Práctica 4 - Segunda parte

1. Sea K un cuerpo. Notemos $(K,+)$ al grupo aditivo de K y $(K^*,\cdot\,)$ al grupo multiplicativo. Probar que $(K,+)$ y $(K^*,\cdot\,)$ nunca son isomorfos como grupos. Caracterizar ambos grupos en el caso en que K es finito.

2. Probar que dos cuerpos finitos de igual cardinal son isomorfos.

3. Sea $f \in \mathbb{F}_q[X]$ un polinomio irreducible y sea C una clausura algebraica de $\mathbb{F}_q$.

   (a) Probar que toda raíz de f en C es simple.

   (b) 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 $\{\alpha^{q^i} : 0 \leq i < m\}$ con $m = \mathrm{gr}(f)$.

4. (a) Sea $f \in \mathbb{F}_q[X]$ irreducible. Probar que $f \mid X^{q^n} - X$ si y sólo si $\mathrm{gr}(f) \mid n$.

   (b) Probar que $X^{q^n} - X = \prod_{d|n}(\prod f)$, donde el producto de adentro recorre todos los polinomios irreducibles mónicos de grado d en $\mathbb{F}_q[X]$.

   (c) Deducir que $q^n = \sum_{d|n} d.u(d)$, donde $u(d)$ es la cantidad de polinomios irreducibles mónicos de grado d en $\mathbb{F}_q[X]$.

   (d) Calcular $u(d)$ para el caso en que d es una potencia de un primo.

5. 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 $d = \mathrm{mcd}(n,k)$. Deducir que f sigue siendo irreducible en $\mathbb{F}_{q^k}[X]$ si y sólo si n y k son coprimos.

6. Sea $p \in \mathbb{N}$ un primo. Probar que para todo $a \neq 0$, el polinomio $X^p - X + a$ es irreducible en $\mathbb{F}_p[X]$.

7. Hallar elementos primitivos de $E/\mathbb{Q}$, donde E es el cuerpo de descomposición de:

   (a) $X^3 - 2$

   (b) $(X^2 - 3)(X^2 - 2)$

   (c) $X^4 - 2$

   (d) $(X^4 + 1)(X^2 + 5)$

8. Sea p un primo y sean u, v algebraicamente independientes sobre $\mathbb{F}_p$.

   (a) Probar que $\mathbb{F}_p(u,v)$ tiene grado p^2 sobre $\mathbb{F}_p(u^p, v^p)$.

   (b) Probar que existen infinitas extensiones entre $\mathbb{F}_p(u,v)$ y $\mathbb{F}_p(u^p, v^p)$.

9. Sea E una extensión finita de un cuerpo K de característica $p > 0$ y sea $p^r = [E : K]_i$. Probar que si $r = \min\{j : \forall \alpha \in E, \alpha^{p^j} \in E_s\}$ entonces E/K es monógena.