

# ÁLGEBRA III

## Práctica 2 – Segundo Cuatrimestre de 2018

### Extensiones de cuerpos, polinomios minimales, elementos algebraicos y trascendentes

Nota: Con  $m(x, K)$  se notará el polinomio minimal del elemento  $x$  sobre el cuerpo  $K$  y con  $\xi_n$  una raíz  $n$ -ésima primitiva de la unidad.

**Ejercicio 1.** Sea  $E/K$  una extensión, y sea  $x \in E$  algebraico sobre  $K$ . Dada una subextensión  $F/K$  de  $E/K$ , probar que  $m(x, F)$  divide a  $m(x, K)$ . Dar ejemplos con  $m(x, F) = m(x, K)$  y con  $m(x, F) \neq m(x, K)$ .

**Ejercicio 2.** Calcular los siguientes polinomios minimales:

- |                                              |                                                  |                                                                      |
|----------------------------------------------|--------------------------------------------------|----------------------------------------------------------------------|
| i) $m(\sqrt[4]{2}, \mathbb{Q})$ .            | iii) $m(\sqrt[4]{2}, \mathbb{Q}[\sqrt[4]{2}])$ . | v) $m(\sqrt[4]{-1}, \mathbb{Q}[i])$ .                                |
| ii) $m(\sqrt[4]{2}, \mathbb{Q}[\sqrt{2}])$ . | iv) $m(\sqrt[4]{-1}, \mathbb{Q})$ .              | vi) $m(w, \mathbb{R})$ con $w \in \mathbb{C} \setminus \mathbb{R}$ . |

**Ejercicio 3.** Calcular:

- |                                                             |                                                                   |                                                                                  |
|-------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------|
| i) $[\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}]$ .               | v) $[\mathbb{Q}[\sqrt{2 - \sqrt{3}}] : \mathbb{Q}]$ .             | viii) $[\mathbb{Q}[\sqrt{7 + 4\sqrt{3}} + \sqrt{7 - 4\sqrt{3}}] : \mathbb{Q}]$ . |
| ii) $[\mathbb{Q}[\sqrt[3]{3}, \sqrt[5]{7}] : \mathbb{Q}]$ . | vi) $[\mathbb{Q}[\sqrt{2 + \sqrt{2 + \sqrt{2}}}] : \mathbb{Q}]$ . | ix) $[\mathbb{Q}[\sqrt{4 + \sqrt{15}} + \sqrt{4 - \sqrt{15}}] : \mathbb{Q}]$ .   |
| iii) $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}]$ .      | vii) $[\mathbb{Q}[\sqrt{4 + \sqrt{15}}] : \mathbb{Q}]$ .          | x) $[\mathbb{Q}[\sqrt{4 + \sqrt{15}}, \sqrt{4 - \sqrt{15}}] : \mathbb{Q}]$ .     |
| iv) $[\mathbb{Q}[\sqrt{2} + \sqrt{3}] : \mathbb{Q}]$ .      |                                                                   |                                                                                  |

**Ejercicio 4.** Calcular  $[\mathbb{Q}[\sqrt[3]{7 + 5\sqrt{2}} + \sqrt[3]{7 - 5\sqrt{2}}] : \mathbb{Q}]$  y  $[\mathbb{Q}[\sqrt[3]{7 + 5\sqrt{2}}, \sqrt[3]{7 - 5\sqrt{2}}] : \mathbb{Q}]$ .

**Ejercicio 5.** Sea  $E = K[a]$  una extensión finita de un cuerpo  $K$ . Para cada  $\alpha \in E$  definimos  $L_\alpha : E \rightarrow E$  la  $K$ -transformación lineal dada por  $L_\alpha(x) = \alpha x$ .

- Probar que  $m(a, K) = \chi_{L_a} := \det(xI - L_a)$ .
- ¿Para cuáles  $\alpha \in E$  vale que  $m(\alpha, K) = \chi_{L_\alpha}$ ?

**Ejercicio 6.** Sea  $E/K$  una extensión. Probar que  $E/K$  es algebraica si y sólo si todo anillo  $A$ , con  $K \subseteq A \subseteq E$ , es un cuerpo.

