Álgebra 3
Segundo cuatrimestre — 2014
Práctica 5

1. 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 $\mathbb{Q}$.

2. (a) Una extensión finita de $\mathbb{Q}$ contiene un número finito de raíces de a unidad.

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

3. Sean $n \in \mathbb{N}$ y $p \in \mathbb{N}$ un número primo.

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

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

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

$$\Phi_n(X) = \Phi_{p_1 \ldots p_s}\big(X^{p_1^{r_1-1} \cdots p_s^{r_s-1}}\big).$$

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

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

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

4. (a) El polinomio ciclotómico Φ_n es reducible en una extensión cuadrática E de $\mathbb{Q}$ sii $E \subseteq \mathbb{Q}(\zeta_n)$.

(b) Encuentre todas las extensiones cuadráticas de $\mathbb{Q}$ sobre las que Φ_{12}, Φ_8 y Φ_{10} son reducibles,

5. ¿Para qué valores de $n \in \mathbb{N}$ es Φ_n irreducible sobre $\mathbb{Q}(\zeta_9)$?

6. Sea K un cuerpo, y consideremos el único morfismo de anillos $g : \mathbb{Z} \to K$ y el morfismo de anillos $\bar{g} : \mathbb{Z}[X] \to K[X]$ tal que $\bar{g}(X) = X$. Sea $\bar{\Phi}_n = \bar{g}(\Phi_n) \in K[X]$.

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

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

(c) Si la 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 $i \in \mathbb{Z}$ vale que $\zeta^i = 1$ sii $n \mid i$.

(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 primitivas de la unidad sii existe $j \in \{1, \ldots, n-1\}$ tal que $(j, n) = 1$ y $x = \zeta^j$.

7. Si n es impar entonces un cuerpo de característica distinta de 2 contiene una raíz n-ésima primitiva de la unidad sii contiene una raíz $2n$-ésima primitiva de la unidad.

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

9. Sea $E/\mathbb{F}_q$ una extensión ciclotómica de índice n coprimo con q.

(a) El cuerpo tiene E tiene q^m elementos, con m el menor número natural tal que $n \mid q^m - 1$.

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

10. (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.

11. (a) No hay en $\mathbb{F}_3$ raíces 13-avas de la unidad distintas de 1.

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

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

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

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

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

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

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

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

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

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

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

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

18. (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 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ no es ni inyectiva ni sobreyectiva.

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

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

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

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

21. 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 $\mathrm{tr}(x^i) = 0$ para todo $i \in \{1, \ldots, n\}$, entonces $x = 0$.

Leopold Kronecker
1823–1891, Alemania