Universidad de la República
Facultad de Ciencias
Centro de Matemática

Grupos y Teoría de Galois
Primer semestre de 2020

Práctico 10

En los siguientes ejercicios todos los cuerpos son subcuerpos de $\mathbb{C}$.

1. Probar que $\mathbb{Q}(i)$ y $\mathbb{Q}(\sqrt{2})$ son isomorfos como $\mathbb{Q}$-espacios vectoriales pero no como cuerpos.

2. Sea $F \supset K$ una extensión. Probar que $F \supset K$ es una extensión algebraica si y solo si para todo cuerpo intermedio $F \supset E \supset K$ y todo K-morfismo $\sigma : E \to E$, se cumple que σ es un isomorfismo.

3. Sea $u = \sqrt{d}$, siendo $d \in \mathbb{Q}$, $d \geq 0$. Probar que $\operatorname{Gal}(\mathbb{Q}(u)/\mathbb{Q})$ es el grupo trivial o el cíclico C_2.

4. Probar que todo automorfismo de $\mathbb{R}$ preserva el orden. Deducir que $\operatorname{Gal}(\mathbb{R}/\mathbb{Q})$ es el grupo trivial.

5. Se considera la torre de extensiones $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt{2}\right) \subset \mathbb{Q}\left(\sqrt[4]{2}\right)$. Probar que $\mathbb{Q}\left(\sqrt{2}\right)/\mathbb{Q}$ y $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ son de Galois pero que $\mathbb{Q}\left(\sqrt[4]{2}\right)/\mathbb{Q}$ no lo es (esto muestra que la relación "ser de Galois" no es transitiva).

6. Sean K un cuerpo, F el cuerpo de descomposición de $f \in K[X]$ y $G = \operatorname{Gal}(F/K)$. Probar:
   a) Si f tiene n raíces (distintas) en F, entonces G es isomorfo a un subgrupo de $\mathcal{S}_n$.
   b) Si f es irreducible, entonces G actúa transitivamente en el conjunto de las raíces de f en F.

7. Sea $f = X^4 - 3 \in \mathbb{Q}[X]$. Determinar el grupo de Galois de f como subgrupo de $\mathcal{S}_4$.

8. Sea $f \in K[X]$ un polinomio y F su cuerpo de descomposición de f. Sea $f = g\,h$ una factorización de f en $K[X]$ y sean E y L los cuerpos de descomposición de g y h respectivamente. Supongamos que vale $E \cap L = K$. Sean G_f, G_g y G_h los grupos de Galois respectivos de f, g y h.
   a) Probar $G_f = HJ$, siendo $H = \operatorname{Gal}(F/E)$ y $J = \operatorname{Gal}(F/L)$.
   b) Probar $G_f \simeq G_g \times G_h$.

9. Identificar los grupos de Galois de las siguientes extensiones
   a) $\mathbb{Q}(\sqrt{2}, \sqrt{5})/\mathbb{Q}$;
   b) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$. *Sugerencia:* usar que si $a_1, \ldots, a_k \in \mathbb{Z}^+$ son distintos y libres de cuadrados (en su descomposición factorial), entonces son linealmente independientes sobre $\mathbb{Q}$.

10. Sea $p > 2$ primo y $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$.
    a) Probar que el cuerpo de descomposición de $X^p - 1 \in \mathbb{Q}[X]$ es $\mathbb{Q}(\zeta)$ (esto no requiere p primo).
    b) Hallar el polinomio irreducible de ζ sobre $\mathbb{Q}$. *Sugerencia:* recordar el práctico 8.
    c) Determinar el grupo de Galois de $X^p - 1 \in \mathbb{Q}[X]$.

11. Determinar los grupos de Galois de los siguientes polinomios sobre los cuerpos indicados.
    a) $X^3 - 2$ sobre $\mathbb{Q}$.
    b) $(X^3 - 2)(X^2 - 5)$ sobre $\mathbb{Q}$.
    c) $(X^3 - 2)(X^2 + 3)$ sobre $\mathbb{Q}$.
    d) $X^4 - 5$ sobre $\mathbb{Q}$, sobre $\mathbb{Q}(\sqrt{5})$ y sobre $\mathbb{Q}(i\sqrt{5})$.

