SEMINARIO: TEORÍA DE MULTIPLICACIÓN COMPLEJA, PANORAMA

RICARDO MENARES

1. Kronecker-Weber

Una extensión de cuerpos L/K se dice *abeliana* si es Galois y $Gal(L/K)$ es un grupo abeliano.

Ejemplo: $m \geq 1$ entero, $\zeta_m := e^{2\pi i/m}$, entonces $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$, luego $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ es una extensión abeliana.

Teorema 1.1. *(Kronecker-Weber) Sea $L/\mathbb{Q}$ una extensión finita y abeliana. Entonces $L \subseteq \mathbb{Q}(\zeta_m)$ para algún $m \geq 1$.*

Este Teorema muestra que la máxima extensión abeliana de $\mathbb{Q}$, usualmente denotada $\mathbb{Q}^{ab}$, puede obtenerse adjuntando a $\mathbb{Q}$ los valores que asume la función trascendente $f(x) = e^{2\pi ix}$ al hacer variar $x \in \mathbb{Q}$.

El problema 12 de Hilbert pide generalizar esta construcción para un cuerpo de números arbitrario. Groso modo, dado un cuerpo de números K, se pide encontrar funciones trascendentes $f_1, f_2, \ldots, f_m$ tal que las extensiones abelianas de K puedan construirse adjuntado a K elementos de la forma $f_i(x)$ donde x varía en un conjunto especial de números algebraicos e $i \in \{1, 2, \ldots, m\}$.

El caso general del problema 12 está ampliamente abierto. La Teoría de Multiplicación Compleja, que estudiaremos en este seminario, concierne la solución[1] de este problema cuando K es un cuerpo cuadrático imaginario (i.e. $[K : \mathbb{Q}] = 2$ y $K \nsubseteq \mathbb{R}$).

2. Ramificación y Cuerpo de clases de Hilbert

Sea L/K una extensión de cuerpo de números. Sea $\mathfrak{p} \subseteq O_K$ un ideal primo. El ideal $\mathfrak{p}O_L \subseteq O_L$ se escribe de manera única como producto de ideales primos de O_L, digamos $\mathfrak{p}O_L = \prod_{i=1}^m \mathfrak{P}_i^{e_i}$. Se dice que $\mathfrak{p}$ se *ramifica* en L si $e_i > 1$ para algún $i = 1, 2, \ldots, m$. La extensión L/K se dice *ramificada* si existe algún ideal primo en O_K que ramifica en L. En caso contrario, decimos que L/K es una extensión *no ramificada*.[2]

Una manera de abordar el problema 12 es primero intentar generalizar de manera apropiada el Teorema de Kronecker-Weber para K. No es claro qué clase de extensiones abelianas finitas de K puede jugar el rol de los cuerpos ciclotómicos cuando $K \neq \mathbb{Q}$. Una idea natural es considerar primero la máxima extensión abeliana que no ramificada. Tal extensión H/K es finita[3] y se conoce como el *cuerpo de clases de Hilbert*. Su nombre viene del hecho que el grupo de clases de K es isomorfo a $Gal(H/K)$.

Cuando K es un cuerpo cuadrático imaginario, es posible construir el cuerpo de clases de Hilbert usando funciones trascendentes.

3. Ordenes

Recordemos que $\alpha \in \mathbb{C}$ es un *entero algebraico* si existe un polinomio mónico con coeficientes enteros $f(x) \in \mathbb{Z}[x]$ tal que $f(\alpha) = 0$. El conjunto $\overline{\mathbb{Z}}$ de todos los enteros algebraicos tiene estructura de anillo.

Sea K un cuerpo de números. Asumiremos $K \subseteq \mathbb{C}$ en todo lo que sigue. El anillo de enteros de K se define como

$$O_K := K \cap \overline{\mathbb{Z}}.$$

Un *orden* $O \subseteq O_K$ es un subanillo de O_K tal que $Frac(O) = K$. En particular, O_K es un orden y es maximal. Cuando K es un cuerpo cuadrático imaginario, los órdenes $O \subseteq O_K$ son todos de la forma

$$O = \mathbb{Z} + fO_K,$$

donde f es un entero.

[1] que Kronecker describe en una carta a Dedekind como su "sueño de juventud"

[2] El Teorema de Hermite-Minkowski asegura que toda extensión finita $K/\mathbb{Q}$ con $K \neq \mathbb{Q}$ es ramificada

[3] Al remover la condición de no ramificación, se vuelve posible construir extensiones abelianas de grado arbitrariamente grande

4. Reticulados complejos

Un reticulado $\Lambda \subseteq \mathbb{C}$ es un subgrupo aditivo discreto de rango 2. Todo reticulado tiene la forma $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, donde ω_1, ω_2 son números complejos linealmente independientes sobre $\mathbb{R}$. El conjunto

$$End(\Lambda) = \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$$

es un sub anillo de $\mathbb{C}$. En particular, siempre se tiene $\mathbb{Z} \subseteq End(\Lambda)$. Más aún, es posible demostrar que o bien $End(\Lambda) = \mathbb{Z}$ o bien $End(\Lambda)$ es isomorfo a un orden dentro de un cuerpo cuadrático imaginario. En el último caso, diremos que Λ *admite multiplicaciones complejas*. Si queremos abreviar diremos que Λ tiene CM.

