EL CUERPO DE CLASES DE HILBERT Y EL SÍMBOLO DE ARTIN PARTE II

RODRIGO GALAZ ALVARADO

1. Preliminares

Sea K un cuerpo de números y O_K su anillo de enteros. Recordemos algunos resultados vistos en el seminario pasado:

Teorema 1.1. Existe una extensión Galois finita L de K tal que:

i) L es una extensión abeliana no ramificada de K.
ii) Toda extensión abeliana no ramificada de K está en L.

Esta extensión L es el *cuerpo de clases de Hilbert* de K. Es la máxima extensión abeliana no ramificada de K y es única.

Lema 1.1. Sea L/K una extensión Galois y sea $\mathfrak{p}$ un primo no ramificado de O_K. Si $\mathfrak{P}$ es un primo de O_L que contiene a $\mathfrak{p}$, entonces existe un único elemento $\sigma \in \mathrm{Gal}(L/K)$ tal que para todo $\alpha \in O_L$

$$\sigma(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \text{ mód } \mathfrak{P}$$

Donde $\mathrm{N}(\mathfrak{p}) = |O_K/\mathfrak{p}|$ es la norma de $\mathfrak{p}$.

Este único elemento σ del lema anterior es el símbolo de Artin y se denota por $((L/K)/\mathfrak{P})$. El símbolo de Artin satisface las siguientes propiedades:

Corolario 1.1. Sea L/K una extensión Galois y $\mathfrak{p}$ un primo no ramificado de K. Dado un primo $\mathfrak{P}$ de L conteniendo a $\mathfrak{p}$, tenemos que:

i) Si $\sigma \in \mathrm{Gal}(L/K)$, entonces
$$\left(\frac{L/K}{\sigma(\mathfrak{P})}\right) = \sigma \left(\frac{L/K}{\mathfrak{P}}\right) \sigma^{-1}$$
ii) El orden de $((L/K)/\mathfrak{P})$ es el grado de inercia f.
iii) $\mathfrak{p}$ escinde completamente en L si y solo si $((L/K)/\mathfrak{P}) = 1$.

2. El símbolo de Artin y reciprocidad

Notemos que cuando L/K es una extensión abeliana, el símbolo de Artin $((L/K)/\mathfrak{P})$ depende solo del primo $\mathfrak{p} = \mathfrak{P} \cap O_K$. En efecto, si $\mathfrak{P}'$ es otro primo sobre $\mathfrak{p}$, entonces, como la acción del grupo de Galois es transitiva, existe un $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Luego, se tiene que

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

donde la ultima igualdad es porque $\mathrm{Gal}(L/K)$ es abeliano. Por lo tanto, para una extensión abeliana L/K, el símbolo de Artin se puede escribir como $((L/K)/\mathfrak{p})$.

Veamos como se relaciona el símbolo de Artin con los teoremas de reciprocidad.

Ejemplo. Sea $K = \mathbb{Q}(\sqrt{-3})$ y $L = K(\sqrt[3]{2})$. Se puede verificar que $O_K = \mathbb{Z}[\omega]$, donde $\omega = \frac{-1+\sqrt{-3}}{2}$, y este contiene las raíces cúbicas de la unidad. Es un dominio de ideales principales (de hecho es un dominio euclidiano [Cox89, Proposition 4.3]) y, por lo tanto, cada ideal primo se puede escribir como $\pi\mathbb{Z}[\omega]$, con π un primo en $\mathbb{Z}[\omega]$.

Proposición 2.1. Si π no divide a 6, entonces π es no ramificado en L.

Demostración. Por [Cox89, Proposition 5.11] si el polinomio minimal de $\sqrt[3]{2}$ sobre K es separable módulo π, entonces π es no ramificado. Por el test de la derivada formal, $x^3 - 2 \bmod \pi$ es separable si y solo si es coprimo con $3x^2 \bmod \pi$. Como π no divide a 3, $3x^2 \bmod \pi$ no es congruente a 0, además, 0 no es raíz de $x^3 - 2 \bmod \pi$ porque π no divide a 2. De esta manera, son coprimos. $\square$

Por otro lado, como $\mathrm{Gal}(L/K) \cong \mathbb{Z}/3\mathbb{Z}$ es abeliano, $((L/K)/\pi)$ está definido. Nos gustaría determinar que automorfismo es $((L/K)/\pi)$. Para esto basta evaluar en $\sqrt[3]{2}$ (porque un automorfismo está completamente determinado por como actúa en $\sqrt[3]{2}$). Necesitamos la siguiente definición