**Ejercicio 7.** Sea  $F/K$  una extensión de cuerpos de grado impar. Probar que si  $F = K[u]$  entonces  $F = K[u^2]$ .

**Ejercicio 8.** Sea  $n \in \mathbb{N}$ ,  $(n : 6) = 1$ , y sea  $F/\mathbb{Q}$  una subextensión de  $\mathbb{C}/\mathbb{Q}$  de grado  $n$ . Probar que  $[F[\sqrt[3]{2}, i] : F] = 6$ .

**Ejercicio 9.** Sean  $L/K$  y  $M/K$  dos subextensiones de grado finito de una extensión  $F/K$ . Probar que:

- i) Si  $\text{mcd}([L : K], [M : K]) = 1$ , entonces  $[L.M : K] = [L : K] \cdot [M : K]$ .
- ii) Si  $[L.M : K] = [L : K] \cdot [M : K]$  entonces  $L \cap M = K$ . ¿Vale la recíproca?

**Ejercicio 10.** Sea  $K$  un cuerpo de característica  $\neq 2$ . Sea  $E/K$  una extensión de grado 2. Probar que existe  $a \in E$  tal que  $E = K[a]$  y  $a^2 \in K$ . Probar que esto no es necesariamente cierto en característica 2.

**Ejercicio 11.** Factorizar  $X^5 + 6X^3 + 15X^2 + 3$  en  $\mathbb{Q}(\sqrt{-3}, \sqrt{-2})[X]$ .

**Ejercicio 12.** Sea  $a \in \mathbb{Z}[i]$  irreducible y sea  $K$  el cuerpo primo de  $\mathbb{Z}[i]/\langle a \rangle$ . Calcular  $[\mathbb{Z}[i]/\langle a \rangle : K]$ .

**Ejercicio 13.**

- i) Sea  $p \in \mathbb{N}$  primo. Calcular  $m(\xi_p, \mathbb{Q})$  y deducir  $[\mathbb{Q}[\xi_p] : \mathbb{Q}]$ .
- ii) Calcular  $m(\xi_6, \mathbb{Q})$ .
- iii) Probar que  $m(\xi_n, \mathbb{Q}) = 1 + X + X^2 + \dots + X^{n-1}$  si y sólo si  $n$  es primo.
- iv) Probar que  $\mathbb{Q}(\xi_5)/\mathbb{Q}$  admite una subextensión cuadrática y caracterizarla.  
*Sugerencia:*  $\xi_5 + \xi_5^{-1}$ .
- v) Calcular  $m(\xi_7 + \xi_7^{-1}, \mathbb{Q})$ .

**Ejercicio 14.** Sea  $p \in \mathbb{N}$  primo y sea  $a \notin \mathbb{Q}^p$ .

- i) Probar que  $m(\sqrt[p]{a}, \mathbb{Q}) = X^p - a$ .
- ii) Sea  $K \subseteq \mathbb{C}$  el mínimo cuerpo que contiene a todas las raíces de  $m(\sqrt[p]{a}, \mathbb{Q})$ . Caracterizar  $K$  y calcular  $[K : \mathbb{Q}]$  y  $[K : \mathbb{Q}[\sqrt[p]{a}]]$ .

**Ejercicio 15.** Se define  $\overline{\mathbb{Q}} = \{x \in \mathbb{C} : x \text{ es algebraico sobre } \mathbb{Q}\}$ . Probar que  $\overline{\mathbb{Q}}$  es una extensión algebraica que no es finita. Probar que  $\overline{\mathbb{Q}}$  es algebraicamente cerrado.

