TEMat

El duodécimo problema de Hilbert para cuerpos cuadráticos imaginarios

Daniel Gil Muñoz[a]
Universitat Politècnica de Catalunya (UPC)
daniel_gilmu@hotmail.com

Resumen: En este artículo se presentan los conceptos y herramientas más básicas para presentar una demostración debida a Deuring de la resolución del caso cuadrático-imaginario del duodécimo problema de Hilbert, que consiste en calcular explícitamente la extensión abeliana maximal de un cuerpo cuadrático imaginario.

Presentamos el teorema de Kronecker-Weber para resolver el caso ciclotómico. Mediante la introducción de la teoría de cuerpos de clases, utilizamos la misma idea del caso ciclotómico para reducir el caso cuadrático-imaginario a describir explícitamente todos los cuerpos de clases radiales del cuerpo cuadrático imaginario. Introducimos la teoría de curvas elípticas con multiplicación compleja para resolver esta nueva formulación del problema y vemos un ejemplo de cálculo.

Abstract: In this article we present the main notions and basic tools to solve the imaginary-quadratic case of Hilbert's 12th problem. This problem consists in computing explicitly the maximal abelian extension of an imaginary quadratic field.

We present Kronecker-Weber's theorem to solve the cyclotomic case. Next, we introduce class field theory and we use it to adapt the idea of the cyclotomic case in order to reduce the imaginary-quadratic case to describe explicitely all Ray class fields of the imaginary quadratic field. We introduce the theory of elliptic curves with complex multiplication to solve this new formulation and we see an example of computation.

Palabras clave: cuerpo cuadrático imaginario, curva elíptica, multiplicación compleja, cuerpo de clases radiales, extensión abeliana maximal, j-invariante.

MSC2010: 11G45, 14K22.

Recibido: 18 de noviembre de 2017.
Aceptado: 3 de febrero de 2018.

Agradecimientos: El contenido de este artículo es un resumen de mi Trabajo Final de Máster para el Máster de Matemática Avanzada de la Universidad de Barcelona. Quiero agradecer a mi tutor del trabajo, Xavier Guitart Morales, por la propuesta del tema así como su dedicación e interés en la tutorización del trabajo, además de todas sus explicaciones y esfuerzo por enseñarme y hacerme comprender esta teoría.

Referencia: Gil Muñoz, Daniel. «El duodécimo problema de Hilbert para cuerpos cuadráticos imaginarios». En: *TEMat*, 2 (2018), págs. 15-30. ISSN: 2530-9633. URL: https://temat.es/articulo/2018-p15/.

[a] El autor estaba afiliado a la Universidad de Barcelona (UB) cuando realizó este trabajo.

1. Introducción

En 1900, Hilbert propuso veintitrés problemas de diferentes áreas de las matemáticas que no habían sido resueltos hasta ese momento y que influirían de manera notable en el desarrollo de las matemáticas del siglo xx. La mayoría de ellos fueron resueltos posteriormente, mientras que algunos continúan hoy sin resolver (véase el libro de Schappacher [10]). En este artículo vamos a ver uno de los problemas del segundo grupo, que es el número doce: el duodécimo problema de Hilbert, también conocido como *Jugendtraum* de Kronecker (sueño de juventud de Kronecker en alemán). Para más información histórica del problema, consúltense el libro de Vladut [13] y las notas de Breiding y Samart [1].

El enunciado del duodécimo problema de Hilbert es el siguiente:

Problema 1 (Duodécimo problema de Hilbert). Sea K un cuerpo numérico. Determinar explícitamente los elementos de un sistema de generadores de la extensión abeliana maximal K^{ab} de K. ◂

Lo primero que vamos a hacer es entender este enunciado. Para ello, vamos a dar algunas pinceladas de la teoría de Galois (si el lector la conoce, se puede saltar esta parte; si, por el contrario, desea conocerla con mayor profundidad de lo aquí mostrado, puede consultar el capítulo V del libro de Hungerford [4] o las notas de Milne [8]).

Sean K y L dos cuerpos de forma que $K \subset L$. Decimos entonces que L es una extensión de K o que L/K es una **extensión de cuerpos**. Nótese que L se puede ver como un espacio vectorial con escalares en K en el que la operación externa es el producto en L. Este espacio se llama el K-espacio vectorial L, y una base de dicho espacio se llama K-base de L. La extensión L/K es finita si el K-espacio vectorial L tiene dimensión finita.