12. Determinar todas las extensiones intermedias entre $\mathbb{Q}$ y el cuerpo de descomposición del polinomio $f \in \mathbb{Q}[X]$, en los casos siguientes.

   a) $f = X^3 - 2$.

   b) $f = X^4 - 10X^2 + 4$.

   c) $f = X^4 + 4X^2 + 2$.

13. Determinación del grupo de Galois de un polinomio de grado tres.

   a) Sea $f = X^3 + pX + q \in K[X]$ irreducible. Sean u_1, u_2, u_3 las raíces de f en $\mathbb{C}$, $F = K(u_1, u_2, u_3)$ y $G = \mathrm{Gal}(F/K)$. Sea $\Delta = (u_1 - u_2)(u_1 - u_3)(u_2 - u_3) \in \mathbb{C}$. Vale[1] $\Delta^2 = -4p^3 - 27q^2$.

      1) Probar que el orden de G es 3 o 6.

      2) Supongamos $\Delta \in K$. Probar que si $\sigma \in G$, entonces σ no puede ser una trasposición de las raíces (*sugerencia:* evaluar σ en Δ). Concluir que G es un grupo cíclico de orden 3.

      3) Probar que si $\Delta \notin K$, entonces $[K(\Delta) : K] = 2$. Concluir $G = \mathcal{S}_3$.

   b) Sea $f = X^3 + aX^2 + bX + c \in K[X]$.

      1) Sea $g = f(X - a/3)$. Probar que g es de la forma $g = X^3 + pX + q$.

      2) Probar que f y g tienen el mismo grupo de Galois.

   c) Determinar el grupo de Galois sobre $\mathbb{Q}$ de $X^3 + 3X^2 - 3$ y $X^3 - 6X^2 + 9X + 1$.

14. Una extensión cuyo grupo de Galois son los cuaternios.

   a) Sea $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$. Probar que $K/\mathbb{Q}$ es de Galois con $\mathrm{Gal}(K/\mathbb{Q}) = C_2 \times C_2$. Sean $\sigma, \tau \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$ tales que $\sigma\left(\sqrt{2}\right) = -\sqrt{2}$, $\sigma\left(\sqrt{3}\right) = \sqrt{3}$, $\tau\left(\sqrt{2}\right) = \sqrt{2}$, $\tau\left(\sqrt{3}\right) = -\sqrt{3}$.

   b) Sea $u = \sqrt{\left(2 + \sqrt{2}\right)\left(3 + \sqrt{3}\right)}$, probar $u \notin K$. *Sugerencia*: mostrar $\sigma\left(u^2\right) = \left(\left(\sqrt{2} - 1\right) u\right)^2$; suponer $u \in K$, hallar los posibles valores de $\sigma(u)$ y luego calcular $\sigma^2(u)$.

   c) Sea $F = K(u)$, siendo u el de la parte anterior. Probar $[F : \mathbb{Q}] = 8$.

   d) Probar que σ y τ se pueden extender a morfismos $\sigma_\pm, \tau_\pm : F \to \mathbb{C}$ tales que $\sigma_\pm\left(u\right) = \pm\left(\sqrt{2} - 1\right) u$ y $\tau_\pm\left(u\right) = \pm\left(\frac{\sqrt{3}-1}{\sqrt{2}}\right) u$. Probar $\sigma_\pm, \tau_\pm \in \mathrm{Gal}\left(F/\mathbb{Q}\right)$, $|\sigma_+| = |\tau_+| = 4$ y $\sigma_+\tau_+ \neq \tau_+\sigma_+$.

   e) Probar que $F/\mathbb{Q}$ es de Galois y deducir que $\mathrm{Gal}\left(F/\mathbb{Q}\right)$ es el grupo de los cuaternios Q.

[1] Esto se prueba usando las relaciones entre coeficientes y raíces, pero no es inmediato.