

Práctico 8

- En los casos siguientes se pide hallar $d = \text{mcd}(f, g)$ y polinomios p, q tales que $d = pf + qg$.
 - $f = 2X^3 + X^2 + 3X + 4$ y $g = X^3 + 2X + 1$.
 - $f = X^6 + X^5 + 3X^4 + 3X^3 + 3X^2 + 2X + 2$ y $g = X^4 + X^3 + 3X^2 + 2X + 2$.
- Probar que si $f \in \mathbb{Z}[X]$ es un polinomio mónico y $u \in \mathbb{Q}$ es una raíz de f , entonces $u \in \mathbb{Z}$.
- Probar que si K es un cuerpo y $f \in K[X]$ tiene grado 2 o 3, entonces f es irreducible si y solo si f no tiene ninguna raíz en K .
- Probar que el polinomio $X^4 + X^3 + X + 1$ no es irreducible sobre $K[X]$, para ningún cuerpo K .
- Sea $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$. Probar que si existe un número primo p que no divide a a_n y que verifica que $\overline{a_n} X^n + \overline{a_{n-1}} X^{n-1} + \dots + \overline{a_1} X + \overline{a_0}$ es irreducible en $\mathbb{Z}_p[X]$, entonces f es irreducible en $\mathbb{Q}[X]$.
 - Aplicar la parte anterior para probar que $3X^3 - 5X^2 + 4X + 21$ y $4X^3 + 3X^2 + 2X + 4$ son irreducibles en $\mathbb{Q}[X]$.
- En cada caso determinar si el polinomio f es irreducible en $\mathbb{Q}[X]$.

$$\begin{array}{lll} f = 2X^5 - 6X^3 + 9X^2 - 15, & f = 2X^3 + 3X^2 + 2X + 3, & f = X^4 + X + 4, \\ f = 3X^4 + 6X^2 + 6, & f = X^3 - 7X + 3, & f = X^4 - X^3 + 2X^2 - X + 1. \end{array}$$

- Sea p un primo.
 - Probar que $p \mid \binom{p}{i}$, para todo $i = 1, \dots, p-1$.
 - Probar que el *polinomio ciclotómico* $f = X^{p-1} + X^{p-2} + \dots + X + 1$ es irreducible en $\mathbb{Q}[X]$.
Sugerencia: es $f = \frac{X^p - 1}{X - 1}$, luego $f(X + 1) = \frac{(X+1)^p - 1}{X}$ y aplicar el criterio de Eisenstein.
- Sea K un cuerpo y G un subgrupo finito del grupo multiplicativo $K^\times = K \setminus \{0\}$.
 - Probar que G es isomorfo al producto directo de sus subgrupos de Sylow.
 - Consideremos S un p -subgrupo de Sylow de G . Sea $r = \text{máx}\{m \in \mathbb{Z}^+ : \exists a \in S, |a| = p^m\}$. Probar que S está contenido en el conjunto de las raíces en K del polinomio $X^{p^r} - 1 \in K[X]$. Deducir $|S| \leq p^r$ y concluir que S es cíclico.
 - Probar que G es cíclico.

Notar que esto implica que si K es finito, entonces K^\times es cíclico.

- Sea K un cuerpo. Para cada $n \in \mathbb{Z}^+$ se define $U_n(K) = \{x \in K : x^n = 1\}$.
 - Probar que existe $\zeta \in U_n(K)$ tal que $U_n(K) = \{\zeta^m : m \in \mathbb{Z}\}$.
 - Probar que si p es un primo tal que $\text{mcd}(n, p-1) = 1$, entonces $U_n(\mathbb{Z}_p) = \{1\}$.
 - Hallar explícitamente $U_3(\mathbb{C})$ y $U_3(\mathbb{Z}_p)$ en los casos $p = 5, 7, 11$.