ÁLGEBRA 3
Segundo cuatrimestre — 2019

Práctica 6: Extensiones ciclotómicas - Norma y traza

Notación: Sea $\Phi_n \in \mathbb{Z}[X]$ el n-ésimo polinomio ciclotómico. Dado un cuerpo K, si $\iota_K : \mathbb{Z}[X] \to K[X]$ es el único morfismo tal que $\iota_K(X) = X$, denotaremos $\bar{\Phi}_n = \iota_K(\Phi_n) \in K[X]$; en particular, a menos que haya lugar a confusión, no haremos referencia a K en la notación para $\iota_K(\Phi_n)$.

1. Para cada $n \geq 1$ sea $\zeta_n \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad.

(*a*) Si $K/\mathbb{Q}$ es una extensión tal que $\bar{\Phi}_n \in K[X]$ es irreducible en $K[X]$, entonces $K(\zeta_n)/K$ es galoisiana de grado $\varphi(n)$, y $\mathsf{Gal}(K(\zeta_n)/K) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

(*b*) Si $K = \mathbb{Q}\left(\sqrt[3]{2}\right)$, describa $\mathsf{Gal}(K(\zeta_{20})/K)$.

2. Encuentre todos los números $m \in \mathbb{N}$ para los que una raíz m-ésima primitiva de la unidad tiene grado 2 o 4 sobre $\mathbb{Q}$.

3. (*a*) Demuestre que toda extensión finita de $\mathbb{Q}$ contiene un número finito de raíces de la unidad.

(*b*) Encuentre todas las raíces de la unidad contenidas en $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{-2}\right)$, $\mathbb{Q}\left(\sqrt{2}\right)$, $\mathbb{Q}\left(\sqrt{-3}\right)$, $\mathbb{Q}\left(\sqrt{-5}\right)$, $\mathbb{Q}\left(\sqrt{2}, \sqrt{-3}\right)$ y $\mathbb{Q}\left(\zeta_9\right)$.

4. Sean $n \in \mathbb{N}$ y $p \in \mathbb{N}$ un número primo. Probar que:

(*a*) $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$.

(*b*) Si $r \in \mathbb{N}$, entonces $\Phi_{p^r}(X) = \Phi_p\left(X^{p^{r-1}}\right)$.

(*c*) Si $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} \in \mathbb{N}$ con $p_1, \ldots, p_s$ primos distintos, entonces

$$\Phi_n(X) = \Phi_m(X^e),$$

siendo $m = p_1 \cdots p_s$ y $e = p_1^{r_1 - 1} \cdots p_s^{r_s - 1}$.

(*d*) Si n es impar, entonces $\Phi_{2n}(X) = \Phi_n(-X)$.

(*e*) Si $p \nmid n$, entonces

$$\Phi_{pn}(X) = \frac{\phi_n(X^p)}{\phi_n(X)}.$$

5. (*a*) Sea $E/\mathbb{Q}$ una extensión cuadrática. Probar que el polinomio ciclotómico $\bar{\Phi}_n \in E[X]$ es reducible sii $E \subseteq \mathbb{Q}(\zeta_n)$.

(*b*) Encuentre todas las extensiones cuadráticas de $\mathbb{Q}$ sobre las que $\bar{\Phi}_{12}, \bar{\Phi}_8$ y $\bar{\Phi}_{10}$ son reducibles.

6. ¿Para qué valores de $n \in \mathbb{N}$ es $\bar{\Phi}_n$ irreducible sobre $\mathbb{Q}\left(\zeta_9\right)$?

7. Sea K un cuerpo. Probar que:

(*a*) El polinomio $\bar{\Phi}_n \in K[X]$ es mónico de grado $\varphi(n)$.

(*b*) Se tiene $X^n - 1 = \prod_{d|n} \bar{\Phi}_d$ en $K[X]$.

(*c*) Si K tiene característica p positiva y n es coprimo con p, entonces $\bar{\Phi}_n$ es un polinomio separable.

(*d*) Sea C/K una clausura algebraica y sea $\zeta \in C$ una raíz n-ésima primitiva de la unidad, de manera que si $k \in \mathbb{Z}$ vale que $\zeta^k = 1$ sii $n \mid k$.

(*i*) La característica de K no divide a n.

(*ii*) Un elemento $x \in C$ es raíz de $\bar{\Phi}_n$ sii x es una raíz n-ésima primitiva de la unidad.

(*iii*) Hay exactamente $\varphi(n)$ raíces n-ésimas primitivas de 1 en C.

