Álgebra III

Práctica 5 - Cuerpos finitos y extensiones ciclotómicas

2do cuatrimestre 2017

Ejercicio 1. Probar que todo polinomio irreducible en $\mathbb{F}_q[X]$, con $q = p^k$, es separable.

Ejercicio 2. Sea $f \in \mathbb{F}_q[X]$, con $q = p^k$, irreducible de grado n y $\alpha \in \overline{\mathbb{F}_q}$ raíz de f. Probar que $\mathbb{F}_q[\alpha]/\mathbb{F}_q$ es Galois y $\mathrm{Gal}(\mathbb{F}_q[\alpha]/\mathbb{F}_q) = \langle \Phi \rangle$ con $\Phi(x) = x^q$, $\forall\, x \in \mathbb{F}_q[\alpha]$.
Concluir que $f = \prod_{0 \leq k \leq n-1} (X - \alpha^{q^k})$.

Ejercicio 3.

1. Sea $f \in \mathbb{F}_q[X]$ 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 $f \in \mathbb{F}_q[X]$ 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 $\mathbb{F}_q[X]$.
4. Utilizar la fórmula de inversión de Möbius para obtener $u(n)$ para todo $n \in \mathbb{N}$.
5. Calcular cuántos polinomios irreducibles de grados 3 y 4 hay en $\mathbb{F}_{2^{12}}[X]$ y en $\mathbb{F}_{3^{12}}[X]$.

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

Ejercicio 5. Sea $p \in \mathbb{N}$ primo. Probar que existe un elemento en $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ que no es una potencia del automorfismo de Frobenius $\Phi : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ dado por $\Phi(x) = x^p$. Caracterizar el grupo de Galois $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$.

Ejercicio 6. Sea $n \in \mathbb{N}$ impar y sea K un cuerpo con $\mathrm{car}(K) \neq 2$. Probar que K contiene una raíz n-ésima primitiva de 1 si y sólo si K contiene una raíz $2n$-ésima primitiva de 1.

Ejercicio 7. Hallar todos los $m \in \mathbb{N}$ para los cuales una raíz m-ésima primitiva de 1 tiene grado 2 o 4 sobre $\mathbb{Q}$.

Ejercicio 8.

1. Sea $K/\mathbb{Q}$ una extensión de grado finito. Probar que existe sólo un número finito de raíces de la unidad en K.
2. Determinar todas las raíces de la unidad contenidas en cada uno de los siguientes cuerpos: $\mathbb{Q}[\,i\,]$, $\mathbb{Q}[\sqrt{-2}\,]$, $\mathbb{Q}[\sqrt{2}\,]$, $\mathbb{Q}[\sqrt{-3}\,]$, $\mathbb{Q}[\sqrt{-5}\,]$, $\mathbb{Q}[\sqrt{2}, \sqrt{-3}\,]$ y $\mathbb{Q}(\xi_9)$.

Ejercicio 9. Sea $\Phi_n \in \mathbb{Z}[X]$ el polinomio ciclotómico de orden n. Probar que:

1. Para cada $r \in \mathbb{N}$ y cada primo $p \in \mathbb{N}$, $\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}})$.
2. Si $n = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$ con $p_1 \dots, p_s$ primos distintos, $\Phi_n(X) = \Phi_{p_1 \dots p_s}\big(X^{p_1^{r_1 - 1} \dots p_s^{r_s - 1}}\big)$.
3. Si n es impar, $\Phi_{2n}(X) = \Phi_n(-X)$.

4. Si p es primo, $p \nmid n$, entonces $\Phi_{pn}(X) = \dfrac{\Phi_n(X^p)}{\Phi_n(X)}$.

Ejercicio 10. Sean E/K y F/K extensiones ciclotómicas de índices m y n respectivamente, con $(m : n) = 1$, contenidas en una clausura algebraica $\overline{K}$ de K. Probar que:

1. EF/K es una extensión ciclotómica de índice mn.
2. Si $K = \mathbb{Q}$, entonces $E \cap F = \mathbb{Q}$.

Ejercicio 11.

