Charla 2: Campo de clase de Hilbert y el símbolo de Artin

Rocío Belén Sepúlveda Manzo

1. Preliminar

Sea K un campo de números Un *lugar* es una clase de equivalencia no trivial de valuaciones. Por un teorema de Ostrowski, cada lugar cae dentro de las siguientes categorías:

(i) Lugares que contienen una de las valuaciones $\mathfrak{p}$-ádicas dada por $\|\alpha\|_{\mathfrak{p}} = \mathfrak{p}^{-v_{\mathfrak{p}}(\alpha)}$, para un ideal primo no nulo de $\mathcal{O}_K$. Estos son los lugares *finitos* (o bien, *no arquimedianos*, o *discretos*) de K.

(ii) Lugares que contienen una de las valuaciones $\|\alpha\|_{\sigma} = |\sigma(\alpha)|_{\mathbb{R}}$, para algún encaje real $\sigma : K \hookrightarrow \mathbb{R}$ de K. Estos son los lugares *infinitos reales* (o bien, *arquimedianos reales*) de K.

(iii) Lugares que contienen una de las valuaciones $\|\alpha\|_{\sigma} = |\sigma(\alpha)|^2_{\mathbb{C}}$ para algún $\sigma : K \hookrightarrow \mathbb{C}$, un encaje complejo de K que no cae en $\mathbb{R}$. Estos son los lugares *infinitos complejos* (o bien, *arquimediano complejo*) de K.

Observación. Note que dos primos no nulos distintos de $\mathcal{O}_K$ no pueden producir valuaciones equivalentes, por lo que están asociados a distintos lugares de K. Similarmente, distintos encajes reales producen lugares valuaciones no equivalentes asociadas a distintos lugares de K. En el caso de los encajes complejos, podemos tener que cada lugar posea dos valuaciones equivalentes correspondientes a cada par de encajes conjugados. Por otro lado, si dos encajes complejos de F no son conjugados, entonces dan a lugar a valuaciones no equivalentes. Por lo tanto, hay un único lugar para cada par conjugado de encajes complejos de K.

Para un campo de números K, existe una cantidad finita de lugares infinitos. También, dado $x \in K^{\times}$, puede existir sólamente una cantidad finita de ideales primos $\mathfrak{p}$ de $\mathcal{O}_K$ para el cual $\|x\|_{\mathfrak{p}} \neq 1$ (específicamente aquellos $\mathfrak{p}$ tales que aparecen en la factorización del ideal fraccionario $x\mathcal{O}_K$).

Definición 1. Sea L/K una extensión de campos. Diremos que un lugar finito de K *ramifica* en L si su ideal primo correspondiente ramifica en L. En el caso de lugares infinitos, diremos que *ramifican* si su encaje correspondiente es real pero posee una extensión en L que es (estrictamente) compleja. Diremos que L/K *no ramifica* si no ramifica en ningún lugar (sea finito o infinito).

Fecha: 04 de abril de 2024.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{3})$ y $L = \mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{3})$. Note que K posee dos encajes reales:

$$\sigma_1 : a + b\sqrt{3} \mapsto a + b\sqrt{3} \quad \text{y} \quad \sigma_2 : a + b\sqrt{3} \mapsto a - b\sqrt{3}.$$

$$\begin{aligned} &\sigma_{1,1} : \sqrt{3} \mapsto \sqrt{3}, i \mapsto i \quad \text{y} \quad \sigma_{1,2} : \sqrt{3} \mapsto \sqrt{3}, i \mapsto -i && \text{extienden a} \quad \sigma_1. \\ &\sigma_{2,1} : \sqrt{3} \mapsto -\sqrt{3}, i \mapsto i \quad \text{y} \quad \sigma_{2,2} : \sqrt{3} \mapsto -\sqrt{3}, i \mapsto -i && \text{extienden a} \quad \sigma_2. \end{aligned}$$

Los lugares reales de K son v_{σ_1} y v_{σ_2}, (K no tiene lugares complejos). Hay un lugar de L sobre v_{σ_1}, es decir, el lugar complejo $v_{\sigma_{1,1}} = v_{\sigma_{1,2}}$, y un lugar de L sobre v_{σ_2}, es decir, el lugar complejo $v_{\sigma_{2,1}} = v_{\sigma_{2,2}}$. Además, ambos ramifican.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-5})$ y L alguna extensión de K. Notemos que K posee dos encajes complejos:

$$\sigma_1 : a + b\sqrt{-5} \mapsto a + b\sqrt{-5} \quad \text{y} \quad \sigma_2 : a + b\sqrt{-5} \mapsto a - b\sqrt{-5}.$$

Las valuaciones que se corresponden a estos dos encajes son equivalentes, por tanto, K tiene un lugar infinito, complejo, y que no ramifica.

