

ÁLGEBRA III

Práctica 6 – Segundo Cuatrimestre de 2023

Ejercicio 1. Pruebe que:

- a) Todo grupo abeliano es resoluble. c) D_n es resoluble.
 b) Todo p -grupo es resoluble. d) S_n es resoluble si y solo si $n \leq 4$.

Ejercicio 2. Muestre explícitamente que las siguientes extensiones son resolubles por radicales:

- a) $\mathbb{Q}[\sqrt[3]{1 + \sqrt{2}}, i + \sqrt{3}]/\mathbb{Q}$
 b) E/\mathbb{Q} cuerpo de descomposición de $f = (X^4 - 2)(X^2 - 5)$

Ejercicio 3. Pruebe que el 65537-ágono regular es construible con regla y compás.

* **Ejercicio 4.** Para hallar una *Lúnula de Hipócrates* de parámetros $(m : n)$ que admita una cuadratura se debe resolver

$$\left(\frac{\operatorname{sen}(m\theta)}{\operatorname{sen}(n\theta)} \right)^2 = \frac{m}{n}.$$

- a) Pruebe que se trata de una ecuación algebraica en $x = \cos(\theta)$.
 b) Pruebe que es equivalente a resolver $(y^m - 1)^2 - \frac{m}{n}y^{m-n}(y^n - 1)^2 = 0$.
 c) Pruebe que las lúnulas cuadrables de parámetros $(m : n)$ son construibles con regla y compás cuando $(m : n) = (2 : 1), (3 : 1), (3 : 2), (5 : 1)$ y $(5 : 3)$.

Ejercicio 5. Decimos que una extensión E/\mathbb{Q} es construible si todos sus elementos lo son (recuerde el Ejercicio 24 de la Práctica 2).

- a) Pruebe que si E/\mathbb{Q} está generada por números construibles, entonces es construible.
 b) Pruebe que si una extensión es construible, entonces su clausura normal también lo es.
 c) ¿Existe una extensión E/\mathbb{Q} de grado 4 que no sea construible?

Ejercicio 6. Sea $G \subseteq S_n$ un subgrupo transitivo que contiene una transposición.

- a) Pruebe que si G también contiene un $(n - 1)$ -ciclo, entonces $G = S_n$.
 b) Pruebe que si $n = p$ es un primo impar, entonces $G = S_p$.

Ejercicio 7. Sea $G \subseteq S_{p+2}$ un subgrupo transitivo, con p primo impar. Supongamos que G contiene una permutación de estructura cíclica $(2, p)$ (es decir, el producto de una transposición y un p -ciclo disjuntos). Pruebe que $G = S_{p+2}$.

Ejercicio 8. Sea $f \in \mathbb{Q}[X]$ irreducible de grado primo mayor o igual que 5. Supongamos además que f tiene exactamente dos raíces no reales. Pruebe que f no es resoluble por radicales en \mathbb{Q} .

Ejercicio 9. Pruebe los siguientes polinomios no son resolubles por radicales sobre \mathbb{Q} .

a) $X^5 - 14X + 7$ b) $X^5 - 7X^2 + 7$ c) $X^7 - 10X^5 + 15X + 5$

Ejercicio 10. Sea $m \in \mathbb{N}$ par y sean $a_1 < a_2 < \dots < a_r$ enteros positivos pares con $r > 1$ impar. Sea $f = (X^2 + m)(X - a_1) \dots (X - a_r) - 2$. Pruebe que:

a. f es irreducible en $\mathbb{Q}[X]$.

b. Para m suficientemente grande, f tiene exactamente dos raíces no reales en \mathbb{C} .

* c. El ítem anterior sigue valiendo si se quita la hipótesis “ m suficientemente grande”.

Ejercicio 11. Pruebe que para cada primo $p \in \mathbb{N}$, existe una extensión normal E/\mathbb{Q} con grupo de Galois isomorfo a \mathbb{S}_p .

Ejercicio 12. Sea $f = X^4 - X - 1 \in \mathbb{Q}[X]$.

a) Pruebe que $\bar{f} \in \mathbb{F}_2[X]$ es irreducible.

d) Factorice $\bar{f} \in \mathbb{F}_7[X]$.

b) Calcule el discriminante de f .

e) ¿Cuántas raíces tiene f en \mathbb{Q}_7 ?

c) Pruebe que f solo tiene dos raíces reales.

f) Halle el grupo de Galois de $\text{Desc}(f|\mathbb{Q})$.