1. Sea $E/\mathbb{Q}$ una extensión cuadrática. Probar que Φ_n es reducible en $E[X]$ si y sólo si $E \subset \mathbb{Q}(\xi_n)$.
2. Determinar todas las extensiones cuadráticas $E/\mathbb{Q}$ tales que Φ_{12} es irreducible en $E[X]$. Idem para Φ_8 y Φ_{10}.

Ejercicio 12. Hallar todos los $n \in \mathbb{N}$ tales que Φ_n es irreducible sobre $\mathbb{Q}(\xi_9)$.

Ejercicio 13. Sea K un cuerpo, sea $\Psi : \mathbb{Z} \to K$ el único morfismo de anillos con unidad y sea $\overline{\Psi} : \mathbb{Z}[X] \to K[X]$ el morfismo de anillos inducido por Ψ definido como $\overline{\Psi}\left(\sum a_i X^i\right) = \sum \Psi(a_i) X^i$. Como $\Phi_n \in \mathbb{Z}[X]$, podemos pensar a Φ_n en $K[X]$ vía $\overline{\Phi}$.

1. Probar que:
   a) $\Phi_n \in K[X]$ es mónico de grado $\varphi(n)$.
   b) $X^n - 1 = \prod_{d|n} \Phi_d$ en $K[X]$.
   c) Si $\mathrm{car}(K) \neq 0$ y n es coprimo con $\mathrm{car}(K)$, entonces Φ_n tiene todas sus raíces simples.
2. Sea $\overline{K}/K$ una clausura algebraica y sea $\xi \in \overline{K}$ una raíz n-ésima primitiva de 1 (i.e. $\xi^n = 1$ y $\xi^r \neq 1,\ \forall\, r < n$). Probar que, si $\mathrm{car}(K) \nmid n$:
   a) $\xi \in \overline{K}$ es raíz de Φ_n si y sólo si ξ es raíz n-ésima primitiva de 1.
   b) La cantidad de raíces n-ésimas primitivas de 1 en $\overline{K}$ es $\varphi(n)$.
   c) Si ξ_n es una raíz n-ésima primitiva de 1 en $\overline{K}$, entonces $\xi \in \overline{K}$ es otra raíz n-ésima primitiva de 1 si y sólo si $\xi = \xi_n^j$ para algún $1 \leq j \leq n$ tal que $(j : n) = 1$.

Ejercicio 14. Sea K un cuerpo y sea $n \in \mathbb{N}$ tal que $\mathrm{car}(K) \nmid n$. Probar que Φ_n se factoriza en $K[X]$ como producto de polinomios irreducibles de grado $[K(\xi_n) : K]$, donde ξ_n es una raíz n-ésima primitiva de 1.

Ejercicio 15. Sea $K/\mathbb{F}_q$ con $q = p^k$, una extensión ciclotómica de índice n, con n coprimo con p. Probar que:

1. $K = \mathbb{F}_{q^m}$, donde m es el menor número natural tal que $n \mid q^m - 1$.
2. Probar que el polinomio ciclotómico $\Phi_n \in \mathbb{Z}[X]$ se factoriza en $\mathbb{F}_q[X]$ como producto de polinomios irreducibles de grado m.
3. Deducir que Φ_n es irreducible en $\mathbb{F}_q[X]$ si y sólo si la clase de q en $\mathcal{U}_n$ tiene orden $\varphi(n)$.

Ejercicio 16. 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 17. Hallar todos los $n \in \mathbb{N}$ tales que Φ_n es irreducible en $\mathbb{F}_9[X]$.

Ejercicio 18. Sea $p \in \mathbb{N}$ primo. Hallar todos los $n \in \mathbb{N}$ tales que Φ_6 es irreducible en $\mathbb{F}_{p^n}[X]$.

Ejercicio 19. Factorizar Φ_7 en $\mathbb{F}_{27}[X]$ y Φ_9 en $\mathbb{F}_7[X]$.

Ejercicio 20. Probar que si p es primo, $p \neq 2, 3$, entonces Φ_{12} es reducible en $\mathbb{F}_p[X]$.

Ejercicio 21.

1. Sea K un cuerpo de 27 elementos. Factorizar Φ_7 como producto de polinomios irreducibles en $K[X]$.
2. Sea t trascendente sobre $\mathbb{F}_7$ y sea $K = \mathbb{F}_7(t)$. Factorizar Φ_9 como producto de polinomios irreducibles en $K[X]$.