Si $L = K(\sqrt{-1}, \sqrt{-5})$, tenemos que L/K no es una extensión trivial, pues $\sqrt{-1} \notin K$. El discriminante de K es $D_{K/\mathbb{Q}} = (2)^2(5)$, por lo cual (2) y (5) son primos que ramifican (ver Apéndice A). Además, notemos que (2) ramifica en $\mathbb{Q}(\sqrt{-1})$. Por tanto, estudiaremos sólo la ramificación de (2):

Tenemos $(2)\mathcal{O}_K = (2, 1+\sqrt{-5})^2$, y denotaremos $\mathfrak{p}$ como el ideal no principal $(2, 1+\sqrt{-5})$. Queremos ver si $\mathfrak{p}$ ramifica en L, considere el polinomio $f_\alpha(x) = x^2 - x - 1$, y note que f_α es irreducible en $\mathcal{O}_K[x]$. Por tanto, podemos deducir que ningún lugar de K ramifica en L, es decir, L/K es una extensión no ramificada.

2. Campo de clase de Hilbert

Para esta sección consideraremos que una extensión L/K es *abeliana* si la extensión es de Galois y su grupo $\mathrm{Gal}(L/K)$ es abeliano.

Teorema 2. *Dado un cuerpo de números K, existe una extensión de Galois finita L de K tal que:*

(i) L es una extensión Abeliana no ramificada de K.

(ii) Cualquier extensión Abeliana no ramificada de K radica en L.

A la extensión L le llamaremos campo de clase de Hilbert.

Ejemplo. El campo de clase de Hilbert de $\mathbb{Q}$ es el mismo $\mathbb{Q}$, pues toda extensión no trivial de $\mathbb{Q}$ es ramificada (Teorema de Minkowski, ver Neukirch [4, p. 207]).

Ejemplo. Las extensiones

$$\begin{array}{cccc} \mathbb{Q}(\sqrt{6},\sqrt{-2}) & \mathbb{Q}(\sqrt{-23},\alpha) & \mathbb{Q}(\sqrt{-31},\beta) & \mathbb{Q}(\sqrt{-14},\sqrt{2\sqrt{2}-1}) \\ \Big| 2 & \Big| 3 & \Big| 3 & \Big| 3 \\ \mathbb{Q}(\sqrt{6}) & \mathbb{Q}(\sqrt{-23}) & \mathbb{Q}(\sqrt{-31}) & \mathbb{Q}(\sqrt{-14}) \end{array}$$

son ejemplos de clases de campo de Hilbert sobre sus campos base, con $\alpha^3 - \alpha - 1 = 0$ y $\beta^3 + \beta + 1 = 0$. Cada una de éstas extensiones tienen grado igual al número de clase del campo base y el grupo de Galois de la extensión es isomorfa al grupo de clase de ideales del campo base.

Este teorema fue una conjetura dada por Hilbert en el año 1898 en el artículo *Ueber die Theorie des relativquadratischen Zahlkörpers*, éste pudo ser demostrado en 1907 por Furtwängler, estudiante de Hilbert.

3. Símbolo de Artin

Lema 3. *Sea $K \subset L$ una extensión de Galois, y sea $\mathfrak{p}$ un primo de $\mathcal{O}_K$ el cual no se ramifica en L. Si $\mathfrak{P}$ es un primo de $\mathcal{O}_L$ conteniendo a $\mathfrak{p}$, entonces existe un único elemento $\sigma \in \mathrm{Gal}(L/K)$ tal que para cada $\alpha \in \mathcal{O}_L$,*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \mod \mathfrak{P},$$

donde $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ es la norma de $\mathfrak{p}$.

Demostración. Como $\mathfrak{p}$ no ramifica, entonces $|I_{\mathfrak{P}}| = e_{\mathfrak{P}|\mathfrak{p}} = 1$, por tanto el grupo de inercia es trivial, y tenemos el siguiente isomorfismo

$$D_{\mathfrak{P}} \cong \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) \tag{1}$$

Denotaremos $\tilde{G}$ a este grupo de Galois. Notemos que podemos calcular $\tilde{G}$, pues, como $\mathcal{O}_K/\mathfrak{p}$ tiene $N_{\mathfrak{p}}$ elementos entonces $\tilde{G}$ es cíclico con el generador canónico dado por el automorfismo de Frobenius $x \mapsto x^{N_{\mathfrak{p}}}$. Luego, existe un único $\sigma \in D_{\mathfrak{P}}$ tal que cumple la condición del enunciado. Éste es único pues si consideramos cualquier otro σ que cumpla la condición del enunciado, podemos deducir que $\sigma \in D_{\mathfrak{P}}$. □

A éste único elemento lo denotaremos como $(L/K, \mathfrak{P})$.

Proposición 4. *Sea L/K una extensión de Galois, y sea $\mathfrak{p}$ un primo que no ramifica en K. Dado un primo $\mathfrak{P}$ de L tal que $\mathfrak{P} \mid \mathfrak{p}$.*

(i) Sea $\tau \in \mathrm{Gal}(L/K)$. Luego,

$$\left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \tau \left(\frac{L/K}{\mathfrak{P}}\right) \tau^{-1}.$$

(ii) *El orden de* $(L/K, \mathfrak{P})$ *es el grado de inercia* $f_{\mathfrak{P}|\mathfrak{p}}$.

