Pontificia Universidad Católica de Chile y Universidad de Chile
Facultad de Matemáticas

Profesor: José Samper
Ayudante: José Cuevas Barrientos
Curso: Álgebra II
Sigla: MPG3201
Fecha: 20 de agosto de 2025

Teoría de Galois

1. Grupos de Galois

◉◉ 1. Pruebe que para todo grupo *abeliano* finito G existe una extensión $K/\mathbb{Q}$ de Galois tal que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

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 $p \equiv a \pmod{n}$. □

2. Sea L/k una extensión normal y definamos el subconjunto:

$$L_{\mathrm{sep}} := \{\alpha \in L : \alpha \text{ es separable sobre } k\}.$$

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

$$\rho\colon \mathrm{Gal}(L/k) \longrightarrow \mathrm{Gal}(L_{\mathrm{sep}}/k), \qquad \sigma \longmapsto \sigma|_{L_{\mathrm{sep}}}$$

está bien definida y es un isomorfismo de grupos.

◉◉ 3. Sea K/k una extensión simple de cuerpos de grado $n := [K : k] < \infty$. Pruebe que K/k tiene a lo sumo 2^n subextensiones (incluyendo a K y k mismos).

Problema: ¿Se puede alcanzar dicha cota? Dicho de otro modo, ¿cuán óptima es?

4. Considere la extensión $\mathbb{Q}\left(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right) \supseteq \mathbb{Q}$ y determine:

a) Si es de Galois.
b) El grupo de Galois de su cuerpo de escisión.

A. Ejercicios adicionales: La correspondencia de Jacobson-Bourbaki

En la siguiente serie de ejercicios, pretendemos probar un resultado un tanto técnico. En la sección, Hom_k denota homomorfismos de k-espacios vectoriales.

5. Sea $k \subseteq K \subseteq L$ una torre de extensiones, posiblemente infinitas. Pruebe que K/k es una extensión finita syss $\mathrm{Hom}_k(K, L)$ es un L-espacio vectorial de dimensión finita (la suma y producto escalar son coordenada a coordenada) y, en cuyo caso, que

$$[K : k] = [\mathrm{Hom}_k(K, L) : L].$$

◉◉ 6. Sea L un cuerpo. Note que el conjunto $\mathrm{End}_{\mathsf{Ab}}(L)$ de endomorfismos de L como grupo abeliano es un anillo (no conmutativo) con la suma coordenada a coordena, y la composición como producto; más aún, hay una inyección de anillos $\mu\colon L \hookrightarrow \mathrm{End}_{\mathsf{Ab}}(L)$ que a un elemento $\alpha \in L$ le asigna el endomorfismo $\mu(\alpha)(x) := \alpha \cdot x$. Sea $A \subseteq \mathrm{End}_{\mathsf{Ab}}(L)$ una L-subálgebra (i.e., un subanillo que contiene a la imagen de L mediante μ) tal que $n := \dim_L(A) < \infty$.

a) Pruebe que existen $\alpha_1, \ldots, \alpha_n \in L$ y $\sigma_1, \ldots, \sigma_n \in A$ tales que $\sigma_i(\alpha_j) = \delta_{ij}$, donde δ es la delta de Kronecker.
Pista: Hay un emparejamiento L-$\mathbb{Z}$-bilineal $A \times L \to L$ (donde A tiene estructura de módulo por la derecha como $(\sigma \cdot x)(y) = \sigma(y) \cdot x$) dado por la evaluación mediante el cual ústed querrá extraer un emparejamiento L-bilineal no degenerado. □

b) Pruebe que
$$k := \{\alpha \in L : \forall \sigma \in A \qquad \alpha \cdot \sigma = \sigma \cdot \alpha\} \subseteq L$$
es un subcuerpo de L y que cada $\sigma_j \in A$ manda $\sigma_j \colon L \to k$.
c) Pruebe que $\alpha_1, \ldots, \alpha_n \in L$ (dados por el primer inciso) forman una k-base.
d) **Correspondencia de Jacobson-Bourbaki** (**[0],** Th. I.2):
Concluya que $[L : k] = n$ y que $A = \mathrm{End}_k(L)$.