**Ejercicio 16.** Sea  $\{p_i\}_{i \in \mathbb{N}}$  una numeración de los primos positivos.

- i) (a) Probar que  $\forall a \in \mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}]$  con  $a \notin \mathbb{Q}$  y  $a^2 \in \mathbb{Q}$ , existen  $b \in \mathbb{Q}$  y enteros  $1 \leq i_1 < \dots < i_k \leq n$  tales que  $a = b\sqrt{p_{i_1}} \dots \sqrt{p_{i_k}}$ .  
*Sugerencia:* Probar por inducción un enunciado ligeramente más fuerte.
- (b) Calcular  $[\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}] : \mathbb{Q}]$ .
- (c) Calcular la cantidad de subextensiones de grado 2 de  $\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n}] / \mathbb{Q}$ .
- ii) Hallar  $[\mathbb{Q}[\sqrt{p_i}]_{i \in \mathbb{N}} : \mathbb{Q}]$ .
- iii) ¿Existen  $\alpha_1, \dots, \alpha_n \in \mathbb{C}$  tales que  $\mathbb{Q}[\sqrt{p_i}]_{i \in \mathbb{N}} = \mathbb{Q}[\alpha_1, \dots, \alpha_n]$ ?
- iv) Sea  $K$  un cuerpo algebraicamente cerrado tal que  $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ . Deducir  $[K : \mathbb{Q}]$ .

**Ejercicio 17.** Sea  $E/K$  una extensión algebraica de grado infinito. Probar que existen subextensiones de  $E/K$  de grado finito arbitrariamente grande. ¿Qué pasa si  $E/K$  es puramente trascendente?

**Ejercicio 18.**

- i) Probar que un cuerpo algebraicamente cerrado es infinito.
- ii) Sea  $E/K$  algebraica. Calcular el cardinal de  $E$  en función del cardinal de  $K$ .
- iii) Deducir que para todo cardinal infinito  $a$  existe un cuerpo algebraicamente cerrado de cardinal  $a$ .

**Ejercicio 19.**

- i) Sea  $K$  un cuerpo y sea  $f = g/h \in K(X) - K$ , donde  $g, h \in K[X]$  sin factores comunes. Probar que  $[K(X) : K(f)] = \max \{\text{gr}(g), \text{gr}(h)\}$ .
- ii) Para cada  $n \in \mathbb{N}$ , calcular  $m(X, K(X^n))$ .
- iii) Probar que  $\exp(2\pi i X)$  no es algebraico sobre  $\mathbb{C}(X)$ .  
Sugerencia: considerar  $X \mapsto X + 1$ .

**Ejercicio 20.** Sea  $E/K$  una extensión de cuerpos y sean  $x, y \in E$ . Determinar si las siguientes afirmaciones son verdaderas o falsas. Justificar.

- i) Si  $x$  e  $y$  son trascendentes sobre  $K$  entonces  $x + y$  o  $x \cdot y$  es trascendente sobre  $K$ .
- ii) Si  $x$  es trascendente e  $y$  es algebraico sobre  $K$  entonces  $x + y$  es trascendente sobre  $K$ .
- iii) Si  $x$  es trascendente e  $y$  es algebraico sobre  $K$  entonces  $x \cdot y$  es trascendente sobre  $K$ .
- iv) Si  $x$  es trascendente sobre  $K$  e  $y$  es trascendente sobre  $K(x)$  entonces  $\{x, y\}$  es algebraicamente independiente sobre  $K$ .
- v) Si  $x$  e  $y$  son trascendentes sobre  $K$  entonces  $\{x, y\}$  es algebraicamente independiente sobre  $K$ .

**Ejercicio 21.**

- i) Sea  $d \in \mathbb{Z}$  libre de cuadrados. Probar que hay sólo dos morfismos de cuerpos  $f : \mathbb{Q}[\sqrt{d}] \rightarrow \mathbb{C}$  y que en cada caso  $f(\mathbb{Q}[\sqrt{d}]) \subseteq \mathbb{Q}[\sqrt{d}]$  (de hecho, vale la igualdad).
- ii) Sea  $d \in \mathbb{Z}$  libre de cubos.
  - (a) Probar que hay sólo tres morfismos de cuerpos  $f : \mathbb{Q}[\sqrt[3]{d}] \rightarrow \mathbb{C}$  pero, en general,  $f(\mathbb{Q}[\sqrt[3]{d}]) \not\subseteq \mathbb{Q}[\sqrt[3]{d}]$ .
  - (b) Considerar  $\mathbb{Q}[\sqrt[3]{d}, \xi_3]$ . ¿Qué sucede en este caso?

