Algebra III

Práctica 6 - Primer cuatrimestre de 2006

Ejercicio 1. Sea K un cuerpo finito. Probar que el grupo multiplicativo K^* es cíclico. Concluir que toda extensión finita de un cuerpo finito es simple.

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

Ejercicio 3. Sea $p \in \mathbb{N}$ un primo y sean $n, m \in \mathbb{N}$. Probar que $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ si y solo si $n|m$.

Ejercicio 4. Sean K un cuerpo finito y $f \in K[X]$ irreducible. Probar que f tiene todas sus raices distintas (en la clausura algebraica C de K). Mas aún, si f tiene grado n y $\alpha \in C$ es raíz de f, entonces todas las raices de f son α^{q^i} con $0 \leqslant i < n$. Concluir que toda extensión finita de K es normal y separable.

Ejercicio 5. Sea K un cuerpo de q elementos y sea E/K una extensión finita. Probar que $\mathrm{Gal}(E/K) = \langle \sigma \rangle$, donde $\sigma : E \to E$ está definido por $\sigma(x) = x^q \; \forall\, x \in E$.

Ejercicio 6. Sea K un cuerpo de q elementos.

1. Sea $f \in K[X]$ irreducible. Probar que $f | X^{q^n} - X$ si y solo si $\mathrm{gr}(f)|n$.
2. Probar que $X^{q^n} - X = \prod_{d|n} (\prod f)$, donde el producto de adentro recorre todos los $f \in K[X]$ irreducibles mónicos de grado d.
3. Probar que $q^n = \sum_{d|n} u(d)d$, donde $u(d)$ es la cantidad de polinomios mónicos irreducibles de grado d en $K[X]$.
4. Utilizar la fórmula de inversión de Moebius para obtener $u(n)$ para todo $n \in \mathbb{N}$.
5. Calcular cuantos polinomios irreducible de grados 3 y 4 hay en un cuerpo de 2^{12} elementos. Lo mismo en un cuerpo de 3^{12} elementos.

Ejercicio 7. 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 n/d, donde $d = \gcd(n, k)$. Concluir que f sigue siendo irreducible en $\mathbb{F}_{q^k}[X]$ si y solo si n y k son coprimos.

Ejercicio 8. Sea $p \in \mathbb{N}$ primo. Probar que para todo $a \in \mathbb{F}_p^*$, el polinomio $X^p - X + a$ es irreducible en $\mathbb{F}_p[X]$.

Ejercicio 9. Sea K un cuerpo de q elementos y sea $n \in \mathbb{N}$ coprimo con $\mathrm{car}(K)$. Sea $E = K[\xi_n]$, donde ξ_n es una raíz primitiva n-ésima de la unidad.

1. Probar que $[E : K] = m$, donde $m \in \mathbb{N}$ es el menor natural tal que $n | q^m - 1$.
2. Probar que Φ_n se factoriza en $K[X]$ como producto de polinomios irreducibles de grado m.
3. Deducir que Φ_n es irreducible en $K[X]$ si y solo si q tiene orden $\varphi(n)$ en $\mathcal{U}_n$.

Ejercicio 10. Probar que $\Phi_{12} = X^4 + 1$ es reducible en $\mathbb{F}_p[X]$ para todo $p \in \mathbb{N}$ primo.

Ejercicio 11. Probar que:

1. $\mathbb{F}_3$ no contiene raices 13-ésimas de la unidad distintas de 1.
2. Si $\xi_{13} \in \overline{\mathbb{F}_3}$ es una raíz 13-ésima primitiva de la unidad, entonces $[\mathbb{F}_3[\xi_{13}] : \mathbb{F}_3] = 3 < \varphi(13)$.

Ejercicio 12. Hallar todos los $n \in \mathbb{N}$ tales que Φ_n es irreducible en $\mathbb{F}_9[X]$.

Ejercicio 13. Sea $p \in \mathbb{N}$ primo. Hallar todos los $n \in \mathbb{N}$ tales que Φ_6 es irreducible en $\mathbb{F}_{p^n}$.

Ejercicio 14. Factorizar Φ_7 en $\mathbb{F}_{27}[X]$ y Φ_9 en $\mathbb{F}_7[X]$.

Ejercicio 15. Sea $p \in \mathbb{N}$ primo. Sea C una clausura algebraica de $\mathbb{F}_p$. Probar que existe un elemento en $\mathrm{Gal}(C/\mathbb{F}_p)$ que no es una potencia del automorfismo de Frobenius $\sigma : C \to C$ dado por $\sigma(x) = x^p$. Mas aún, caracterizar el grupo de Galois $\mathrm{Gal}(C/\mathbb{F}_p)$.