Definición 2.1. Sea π un primo en $\mathbb{Z}[\omega]$ y $a \in \mathbb{Z}[\omega]$ tal que $\pi \nmid 3a$. El símbolo cúbico de Legendre $(a/\pi)_3$ es la única raíz cúbica de la unidad tal que

$$a^{(\mathrm{N}(\pi)-1)/3} \equiv \left(\frac{a}{\pi}\right)_3 \bmod \pi$$

Está bien definido porque $x^3 - 1 \bmod \pi$ es separable y, por lo tanto, las raíces de la unidad $1, \omega$ y ω^2 son distintas módulo π. Además, $a^{(\mathrm{N}(\pi)-1)/3}$ es congruente a una raíz de la unidad módulo π porque

$$(a^{(\mathrm{N}(\pi)-1)/3})^3 \equiv a^{\mathrm{N}(\pi)-1} \equiv 1 \bmod \pi$$

donde la última igualdad es porque $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$ es un grupo finito de orden $\mathrm{N}(\pi)-1$. Finalmente, $3 \mid \mathrm{N}(\pi) - 1$ porque el orden de ω es 3.

Proposición 2.2.

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) = \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2}$$

Demostración. Sea $\mathfrak{P}$ un primo de O_L que contiene a π. Por la propiedad del símbolo de Artin

$$\begin{aligned}\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) &\equiv \sqrt[3]{2}^{\mathrm{N}(\pi)} \bmod \mathfrak{P} \\ &\equiv 2^{(\mathrm{N}(\pi)-1)/3}\sqrt[3]{2} \bmod \mathfrak{P}\end{aligned}$$

Por definición del símbolo cúbico

$$2^{(\mathrm{N}(\pi)-1)/3} \equiv \left(\frac{2}{\pi}\right)_3 \bmod \pi$$

Luego, como $\pi \in \mathfrak{P}$

$$\left(\frac{L/K}{\pi}\right)(\sqrt[3]{2}) \equiv \left(\frac{2}{\pi}\right)_3 \sqrt[3]{2} \bmod \mathfrak{P}$$

Notemos que $((L/K)/\pi)(\sqrt[3]{2}) = \omega^k\sqrt[3]{2}$ (permuta las raíces de $x^3 - 2$), reescribiendo esto

$$\left(\omega^k - \left(\frac{2}{\pi}\right)_3\right)\sqrt[3]{2} \equiv 0 \bmod \mathfrak{P}$$

Como $\sqrt[3]{2} \notin \mathfrak{P}$, entonces

$$\omega^k \equiv \left(\frac{2}{\pi}\right)_3 \bmod \mathfrak{P}$$

Por unicidad de la raíz de la unidad que cumple esto, se tiene lo pedido.

□

De esta manera, vemos que el símbolo de Artin generaliza el símbolo de Legendre. Más generalmente, si K es un cuerpo de números que contiene una raíz n-ésima primitiva de la unidad ζ, $a \in O_K$ y $\mathfrak{p}$ es un ideal primo de O_K tal que $na \notin \mathfrak{p}$, entonces

Definición 2.2. El n-ésimo símbolo de Legendre $(a/\mathfrak{p})_n$ es la única raíz n-ésima de la unidad tal que

$$a^{(\mathrm{N}(\mathfrak{p})-1)/n} \equiv \left(\frac{a}{\mathfrak{p}}\right)_n \text{ mód } \mathfrak{p}$$

Igual que para el símbolo cúbico, está bien definido porque $x^n - 1$ mód $\mathfrak{p}$ es separable y, por lo tanto, las raíces de la unidad $1, \zeta, \dots, \zeta^{n-1}$ son distintas módulo π. Además, $a^{(\mathrm{N}(\mathfrak{p})-1)/n}$ es congruente a una raíz de la unidad módulo $\mathfrak{p}$ y $n \mid \mathrm{N}(\mathfrak{p}) - 1$ porque el orden de ζ en $(O_K/\mathfrak{p})^*$ es n. El símbolo de Legendre cumple lo esperado, es decir:

Proposición 2.3. $\left(\frac{a}{\mathfrak{p}}\right)_n = 1$ si y solo si a es una potencia n-ésima módulo $\mathfrak{p}$.