Definición 1. Un **cuerpo numérico** es una extensión finita de $\mathbb{Q}$. ◂

Por ejemplo, el conjunto

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

es un cuerpo numérico: se puede comprobar que tiene estructura de cuerpo y claramente contiene a todos los números racionales. Además $\{1, \sqrt{2}\}$ es una base del $\mathbb{Q}$-espacio vectorial $\mathbb{Q}(\sqrt{2})$, por lo que tal espacio tiene dimensión 2.

El concepto de cuerpo numérico es fundamental en esta teoría. Presentaremos todo lo que necesitamos saber sobre ellos. Sin embargo, el lector interesado en conocer más información puede consultar el capítulo 2 del libro de Marcus [7].

En este ejemplo, la notación $\mathbb{Q}(\sqrt{2})$ significa que se trata del menor subcuerpo de $\mathbb{C}$ que contiene a $\mathbb{Q}$ y $\sqrt{2}$ para la inclusión de conjuntos. Es decir, si L es otro subcuerpo de $\mathbb{C}$ tal que $\mathbb{Q} \subset L$ y $\sqrt{2} \in L$, entonces $\mathbb{Q}(\sqrt{2}) \subset L$.

Más generalmente, si K es un subcuerpo de $\mathbb{C}$ y $x \in \mathbb{C}$, $K(x)$ denota el menor subcuerpo de $\mathbb{C}$ que contiene a K y a x. Esta notación se extiende de manera natural a un subconjunto $S \subset \mathbb{C}$: $K(S)$ es el menor subcuerpo de $\mathbb{C}$ que contiene a K y a S. El conjunto S se llama **sistema de generadores** de la extensión L/K. Partiendo de un sistema de generadores de L/K, podemos obtener una K-base de L.

Definición 2. Sea L/K una extensión de cuerpos. Se define el **grupo de Galois** de L/K como el grupo

$$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(\alpha) = \alpha \text{ para todo } \alpha \in K\}$$

con la composición de aplicaciones, donde $\mathrm{Aut}(L)$ es el grupo de automorfismos de cuerpos de L. ◂

El grupo de Galois es un objeto fundamental desde el punto de vista de la teoría de Galois. Este grupo se puede describir de una manera más fácil cuando la extensión es de Galois. La definición de extensión de Galois no la vamos a necesitar en este artículo. Todo lo que vamos a necesitar saber de estas extensiones es que nos permiten definir el concepto de extensión abeliana.

Definición 3. Una extensión de cuerpos L/K se dice **abeliana** si es de Galois y $\mathrm{Gal}(L/K)$ es abeliano. ◂

Definición 4. Sea K un subcuerpo de $\mathbb{C}$. Una extensión abeliana L de K se dice **maximal** si para toda extensión abeliana M de K tal que $L \subset M$ se tiene que $L = M$. ◂

La extensión abeliana maximal de un tal subcuerpo K siempre existe, y es única salvo isomorfismo que fije los elementos de K. Así, el duodécimo problema de Hilbert nos propone, dado un cuerpo numérico K, hallar un sistema de generadores de la extensión abeliana maximal de K. Preguntamos además por la forma explícita de tales generadores, es decir, queremos expresarlos en términos de objetos matemáticos conocidos.

Como ya hemos mencionado, el caso general del duodécimo problema de Hilbert permanece sin resolver a día de hoy. Sin embargo, está completamente resuelto para tres casos particulares de K:

1. Cuando K es el propio cuerpo $\mathbb{Q}$ de los números racionales.
2. Cuando K es un cuerpo cuadrático imaginario (es decir, de la forma $K = \mathbb{Q}(\sqrt{-n})$, con n un entero positivo).
3. Cuando K es un cuerpo de multiplicación compleja.

El tercer caso es más complicado y no lo vamos a tratar en este artículo (una demostración se puede encontrar en el artículo de Wei [14]). El objetivo fundamental es probar el segundo caso, es decir, el caso cuadrático-imaginario. Primero veremos la solución para el caso 1 (también conocido como caso ciclotómico; en la siguiente sección veremos por qué) y esto nos permitirá plasmar algunas de las ideas que utilizaremos en el caso 2. Para entender la resolución de este segundo caso, utilizaremos la teoría de cuerpos de clases y la teoría de curvas elípticas con multiplicación compleja.

