Teoría de Galois: Repaso y herramientas básicas

Rocío Belén Sepúlveda Manzo

Resumen. En el contexto de la teoría de representación de Galois, se utiliza ampliamente la teoría de Galois. En esta charla, exploraremos los conceptos fundamentales necesarios para comprender los grupos de Galois y examinaremos resultados esenciales en este campo.

1. Introducción

Sean L y K campos. Denotaremos L/K como la extensión de campos.

Dada una extensión L/K diremos que f *escinde* sobre L si f se puede factorizar completamente en polinomios lineales de $L[x]$. Un *campo de escición* de f sobre K es una extensión L/K en el cual f escinde y tal que el único campo intermedio $L/F/K$ donde f escinde es $F = L$. Un resultado intermedio es

Lema 1. *Sea $f \in K[x]$ y sea L/K una extensión, L es un campo de escición de f sobre K si y solo si f escinde en L y se tiene $L = K(S)$ donde S es el conjunto de las raíces de f en L.*

2. Extensiones normales y separables

2.1. Extensiones normales Una extensión L/K es *normal* si es algebraica y si para todo $a \in L$ el polinomio minimal $f_a \in K[x]$ de a sobre K escinde en L.

Observación. Sea L/K de grado 2. Entonces L/K es normal.

Teorema 2 (Caracterización de extensiones normales finitas)**.** *Sea L/K una extensión finita. Son equivalentes:*

(i) *L/K es normal*

(ii) *$L = K(a_1, \dots, a_n)$ para ciertos a_j tales que cada polinomio minimal $f_j \in K[x]$ de a_j sobre K escinde en L.*

(iii) *Existe $f \in K[x]$ tal que L es un campo de escición de f sobre K.*

(iv) *Para toda extensión de campos F/L y todo morfismo de K-álgebras $\sigma : L \to F$ se cumple $\sigma(L) = L$.*

(v) *Existe una extensión de finita F/L tal que para todo $a \in L$ el polinomio minimal f_a de a sobre K escinde en F, y satisfaciendo además que para todo morfismo de K-álgebras $\sigma : L \to F$ se cumple $\sigma(L) = L$.*

Lema 3 (Normalidad en torres)**.** *Sean F/L y L/K extensiones algebraicas. Si F/K es normal, entonces F/L es normal.*

Una consecuencia es el siguiente:

Corolario 4 (Las extensiones entre campos finitos son normales)**.** *Sea L/K una extensión con L y K campos finitos. Entonces L/K es normal.*

Fecha: 08 de septiembre, 2023.

2.2. Extensiones separables Sea K un campo. Un polinomio no nulo $f \in K[x]$ es *separable* si no tiene raíces repetidas en su campo de escisión.

Ejemplo. $K = \mathbb{F}_p(t)$ con t una variable. Tomemos $f(x) = x^p - t \in K[x]$. El campo de escición de f sobre K es $L = K(t^{1/p})$ porque

$$(x - t^{1/p})^p = x^p - (t^{1/p})^p = x^p - t = f.$$

Por otro lado, notemos que f no es separable ya que posee raíces repetidas.

Sea L/K una extensión algebraica de campos. Un $a \in L$ es *separable* sobre K si el polinomio minimal $f_a \in K[x]$ de a sobre K es separable. Decimos que la extensión L/K es *separable* si todo elemento $a \in L$ es separable.

Lema 5 (Extensiones separables notables)**.** *Sea L/K una extensión algebraica.*

(i) Si $\mathrm{car}(K) = 0$, entonces L/K es separable.
(ii) Si L y K son campos finitos, entonces L/K es separable.

Ejemplo. (i) Todas las extensiones algebraicas de campos del tipo $\mathbb{Q}(S)$ son extensiones separables, pues son de característica cero.
(ii) $K = \mathbb{F}_p(t)$ con t una variable, y sea $L = K(t^{1/p})$ como antes. Entonces L/K no es separable pues, como se vió anteriormente, $t^{1/p}$ no es separable, por tanto, la extensión tampoco.

