1er cuatrimestre 2001

ALGEBRA III
Práctica 4

1. Sea K un cuerpo. Probar que los grupos $(K,+)$ y $(K^*,\cdot)$ nunca son isomorfos. Caracterizar ambos grupos en el caso en que K sea finito.

2. Sea E/K extensión y F/K una subextensión. Probar que:

   (i) Si $x \in E$ es separable sobre K entonces lo es sobre F.

   (ii) E/K es separable si y sólo si E/F y F/K lo son.

   (iii) $x \in E$ es separable sobre K si y sólo si $K(x)/K$ es separable.

3. Probar que toda extensión algebraica de un cuerpo de característica 0 es separable.

4. Probar que toda extensión algebraica de un cuerpo finito es separable.

5. Sea E/K una extensión separable que es cuerpo de descomposición de un polinomio $f \in K[X]$ de grado n. Probar que $[E:K]/n!$.

6. Sea $C/\mathbb{Z}_p$ una clausura algebraica y sean F_{p^m} y F_{p^n} los cuerpos de p^m y p^n elementos en C.

   Probar que $F_{p^m} \subseteq F_{p^n} \Leftrightarrow m/n$

7. Sea $F_q = F_{p^n}$ un cuerpo finito y F_{q^d} una extensión de F_q. Probar que F_{q^d} es normal y separable sobre F_q y que $\mathrm{Gal}(F_{q^d}/F_q)$ es cíclico de orden d generado por el automorfismo $\phi_q = (\phi_p)^n$, donde ϕ_p es el automorfismo de Frobenius.

8. Sea K un cuerpo de q elementos (es claro que $q = p^r$)

   (i) Sea $f \in K[X]$ irreducible. Probar que f divide a $X^{q^n} - X$ sii $gr\, f$ divide a n.

   (ii) Probar que $X^{q^n} - X = \prod_{d|n}(\prod f_d)$, donde el producto de adentro recorre todos los polinomios irreducibles mónicos de grado d en $K[X]$.

   (iii) Deducir que $q^n = \sum_{d|n} d.u(d)$, donde $u(d)$ es la cantidad de polinomios irreducibles mónicos de grado d.

   (iv) Calcular $u(d)$ para el caso en que d es una potencia de un primo.

   (v) Calcular la cantidad de polinomios de grado 3 y 4 mónicos e irreducibles que hay en un cuerpo de 2^{12} y 3^{12} elementos.

9. 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 inducido por g (ie: $\overline{g}(\sum a_i X^i) = \sum g(a_i) X^i$).

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

(i) 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 $car\, K \neq 0$ y n es coprimo con $car\, K$ entonces ϕ_n tiene todas sus raíces simples.

(ii) Sea C/K una clausura algebraica y $\xi \in C$ una raíz primitiva n-ésima de 1 (i.e: $\xi^n = 1$ y $\xi^r \neq 1\ \forall r < n$). Si n es coprimo con $car\, K$, probar que:

a. $\xi \in C$ es raíz de ϕ_n sii ξ es raíz n-ésima primitiva de 1.

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

c. Sea ξ_n una primitiva n-ésima de 1 en C, entonces $\xi \in C$ es otra raíz primitiva n-ésima de 1 sii $\xi = \xi_n^j$ para algún $1 \leq j \leq n$ tal que $(j; n) = 1$.

10. Sea K un cuerpo de característica positiva y $n \in \mathbb{N}$ coprimo con la característica de K. Sea C/K una clausura algebraica y $\xi_n \in C$ una raíz n-ésima primitiva de 1. Probar que si ϕ_n es irreducible en $K[X]$, entonces $K(\xi_n)/K$ es separable, normal y de grado $\varphi(n)$ y que $G(K(\xi_n)/K) \simeq \mathcal{U}_n$.

11. Sea n un natural impar y K cuerpo de característica distinta a 2. Probar que K contiene una raíz n-ésima primitiva de 1 sii contiene una raíz $2n$-ésima primitiva de 1.

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

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

13. 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 $E.F/K$ es ciclotómica de índice mn. Probar además que si $K = \mathbb{Q}$, entonces $E \cap F = \mathbb{Q}$.

14. Sea K cuerpo finito de q elementos y E/K extensión ciclotómica de índice n, con n coprimo con la característica de K.

(i) Probar que E es un cuerpo de q^m elementos, donde m es el menor natural tal que $n|q^m - 1$

(ii) ϕ_n es irreducible en $K[X]$ sii la clase de q en $\mathcal{U}_n$ tiene orden $\varphi(n)$.

(iii) Si $p \neq 2, 3$ entonces ϕ_{12} es reducible en $\mathbb{Z}_p[X]$.

(iv) Probar que, para todo p, $X^4 + 1$ es reducible en $\mathbb{Z}_p[X]$.

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

16. (i) Sea $E/\mathbb{Q}$ una extensión cuadrática. Probar que ϕ_n es reducible en $E[X]$ sii $E \subseteq \mathbb{Q}(\xi_n)$.

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

17. ¿Para qué valores de n es ϕ_n irreducible sobre un cuerpo de 9 elementos?

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

19. Sea K cuerpo y $n \in \mathbb{N}$ coprimo con la característica de K. Probar que los factores irreducibles de ϕ_n sobre K son todos de igual grado.

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

21. Sea t trascendente sobre $\mathbb{Z}_7$ y sea $K = \mathbb{Z}_7(t)$. Hallar la factorización de ϕ_9 como producto de irreducibles en $K[X]$.

22. Sean $p_1, \ldots, p_n \in \mathbb{Z}$ primos distintos y sea

$$f_n(x) = \prod_{(\varepsilon_1,\ldots,\varepsilon_n)\in\{-1,1\}} (x - \sum_{i=1}^{n} \varepsilon_i \sqrt{p_i})$$

   (i) Probar que $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]/\mathbb{Q}$ es normal y que $\mathrm{Gal}(\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_n}]/\mathbb{Q})$ es $(\mathbb{Z}_2)^n$.

   (ii) Probar que f_n es irreducible en $\mathbb{Q}[x]$.

   (iii) Probar que $f_n \in \mathbb{Z}[x]$ (hint: $f_n(x) = f_{n-1}(x - \sqrt{p_n}) f_{n-1}(x + \sqrt{p_n})$).

   (iv) Sea $\overline{f_n} \in \mathbb{Z}_q[x]$, q primo. Probar que $\overline{f_n}$ se factoriza con factores de grado a lo sumo 2 en $\mathbb{Z}_q[x]$.