**Ejercicio 22.** Sea  $K \subseteq \mathbb{C}$  el mínimo cuerpo que contiene a todas las raíces de  $x^8 - 2$ . Caracterizar  $K$  y calcular  $[K : \mathbb{Q}]$ . Hacer lo mismo con  $x^4 + 2x^2 + 2$ ,  $x^4 + 3x^2 + 1$ ,  $x^6 + 3$  y  $x^8 - 3$ .

**Ejercicio 23.** Sea  $\alpha$  la raíz real de  $f(X) = X^3 + 2X^2 - 2X + 2$ . Escribir a  $(\alpha + 3)^{-1}$  como combinación  $\mathbb{Q}$ -lineal de  $1, \alpha$  y  $\alpha^2$ .

**Ejercicio 24.** Decimos que un número  $x \in \mathbb{R}$  es *construible* si existe una cadena de cuerpos  $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n \subseteq \mathbb{R}$  tales que  $[F_k : F_{k-1}] \leq 2$  para todo  $k = 1, \dots, n$  y  $x \in F_n$ , y que un número complejo  $z$  es *construible* si sus partes real y compleja lo son.

- a) Probar que  $\sqrt[3]{2}$  no es construible.
- b) Probar que  $z \in \mathbb{C}$  es construible si y sólo si existe una cadena de cuerpos

$$\mathbb{Q}[i] = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n \subseteq \mathbb{C}$$

tales que  $[F_k : F_{k-1}] \leq 2$  para todo  $k = 1, \dots, n$  y  $z \in F_n$ .

- c) Probar que si  $\xi_n \in \mathbb{C}$  es construible, entonces  $\phi(n)$  es una potencia de 2.

**Ejercicio 25.** Sean  $\{\alpha_1, \dots, \alpha_5\}$  las raíces de  $X^5 - X - 1 \in \mathbb{C}[X]$ . Hallar un polinomio cuyas raíces sean

- (a)  $\{\alpha_1 - 2, \dots, \alpha_5 - 2\}$ .      (b)  $\{\alpha_1^{-1}, \dots, \alpha_5^{-1}\}$ .      (c)  $\{\alpha_1^5, \dots, \alpha_5^5\}$ .

**Ejercicio 26.** Sean  $A_1, A_2, \dots, A_n$  los vértices de un  $n$ -ágono regular inscripto en una circunferencia de radio 1.

1. Hallar el producto de las longitudes de  $A_1 A_i$  con  $i = 2, \dots, n$ .
2. Hallar la suma

$$\sum_{i=2}^n \frac{1}{A_1 A_i^2}.$$

\* 3 Tomar límite adecuadamente y probar que

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

**Ejercicio 27.** Sea  $f(X) = m(\xi_n, \mathbb{Q}[\xi_m]) \in \mathbb{Q}[\xi_m][X]$ .

- (i) Calcular  $\text{gr } f$ .      (ii) Hallar  $f(X)$  cuando  $(m, n) = 1$ .

**Ejercicio 28.** Sea  $A_n = \text{Van}(1, \xi_n, \xi_n^2, \dots, \xi_n^{n-1}) \in \mathbb{C}^{n \times n}$  la matriz de Vandermonde con las raíces  $n$ -ésimas de la unidad.

- (a) Calcular  ${}^t A A$ .
- (b) Si  $n$  es impar, probar que  $\sqrt{\pm n} \in \mathbb{Q}[\xi_n]$  para cierta elección del signo.
- (c) Probar que cualquier extensión cuadrática de  $\mathbb{Q}$  está contenida en una ciclotómica.

\* **Ejercicio 29.** Sea  $K$  un cuerpo de característica 0 y  $A \in K^{n \times n}$ .

