Pontificia Universidad Católica de Chile
Facultad de Matemáticas

Profesor: Héctor Pastén Vásquez **Ayudante:** José Cuevas Barrientos
Curso: Álgebra abstracta II **Sigla:** MAT2244
Fecha: 10 de abril de 2025

Extensiones resolubles

1. Una extensión L/k se dice ***abeliana*** (resp. ***cíclico***) si existe una extensión A/k de Galois con $\operatorname{Gal}(A/k)$ abeliano (resp. cíclico), tal que $k \subseteq L \subseteq A$.
   a) Pruebe que si L/k es abeliano (resp. cíclico), entonces L/k es de Galois y $\operatorname{Gal}(L/k)$ es abeliano (resp. cíclico).
   b) En la extensión $F/L/k$, pruebe que si F/k es abeliano (resp. cíclico), entonces F/L y L/k son abelianos (resp. cíclicos).

   Problema: Si en la extensión $F/L/k$, se cumple que F/L y L/k son abelianos (resp. cíclicos), entonces ¿F/k es siempre abeliano (resp. cíclico)?

2. Pruebe que si $L_1, \dots, L_n/k$ son extensiones abelianas (resp. resolubles) contenidas en otra extensión Ω/k, entonces el composito $L_1 \cdots L_n$ es abeliano (resp. resoluble).
3. Pruebe, sin usar las fórmulas cuadrática y de Cardano, que todo polinomio (separable) de grado ≤ 3 es resoluble por radicales.
4. Sea K/k una extensión finita. Dado $\alpha \in K$, denotemos por $m_\alpha(x) := \alpha \cdot x$ el cual determina un k-endomorfismo $m_\alpha \colon K \to K$. Defina la ***norma*** y ***traza*** de α como
$$\operatorname{Nm}_{K/k}(\alpha) := \det m_\alpha, \qquad \operatorname{Tr}_{K/k}(\alpha) := \operatorname{tr} m_\alpha.$$
   (Recuerde, de su curso de álgebra lineal, que el determinante y la traza de un endomorfismo no dependen de la elección de base.)
   a) Pruebe que, para $\alpha, \beta \in K$ se cumple que
$$\operatorname{Tr}_{K/k}(\alpha+\beta) = \operatorname{Tr}_{K/k}(\alpha) + \operatorname{Tr}_{K/k}(\beta), \qquad \operatorname{Nm}_{K/k}(\alpha\cdot\beta) = \operatorname{Nm}_{K/k}(\alpha)\cdot\operatorname{Nm}_{K/k}(\beta).$$
   b) Sea $G = \{\sigma \colon K \to k^{\mathrm{alg}}\}$ el conjunto de los homomorfismos de K-álgebras. Pruebe que
$$\operatorname{Tr}_{K/k}(\alpha) = \sum_{\sigma\in G} \sigma(\alpha), \qquad \operatorname{Nm}_{K/k}(\alpha) = \prod_{\sigma\in G} \sigma(\alpha).$$
   Pista: Haga el caso $K = k(\alpha)$ y luego emplee que hay tantos $k(\alpha)$-homomorfismos $K \to k(\alpha)^{\mathrm{alg}} = k^{\mathrm{alg}}$ como grado $[K : k(\alpha)]$. □
   c) Sea L/K una extensión finita y sea $\gamma \in L$, pruebe que
$$\operatorname{Tr}_{L/k} = \operatorname{Tr}_{K/k} \circ \operatorname{Tr}_{L/K}, \qquad \operatorname{Nm}_{L/k} = \operatorname{Nm}_{K/k} \circ \operatorname{Nm}_{L/K}.$$
5. Empleando lo anterior vamos a probar que $\mathbb{Q}(\sqrt[n]{a}) \neq \mathbb{Q}(\sqrt[n]{b})$ con $a \neq b$ enteros *coprimos* libres de potencias n-ésimas para $n > 1$ un entero *primo*.
   Pista: Use la traza con $K := \mathbb{Q}(\sqrt[n]{a})$. Pruebe que $\operatorname{Tr}_{K/\mathbb{Q}}(\sqrt[n]{a}) = 0$ y $\operatorname{Tr}_{K/\mathbb{Q}}(\sqrt[n]{a^j b}) = 0$ para $0 \leq j < n$, para llegar a una contradicción. □

A. Ejercicios propuestos

1. Pruebe, sin usar la fórmula de Ferrari, que todo polinomio de grado ≤ 4 es resoluble por radicales.
2. Construya $f \in \mathbb{C}(t)$ no constante de modo que la extensión $\mathbb{C}(t)/\mathbb{C}(f)$ sea de Galois y
$$\operatorname{Gal}(\mathbb{C}(t)/\mathbb{C}(f)) \cong D_6.$$
   (Para mí, D_6 es el diedral con 6 elementos.)

Pista: Primero, construya un subgrupo $G \leq \mathrm{Gal}(\mathbb{C}(t)/\mathbb{C})$ tal que $G \cong D_6$. Para lograrlo, encuentre un elemento σ en G de orden 2 (como $\sigma(t) = 1/t$) y otro τ de orden 3 tales que $\sigma\tau\sigma = \tau^{-1}$. Finalmente, explicite el cuerpo fijo $\mathbb{C}(t)^G$. □

B. Comentarios adicionales

El ejercicio propuesto 2 es generalizable para ver que para todo $n > 1$ existe f tal que $\mathrm{Gal}(\mathbb{C}(t)/\mathbb{C}(f)) \cong D_{2n}$. El ejercicio propuesto 1 es lo mejor posible, pues precisamente el teorema de Abel-Ruffini dice que hay polinomios separables de grado 5 que no son resolubles por radicales, precisamente porque los grupos A_5 y S_5 no son resolubles.

En la ayudantía pasada vimos un ejemplo de extensión abeliana, las ciclotómicas $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Por lo demás, toda subextensión de una ciclotómica es también abeliana y el composito de dos extensiones ciclotómicas es también ciclotómica (pues $\mathbb{Q}(\zeta_n)\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{nm})$ cuando n, m son coprimos). Es altamente interesante que un teorema de Kronecker-Weber nos da un recíproco, a decir:

Teorema B.1: Toda extensión abeliana de $\mathbb{Q}$ es subextensión de una ciclotómica.

Este resultado es difícil y se puede probar con teoría de cuerpos de clase. Vea **[3].**

Referencias

1. Lang, S. *Algebra* (Springer-Verlag New York, 2002).
2. Nagata, M. *Theory of Commutative Fields Translations in Mathematical Monographies* **125** (American Mathematical Society, 1967).
3. Neukirch, J. *Algebraic Number Theory* trad. del alemán por Schappacher, N. (Springer-Verlag Berlin Heidelberg, 1999). Trad. de *Algebraische Zahlentheorie* (Springer-Verlag Berlin Heidelberg, 1992).

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