Salvo homotecia, todo reticulado puede escribirse de la forma

$$\Lambda = \mathbb{Z} + \tau\mathbb{Z}, \tag{4.1}$$

donde $\tau \in \mathbb{C}$ es tal que $Im(\tau) > 0$. Se puede demostrar que Λ tiene CM si y solo si $\mathbb{Q}(\tau)/\mathbb{Q}$ es una extensión cuadrática (necesariamente imaginaria). Dado Λ, hay más de una elección posible τ que cumpla (4.1). Para clasificar el conjunto de τs posibles introducimos $\mathbb{H} = \{\tau \in \mathbb{C} : Im(\tau) > 0\}$ el semiplano superior. Este semiplano admite una acción del grupo

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : ad - bc = 1 \right\}.$$

Dada una matriz $\gamma \in SL_2(\mathbb{Z})$ con coeficientes a, b, c, d, la acción se describe por

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Entonces se verifica que $\tau_1, \tau_2 \in \mathbb{C}$ cumplen (4.1) si y solo si existe $\gamma \in SL_2(\mathbb{Z})$ tal que $\tau_1 = \gamma \cdot \tau_2$. Además, claramente $\mathbb{Q}(\tau_1) = \mathbb{Q}(\tau_2)$.

Existe una única función holomorfa $j : \mathbb{H} \to \mathbb{C}$ que es sobreyectiva, invariante bajo la acción de $SL_2(\mathbb{Z})$ y que cumple

$$\lim_{\substack{Im(\tau)\to\infty \\ Re(\tau) acotada}} e^{2\pi i\tau} j(\tau) = 1.$$

Tal función se conoce como *el invariante jota*.[4] Podemos extender esta función a reticulados de la forma $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ por

$$j(\Lambda) := j(\tau).$$

Este valor no depende de la elección de τ debido a la invarianza de j bajo $SL_2(\mathbb{Z})$.

Cuando K es un cuerpo cuadrático imaginario, el anillo de enteros O_K es un reticulado.

Teorema 4.1. *(Teorema principal de la Teoría CM) Si K es cuadrático imaginario y H/K es el cuerpo de clases de Hilbert, entonces $H = K(j(O_K))$.*

En realidad el Teorema 4.1 es un caso particular de la teoría CM. Más generalmente, al tomar un orden $O \subseteq O_K$, se tiene que el cuerpo $K(j(O))$ también tiene una interpretación en términos de la aritmética de K. Se deduce en particular que cuando $\tau \in \mathbb{H}$ es un número algebraico de grado 2, entonces $j(\tau)$ es un número algebraico. Recíprocamente, un teorema de Schneider asegura que cuando $\tau \in \mathbb{H}$ es algebraico, $j(\tau)$ es algebraico si y solo si τ es cuadrático. Los números algebraicos de grado 2 en $\mathbb{H}$ son "especiales" en el sentido del problema 12 de Hilbert.

En el seminario estudiaremos una versión más general de este teorema, que requerirá algunos elementos de la Teoría del cuerpo de clases.

5. Nexo con curvas elípticas

Una curva elíptica sobre un cuerpo K es una curva proyectiva suave E definida sobre K, de género 1, junto con un punto $P \in E(K)$. Por argumentos generales de geometría algebraica, cuando la característica de K no es 2 ni 3, tal curva siempre admite un modelo afín de la forma

$$y^2 = x^3 + ax + b, \quad a, b \in K, \tag{5.2}$$

(cuando car $K \in \{2, 3\}$ hay una ecuación similar, un poco más complicada) con P el punto al infinito. Además, la curva E posee una única estructura de grupo algebraico en que P es el elemento neutro. Como tal, posee un anillo de endomorfismos $End(E)$.

[4] La creatividad de los matemáticos suele no llegar hasta la elección de nombre

Cuando $K = \mathbb{C}$, tenemos que $E(\mathbb{C})$ es una superficie de Riemann compacta de género 1. Como tal, su cubrimiento universal es $\mathbb{C}$ y esta uniformización implica la existencia de un biholomorfismo de la forma

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda,$$

donde $\Lambda \subset \mathbb{C}$ es un reticulado. El reticulado Λ asociado a E es único salvo homotecia. Además, $End(E) \simeq End(\Lambda)$ y podemos definir $j(E) := j(\Lambda)$.

Deducimos que $End(E)$ es o bien $\mathbb{Z}$ o bien isomorfo a un orden en un cuerpo cuadrático imaginario. En el último caso diremos que E tiene CM.

Este invariante j de curvas elípticas tiene la propiedad que los coeficientes a, b en (5.2) pueden tomarse en $\mathbb{Q}(j(E))$. Del Teorema 4.1, deducimos que cuando E tiene CM por el anillo de enteros de un cuerpo cuadrático imaginario K, admite una ecuación del tipo (5.2) con los coeficientes a, b en el cuerpo de clases de Hilbert de K. Este hecho tiene innumerables aplicaciones en Teoría de Números.

6. Objetivos del seminario

Los objetivos principales del seminario son

- Entender el Teorema 4.1, así como sus variantes y complementos en el lenguaje de la Teoría del cuerpo de clases
- Entender el nexo entre la Teoría CM y las curvas elípticas

Por limitaciones de tiempo, priorizaremos el primer objetivo.

References

[Cox13] David A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

E-mail address: rmenares@mat.uc.cl