Anexo: El anillo de polinomios $K[x]$.

1. Construcción del anillo de polinomios $K[x]$.

Dado un cuerpo K, se define

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

donde $p(x) = \sum_{i=0}^{m} a_i x^i$, siendo $a_i \in K, i = 0, \ldots, m, m \in \mathbb{N} \cup \{0\}$ recibe el nombre de **polinomio en x con coeficientes en K**.

Dos polinomios $p(x) = \sum_{i=0}^{m} a_i x^i$ y $q(x) = \sum_{i=0}^{m} b_i x^i$ son iguales si $a_i = b_i$, para todo i.

Por convenio, si $a_i = 0$, entonces $a_i x^i = 0$ y $x^0 = 1$. 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 $i > m$.

En $K[x]$ se pueden definir dos operaciones internas: la suma y el producto de polinomios. En concreto,

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**.

2. Grado de un polinomio.

Dado $p(x) \in K[x]$, se llama el **grado del polinomio** $p(x) = \sum a_i x^i \neq 0$ y de denota por deg(p), al mayor exponente m al que aparece elevado la varible x, siendo $a_m \neq 0$, esto es,

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

y si $p(x) = 0$, entonces el grado de p es $-\infty$. Si $p(x) = \sum a_i x^i$ es un polinomio de grado m, al coeficiente a_m se le llama **coeficiente director** de $p(x)$ y si el coeficiente director de $p(x)$ es 1, se dice que $p(x)$ es un **polinomio mónico**. Obviamente, si $p(x) = \sum a_i x^i \neq 0$ es un polinomio de grado m, entonces $a_j = 0$, si $j > m$.

En relación al grado de un polinomio se tiene el siguiente resultado:

Proposición 2.1. *Sean $p(x)$ y $q(x)$ son dos polinomios de $K[x]$ de grados m y n, respectivamente, entonces*

(i) El grado de $p(x) + q(x)$ es menor o igual que el máximo entre m y n.

(ii) El grado de $p(x).q(x)$ es igual a $n + m$.

Además, si $\deg(\mathrm{p}) \neq \deg(\mathrm{q})$, *entonces* $\deg(\mathrm{p} + \mathrm{q}) = \max\{\deg(\mathrm{p}), \deg(\mathrm{q})\}$.

3. Divisibilidad. Algoritmo de la división.

El **Algoritmo de división en** $K[x]$ nos da la manera de dividir dos polinomios esto es, que si $p(x), q(x) \in K[x]$, siendo $q(x) \neq 0$, el Algoritmo de la división permite localizar unos únicos polinomios $c(x)$ y $r(x)$ tales que $p(x) = q(x)c(x)+r(x)$, siendo $\deg(r) < \deg(q)$. 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** $q(x)$. La demostración del Algoritmo de la división consta de dos partes. En la primera se prueba la existencia de los polinomios $c(x)$ y $r(x)$ y en la segunda parte se prueba su unicidad. Para construir $c(x)$ y $r(x)$ se siguen los siguientes pasos:

1. Si $\deg(p) < \deg(q)$, se elige $c(x) = 0$ y $r(x) = p(x)$.

2. Si $n = \deg(p) \geq \deg(q) = m$ se elige $c_1(x) = a_n b_m^{-1} x^{n-m}$, donde a_n es el coeficiente director de $p(x)$ y b_m^{-1} es el coeficiente director de $q(x)$ y se toma $p_1(x) = p(x) - c_1(x)q(x)$.

3. Si $\deg(p_1) < \deg(q)$, entonces se toma $r(x) = p_1(x)$ y $c(x) = a_n^{-1} x^{n-m}$.

4. Si $\deg(p_1) \geq \deg(q)$, se reitera el paso 2 pero tomando como $p(x)$ a $p_1(x)$ y se construye un nuevo polinomio $p_2(x) = p_1(x) - c_2(x)q(x)$. Si $\deg(p_2) < \deg(q)$ se elige $c(x) =$

$c_1(x) + c_2(x)$ y $r(x) = p_2(x)$ y si $\deg(p_2) \geq \deg(q)$ se repite el proceso con $p_2(x)$ y así sucesivamente.

Observamos que como los polinomios $p_i(x)$ que se van construyendo verifican $\deg(p) > \deg(p_1) > \deg(p_2) > \ldots$ llegará un momento en el que el polinomio obtenido $p_i(x)$ sea de grado menor que $q(x)$.