Lema 6 (Separabilidad en torres)**.** *Sean F/L y L/K extensiones algebraicas. Si F/K es separable, entonces F/L y L/K son separables.*

Un teorema relevante sobre separabilidad es el siguiente:

> **Teorema 7** (Teorema del elemento primitivo)**.** *Sea L/K una extensión finita separable. Entonces es primitva: existe $a \in L$ tal que $L = K(a)$.*

3. Extensiones Galois y automorfismos

Una extensión algebraica de campos L/K es *Galois* si es normal y separable. El objetivo de estudiar extensiones de Galois es precisamente para poder contar automorfismos.

Por los lemas y corolarios enunciados en las secciones anteriores se puede deducir los siguientes lemas:

Lema 8 (Ejemplos notables de extensiones de Galois)**.** *(i) Si $\mathrm{car}(K) = 0$ y L/K es normal, entonces L/K es Galois.*
(ii) Si L y K son campos finitos, entonces L/K es Galois.

Para una extensión L/K se define:

$$\begin{aligned} \mathrm{Aut}(L/K) &= \{\sigma : L \to L \text{ automorfismo de } K\text{-álgebra}\} \\ &= \{\sigma : L \to L \text{ automorfismo de campo con } \sigma(a) = a \text{ para todo } a \in K\} \end{aligned}$$

Observación. Notemos que $\mathrm{Aut}(L/K)$ es un grupo con la composición de funciones, y su neutro es Id_L. Cuando L/K es finita, es inmediato que todo automorfismo de K-álgebras $\sigma : L \to L$ es autmáticamente un automorfismo.

Lema 9 (Conteo de automorfismos)**.** *Sea L/K una extensión finita de grado n. Entonces $\#\,\mathrm{Aut}(L/K) \leq n$. Además, si L/K es Galois, entonces $\#\,\mathrm{Aut}(L/K) = n$.*

Si L es un campo, escribimos $\mathrm{Aut}(L)$ por el grupo de todos los automorfismos de campo de L. Si $H \leq \mathrm{Aut}(L)$, se define

$$L^H = \{a \in L : \forall \sigma \in H,\ \sigma(a) = a\}$$

Lema 10 (de Artin)**.** *Sea L un campo y sea $H \leq \mathrm{Aut}(L)$ un subgrupo finito de automorfismos de L. Entonces la extensión L/L^H es finita Galois de grado $\#H$ y $\mathrm{Aut}(L/L^H) = H$.*

Corolario 11 (Galois es caracterizado por conteo)**.** *Sea L/K una extensión finita de grado n. Tenemos que $\#\mathrm{Aut}(L/K) = n$ si y solo si L/K es Galois.*

3.1. El teorema fundamental Denotaremos como $\mathrm{Gal}(L/K)$ a $\mathrm{Aut}(L/K)$ cuando la extensión es de Galois. En esta sección veremos el teorema fundamental de la teoría de Galois, comenzando primero con el siguiente lema:

Teorema 12 (Galois, 1830)**.** *Sea L/K una extensión Galois finita. Dado un campo intermedio $L/M/K$, la extensión L/M es Galois y el grupo $\mathrm{Gal}(L/M)$ es un subgrupo de $\mathrm{Gal}(L/K)$. La asignación $M \mapsto \mathrm{Gal}(L/M)$ define una biyección*

$$\{M \text{ campo } : L/M/K\} \to \{H : H \leq \mathrm{Gal}(L/K)\}$$

Cuya inversa es $H \mapsto L^H$. Esta biyección tiene las siguientes propiedades básicas:

(i) *Las inclusiones se invierten*
(ii) $[L : M] = \#\mathrm{Gal}(L/M)$ *para cada* $L/M/K$.
(iii) $[L^H : K] = [\mathrm{Gal}(L/K) : H]$ *para cada subgrupo* $H \leq \mathrm{Gal}(L/K)$.

