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 $p_1(x), \dots, p_m(x) \in K[x]$ polinomios irreducibles sobre K tales que*

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

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 $r \in \{1, \dots, n\}$ tal que

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

(ii) $p^2 \nmid a_0$.

(iii) $p \nmid a_r$. 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 $\mathbb{Q}$.