(*iv*) Un elemento $x \in C$ es una raíz n-ésima primitiva de la unidad sii existe $k \in \{1, \dots, n-1\}$ tal que $(k, n) = 1$ y $x = \zeta^k$.

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

9. Sea K un cuerpo y sea $n \in \mathbb{N}$ coprimo con la característica de K. Sea ζ_n una raíz n-ésima primitiva de la unidad en una clausura algebraica C de K. Sea $f \in K[X]$ irreducible. Probar que si f divide a $\bar{\Phi}_n$, entonces $\deg f = [K(\zeta_n) : K]$.

10. Sea q una potencia de un primo, y sea n un natural coprimo con q.

(*a*) Sea E una extensión ciclotómica de $\mathbb{F}_q$ de índice n. Probar que E tiene q^m elementos, con m el menor número natural tal que $n \mid q^m - 1$.

(*b*) Probar que el polinomio $\bar{\Phi}_n \in \mathbb{F}_q[X]$ es irreducible sii q tiene orden $\varphi(n)$ en $(\mathbb{Z}/n\mathbb{Z})^\times$.

11. Probar que:

(*a*) Si p es un primo mayor que 3, entonces $\bar{\Phi}_{12}$ es reducible en $\mathbb{F}_p[X]$.

(*b*) El polinomio $X^4 + 1$ es reducible en $\mathbb{F}_p[X]$ cualquiera sea el primo p.

12. Probar que:

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

(*b*) Si E es una extensión ciclotómica de índice 13 de $\mathbb{F}_3$, entonces

$$[E : \mathbb{F}_3] = 3 < \varphi(13).$$

13. (*a*) Encuentre todos los $n \in \mathbb{N}$ tales que $\bar{\Phi}_n$ es irreducible sobre $\mathbb{F}_9[X]$.

(*b*) Si p es un primo, encuentre los números $m \in \mathbb{N}$ tales que $\bar{\Phi}_6$ es irreducible sobre $\mathbb{F}_{p^m}[X]$.

14. Encuentre la factorización de $\bar{\Phi}_7$ como producto de polinomios irreducibles en $\mathbb{F}_{27}[X]$.

15. (*a*) Calcule la norma y la traza de $\sqrt[3]{2}$ en $\mathbb{Q}\left(\sqrt[3]{2}\right)/\mathbb{Q}$ y en $\mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)/\mathbb{Q}$.

(*b*) Si p es primo, calcule la norma y la traza de ζ_p en $\mathbb{Q}\left(\zeta_p\right)/\mathbb{Q}$.

(*c*) Si d es un entero libre de cuadrados y $a \in \mathbb{Q}\left(\sqrt{d}\right) \setminus \mathbb{Q}$, entonces

$$m(a, \mathbb{Q}) = X^2 - \mathrm{tr}(a)X + \mathsf{N}(a).$$

16. Sea K un cuerpo de característica positiva p y sea t trascendente sobre K. Calcule la norma y la traza de t en $K(t)/K(t^p)$.

17. Sea $p \in \mathbb{N}$ un primo mayor que 3 y sean u y v algebraicamente independientes sobre $\mathbb{F}_p$. Sean $K = \mathbb{F}_p\left(u^3, v^2\right)$ y $E = \mathbb{F}_p(u, v)$. Calcule la norma y la traza de $u + v$ en E/K.

18. Sea K un cuerpo de característica positiva p y sea E/K una extensión de grado l, con l un número primo distinto de p. Existe $a \in E$ tal que $E = K(a)$ y tal que el coeficiente de grado $l - 1$ de $m(a, K)$ es cero.

19. (a) La norma de la extensión $\mathbb{C}/\mathbb{R}$ se restringe a un morfismo de grupos $\mathbb{C}^\times \to \mathbb{R}^\times$. Calcule su núcleo y su imagen.

(b) La norma de la extensión $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ no es ni inyectiva ni sobreyectiva.

20. Si L/K es una extensión finita de un cuerpo finito K, entonces la norma y la traza de L/K son funciones sobreyectivas.

21. Sea $K = \mathbb{F}_7\left(t^7 - t\right)$ y sea $E = \mathbb{F}_7(t)$ con t trascendente sobre $\mathbb{F}_7$.

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

(b) Encuentre una base de E como K-espacio vectorial cuyos elementos tengan traza igual a 1.

22. Sea K un cuerpo de característica positiva p, sea E/K una extensión de grado n coprimo con p y sea $x \in E$. Si $\mathrm{tr}_{E/K}\left(x^i\right) = 0$ para todo $i \in \{1, \ldots, n\}$, entonces $x = 0$.

Leopold Kronecker
1823–1891, Alemania