La biyección del teorema se denomina *Correspondencia de Galois*. A continuación enunciaremos un complemento importante:

Lema 13 (Complemento de normalidad)**.** *Sea L/K una extensión de Galois finita. Sea M campo intermedio y sea $H \leq \mathrm{Gal}(L/K)$ el subgrupo de Galois correspondiente a M. Son equivalentes:*

(i) *M/K es Galois,*
(ii) *M/K es normal,*
(iii) *$H \leq \mathrm{Gal}(L/K)$ es un subgrupo normal.*

Cuando estas condiciones equivalentes ocurren, la función restricción

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K),\ \sigma \mapsto \sigma|_M$$

es bien definida, es un morfismo de grupos, es sobreyectiva y tiene kernel $\mathrm{Gal}(L/M)$. En particular, el morfismo de restricción induce un isomorfismo.

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) \cong \mathrm{Gal}(M/K).$$

3.2. Calculando grupos de Galois

Ejemplo ($\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$). Notemos que un elemento del grupo de galois es el frobenius: $\phi_p : \mathbb{F}_q \to \mathbb{F}_q,\ \alpha \mapsto \alpha^p$. En efecto, es un automorfismo que fija $\mathbb{F}_p$ pues para $\alpha \in \mathbb{F}_p,\ \phi_p(\alpha) = \alpha^p = \alpha$. Por el pequeño teorema de Fermat. Y es una biyección, pues es inyectiva (su kernel es trivial).

Veamos que el frobenius genera el grupo de Galois, para ello necesitamos saber que el $\#\langle\phi_p\rangle = [\mathbb{F}_q : \mathbb{F}_p] =: d$. Notemos que $(\phi_p)^d(\alpha) = (\alpha^p)^d = \alpha^{p^d} = \alpha^q = \alpha$.

Supongamos que existe un $j < d$ tal que $\phi_p^j = \mathrm{Id}$, entonces $\phi_p^j(\alpha) = \alpha^{p^j} = \alpha$. Así que para cada $\alpha \in \mathbb{F}_p$ es raíz del polinomio $f(x) = x^{p^j} - x$ y su grado es menor estricto que q. Así que f no puede poseer todas las raíces, lo que genera una contradicción.

Así que $\#\langle\phi_p\rangle = d \geq \#\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ y como el frobenius es un elemento del grupo, se tiene que son isomorfos $\langle\phi_p\rangle = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. Y como $\langle\phi_p\rangle \cong \mathbb{Z}/d\mathbb{Z}$. Se tiene que $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z}$

Ejemplo ($\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$). Notemos que los automorfismos del grupo de galois cumplen la siguiente condición:

$$\sigma_j : \mathbb{Q}(\zeta_p) \to \mathbb{Q}(\zeta_p),\ \zeta_p \mapsto \zeta_p^j.$$

Donde $(j, p) = 1$. Por otro lado, si $i \equiv j \mod p$ entonces $\sigma_i = \sigma_j$. Así que la cantidad de automorfismos está dada por la cantidad de elementos coprimos a p, $\varphi(p) = p - 1$.

Luego considere el siguiente morfismo:

$$F : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}),\ j \mapsto \sigma_j$$

Este es un isomorfismo pues $\#(\mathbb{Z}/p\mathbb{Z})^\times = \#\,\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ y $\ker F = \{j \in (\mathbb{Z}/p\mathbb{Z})^\times\} = \{1\}$. Así que $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.
¿Qué ocure con $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$? Basta considerar el siguiente morfismo:

$$G : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}),\ j \mapsto \sigma_j$$

Notemos, además, que el polinomio ciclotómico (minimal de ζ_n) es irreducible de grado $\varphi(n)$ (la cantidad coprimos menores a n). Luego, $\varphi(n) = [\mathbb{Q}(\zeta_n)/\mathbb{Q}]$. Por otro lado, $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$. Así que, basta ver que el morfismo entre el grupo de inversibles y el grupo de Galois es inyectivo o sobreyectivo de la misma forma que antes. Además, con la igualdad de grados mostramos que esta extensión es de Galois.

Correo electrónico: `rseplveda@uc.cl`