Ejercicio 13. Sea $f = X^5 + 2X^3 + 2X + 10 \in \mathbb{Q}[X]$.

a) Pruebe que f es irreducible.

d) ¿Cuántas raíces tiene f en \mathbb{Q}_5 ?

b) Pruebe que f tiene una única raíz real.

c) Factorice $\bar{f} \in \mathbb{F}_5[X]$.

e) Halle el grupo de Galois de $\text{Desc}(f|\mathbb{Q})$.

Ejercicio 14. Sea $f = X^5 + 20X + 16 \in \mathbb{Q}[X]$.

a) Pruebe que $\bar{f} \in \mathbb{F}_3[X]$ es irreducible.

d) Factorice $\bar{f} \in \mathbb{F}_7[X]$.

b) Calcule el discriminante de f .

e) ¿Cuántas raíces tiene f en \mathbb{Q}_7 ?

c) Pruebe que f tiene una única raíz real.

f) Halle el grupo de Galois de $\text{Desc}(f|\mathbb{Q})$.

Ejercicio 15. Sea $f = X^5 - X - 1 \in \mathbb{Q}[X]$.

a) Pruebe que f es irreducible.

d) Factorice $\bar{f} \in \mathbb{F}_2[X]$.

b) Calcule el discriminante de f .

e) ¿Qué grado tiene $\text{Desc}(f|\mathbb{Q}_2)/\mathbb{Q}_2$?

c) Pruebe que f tiene una única raíz real.

f) Halle el grupo de Galois de $\text{Desc}(f|\mathbb{Q})$.

Ejercicio 16. Sea $K \subseteq \mathbb{C}$ un cuerpo. Sea $f \in K[X]$ irreducible de grado primo $p \geq 5$. Sean $\alpha_1, \dots, \alpha_p \in \mathbb{C}$ las raíces de f y sea $N = K[\alpha_1, \dots, \alpha_p]$ el cuerpo de descomposición de f sobre K . Pruebe que f es resoluble por radicales sobre K si y solo si $N = K[\alpha_i, \alpha_j]$ para todos $1 \leq i < j \leq p$.

Ejercicio 17. Sea $f = X^6 - 2X^3 - 2$ y $E = \text{Desc}(f|\mathbb{Q})$.

- Pruebe que $\text{Gal}(E/\mathbb{Q})$ es resoluble.
- Pruebe que no alcanzan dos raíces de f para generar E .

Reducción módulo p y teorema de Dedekind

Nota: En esta práctica trabajamos con polinomios con coeficientes enteros. Dado un polinomio separable $f \in \mathbb{Z}[X]$ de grado n , denotamos G_f al grupo de Galois de f sobre \mathbb{Q} , el cual identificamos con un subgrupo de \mathbb{S}_n . Para cada primo p , la reducción de f módulo p es la imagen de f por el morfismo canónico $\mathbb{Z}[X] \rightarrow \mathbb{F}_p[X]$, y la denotamos f_p .

Ejercicio 18. Sea $f \in \mathbb{Q}[X]$ un polinomio mónico de grado n , y sea c un número entero divisible por todos los denominadores en los coeficientes de f . Pruebe que el polinomio $g(x) = c^n f\left(\frac{x}{c}\right)$ es mónico, tiene coeficientes enteros, y su cuerpo de descomposición sobre \mathbb{Q} coincide con el de f .

Ejercicio 19. Sea $p > 2$ un número primo y sea $f \in \mathbb{Z}[X]$ un polinomio mónico e irreducible de grado $p+2$. Supongamos que para un cierto primo p' , el polinomio $f_{p'}$ se factoriza en $\mathbb{F}_{p'}[X]$ como producto de dos polinomios irreducibles cuyos grados son 2 y p . Pruebe que $G_f = \mathbb{S}_{p+2}$.

Ejercicio 20. Para cada uno de los siguientes polinomios f , pruebe que $G_f = \mathbb{S}_n$, donde $n = \deg(f)$:

- $X^5 + 4X^4 + 4X^3 + 5X^2 - 2X + 3$;
- $X^6 - 12X^4 + 15X^3 - 6X^2 + 15X + 12$;
- $X^5 + 25X^4 + 10X^3 + 10X^2 + 10X + 15$;
- $X^9 + 3X^8 + 3X^7 - 9X^3 - 9$.