Para finalizar este apartado introducimos el concepto de *dividir a* :

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 $p(x)$.

Si $q(x)$ divide a $p(x)$ se escribirá: $q(x)|p(x)$ y en caso contrario $q(x) \not| p(x)$.

4. Raíces de un polinomio.

Otro concepto fundamental relacionado con los polinomio 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 $q(\alpha) \neq 0_K$.

Como consecuencia inmediata del Algoritmo de la división, se tiene

Proposición 4.1. *Sea $p(x) \in K[x]$ y $\alpha \in K$ una raíz de $p(x)$. Entonces, α es raíz de multiplicidad mayor que 1 si y sólo si α es raíz de p y de p', donde $p'(x)$ es el polinomio derivada de $p(x)$.*

Por otro lado, es fácil probar que

Proposición 4.2. *Sea $p(x) \in K[x]$ un polinomio de grado n. Entonces, $p(x)$ tiene a lo más n raíces en K.*

En el caso particular de $K = \mathbb{Q}$, se existe una forma sencilla de localizar las raíces de un polinomio con coeficientes enteros:

Proposición 4.3. *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 coeficienters 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.

5. Polinomios irreducibles. Factorización de un polinomio.

Definición. Un polinomio $p(x) \in K[x]$ de grado mayor o igual que 1 se dice que es **irreducible sobre** K si al expresar $p(x)$ como producto de dos polinomios de $K[x]$, siempre es uno de los factores de grado 0.

Una propiedad interesante de los polinomios irreducibles aparece en el siguiente resultado:

Proposición 5.1. *Sean $p(x), f(x), g(x) \in K[x]$ tales que $p(x)$ es irreducible sobre K y $p(x)|f(x)g(x)$. Entonces, $p(x)|f(x)$ ó $p(x)|g(x)$.*

Otro de los resultados interesantes que se tenemos es la factorización en polinomios irreducibles sobre $K[x]$ de cualquier polinomio $p(x)$ de grado mayor o igual que 1.

Proposición 5.2. Factorización de un polinomio en irreducibles *Sea $f(x) \in K[x]$ un polinomio de gradomayor o igual a 1. Entonces, existen $p_1(x), \ldots, p_m(x) \in K[x]$ polinomios irreducibles sobre K tales que*

$$f(x) = p_1(x) \ldots p_m(x).$$

Además, en el producto anterior los factores están univocamente determinados salvo el orden o factores constantes $\alpha \in K - \{0\}$.

Como consecuencia del resultado anterior deducimos que

Corolario 5.3. *Sea $f(x) \in K[x]$ un polinomio de grado $n \geq 1$. Entonces, en la descomposición en factores irreducibles de $f(x)$ aparecen a lo más n factores irreducibles sobre K.*

Por último, vamos a dar criterios de irreducibilidad que nos podemos utilizar para saber si un polinomio es irreducible o no.

Criterio 1. Sea $f(x) \in K[x]$ tal que $2 \leq \deg(f) \leq 3$. Entonces, $f(x)$ es irreducible sobre K si y sólo si $f(x)$ no tiene raíces en K.

Criterio 2. (Lema de Gauss). Sea $f(x) \in \mathbb{Z}[x]$. Entonces, $f(x)$ factoriza como producto de dos polinomios de grado menor r y s en $\mathbb{Q}[x]$ si y sólo si $f(x)$ factoriza como producto de dos polinomios de grado menor r y s en $\mathbb{Z}[x]$.

Criterio 3. (Criterio de Eisenstein generalizado). Sea p un número primo y $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ con $a_n \neq 0$. Supongamos que existe $r \in \{1, \ldots, n\}$ tal que

(i) $p|a_i$ para $i = 0, \ldots, r-1$.

(ii) $p^2 \not| a_0$.

(iii) $p \not| a_r$. Entonces, en la descomposición en factores irreducibles sobre $\mathbb{Q}$ de $f(x)$ aparece un factor irreducible de grado mayor o igual a r.

Criterio 4. (Reducción módulo m) Sean $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ y $\overline{f}(x) = \sum_{i=0}^{n} \overline{a_i} x^i \in \mathbb{Z}/m\mathbb{Z}[x]$ tales que $\deg(f)=\deg(\overline{f})$. Si $\overline{f}(x)$ es irreducible sobre $\mathbb{Z}/m\mathbb{Z}[x]$, entonces $f(x)$ es irreducible sobre $\mathbb{Q}$.