Demostración. Si a es una potencia n-ésima módulo $\mathfrak{p}$, entonces existe $x \in O_K$ tal que

$$a^{(\mathrm{N}(\mathfrak{p})-1)/n} \equiv x^{n(\mathrm{N}(\mathfrak{p})-1)/n} \equiv x^{\mathrm{N}(\mathfrak{p})-1} \equiv 1 \text{ mód } \mathfrak{p}$$

Por otro lado, si $\left(\frac{a}{\mathfrak{p}}\right)_n = 1$, como $(O_K/\mathfrak{p})^*$ es cíclico, existe un generador $x \in (O_K/\mathfrak{p})^*$. Luego

$$a^{(\mathrm{N}(\mathfrak{p})-1)/n} \equiv x^{k(\mathrm{N}(\mathfrak{p})-1)/n} \equiv 1 \text{ mód } \mathfrak{p}$$

Como el orden de x es $\mathrm{N}(\mathfrak{p}) - 1$, esto ocurre si y solo si $k \equiv 0$ mód n, es decir, a es una potencia n-ésima módulo $\mathfrak{p}$. □

Si $L = K(\sqrt[n]{a})$, la extensión L/K es abeliana y el ideal $\mathfrak{p}$ es no ramificado porque $x^n - a$ mód $\mathfrak{p}$ es separable. De esta manera, el símbolo de Artin $((L/K)/\mathfrak{p})$ está definido y se cumple que

Proposición 2.4.

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}$$

Demostración. Sea $\mathfrak{P}$ un primo de O_L que contiene a $\mathfrak{p}$. Por la propiedad del símbolo de Artin

$$\begin{aligned}\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{a}) &\equiv \sqrt[n]{a}^{\mathrm{N}(\mathfrak{p})} \text{ mód } \mathfrak{P} \\ &\equiv a^{(\mathrm{N}(\mathfrak{p})-1)/n} \sqrt[n]{a} \text{ mód } \mathfrak{P} \\ &\equiv \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a} \text{ mód } \mathfrak{P}\end{aligned}$$

El mismo argumento usado en el ejemplo nos permite concluir la igualdad. □

3. Teorema de reciprocidad de Artin

Cuando L/K es una extensión abeliana no ramificada (en sus lugares finitos e infinitos), se tiene que $((L/K)/\mathfrak{p})$ está definido para todos los primos $\mathfrak{p}$ de O_K. De esta forma, podemos extender el símbolo de Artin a I_K, el grupo de los ideales fraccionarios de O_K. Sea $\mathfrak{a} \in I_K$, por la factorización única en ideales primos

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{r_i}, \ r_i \in \mathbb{Z}$$

luego, definimos el símbolo de Artin como

$$\left(\frac{L/K}{\mathfrak{a}}\right) := \prod_{i=1}^{r} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{r_i}$$

De esta manera, el símbolo de Artin define un homomorfismo llamado el *morfismo de Artin*

$$\left(\frac{L/K}{\cdot}\right) : I_K \longrightarrow \mathrm{Gal}(L/K)$$

En general, si L/K es ramificada, entonces el morfismo de Artin no está definido en todo I_K. El teorema de reciprocidad de Artin relaciona el cuerpo de clases de Hilbert con el grupo de clases $\mathrm{Cl}(O_K)$.

Teorema 3.1 (Teorema de reciprocidad de Artin)**.** Si L es el cuerpo de clases de Hilbert de K, entonces el morfismo de Artin es sobreyectivo y su kernel es el subgrupo P_K de ideales fraccionarios principales. Así, el morfismo de Artin induce un isomorfismo

$$\mathrm{Cl}(O_K) = I_K/P_K \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

Ejemplo. Consideremos $K = \mathbb{Q}(\sqrt{-5})$, $L = K(\sqrt{-1})$ y H el cuerpo de clases de Hilbert de K. En el seminario anterior vimos que L/K es no ramificada y, por lo tanto, $K \subseteq L \subseteq H$. Por otro lado, es posible demostrar que $h_K = |\mathrm{Cl}(O_K)| = 2$ (ver [Mil20, Example 4.6]) y por el teorema anterior tenemos que $[H : K] = 2$. De esta manera, $L = H$.

Usando teoría de Galois obtenemos el siguiente resultado.

