Práctica 7

1. Sean K un cuerpo, C/K una clausura algebraica de K y $f \in K[X]$ un polinomio mónico de grado $n \geq 1$. Si $f = (X-\alpha_1)\dots(X-\alpha_n)$ (con $\alpha_i \in C$) se define el discriminante de f en la forma:
$$\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2.$$
   (a) Probar que:
      (i) Si $f = X^2 + bX + c$, entonces $\Delta(f) = b^2 - 4c$.
      (ii) Si $f = X^3 + bX + c$, entonces $\Delta(f) = -4b^3 - 27c^2$.
   (b) Sea $E/\mathbb{Q}$ una extensión de grado n. Sea $\alpha \in E$ tal que $E = \mathbb{Q}(\alpha)$ y sea $f = \boldsymbol{m}(\alpha, \mathbb{Q})$. Probar que $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{\mathbb{Q}}^{E}(f'(\alpha))$, donde f' es el polinomio derivado de f.

2. Sea $n \in \mathbb{N}$, $n \geq 2$. Probar que si $f = X^n + bX + c \in \mathbb{Q}[X]$, entonces $\Delta(f) = (-1)^{\frac{n(n-1)}{2}}(n^n c^{n-1} + (1-n)^{n-1} b^n)$.

3. Sea $E/\mathbb{Q}$ un cuerpo de descomposición de $X^3 + X + 1 \in \mathbb{Q}[X]$. Probar que el polinomio $X^4 - 6X^2 + 40$ es reducible en $E[X]$.

4. Sea K un cuerpo. Sean $E = K(t_1, \dots, t_n)$ y $F = K(s_1, \dots, s_n)$, con $\{t_1, \dots t_n\}$ algebraicamente independientes sobre K y $\{s_1, \dots, s_n\}$ los polinomios simétricos elementales en $\{t_1, \dots t_n\}$.
   (a) Supongamos que $\mathrm{car}(K) \neq 2$. Caracterizar las subextensiones de grado 2 de E/F.
   (b) Sean $a_1, \dots, a_n \in \mathbb{N}$. Probar que $t_1^{a_1} + \dots + t_n^{a_n}$ genera E/F si y sólo si $a_i \neq a_j$ para $i \neq j$.

5. Sea K un cuerpo y sea $n \in \mathbb{N}$ tal que $\mathrm{car}(K) \nmid n$. Supongamos que K contiene a las raíces n-ésimas de la unidad. Sea E/K una extensión cíclica de grado d con $d \mid n$ y sea σ un generador de $G(E/K)$. Probar que:
   (a) $E = K(\sqrt[n]{a})$ para algún $a \in K^*$.
   (b) $\sigma(\sqrt[n]{a}) = \xi \sqrt[n]{a}$ con ξ una raíz d-ésima primitiva.
   (c) Supongamos que $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$. Usar (b) para mostrar que $\frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \left(\frac{\sigma(\sqrt[n]{b})}{\sqrt[n]{b}}\right)^i$, donde i es coprimo con d. Concluir que $\frac{\sqrt[n]{a}}{(\sqrt[n]{b})^i} \in K$.
   (d) Probar que $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$ si y sólo si $a = b^i c_1^n$ y $b = a^j c_2^n$ para ciertos $c_1, c_2 \in K$. Es decir, $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$ si y sólo si a y b generan el mismo subgrupo de K^*/H, donde H el subgrupo de las potencias n-ésimas.

6. Probar que:
    (a) Todo grupo abeliano es resoluble.
    (b) Todo p-grupo es resoluble.
    (c) D_n es resoluble.
    (d) $\mathbb{S}_n$ es resoluble si y sólo si $n \leq 4$.
7. Mostrar 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 $f = (X^4-2)(X^2-5)$.
    (c) $K(t_1,t_2)/K(s_1,s_2)$, donde K es un cuerpo con $\mathrm{car}(K) \neq 2$, $\{t_1,t_2\}$ son algebraicamente independientes sobre K, y $\{s_1,s_2\}$ son los polinomios simétricos elementales en $\{t_1,t_2\}$.
8. Sea K un cuerpo. Sea $f \in K[X]$ un polinomio de grado n y sea E un cuerpo de descomposición de f sobre K. Probar que si $G(E/K) \simeq \mathbb{S}_n$ entonces f es irreducible en $K[X]$.
9. (a) Sea $p \in \mathbb{N}$ primo. Sea $H \subseteq \mathbb{S}_p$ un subgrupo que contiene una transposición y una permutación de orden p. Probar que $H = \mathbb{S}_p$.
    (b) Sea $f \in \mathbb{Q}[X]$ irreducible de grado primo, y sea $E \subset \mathbb{C}$ el cuerpo de descomposición de f. Probar que si f tiene exactamente dos raíces no reales en $\mathbb{C}$, entonces $G(E/\mathbb{Q}) \simeq \mathbb{S}_p$.
10. (a) Sea $m \in \mathbb{N}$ par, y sean $a_1 < \cdots < a_r$ enteros positivos pares, con $r > 1$ impar. Sea $f = (X^2+m)(X-a_1)\ldots(X-a_r) - 2$. Probar que:
        (i) f es irreducible en $\mathbb{Q}[X]$.
        (ii) Para m suficientemente grande, f tiene exactamente dos raíces no reales en $\mathbb{C}$.
    (b) Deducir que para cada primo $p \in \mathbb{N}$ existe una extensión de Galois $E/\mathbb{Q}$ con grupo de Galois $\mathbb{S}_p$.