Práctica 6

Notación: a lo largo de esta práctica, φ denota la función de Euler, ϕ_n el polinomio ciclotómico de orden n y ξ_n una raíz n-ésima primitiva de la unidad.

1. Sea K un cuerpo, sea $g : \mathbb{Z} \to K$ el único morfismo de anillos con unidad. Sea $\bar{g} : \mathbb{Z}[X] \to K[X]$ el morfismo de anillos inducido por g, es decir,

$$\bar{g}(\sum a_i X^i) = \sum g(a_i) X^i.$$

   Como $\phi_n \in \mathbb{Z}[X]$, podemos pensar a ϕ_n en $K[X]$ vía $\bar{g}$.

   (a) Probar que:
   - $\phi_n \in K[X]$ es mónico de grado $\varphi(n)$
   - $X^n - 1 = \prod_{d|n} \phi_d$ en $K[X]$.
   - Si $\text{car}(K) \neq 0$ y n es coprimo con $\text{car}(K)$ entonces ϕ_n tiene todas sus raíces simples.

   (b) Sea C/K una clausura algebraica. Si n es coprimo con $\text{car}(K)$, probar que:
   - $\xi \in C$ es raíz de ϕ_n si sólo si ξ es raíz n-ésima primitiva de 1.
   - La cantidad de raíces n-ésimas primitivas de 1 en C es $\varphi(n)$.
   - $\xi \in C$ es otra raíz primitiva n-ésima de 1 si y sólo si $\xi = \xi_n^j$ para algún $1 \leq j \leq n$ tal que $(j; n) = 1$.

2. (a) Sea $E/\mathbb{Q}$ una extensión de grado finito. Probar que existe sólo un número finito de raíces de la unidad en E.

   (b) Determinar qué raíces de la unidad contienen $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2}, \sqrt{-3}), \mathbb{Q}(\xi_9)$.

3. (a) Sea $E/\mathbb{Q}$ una extensión cuadrática. Probar que ϕ_n es reducible en $E[X]$ si y sólo si $E \subseteq \mathbb{Q}(\xi_n)$.

   (b) Determinar las extensiones cuadráticas $E/\mathbb{Q}$ tales que ϕ_{12} es irreducible en $E[X]$. Idem para ϕ_8 y ϕ_{10}.

4. Sean E/K y F/K dos extensiones ciclotómicas de índices m y n respectivamente, contenidas en una misma clausura algebraica C/K y tales que $(m; n) = 1$. Probar que $E \cdot F/K$ es ciclotómica de índice mn. Probar además que si $K = \mathbb{Q}$, entonces $E \cap F = \mathbb{Q}$.

5. Sean K un cuerpo de característica positiva y $n \in \mathbb{N}$ coprimo con la característica de K. Sea C/K una clausura algebraica. Probar que si ϕ_n es irreducible en $K[X]$, entonces $K(\xi_n)/K$ es separable, normal y de grado $\varphi(n)$.

6. Sea K cuerpo de q elementos y sea $n \in \mathbb{N}$ coprimo con $\text{car}(K)$. Sea $E = K(\xi_n)$.

(a) Probar que $[E : K] = m$, donde m es el menor natural tal que $n \mid q^m - 1$.
(b) Probar que ϕ_n se factoriza en $K[X]$ como producto de polinomios irreducibles de grado m.
(c) Deducir que ϕ_n es irreducible en $K[X]$ si y sólo si q tiene orden $\varphi(n)$ en $\mathcal{U}_n$.

7. Si $p \neq 2, 3$ entonces ϕ_{12} es reducible en $\mathbb{F}_p[X]$.

8. Probar que, para todo p, $X^4 + 1$ es reducible en $\mathbb{F}_p[X]$.

9. Probar que $\mathbb{F}_3$ no contiene raíces 13-ésimas de la unidad distintas de 1. Probar también que si $E/\mathbb{F}_3$ es ciclotómica de índice 13, entonces su grado es $3 < \varphi(13)$.

10. ¿Para qué valores de n es ϕ_n irreducible sobre un cuerpo de 9 elementos? ¿Para qué valores de n es ϕ_6 irreducible sobre un cuerpo de p^n elementos?

11. Sea K un cuerpo de 27 elementos. Factorizar ϕ_7 como productos de irreducibles en $K[X]$.

12. Sea t una variable y sea $K = \mathbb{F}_7(t)$. Hallar la factorización de ϕ_9 como producto de irreducibles en $K[X]$.

13. (a) Calcular la norma y la traza de $\sqrt[3]{2}$ en $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ y en $\mathbb{Q}(\sqrt[3]{2}, \xi_3)\mathbb{Q}$.
(b) Sea $p \in \mathbb{N}$ primo. Calcular la norma y la traza de ξ_p en $\mathbb{Q}(\xi_p)/\mathbb{Q}$.
(c) Sea d un entero libre de cuadrados y sea $a \in \mathbb{Q}(\sqrt{d}) \setminus \mathbb{Q}$. Probar que $m(a, \mathbb{Q}) = X^2 - \mathrm{Tr}(a)X + \mathrm{N}(a)$.

14. Sea K un cuerpo de característica $p > 0$ y sea X una indeterminada. Calcular la norma y la traza de X en:

(a) $K(X)/K(X^p)$,
(b) $K(X)/K(X^p - X - a)$, $a \in K$.

15. Sea $p \in \mathbb{N}$ un primo mayor que 3 y sean u, v indeterminadas. Sean $K = \mathbb{F}_p(u^3, v^2)$ y $E = \mathbb{F}_p(u, v)$. Calcular la norma y la traza de $u + v$ en E/K.

16. Sea K un cuerpo de característica $p > 0$ y sea E/K una extensión de grado q, con q primo distinto de p. Probar que existe un $\alpha \in E$ tal que $E = K(\alpha)$ y tal que el coeficiente de grado $q - 1$ de $m(\alpha, K)$ es cero.

17. (a) Calcular el núcleo y la imagen del morfismo de grupos de $\mathbb{C}^\times$ en $\mathbb{R}^\times$ inducido por la aplicación $\mathrm{N} : \mathbb{C} \to \mathbb{R}$.
(b) Probar que en $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ la norma no es inyectiva ni suryectiva.

18. Sea K un cuerpo finito y sea L/K una extensión finita. Probar que la norma y la traza en L/K son suryectivas.

19. Sea t una indeterminada. Sean $K = \mathbb{F}_7(t^7 - t)$ y $E = \mathbb{F}_7(t)$.

(a) Hallar una base del núcleo de la transformación lineal $\mathrm{Tr}_{E/K} : E \to K$.
(b) Encontrar una base de E como K-espacio vectorial formada por elementos de traza 1.

20. Sea K un cuerpo de característica p y sea E/K una extensión de grado n, $(n, p) = 1$. Sea $x \in E$. Probar que si $\mathrm{Tr}(x^i) = 0$ para todo $1 \leq i \leq n$, entonces $x = 0$.