Práctica 7: Resolubilidad - Dedekind - Regla y compás

- Una extensión E/K es *radical* si es de la forma $E = K(\alpha_1, \dots, \alpha_r)$ y existen naturales $n_1, \dots, n_r$ tales que

$$\alpha_1^{n_1} \in K, \quad \alpha_2^{n_2} \in K(\alpha_1), \quad \alpha_3^{n_3} \in K(\alpha_1, \alpha_2), \quad \dots, \quad \alpha_r^{n_r} \in K(\alpha_1, \alpha_2, \dots, \alpha_{r-1}).$$

- Un polinomio $f \in K[X]$ es *resoluble por radicales* si existe una extensión radical E/K tal que f se factoriza linealmente en $E[X]$.

- Un grupo G es *resoluble* si existe una cadena decreciente de subgrupos $G = G_0 \supset G_1 \supset \dots \supset G_r = \{1\}$ tal que para todo $0 \leq i < r$ vale que $G_{i+1} \triangleleft G_i$ y G_i/G_{i+1} es abeliano. Esta cadena de subgrupos se llama una *serie resoluble* para G.

1 Probar, exhibiendo una torre adecuada, que la extensión $\mathbb{Q}\left(\sqrt[3]{1+\sqrt{2}}, i+\sqrt{3}\right)/\mathbb{Q}$ es radical.

2 Sea E/K una extensión radical y sea N/K su clausura normal. Probar que N/K también es radical.

3 (*a*) Probar que para todo $n \in \mathbb{N}$ el grupo diedral D_n es resoluble.

(*b*) Probar que todo p-grupo finito es resoluble.

4 Probar que si G es finito y resoluble entonces G admite una serie resoluble donde todos los cocientes G_i/G_{i+1} son cíclicos de orden primo.

5 Sea $f = X^5 - bx - a$ un polinomio irreducible en $\mathbb{Q}[X]$. Sea α una raíz de f y sea $E = \mathbb{Q}(\alpha)$. Sabiendo que $N_{E/\mathbb{Q}}(\alpha+1) = -77$ y $N_{E/\mathbb{Q}}(\alpha-1) = 81$, determinar si f es resoluble por radicales.

6 Sean $a_1 < a_2 < \dots < a_r$ enteros positivos pares, con $r > 1$. Dado $m \in \mathbb{N}$ par, consideramos el polinomio $f = (X^2+m)(X-a_1)\cdots(X-a_r) - 2$.

(*a*) Probar que f es irreducible en $\mathbb{Q}[X]$.

(*b*) Probar que si m es suficientemente grande, entonces f tiene exactamente dos raíces no reales.

(*c*) Deducir que para todo primo $p \geq 5$ existe un polinomio $f \in \mathbb{Q}[X]$ de grado p que no es resoluble por radicales.

En lo que sigue, dado un polinomio separable $f \in \mathbb{Z}[X]$ de grado n, llamamos G_f a su grupo de Galois sobre $\mathbb{Q}$, al cual identificamos con un subgrupo de S_n. Además, para cada primo p, llamamos f_p a la imagen de f por el morfismo canónico $\mathbb{Z}[X] \to \mathbb{F}_p[X]$.

7 Para cada uno de los siguientes polinomios f, probar que $G_f = S_n$, siendo n el grado del polinomio:

(*a*) $X^5 + 4X^4 + 4X^3 + 5X^2 - 2X + 3$

(*b*) $X^6 - 12X^4 + 15X^3 - 6X^2 + 15X + 12$

(*c*) $X^5 + 25X^4 + 10X^3 + 10X^2 + 10X + 15$

8 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 $G_f = S_5$?

9 Sea $f \in \mathbb{Z}[X]$ mónico e irreducible de grado 4 tal que $G_f \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Probar que para todo primo p, el polinomio f_p es reducible en $\mathbb{F}_p[X]$.

10 Sea G un subgrupo de S_n. Definimos una relación $\sim$ en el conjunto $\{1, 2, \ldots, n\}$ de la siguiente manera: $a \sim b$ si y sólo si $(ab) \in G$ (entendiendo que $(aa) = \mathrm{id}$).

(a) Probar que $\sim$ es relación de equivalencia.

(b) Probar que si $a \sim b$ y $g \in G$, entonces también $g(a) \sim g(b)$. Luego, queda bien definida una acción de G en el conjunto de clases de equivalencia, dada por $g \cdot [a] := [g(a)]$.

(c) Probar que si G es transitivo, entonces todas las clases de equivalencia de $\sim$ tienen el mismo cardinal.

11 Sea G un subgrupo transitivo de S_n que contiene una trasposición y un p-ciclo, donde $p > \frac{n}{2}$ es un número primo. Probar que $G = S_n$.

Sugerencia. Probar que la relación $\sim$ definida en el ejercicio anterior tiene una única clase de equivalencia.

12 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 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 $G_f = S_{p+2}$.

13 Calcular el grupo de Galois sobre $\mathbb{Q}$ del polinomio $X^9 + 3X^8 + 3X^7 - 9X^3 - 9$.

Recordemos que un número $\alpha \in \mathbb{R}$ es construible (con regla y compás) si y sólo si existe una torre de cuerpos $\mathbb{Q} = F_0 \subset F_1 \subset \ldots \subset F_n$ con $\alpha \in F_n$ y $[F_i : F_{i-1}] = 2$ para todo $i = 1, \ldots, n$.

14 Probar que un número α es construible si y sólo si es algebraico sobre $\mathbb{Q}$ y $[N : \mathbb{Q}]$ es una potencia de 2, donde $N/\mathbb{Q}$ es la clausura normal de $\mathbb{Q}(\alpha)/\mathbb{Q}$.

15 Caracterizar todos los $n \in \mathbb{N}$ tales que $\cos\left(\frac{2\pi}{n}\right)$ es construible. (Notar que esto equivale a que se pueda construir un polígono regular de n lados con regla y compás.)

16 Dar un procedimiento para construir un pentágono regular con regla y compás.

17 Sea n un entero positivo. Probar que se puede construir un ángulo de n grados con regla y compás si y sólo si n es divisible por 3.

18 Probar que un ángulo dado θ se puede trisecar con regla y compás si y sólo si el polinomio $4X^3 - 3X - \cos(\theta)$ es reducible sobre $\mathbb{Q}(\cos(\theta))$.

19 Mostrar como se puede trisecar un ángulo dado de $\frac{3\pi}{7}$ usando regla y compás.

20 Decidir si es posible construir con regla y compás un triángulo isósceles no rectángulo cuyos vértices estén sobre la circunferencia unitaria y su área sea 1.