Corolario 3.1. Dado un cuerpo de números K, hay una biyección entre las extensiones abelianas no ramificadas M de K y los subgrupos H del grupo de clases $\mathrm{Cl}(O_K)$. Además, si la extensión M/K corresponde al subgrupo $H \subseteq \mathrm{Cl}(O_K)$, entonces el morfismo de Artin induce un isomorfismo

$$\mathrm{Cl}(O_K)/H \xrightarrow{\sim} \mathrm{Gal}(M/K)$$

Idea de la demostración. Si $K \subseteq M \subseteq L$ es una torre de extensiones, es posible demostrar que L es una extensión no ramificada sobre K si y solo si L es no ramificada sobre M y M es no ramificada sobre K. Por otro lado, si L/K es abeliana y no ramificada, entonces M/K también lo será. Además, el morfismo de restricción

$$\begin{aligned} r : \mathrm{Gal}(L/K) &\to \mathrm{Gal}(M/K) \\ \sigma &\mapsto \sigma_{|_M} \end{aligned}$$

satisface que

$$\left(\frac{M/K}{\cdot}\right) = r \circ \left(\frac{L/K}{\cdot}\right)$$

Luego, si L es el cuerpo de clases de Hilbert de K, el isomorfismo del teorema 3.1 induce una biyección

$$\{\text{Subgrupos de } \mathrm{Cl}(O_K)\} \longleftrightarrow \{\text{Subgrupos de } \mathrm{Gal}(L/K)\}$$

Como L/K es abeliana y no ramificada, todo subgrupo de $\mathrm{Gal}(L/K)$ es normal y corresponde, por el teorema fundamental de la teoría de Galois, a una extensión normal que es abeliana y no ramificada. Por lo tanto, hay una biyección

$$\{\text{Subgrupos de } \mathrm{Gal}(L/K)\} \longleftrightarrow \{M/K : \text{ es Galois, abeliana y no ramificada}\}$$

Lo que nos da la primera parte. Ahora si la extensión M/K corresponde al subgrupo $H \subseteq \mathrm{Cl}(O_K)$, el morfismo de restricción nos entrega

$$\mathrm{Cl}(O_K) \xrightarrow{\sim} \mathrm{Gal}(L/K) \xrightarrow{r} \mathrm{Gal}(M/K)$$

Por teoría de Galois, r es sobreyectiva y tiene kernel $\mathrm{Gal}(L/M)$. Por el teorema fundamental, este grupo corresponde a la extensión M/K y esta última corresponde al subgrupo H. Finalmente, el morfismo de Artin induce el isomorfismo

$$\left(\frac{M/K}{\cdot}\right) : \mathrm{Cl}(O_K)/H \xrightarrow{\sim} \mathrm{Gal}(M/K)$$

□

Este corolario ilustra uno de los temas principales de la teoría de cuerpos de clases. Ciertas extensiones de K están clasificadas por información intrínseca a K.

Ejemplo. Notemos que si O_K es un dominio de factorización única, entonces es un dominio de ideales principales, por lo tanto, $\mathrm{Cl}(O_K) \cong (1)$. Luego, por el teorema 3.1, $|\mathrm{Gal}(L/K)| = [L : K] = 1$, es decir, K es su propio cuerpo de clases de Hilbert y, además, no tiene extensiones abelianas no ramificadas propias. En particular, si $K = \mathbb{Q}$, entonces $O_K = \mathbb{Z}$ y concluimos que $\mathbb{Q}$ no tiene extensiones abelianas no ramificadas.

Corolario 3.2. Sea L el cuerpo de clases de Hilbert de un cuerpo de números K, y sea $\mathfrak{p}$ un ideal primo de K. Entonces

$$\mathfrak{p} \text{ escinde completamente en } L \iff \mathfrak{p} \text{ es un ideal principal}$$

Demostración. El corolario 1.1 implica que el primo $\mathfrak{p}$ escinde completamente en L si y solo si $((L/K)/\mathfrak{p}) = 1$. Como el morfismo de Artin induce un isomorfismo, vemos que $((L/K)/\mathfrak{p}) = 1$ si y solo si $\mathfrak{p}$ determina la clase trivial de $\mathrm{Cl}(O_K)$, es decir, $\mathfrak{p}$ es un ideal principal. □

Referencias

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[Mil20] James S. Milne. Algebraic number theory (v3.08), 2020. Available at www.jmilne.org/math/.