Práctica 6

Nota: En esta práctica φ es la función de Euler, $\phi_n \in \mathbb{Z}[X]$ es el polinomio ciclotómico de orden n y ξ_n es una raíz enésima primitiva de la unidad.

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

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 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 $\mathbb{Q}(\xi_9)$.

3. Probar que:
   a) Si $p \in \mathbb{N}$ es primo, entonces $\phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$.
   b) Para cada $r \in \mathbb{N}$ y cada primo $p \in \mathbb{N}$, $\phi_{p^r}(X) = \phi_p(X^{p^{r-1}})$.
   c) Si $n = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$ con $\{p_i\}$ primos distintos, $\phi_n(X) = \phi_{p_1 \dots p_s}\left(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}}\right)$.
   d) Si n es impar, $\phi_{2n}(X) = \phi_n(-X)$.
   e) Si p es primo, $p \nmid n$, entonces $\phi_{pn}(X) = \dfrac{\phi_n(X^p)}{\phi_n(X)}$.

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

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

6. Sea K un cuerpo, sea $g : \mathbb{Z} \to K$ el único morfismo de anillos con unidad y sea $\overline{g} : \mathbb{Z}[X] \to K[X]$ el morfismo de anillos definido por

$$\overline{g}\left(\sum a_i X^i\right) = \sum g(a_i) X^i.$$

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

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

b) Sea C/K una clausura algebraica y sea $\xi \in C$ una raíz n-ésima primitiva de 1 (i.e. $\xi^n = 1$ y $\xi^r \neq 1 \ \forall\, r < n$). Si $\mathrm{car(K)} \nmid n$, probar que:

(i) $\xi \in C$ es raíz de ϕ_n si y sólo si ξ es raíz n-ésima primitiva de 1.

(ii) La cantidad de raíces n-ésimas primitivas de 1 en C es $\varphi(n)$.

(iii) Si ξ_n es una raíz n-ésima primitiva de 1 en C, entonces $\xi \in C$ 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 $(j : n) = 1$.

7. 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.

8. 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.

9. Sea $E/\mathbb{F}_q$ una extensión ciclotómica de índice n, con $(n, q) = 1$. Probar que:

a) E es un cuerpo de q^m elementos, donde m es el menor número natural tal que $n \mid q^m - 1$.

b) Deducir que ϕ_n es irreducible en $\mathbb{F}_q[X]$ si y sólo si q tiene orden $\varphi(n)$ en $\mathcal{U}_n$.

10. Probar que:

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

b) El polinomio $X^4 + 1$ es reducible en $\mathbb{F}_p[X]$ para todo primo p.

11. Probar que:

a) $\mathbb{F}_3$ no contiene raíces 13-ésimas de la unidad distintas de 1.

b) Si $E/\mathbb{F}_3$ es una extensión ciclotómica de índice 13, entonces $[E : \mathbb{F}_3] = 3 < \varphi(13)$.

12. a) Hallar todos los $n \in \mathbb{N}$ tales que ϕ_n es irreducible sobre $\mathbb{F}_9$.

b) Sea $p \in \mathbb{N}$ primo. Hallar todos los $m \in \mathbb{N}$ tales que ϕ_6 es irreducible sobre $\mathbb{F}_{p^m}$.

13. Factorizar ϕ_7 como producto de polinomios irreducibles en $\mathbb{F}_{27}[X]$.

14. 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 $p \in N$ 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 $a \in \mathbb{Q}(\sqrt{d}) - \mathbb{Q}$. Probar que $\boldsymbol{m}(a, \mathbb{Q}) = X^2 - \mathrm{Tr}(a)X + \mathrm{N}(a)$.

15. Sea K un cuerpo de característica $p > 0$ y sea X trascendente sobre K. Calcular la norma y la traza de X en $K(X)/K(X^p)$.

16. Sea $p \in \mathbb{N}$ un primo mayor que 3 y sean u, v algebraicamente independientes sobre $\mathbb{F}_p$. 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.

17. 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 $\alpha \in E$ tal que $E = K(\alpha)$ y tal que el coeficiente de grado $q-1$ de $\boldsymbol{m}(\alpha, K)$ es cero.

18. (a) Calcular el núcleo y la imagen del morfismo de grupos $\mathbb{C}^* \to \mathbb{R}^*$ 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 ni inyectiva ni suryectiva.

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

20. Sean $K = \mathbb{F}_7(t^7 - t)$ y $E = \mathbb{F}_7(t)$ con t trascendente sobre $\mathbb{F}_7$.

    a) Hallar una base del núcleo de la transformación lineal $\mathrm{Tr}_{E/K} : E \to K$.

    b) Hallar una base de E como K-espacio vectorial formada por vectores de traza 1.

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