Álgebra III

Práctica 5 - Segundo cuatrimestre de 2016
Cuerpos finitos y extensiones ciclotómicas

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 monógena.

Ejercicio 2. 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 3. 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. Calcular cuántos polinomios irreducibles de grados 3 y 4 hay en un cuerpo de 2^{12} elementos. Lo mismo en un cuerpo de 3^{12} elementos.
5. * Obtener una fórmula cerrada para $u(n)$ para todo $n \in \mathbb{N}$.

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

Ejercicio 5. 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 $\sigma(x) = x^p$. Más aún, caracterizar $\mathrm{Gal}(C/\mathbb{F}_p)$.

Ejercicio 6. Sea $n \in \mathbb{N}$ impar, y sea K un cuerpo de característica distinta de 2. Probar que K contiene a una raíz n-ésima primitiva de la unidad si y solo si contiene una raíz $2n$-ésima primitiva de la unidad.

Ejercicio 7.

1. Sea $K/\mathbb{Q}$ una extensión finita. Probar que hay sólo un número finito de raíces de la unidad en K.
2. Hallar todas las raíces de la unidad en K cuando K es uno de los siguientes cuerpos: $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt{-2}]$, $\mathbb{Q}[\xi_9]$, $\mathbb{Q}[\sqrt{2}, \sqrt{-3}]$, $\mathbb{Q}[\sqrt[p]{2}]$.

Ejercicio 8. Para cada $n \in \mathbb{N}$ sea Φ_n el polinomio ciclotómico de orden n sobre $\mathbb{Q}$. Probar que

1. Si p es primo y $r \in \mathbb{N}$ entonces $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.
2. Si p es primo y p no divide a n entonces $\Phi_{pn}(X)\Phi_n(X) = \Phi_n(X^p)$.
3. Calcular explícitamente Φ_{18} y Φ_{30}.

Ejercicio 9. Hallar todos los $n \in \mathbb{N}$ tales que Φ_n es irreducible sobre $\mathbb{Q}(\xi_9)$.

Ejercicio 10. 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 11. Probar que $f = X^4 + 1$ es reducible en $\mathbb{F}_p[X]$ para todo $p \in \mathbb{N}$ primo. ¿ Es f reducible en $\mathbb{Z}[X]$?

Ejercicio 12. Probar que:

1. $\mathbb{F}_3$ no contiene raíces 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 13. Sea $n, m \in \mathbb{Z}$. Probar que el polinomio $X^6 - (5n + 1)X^3 + (5m + 1)$ es irreducible en $\mathbb{Q}[X]$.

Ejercicio 14. Hallar todos los $n \in \mathbb{N}$ tales que Φ_n es irreducible en $\mathbb{F}_9[X]$.

Ejercicio 15. 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 16. Factorizar $\Phi_7(X)$ en $\mathbb{F}_{27}[X]$ y $\Phi_9(X)$ en $\mathbb{F}_7(t)[X]$.

Ejercicio 17. Sea K un cuerpo de q elementos y sea n coprimo con q. Sea $\xi_n \in \overline{K}$ una raíz primitiva n-ésima de la unidad. Probar que

$$\xi_n + {\xi_n}^{-1} \in K \iff q \equiv \pm 1 \bmod n.$$