## Polinomios

**1.** Sea $K$ un cuerpo.

**a)** Demostrar el Algoritmo de Euclides en $K[x]$.

**b)** Demostrar la Identidad de Bezout en $K[x]$.

**c)** Demostrar el Lema de Gauss en $K[x]$.

**2.** Sea $K$ un cuerpo y $f(x) \in K[x]$ un polinomio no nulo. Demuestra que las siguientes condiciones son equivalentes:

(i) $f(x)$ es irreducible.

(ii) si $f(x)$ divide al producto $g(x)h(x)$ (para $g(x), h(x) \in K[x]$) entonces $f(x)$ divide a $g(x)$ o $f(x)$ divide a $h(x)$.

**3.** Sea $K$ un cuerpo. Demuestra que todo polinomio no constante con coeficientes en $K$ se puede escribir de forma única (salvo el orden de los factores y multiplicación por escalares) como producto finito de polinomios irreducibles.
(Ayuda: Considerar el conjunto $S = \{\mathrm{gr}(f) : f(x) \in K[x]$ no se factoriza en producto de irreducibles$\}$).

**4.** Sea $K$ un cuerpo y $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ con $\mathrm{gr}(f) \in \mathbb{N}$. Si $\alpha_1, \ldots, \alpha_n \in K$ son raíces de $f(x)$ (contadas con multiplicidad, es decir, si $\alpha$ tiene multiplicidad $m$, aparece $m$ veces en la lista). Entonces:

$$f(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n).$$

**5.** Sea $f(x) \in \mathbb{Z}[x]$. Demuestra que existe $g(x) \in \mathbb{Z}[x]$ es primitivo tal que $f(x) = c(f) \cdot g(x)$.

**6.** Sea $f(x) \in \mathbb{Q}[x]$. Demuestra que existe $\alpha \in \mathbb{Q}$ tal que $g(x) = \alpha f(x) \in \mathbb{Z}[x]$ es primitivo.

**7.** Reducción módulo un primo: Sea $f(x), g(x) \in \mathbb{Z}[x]$. Si $p \in \mathbb{N}$ es un primo, denotamos por $\overline{f}(x) \in \mathbb{F}_p[x]$ a su reducción módulo $p$. Demuestra:

**a)** $\overline{f + g} = \overline{f} + \overline{g}$.

**b)** $\overline{f \cdot g} = \overline{f} \cdot \overline{g}$.