Práctica 4 - Segunda Parte

1. Sean K un cuerpo finito de $q = p^n$ elementos y $f \in K[X]$ irreducible.
- Probar que si C es una clausura algebraica de K , entonces toda raíz de f en C es simple.
 - Probar que si $\alpha \in C$ es raíz de f , entonces α^q también es raíz de f . Probar que el conjunto de raíces de f en C es

$$\{\alpha^{q^i} : 0 \leq i < m\}.$$

2. Sea K un cuerpo finito de p^n elementos.

- Si r es coprimo con $p^n - 1$, entonces todo elemento de K es una potencia r -ésima.
- Si $r \mid (p^n - 1)$, entonces $\alpha \in K$ es una potencia r -ésima si y sólo si

$$\alpha^{\frac{p^n-1}{r}} = 1.$$

Sugerencia: Recordar que $K^\times$ es cíclico.

3. Sea K un cuerpo de q elementos.

- Sea $f \in K[X]$ irreducible. Probar que f divide a $X^{q^n} - X$ sii $\text{gr}(f)$ divide a n .
- Probar que $X^{q^n} - X = \prod_{d|n} (\prod f_d)$, donde el producto de adentro recorre todos los polinomios irreducibles mónicos de grado d en $K[X]$.
- Deducir que $q^n = \sum_{d|n} d \cdot u(d)$, donde $u(d)$ es la cantidad de polinomios irreducibles mónicos de grado d en $K[X]$.
- Calcular $u(d)$ para el caso en que d es una potencia de un primo.
- Calcular la cantidad de polinomios de grado 3 y 4 mónicos e irreducibles que hay en un cuerpo de 2^{12} y en uno de 3^{12} elementos.

4. Sea $f \in \mathbb{F}_q[X]$ irreducible de grado n y sea $k \in \mathbb{N}$. Probar que f se factoriza en $\mathbb{F}_{q^k}[X]$ como producto de polinomios irreducibles de grado $\frac{n}{d}$, donde $d = \text{mcd}(n, k)$. Deducir que f sigue siendo irreducible en $\mathbb{F}_{q^k}[X]$ si y sólo si n y k son coprimos.

5. Sea $p \in \mathbb{N}$ primo. Probar que para todo $a \in \mathbb{F}_p^\times$, el polinomio $X^p - X + a$ es irreducible en $\mathbb{F}_p[X]$.

6. Hallar elementos primitivos de $E/\mathbb{Q}$, donde E es cuerpo de descomposición del polinomio:

- $X^3 - 2$
- $(X^2 - 3)(X^2 - 2)$
- $X^4 - 2$
- $(X^4 + 1)(X^2 + 5)$

7. Hallar un elemento primitivo de $E/\mathbb{F}_2$, donde E es un cuerpo de 8 elementos.
8. Sea K un cuerpo de característica p y sean u y v indeterminadas.
- Probar que $K(u, v)$ tiene grado p^2 sobre $K(u^p, v^p)$.
 - Probar que existen infinitas extensiones entre $K(u, v)$ y $K(u^p, v^p)$.
9. Sea E una extensión finita de un cuerpo K de característica p y sea $p^r = [E : K]_i$. Sea

$$k = \min\{i : \forall \alpha \in E, \alpha^{p^i} \in E_s\}.$$

Probar que si $k = r$ entonces E/K es monógena.

10. Sea C una clausura algebraica de $\mathbb{F}_p$ y sea q un primo distinto de p . Sea L la unión de todas las subextensiones K de $C/\mathbb{F}_p$ cuyo grado sobre $\mathbb{F}_p$ es una potencia de q . Probar que $[L : \mathbb{F}_p] = \infty$ y que toda subextensión propia de $L/\mathbb{F}_p$ es monógena.