)$. A $r(x)$ se le llama **resto de la división de** $p(x)$ **entre** $q(x)$ y a $c(x)$ **cociente de la división de** $p(x)$ **entre** $q(x)$.

Definición. Sean $p(x), q(x) \in K[x]$, siendo $q(x) \neq 0$. Se dice que $q(x)$ divide a $p(x)$ si $r(x) = 0$, siendo $r(x)$ el resto de la división de $p(x)$ entre $q(x)$.

Si $r(x) \neq 0$, entonces se dice que $q(x)$ no divide a $p(x)$.

Por ltimo, otro concepto que utilizaremos es el de raíz de un polinomio. Si $p(x) \in K[x]$ y $\alpha \in K$, entonces se dice que α es una **raíz** de $p(x)$ de multiplicidad m si $(x-\alpha)^m$ divide a $p(x)$ y $(x-\alpha)^{m+1}$ no divide a $p(x)$.

Lo anterior equivale a decir que $p(x) = (x-\alpha)^m q(x)$, siendo $q(\alpha) \neq 0_K$.

Se puede demostrar que

Proposición 6.1. *Sea $p(x) \in K[x]$ un polinomio de grado n. Entonces, $p(x)$ tiene a lo más n raíces en K.*

En los ejemplos utilizaremos frecuentemente el cuerpo $K = \mathbb{Q}$, esto es, trabajaremos con los polinomios en la indeterminada x con coeficientes racionales. Para stos, existe una forma sencilla de localizar sus raíces racionales, basandonos en el siguiente resultado que busca las posibles raíces racionales de un polinomio con coeficientes enteros:

Proposición 6.2. *Sea $p(x) = \sum a_i x^i \in \mathbb{Z}[x]$ un polinomio de grado m. Entonces, las raíces racionales de $p(x)$ son de la forma a/b, con a, b primos entre sí, a divisor de a_0 y b divisor de a_m.*

A partir del estudio de las raíces racionales de un polinomio con coeficientes enteros, se puede calcular las raíces racionales de un polinomio con coeficientes racionales. En efecto, si $p(x) = \sum a_i x^i \in \mathbb{Q}[x]$, entonces los coeficientes de este polinomio son de la forma $a_i = \frac{b_i}{c_i}$, siendo $b_i, c_i \in \mathbb{Z}$. Entonces, el polinomio $q(x) = \sum e_i x^i$, donde $e_i = \frac{a_i c}{c_i}$, siendo c el mínimo común múltiplo de los c_i. Entonces, $q(x) \in Z[x]$ tiene las mismas raíces que $p(x)$ y las raíces de $q(x)$ se pueden calcular por el método descrito en el resultado anterior.