La razón de la inclusión de la *correspondencia de Jacobson-Bourbaki* está en que, en cierto modo, generaliza la correspondencia clásica de Galois: incluye tanto al caso finito, como ciertos casos de extensiones inseparables; vid. **[0].**

B. Teoría de Galois profinita

Hay, asimismo, una generalización de la teoría de Galois al caso infinito, para la cual se requiere de la noción categorial de «límite inverso» (vid. **[0,** pág. 490]); daremos primero un contraejemplo ilustrativo y opcional:

A. Sea K/k una extensión algebraica de Galois posiblemente infinita. Vamos a considerar el *conjunto dirigido* (o «categoría de índices») $\mathscr{I}$ cuyos objetos son subextensiones $k \subseteq F \subseteq K$ de Galois *finitas*, donde $F \leq F'$ (o donde hay una única flecha $F \to F'$) syss $F \subseteq F'$. Tenemos el sistema inverso (o «funtor contravariante») donde $\rho_F^{F'} \colon \mathrm{Gal}(F'/k) \twoheadrightarrow \mathrm{Gal}(F/k)$ es la restricción para $F \leq F' \in \mathscr{I}$. Pruebe que
$$\mathrm{Gal}(K/k) = \varprojlim_{F \in \mathscr{I}} \mathrm{Gal}(F/k),$$

B. Definamos $\mathbb{Z}_\ell$, el anillo de enteros ℓ-ádicos, como el límite inverso del diagrama $\rho_{n-1}^n \colon \mathbb{Z}/\ell^n\mathbb{Z} \to \mathbb{Z}/\ell^{n-1}\mathbb{Z}$ (dado por $n \mod \ell^n \mapsto n \mod \ell^{n-1}$) con el conjunto dirigido $(\mathbb{N}, \leq)$. Pruebe que
$$\mathrm{Gal}(\mathbb{F}_p^{\mathrm{alg}}/\mathbb{F}_p) \cong \prod_\ell \mathbb{Z}_\ell =: \hat{\mathbb{Z}},$$
donde ℓ recorre todos los números primos.

C. Pruebe, mediante un simil del argumento diagonal de Cantor, que $\mathbb{Z}_\ell$ es no numerable y, por tanto, concluya que existe $\sigma \in \mathrm{Gal}(\mathbb{F}_p^{\mathrm{alg}}/\mathbb{F}_p)$ que no está en el grupo generado por el automorfismo de Frobenius Frob_p. No obstante, el cuerpo fijo por $\langle \mathrm{Frob}_p \rangle$ es $\mathbb{F}_p$, pese a que $\langle \mathrm{Frob}_p \rangle \neq \mathrm{Gal}(\mathbb{F}_p^{\mathrm{alg}}/\mathbb{F}_p)$.

Esto prueba que la biyección entre subgrupos y subextensiones se rompe en el caso infinito. ¿Cómo se arregla? Mediante el ejercicio A, vemos que el grupo de Galois es el límite inverso de grupos finitos,[1] con lo que lo podemos dotar de la topología del límite inverso (a veces llamada *topología de Krull*). Ahora, habrá una biyección entre subextensiones y subgrupos *cerrados* del grupo de Galois. El ejercicio C muestra entonces que $\langle \mathrm{Frob}_p \rangle$ es denso en $\mathrm{Gal}(\mathbb{F}_p^{\mathrm{alg}}/\mathbb{F}_p)$ con dicha topología. Una referencia del tema es Neukirch **[0],** §§IV.1-3.

Referencias

0. Aluffi, P. *Algebra. Chapter 0* (American Mathematical Society, 1960).
0. Jacobson, N. *Lectures in Abstract Algebra.* 3: *Theory of Fields and Galois Theory* (Van Nostrand, 1964).
0. Lang, S. *Algebra* (Springer-Verlag New York, 2002).
0. 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/2025-2-alg/

[1] De ahí el nombre «profinito.»