2. El caso ciclotómico

En esta sección vamos a resolver el duodécimo problema de Hilbert para el primer caso de los listados anteriormente. En este caso, el problema es el siguiente:

Problema 2. Determinar explícitamente un sistema de generadores de la extensión abeliana maximal $\mathbb{Q}^{\mathrm{ab}}$ de $\mathbb{Q}$. ◂

La resolución de este problema pasa por el estudio de las extensiones ciclotómicas de $\mathbb{Q}$ (de ahí que este problema sea nombrado como el caso ciclotómico del duodécimo problema de Hilbert).

Sea $m \in \mathbb{Z}_{>0}$. El conjunto de las raíces complejas m-ésimas de la unidad (es decir, las raíces del polinomio $X^m - 1$ en $\mathbb{C}$) es

$$\{e^{\frac{2\pi i k}{m}} \mid k \in \{0, \dots, m-1\}\}.$$

Si consideramos el producto de números complejos, este conjunto tiene estructura de grupo cíclico (es decir, está generado por un solo elemento). Cualquier generador de dicho grupo es llamado **raíz m-ésima primitiva de la unidad**. Usando teoría de grupos básica (véase el libro de Hungerford [4, capítulo I, teorema 3.6]), se puede ver fácilmente que el conjunto de tales raíces es

$$\{e^{\frac{2\pi i k}{m}} \mid k \in \{0, \dots, m-1\},\ \mathrm{mcd}(k, m) = 1\},$$

donde $\mathrm{mcd}(k, m)$ denota el máximo común divisor de k y m.

Definición 5. Sea $m \in \mathbb{Z}_{>0}$. La m-ésima extensión ciclotómica de $\mathbb{Q}$ se define como

$$K = \mathbb{Q}(e^{\frac{2\pi i}{m}}).$$ ◂

Como primer apunte, una extensión ciclotómica K de $\mathbb{Q}$ es un cuerpo numérico. En efecto, es un cuerpo que, por definición, contiene a $\mathbb{Q}$, y el conjunto de las raíces m-ésimas primitivas de la unidad es una base de K como $\mathbb{Q}$-espacio vectorial (esto se puede deducir, por ejemplo, del libro de Marcus [7, teorema 3]).

Cualquier extensión ciclotómica de $\mathbb{Q}$ es de Galois (véase la proposición 5.8 de Milne [8]). Otra propiedad que tiene la extensión ciclotómica m-ésima es que se puede expresar como $K = \mathbb{Q}(\xi)$, donde ξ es *cualquier* raíz m-ésima primitiva de la unidad. Esto hace que la aplicación

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & \mathrm{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}) \\ \overline{k} & \longmapsto & \xi \mapsto \xi^k \end{array}$$

sea un isomorfismo de grupos, donde $(\mathbb{Z}/m\mathbb{Z})^*$ denota al grupo de los enteros módulos m invertibles para el producto (es decir, los de la forma $\overline{k}$ con $k \in \mathbb{Z}$ coprimo con m). Esta aplicación se llama **aplicación de Artin** de la extensión ciclotómica. Así, como el grupo $(\mathbb{Z}/m\mathbb{Z})^*$ es claramente abeliano y es isomorfo al grupo de Galois de $\mathbb{Q}(\xi)/\mathbb{Q}$, concluimos que $\mathbb{Q}(\xi)$ es una extensión abeliana de $\mathbb{Q}$.

Así, hemos probado que cualquier extensión ciclotómica de $\mathbb{Q}$ es una extensión abeliana de $\mathbb{Q}$. De hecho, se tiene un resultado mucho más potente:

Teorema 1 (teorema de Kronecker-Weber). *Cualquier extensión abeliana y finita de $\mathbb{Q}$ está contenida en una extensión ciclotómica.*

Este resultado es muy conocido en teoría de números y se puede probar usando teoría de cuerpos de clases, que introduciremos en la siguiente sección, aunque no veremos la demostración. El lector puede consultar una demostración usando este enfoque en el libro de Cox [2, teorema 8.8]. También es posible probarlo usando técnicas de teoría algebraica de números [7, capítulo 4, ejercicios 29-36].

El teorema de Kronecker-Weber nos permite resolver el duodécimo problema de Hilbert para el caso que tratamos. Para entender cómo, debemos introducir un concepto más de teoría de Galois. Dados dos subcuerpos K y F de $\mathbb{C}$, en general su unión $K \cup F$ *no* es un cuerpo. Pero no hay ningún problema en considerar el menor subcuerpo de $\mathbb{C}$ (de nuevo para la inclusión) que contiene a ambos. Este cuerpo se llama la **composición** de K y F, y se denota por $K \vee F$. De manera completamente análoga se define la composición de una cantidad arbitraria de subcuerpos de $\mathbb{C}$. Claramente, si $F \subset K$, $K \vee F = K$.

