Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Héctor Pastén Vásquez **Ayudante:** José Cuevas Barrientos
Curso: Álgebra abstracta II **Sigla:** MAT2244
Fecha: 3 de abril de 2025

Grupos de Galois

1. Pruebe que el nonágono (= 9-gono) no es constructible con regla y compás.
2. Sea L/k una extensión normal y definamos el subconjunto:
$$L_{\text{sep}} := \{\alpha \in L : \alpha \text{ es separable sobre } k\}.$$
   a) Pruebe que L_{sep} es un subcuerpo de L.
   b) Pruebe que la extensión L_{sep}/k es de Galois y L/L_{sep} es puramente inseparable.
   c) Pruebe que la siguiente aplicación
$$\rho\colon \operatorname{Gal}(L/k) \longrightarrow \operatorname{Gal}(L_{\text{sep}}/k), \qquad \sigma \longmapsto \sigma|_{L_{\text{sep}}}$$
   está bien definida y es un isomorfismo de grupos.
3. Sea K/k una extensión simple de cuerpos (i.e., hay $\alpha \in K$ tal que $K = k(\alpha)$) de grado $n := [K : k] < \infty$. Pruebe que K/k tiene a lo sumo 2^n subextensiones (incluyendo a K y k mismos).
4. Sea $\zeta_n = \exp(2\pi i/n) \in \mathbb{C}$ una raíz n-ésima primitiva de la unidad. Pruebe que $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es una extensión de Galois y que $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
5. Pruebe que para todo grupo *abeliano* finito G existe una extensión $K/\mathbb{Q}$ de Galois tal que $\operatorname{Gal}(K/\mathbb{Q}) \cong G$.

   Pista: Para la prueba puede ser útil emplear el **teorema de Dirichlet** que dice que dado $n > 1$ entero y a coprimo con n, existen infinitos primos p tales que $p \equiv a \pmod{n}$. □

A. Ejercicios propuestos

1. ¿El pentágono regular es constructible con regla y compas?
2. Cuente la cantidad de subextensiones de las siguientes extensiones:
   a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}$.
   b) $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$, donde ζ_3 es una raíz cúbica (primitiva) de la unidad.
   c) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$.

B. Comentarios adicionales

En el ejercicio 3 es importante que la extensión sea *simple*. Si la extensión es separable finita, el resultado también aplica, pero, por ejemplo, la extensión inseparable $\mathbb{F}_p(t^{1/p}, s^{1/p}) \supseteq \mathbb{F}_p(t, s)$ posee infinitas subextensiones.

El ejercicio 5 es un caso sencillo del *problema inverso de Galois*: ¿será acaso que todo grupo finito es isomorfo a un grupo de Galois de una extensión $K/\mathbb{Q}$? ¿De no ser así, habrá un invariante que permita discriminar cuáles sí o no?

Referencias

1. Jacobson, N. *Basic Algebra* 2 vols. (Freeman y Company, 1910).
2. Lang, S. *Algebra* (Springer-Verlag New York, 2002).

Correo electrónico: `josecuevasbtos@uc.cl`
URL: `https://josecuevas.xyz/teach/2025-1-ayud/`