(iii) *El ideal primo* $\mathfrak{p}$ *escinde completamente en* L *si y solo si* $(L/K, \mathfrak{P}) = 1$.

Demostración. Denotaremos σ como el símbolo de Artin de L/K y $q := N_{\mathfrak{p}}$. Luego, para algún $a \in \mathfrak{p}$, tenemos

$$\begin{aligned}\tau\sigma\tau^{-1}(\alpha) &= \tau((\tau^{-1}\alpha)^q) + a \\ &= \tau(\tau^{-1}\alpha)^q + \tau a \\ &\equiv \alpha^q \mod \tau\mathfrak{P}.\end{aligned}$$

Obteniendo así la parte (i). Para la parte (ii) basta considerar el isomorfismo (1) dado en la demostración anterior, y notar que $f = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$, por tanto, como el símbolo de Artin es generador, tenemos lo deseado. Para la última parte (iii), recordemos que $\mathfrak{p}$ escinde completamente en L si y sólo si $e = f = 1$, como ya asumimos que $e = 1$, por parte (ii), tenemos lo deseado. □

A. Discriminante y ramificación

Sea L/K una extensión de campos separable finita de grado n y sean $x_1, \ldots, x_n \in L$ una K-base. Sea L' la clausura normal de L sobre K y sean $\sigma_1, \ldots, \sigma_n : L \to L'$ monomorfismos de K-álgebras. Se define el discriminante como:

$$\mathrm{Disc}_{L/K}(x_1, \ldots, x_n) := \det[\sigma_i(x_j)]_{ij}^2$$

Proposición 5. *Sea* $K/\mathbb{Q}$ *extensión finita de campos y sea* $B := \mathcal{O}_K$. *Entonces todo* B*-submódulo finitamente generado* M *no nulo de* K *es un* $\mathbb{Z}$*-módulo libre de rango* $[K : \mathbb{Q}]$. *En particular,* B *admite una base entera sobre* $\mathbb{Z}$.

El discriminante $\mathrm{Disc}_{K/\mathbb{Q}}(x_1, \ldots, x_n)$ es independiente a la elección de una $\mathbb{Z}$-base. Así que, si consideramos una base entera $y_1, \ldots, y_n$ de $\mathcal{O}_K$ obtenemos el *discriminante del campo de números algebraico* K,

$$D_{K/\mathbb{Q}} := \mathrm{Disc}_{K/\mathbb{Q}}(y_1, \ldots, y_n).$$

Presentaremos un ejemplo destacable:

Ejemplo. Considere el campo de números cuadrático $K = \mathbb{Q}(\sqrt{d})$ donde $d \not\equiv 0, 1$ es un entero libre de cuadrados. Luego,

$$D_{K/\mathbb{Q}} = \begin{cases} d, & \text{si } d \equiv 1 \mod 4, \\ 4d & \text{si } d \not\equiv 1 \mod 4. \end{cases}$$

Para profundizar más, véase Neukirch [4, págs. 11-15].

Teorema 6 (Dedekind). *Sea K un campo de números y sea p un primo racional. Tenemos que $p \mid D_{K/\mathbb{Q}}$ si y solo si existe un primo $\mathfrak{p}$ de $\mathcal{O}_K$ sobre p con $e(\mathfrak{p}) > 1$, i.e. si ramifica en K.*

Corolario 7. *Los primos que ramifican son finitos.*

Ejemplo. Sea $K = \mathbb{Q}(i)$ tenemos que su anillo de enteros es $\mathcal{O}_K = \mathbb{Z}[i]$, anteriormente vimos que $2\mathcal{O}_K = \mathfrak{p}^2$ con $\mathfrak{p} = (1+i)$. Así que $p = 2$ ramifica en K. Calcularemos el discriminante respecto a la base entera $\{1, i\}$ de $\mathcal{O}_K$, y los automorfismos en $\mathrm{Gal}(K/\mathbb{Q})$: σ_1 la identidad y σ_2 la conjugación, luego

$$D_{K/\mathbb{Q}} = \det[\sigma_i(x_j)]_{ij} = \det \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}^2 = (-2i)^2 = -4.$$

Por tanto, el único primo que ramifica en $K = \mathbb{Q}(i)$ es 2.

Referencias

1. Childress, N. *Class Field Theory* (Springer, New York, 2010).
2. Conrad, K. *History of Class Field Theory* https://kconrad.math.uconn.edu/blurbs/.
3. Janusz, G. *Algebraic number theory* 2.ª ed. (Academic Press, 1973).
4. Neukirch, J. *Algebraic number theory* (Springer-Verlag, 1999).

Correo electrónico: rseplveda@uc.cl