La clave en el problema que nos compete es que la composición de extensiones abelianas de un mismo cuerpo es de nuevo abeliana (pues hay un monomorfismo de grupos del grupo de Galois de la composición en el producto directo de los grupos de Galois de cada extensión). Por tanto, la extensión abeliana maximal de $\mathbb{Q}$ se puede escribir como la composición de *todas* las extensiones abelianas de $\mathbb{Q}$. En particular, esto prueba que la extensión abeliana maximal de $\mathbb{Q}$ existe y es única salvo $\mathbb{Q}$-isomorfismo, y el mismo razonamiento sirve si sustituimos $\mathbb{Q}$ por cualquier subcuerpo K de $\mathbb{C}$.

Ahora bien, la composición de cuerpos, tal y como la hemos definido, es claramente conmutativa y asociativa. Usando el teorema de Kronecker-Weber y que las extensiones ciclotómicas son abelianas, podemos reordenar los cuerpos de la expresión de $\mathbb{Q}^{\text{ab}}$ de forma que agrupemos los que están contenidos en la misma extensión ciclotómica. Así, $\mathbb{Q}^{\text{ab}}$ es de hecho la composición de todas las extensiones ciclotómicas de $\mathbb{Q}$, es decir,

$$\mathbb{Q}^{\text{ab}} = \vee_{m \in \mathbb{Z}_{>0}} \mathbb{Q}(\xi_m),$$

donde ξ_m es una raíz m-ésima de la unidad.

Queda, pues, determinar el menor cuerpo que contiene a todas las extensiones ciclotómicas de $\mathbb{Q}$. Lo único que tenemos que hacer es reunir los generadores de todas ellas. Es decir,

$$\mathbb{Q}^{\text{ab}} = \mathbb{Q}(\mu),$$

donde μ es el conjunto de *todas* las raíces de la unidad. Este conjunto es, por tanto, un sistema de generadores de $\mathbb{Q}^{\text{ab}}/\mathbb{Q}$. Esto resuelve el primer caso.

3. Teoría de cuerpos de clases

Para resolver el caso cuadrático-imaginario del duodécimo problema de Hilbert, la teoría de cuerpos de clases será una herramienta crucial. En esta sección veremos la formulación clásica de esta teoría, que se encarga del estudio del grupo de Galois de las extensiones abelianas de un cuerpo numérico K fijado usando la *aritmética de K* (más adelante veremos qué significa esto último). Como los contenidos expuestos a continuación son de un elevado nivel técnico, no los vamos a presentar minuciosamente en este artículo, sino que daremos algunas pinceladas para facilitar su comprensión. Para conocer los detalles se recomienda al lector consultar el libro de Cox [2, capítulo 2, sección 8].

Antes de empezar, necesitamos dos conceptos básicos en teoría algebraica de números.

Definición 6. Un **entero algebraico** es cualquier raíz de un polinomio mónico con coeficientes enteros. ◂

Definición 7. Sea K un cuerpo numérico. Se define el **anillo numérico** $\mathcal{O}_K$ asociado a K como el conjunto de los enteros algebraicos de dicho cuerpo numérico. ◂

El anillo numérico de un cuerpo numérico K, como su propio nombre indica, tiene estructura de anillo. Más aún, se trata de un dominio de integridad (un anillo conmutativo y unitario sin divisores de cero), por lo que podemos considerar su cuerpo de fracciones. Resulta que K es isomorfo al cuerpo de fracciones de su anillo numérico $\mathcal{O}_K$, por lo que no puede haber dos cuerpos numéricos que tengan el mismo anillo numérico asociado.

También necesitaremos el concepto de ideal fraccionario del anillo de enteros.

Definición 8. Sea K un cuerpo numérico. Se define un **ideal fraccionario** de $\mathcal{O}_K$ como un subconjunto $\mathfrak{a} \subset K$ de la forma

$$\mathfrak{a} = \alpha\, I,$$

donde $\alpha \in K$ e I es un ideal de $\mathcal{O}_K$. ◂

El nombre de ideal fraccionario se debe a que K es isomorfo al cuerpo de fracciones de $\mathcal{O}_K$. Con esta definición, cuando a un ideal de $\mathcal{O}_K$ le multiplicamos un elemento de su cuerpo de fracciones, que es K, obtenemos un ideal fraccionario. De hecho, esta definición se puede hacer más general tomando cualquier dominio de integridad y su cuerpo de fracciones.