Ejercicio 21. Sea f el polinomio $X^5 - X^4 + 2X^2 - 2$. Factorizando f módulo 3 y módulo 7, pruebe que G_f contiene una trasposición y un 4-ciclo. ¿Es $G_f = \mathbb{S}_5$?

Ejercicio 22. Decida si el polinomio $X^7 + 12X^5 - 2X^2 - 2$ es resoluble por radicales.
Sugerencia: reduzca módulo 11.

Ejercicio 23. Sea $G \subseteq \mathbb{S}_n$ un subgrupo transitivo que contiene un p -ciclo para cierto primo $p > \frac{n}{2}$. Pruebe que:

- Si G contiene una trasposición, entonces $G = \mathbb{S}_n$.
- Si G contiene un 3-ciclo, entonces $\mathbb{A}_n \subseteq G$.

Ejercicio 24. Factorice $f = X^7 - X - 1$ módulo 2, 3 y 5 y concluya que $G_f \simeq \mathbb{S}_7$.

Ejercicio 25. Factorice $f = X^7 - 7X + 10$ módulo 2 y 3. Pruebe que $G_f \not\simeq \mathbb{S}_7$.

* **Ejercicio 26.** Sea $\theta = \sqrt[3]{\sqrt[3]{2} - 1}$.

- Pruebe que $x^3 - 2$ se descompone linealmente en \mathbb{Q}_{31} .
- Halle $m(\theta, \mathbb{Q}[\sqrt[3]{2}])$. Deduzca $[\mathbb{Q}[\theta] : \mathbb{Q}]$ y $\text{tr}_{\mathbb{Q}[\theta]/\mathbb{Q}}(\theta)$.

- c) Calcule $\text{tr}_{\mathbb{Q}[\theta]/\mathbb{Q}[\sqrt[3]{2}]}(\sqrt[3]{3}\theta)$.
- d) Decida si $\sqrt[3]{3} \in \mathbb{Q}[\theta]$.
- e) Deduzca el grupo de Galois de la clausura normal de $\mathbb{Q}[\theta]/\mathbb{Q}$.
- f) ¿Existe p primo tal que $(x^3 + 1)^3 - 2$ resulta irreducible en $\mathbb{F}_p[x]$?

Ejercicio 27. Sean E/F y L/F subextensiones finitas de K/F con E/F de Galois.

- a) Pruebe que $[EL : E] = [L : E \cap L]$.
- b) Sea M/L subextensión de EL/L . Pruebe que $M = (E \cap M)L$.

Ejercicio 28. Sea E/F una extensión tal que $E = F[\alpha]$ donde $\alpha^n \in F$ para cierto $n \in \mathbb{N}$. Supongamos además que F contiene alguna raíz n -ésima primitiva de la unidad. Si $m = [E : F]$, pruebe que $\alpha^m \in F$.

Ejercicio 29. Sea $K[\alpha]/K$ separable y finita, y L/K su clausura normal. Sea p un primo que divide al orden de $\text{Gal}(L/K)$. Pruebe que existe una subextensión $F \subseteq L$ tal que $L = F[\alpha]$ y $[L : F] = p$.

Ejercicio 30. Sean $F \subseteq K \subseteq \mathbb{R}$ cuerpos con $K = F[\sqrt[n]{a}]$ para cierto $a \in F$. Pruebe que si L/F es Galois y $L \subseteq K$ entonces $[L : F] \leq 2$.

* **Ejercicio 31.** Sea $f \in \mathbb{Q}[X]$ tal que $\text{Desc}(f|\mathbb{Q}) \subseteq \mathbb{R}$ y alguna de sus raíces se puede expresar con radicales *reales*. Es decir, dicha raíz α pertenece al último cuerpo de una cadena

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$$

de subcuerpos de \mathbb{R} , donde $K_{i+1} = K_i[\sqrt[n_i]{a_i}]$ para ciertos $a_i \in K_i$ y n_i enteros, $i = 1, \dots, m-1$. Pruebe que todas sus raíces son construibles (con regla y compás).

Sugerencia: use los dos ejercicios anteriores.

* **Ejercicio 32.** Sea $p \neq 2$ primo y

$$E = \mathbb{Q}[\alpha : \alpha^{2^n} = p \text{ para cierto } n \geq 1]$$

(es decir, el cuerpo de descomposición de todos los polinomios de la forma $X^{2^n} - p$). Pruebe que $\text{Gal}(E/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2^\times$.