

ÁLGEBRA III

Práctica 5 – Segundo Cuatrimestre de 2018

Ejercicio 1. Probar que:

1. Todo grupo abeliano es resoluble.
2. Todo p -grupo es resoluble.
3. D_n es resoluble.
4. S_n es resoluble si y solo si $n \leq 4$.

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

1. $\mathbb{Q}[\sqrt[3]{1+\sqrt{2}}, i+\sqrt{3}]/\mathbb{Q}$
2. $E/\mathbb{Q}$ cuerpo de descomposición de $f = (X^4 - 2)(X^2 - 5)$
3. $N/\mathbb{C}(a, b)$ cuerpo de descomposición de $f = X^2 + aX + b$
4. $N/\mathbb{C}(a, b, c)$ cuerpo de descomposición de $f = X^3 + aX^2 + bX + c$
5. $N/\mathbb{C}(a, b, c, d)$ cuerpo de descomposición de $f = X^4 + aX^3 + bX^2 + cX + d$

Ejercicio 3. Probar 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

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

1. Probar que se trata de una ecuación algebraica en $x = \cos(\theta)$.
2. Probar que es equivalente a resolver $(y^m - 1)^2 - \frac{m}{n}y^{m-n}(y^n - 1)^2 = 0$.
3. Probar 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 miembros lo son.

1. Probar que si $E/\mathbb{Q}$ está generada por números construibles, entonces es construible.
2. Probar que si una extensión es construible, entonces su clausura normal también lo es.
3. ¿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

1. si también contiene un $(n - 1)$ -ciclo entonces $G = S_n$.
2. si $n = p$ es un primo impar entonces $G = S_p$.

Ejercicio 7. Sea $G \subseteq \mathbb{S}_{p+2}$ 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). Probar que $G = \mathbb{S}_{p+2}$.

Ejercicio 8. Sea $f \in \mathbb{Q}[X]$ irreducible de grado primo ≥ 5 . Suponer que f tiene exactamente dos raíces no reales. Probar que f no es resoluble por radicales sobre $\mathbb{Q}$.

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

$$(I) \quad X^5 - 14X + 7 \qquad (II) \quad X^5 - 7X^2 + 7 \qquad (III) \quad X^7 - 10X^5 + 15X + 5$$

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 $f = (X^2 + m)(X - a_1) \dots (X - a_r) - 2$. Probar que:

1. f es irreducible en $\mathbb{Q}[X]$.
2. Para m suficientemente grande, f tiene exactamente dos raíces no reales en $\mathbb{C}$.
- * 3. Probar que el ítem anterior sigue valiendo si se quita la hipótesis “ m suficientemente grande”.

Ejercicio 11. Probar 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 $f = X^4 - X - 1 \in \mathbb{Q}[X]$.

1. Probar que $\bar{f} \in \mathbb{F}_2[X]$ es irreducible.
2. Calcular su discriminante.
3. Probar que sólo tiene dos raíces reales.
4. Factorizar $\bar{f} \in \mathbb{F}_7[X]$.
5. ¿Cuántas raíces tiene f en $\mathbb{Q}_7$?
6. Hallar el grupo de Galois de $\text{Desc}(f|\mathbb{Q})$.

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

1. Probar que es irreducible.
2. Probar que sólo tiene una raíz real.
3. Factorizar $\bar{f} \in \mathbb{F}_5[X]$.
4. ¿Cuántas raíces tiene f en $\mathbb{Q}_5$?
5. Hallar el grupo de Galois de $\text{Desc}(f|\mathbb{Q})$.

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

1. Probar que $\bar{f} \in \mathbb{F}_3[X]$ es irreducible.
2. Calcular su discriminante.
3. Probar que sólo tiene una raíz real.
4. Factorizar $\bar{f} \in \mathbb{F}_7[X]$.
5. ¿Cuántas raíces tiene f en $\mathbb{Q}_7$?
6. Hallar el grupo de Galois de $\text{Desc}(f|\mathbb{Q})$.

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

1. Probar que es irreducible.
2. Calcular su discriminante.
3. Probar que sólo tiene una raíz real.
4. Factorizar $\bar{f} \in \mathbb{F}_2[X]$.
5. ¿Qué grado tiene $\text{Desc}(f|\mathbb{Q}_2)/\mathbb{Q}_2$?
6. Hallar 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 . Probar 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 $E = \text{Desc}(f|\mathbb{Q})$.

1. Probar que $\text{Gal}(E/\mathbb{Q})$ es resoluble.
- * 2. Probar 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 . Probar que el polinomio $g(x) = c^n f\left(\frac{x}{c}\right)$ es mónico, tiene coeficientes enteros, y $\text{Desc}(g|\mathbb{Q}) = \text{Desc}(f|\mathbb{Q})$.

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 . Probar que $G_f = \mathbb{S}_{p+2}$.

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

- (a) $X^5 + 4X^4 + 4X^3 + 5X^2 - 2X + 3$;
- (b) $X^6 - 12X^4 + 15X^3 - 6X^2 + 15X + 12$;
- (c) $X^5 + 25X^4 + 10X^3 + 10X^2 + 10X + 15$;
- (d) $X^9 + 3X^8 + 3X^7 - 9X^3 - 9$.

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

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

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

- a. si contiene una transposición, entonces $G = \mathbb{S}_n$.
- * b. si contiene un 3-ciclo entonces $\mathbb{A}_n \subseteq G$.

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

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

Ejercicio 26. Sean E/F y L/F subextensiones finitas de K/F con E/F de Galois.

1. Probar que $[EL : E] = [L : E \cap L]$.
2. Sea M/L subextensión de EL/L . Probar que $M = (E \cap M)L$.

Ejercicio 27. 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 $m = [E : F]$, probar que $\alpha^m \in F$.

Ejercicio 28. Sea $K[\alpha]/K$ separable y finita, y L/K su clausura normal. Sea p un primo que divide al orden de $\text{Gal}(L/K)$. Probar que existe una subextensión $F \subseteq L$ tal que $L = F[\alpha]$ y $[L : F] = p$.

Ejercicio 29. Sean $F \subseteq K \subseteq \mathbb{R}$ cuerpos con $K = F[\sqrt[n]{a}]$ para cierto $a \in F$. Probar que si L/F es Galois y $L \subseteq K$ entonces $[L : F] \leq 2$.

* **Ejercicio 30.** 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, $i = 1, \dots, m-1$. Probar que todas sus raíces son construibles (con regla y compás).
Sugerencia: usar los dos ejercicios anteriores.

* **Ejercicio 31.** 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 $X^{2^n} - p$). Probar que $\text{Gal}(E/\mathbb{Q}) \simeq \mathbb{Z}_2 \rtimes \mathbb{Z}_2^\times$.