Un apunte importante es que es que el conjunto I_K de los ideales fraccionarios tiene estructura de grupo cuando consideramos el producto natural $(\alpha\, I)\,(\beta\, J) = (\alpha\,\beta)\,(I\,J)$ de ideales fraccionarios.

La teoría de cuerpos de clases se puede formular para un cuerpo numérico K general, pero nosotros tomaremos un cuerpo cuadrático imaginario. El motivo es que es todo lo que necesitamos para resolver el segundo caso del duodécimo problema de Hilbert, y la teoría además en este caso presenta algunas simplificaciones. Por tanto, de aquí en adelante *K siempre denotará un cuerpo cuadrático imaginario.*

El primer concepto que vamos a introducir es el de subgrupo de congruencia para un ideal $\mathfrak{m}$ de $\mathcal{O}_K$ fijado.

Antes de esto, definimos el conjunto $I_K(\mathfrak{m})$ como el conjunto de los ideales fraccionarios de $\mathcal{O}_K$ coprimos con $\mathfrak{m}$. No vamos a ver la definición rigurosa, pero la idea es que tanto ideales fraccionarios como ideales tienen factorización única como productos de ideales primos de $\mathcal{O}_K$, y son coprimos si no comparten ideales primos en sus factorizaciones (como en el caso de los números enteros coprimos). Tiene estructura de grupo, pues se trata de un subgrupo de I_K.

Un ideal fraccionario $\mathfrak{a} = \alpha\, I$ es **principal** si I es un ideal principal de $\mathcal{O}_K$, es decir, generado por un solo elemento, digamos $I = \langle\beta\rangle$. En tal caso, $\mathfrak{a}$ está generado por $\alpha\,\beta$ como $\mathbb{O}_K$-módulo, es decir, $\mathfrak{a} = \langle\alpha\,\beta\rangle$. Así, dentro de $I_K(\mathfrak{m})$, definimos el grupo $P_{K,1}(\mathfrak{m})$ de los ideales fraccionarios principales $\langle\alpha\rangle$ coprimos con $\mathfrak{m}$ tales que $\alpha - 1 \in \mathfrak{m}$.

Definición 9. Sea $\mathfrak{m}$ un ideal de $\mathcal{O}_K$. Se dice que un subgrupo G del grupo I_K de los ideales fraccionarios de $\mathcal{O}_K$ es un **subgrupo de congruencia** para $\mathfrak{m}$ si $P_{K,1}(\mathfrak{m}) \subset G \subset I_K(\mathfrak{m})$. ◂

El siguiente concepto que vamos a introducir es el de símbolo de Artin, pero no lo haremos de manera rigurosa, sino que daremos una idea.

Sea L una extensión abeliana de K. Sea $\mathfrak{m}$ un ideal de $\mathcal{O}_K$ divisible por todos los primos de K que ramifican en L. Esta condición se necesita para que la definición de símbolo de Artin que haremos en breves momentos sea correcta, pero no necesitamos saber qué significa. El lector puede encontrar la definición de ramificación en el libro de Marcus [7, capítulo 3, página 71].

Sea $\mathfrak{a} \in I_K(\mathfrak{m})$. El **símbolo de Artin** de L/K sobre $\mathfrak{a}$, denotado por $\left(\frac{L/K}{\mathfrak{a}}\right)$, es un elemento del grupo de Galois $\mathrm{Gal}(L/K)$ de forma que la aplicación

$$\begin{array}{rccc} \Phi_{\mathfrak{m}}\colon & I_K(\mathfrak{m}) & \longrightarrow & \mathrm{Gal}(L/K) \\ & \mathfrak{a} & \longmapsto & \left(\frac{L/K}{\mathfrak{a}}\right) \end{array}$$

sea, en cierto sentido, una generalización de la aplicación de Artin que vimos en el caso ciclotómico. Esta aplicación $\Phi_{\mathfrak{m}}$ se llama **aplicación de Artin** de L/K para $\mathfrak{m}$.

Con los conceptos introducidos hasta ahora, estamos preparados para ver el resultado clave de la teoría de cuerpos de clases.