- a) Probar que

$$\det(1 - AX) = \exp \left( - \sum_{k=1}^{\infty} \frac{\text{tr}(A^k) X^k}{k} \right) \in K[[X]].$$

- b) Probar que  $A$  es nilpotente si y sólo si  $\text{tr}(A^k) = 0$  para todo  $k = 1, \dots, n$ .

c) Probar las *identidades de Newton*:

$$ke_k = \sum_{i=1}^k (-1)^{i-1} e_{k-i} p_i$$

donde  $p_k = \sum_{i=1}^n X_i^k$ ,  $e_0 = 1$ ,  $e_k = \sum_{i_1 < \dots < i_k} X_{i_1} \dots X_{i_k}$  y  $e_k = 0$  si  $k > n$ .

\* **Ejercicio 30. (Lema de Hensel)** Sea  $p \geq 1$  primo y  $f \in \mathbb{Z}[X]$  un polinomio mónico.

(i) Sea  $b_1 \in (\mathbb{Z}/p\mathbb{Z})$  una raíz simple de  $\bar{f} \in (\mathbb{Z}/p\mathbb{Z})[X]$  (es decir,  $\bar{f}'(b_1) \neq 0$ ). Probar que existen  $b_n \in (\mathbb{Z}/p^n\mathbb{Z})$  tales que

- $b_n \equiv b_{n+1} \pmod{p^n}$  y
- $\bar{f}(b_n) \equiv 0 \pmod{p^n}$ .

Concluir que existe  $b \in \mathbb{Z}_p$  raíz de  $f$ .

Sugerencia: Newton – Raphson.

(ii) Supongamos que  $f$  se factoriza módulo  $p$  como  $\bar{f} = \bar{g}\bar{h}$  con  $\bar{g}$  y  $\bar{h}$  coprimos en  $(\mathbb{Z}_p/p\mathbb{Z}_p)[X] = \mathbb{F}_p[X]$ . Probar que existe una factorización  $f = gh$  en  $\mathbb{Z}_p[X]$  tal que  $\bar{g}$  y  $\bar{h}$  son las reducciones de  $g$  y  $h$  respectivamente.

\* **Ejercicio 31.** Probar que  $K[X][[Y]] \neq K[[Y]][X]$ .

\* **Ejercicio 32. (Función implícita)** Sea  $f \in K[X, Y]$  tal que  $f(0, 0) = 0$  y  $\partial_Y f(0, 0) \neq 0$ . Probar que existe  $g \in K[[X]]$  múltiplo de  $X$  tal que  $f(X, g(X)) = 0$  en  $K[[X]]$ .

\* **Ejercicio 33.** Factorizar

1.  $X^2 - 2$  en  $\mathbb{Z}_7[X]$ .
2.  $X^2 + 1$  en  $\mathbb{Z}_5[X]$ .
3.  $Y^2 - 1 - X$  en  $\mathbb{C}[[X]][Y]$ .
4.  $Y^2 - X^2 - X^3$  en  $\mathbb{C}[[X]][Y]$ .

\* **Ejercicio 34.** Sean  $m, n \geq 1$  enteros y  $A \in \mathbb{C}^{n \times n}$  y  $B \in \mathbb{C}^{m \times m}$  matrices. Las transformaciones lineales

$$L_A, R_B : \mathbb{C}^{n \times m} \rightarrow \mathbb{C}^{n \times m}$$

se definen por  $L_A(X) = AX$  y  $R_B(X) = XB$ .

- i) Probar que  $L_A$  y  $R_B$  conmutan.
- ii) Hallar el polinomio característico de  $L_A$  en función del de  $A$ .
- iii) Si  $A$  y  $B$  son diagonalizables, hallar los autovectores de  $L_A + R_B$  en función de los de  $A$  y  $B$ .
- iv) Probar que el conjunto de *enteros algebraicos*

$$\bar{\mathbb{Z}} := \{\alpha \in \mathbb{C} : \exists f \in \mathbb{Z}[X] \text{ mónico que verifica } f(\alpha) = 0\}$$

es un anillo.

\* **Ejercicio 35.** Sean  $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \subseteq \mathbb{C}$  las raíces de  $f(X) = X^4 + X + 1 \in \mathbb{Q}[X]$ . Hallar  $g(X) \in \mathbb{Q}[X]$  de grado 6 tal que sus raíces sean los productos  $\alpha_i \alpha_j$  con  $1 \leq i < j \leq 4$ .