Teorema 2 (teorema de existencia). *Sea $\mathfrak{m}$ un ideal de O_K y sea G un subgrupo de congruencia para $\mathfrak{m}$. Entonces existe una única extensión abeliana L de K tal que:*

1. *$\mathfrak{m}$ es divisible por todos los primos de K que ramifican en L.*
2. *$G = \mathrm{Ker}(\Phi_{\mathfrak{m}})$, donde $\Phi_{\mathfrak{m}}$ es la aplicación de Artin de L/K para $\mathfrak{m}$.*

La demostración de este teorema está fuera del alcance de este artículo y puede consultarse en el libro de Janusz [5, capítulo v, teorema 9.16]. Nuevamente, el resultado 1 del teorema anterior es una condición necesaria para que la aplicación de Artin $\Phi_{\mathfrak{m}}$ de la extensión L/K para $\mathfrak{m}$ esté bien definida. El resultado 2 nos permite, usando otro resultado llamado teorema de reciprocidad de Artin (Cox [2, teorema 8.5]), establecer un isomorfismo de grupos entre $\mathrm{Gal}(L/K)$ y el grupo cociente $I_K(\mathfrak{m})/\mathrm{Ker}(\Phi_{\mathfrak{m}})$. Esto ilustra la idea de la teoría de cuerpos de clases: hemos logrado determinar la estructura del grupo de Galois de extensiones abelianas de K usando los grupos de ideales fraccionarios de O_K (lo que hemos llamado anteriormente como *aritmética de K*).

Pero más que los resultados 1 y 2 del teorema anterior, lo que nos interesa en este artículo es que, fijados un ideal de O_K y un subgrupo de congruencia para este ideal, existe una única extensión abeliana L de K cuyo grupo de Galois podemos describir en términos del ideal y el subgrupo de congruencia. Esto nos va a permitir introducir un concepto fundamental para nuestros propósitos.

Definición 10. Sea $\mathfrak{m}$ un ideal de O_K. Se define el **cuerpo de clases radiales** de K para $\mathfrak{m}$, denotado por $K_{\mathfrak{m}}$, como la extensión abeliana dada por el teorema anterior cuando tomamos el ideal $\mathfrak{m}$ y el subgrupo de congruencia $G = P_{K,1}(\mathfrak{m})$. ◂

Además, nos va a interesar un caso concreto del cuerpo de clases radiales de K.

Definición 11. Se define el **cuerpo de clases de Hilbert** de K, denotado por H, como el cuerpo de clases radiales de K para el ideal $\mathfrak{m} = O_K$. ◂

La importancia del cuerpo de clases radiales de un cuerpo cuadrático imaginario radica en que juega el papel de las extensiones ciclotómicas en el caso ciclotómico. En efecto, los cuerpos de clases radiales de K son por definición extensiones abelianas de K, y se tiene además el siguiente resultado:

Teorema 3. *Dada una extensión abeliana L de K, existe algún ideal $\mathfrak{m}$ de O_K tal que $L \subset K_{\mathfrak{m}}$.*

Utilizando el mismo razonamiento que en el caso ciclotómico, obtenemos lo siguiente:

Corolario 4. *Sea K un cuerpo cuadrático imaginario. Entonces,*

$$K^{\mathrm{ab}} = \vee_{\mathfrak{m} \triangleleft O_K} K_{\mathfrak{m}}.$$

Y, por tanto, si calculamos un sistema de generadores de $K_{\mathfrak{m}}/K$ para cada ideal $\mathfrak{m}$ de O_K, la unión de todos ellos será un sistema de generadores de K^{ab}. Hemos, pues, *reformulado el problema*: queremos describir explícitamente un sistema de generadores de cada cuerpo de clases radiales $K_{\mathfrak{m}}$ de K.

4. Curvas elípticas y multiplicación compleja

Sin perder de vista nuestro objetivo, que es describir explícitamente todos los cuerpos de clases radiales $K_{\mathfrak{m}}$ de un cuerpo cuadrático imaginario K, hacemos una pausa para introducir la teoría de curvas elípticas y multiplicación compleja. En la introducción comentamos que queremos describir los generadores que vamos a obtener en términos de objetos matemáticos conocidos. Estos objetos se encuadran en la teoría que vamos a introducir en esta sección. La principal referencia utilizada es el libro de Silverman [11].

4.1. Curvas elípticas: definición y propiedades

Una curva elíptica es un caso particular de lo que llamamos curva algebraica plana. La definición de curva algebraica plana es algo elaborada y no la vamos a ver (para una definición rigurosa, véanse los capítulos 1 y 2 del citado libro de Silverman [11]). Se trata, esencialmente, de una abstracción de la idea intuitiva que tenemos de curva en el plano afín $\mathbb{A}^2(\mathbb{R})$, que corresponde al conjunto de puntos de $\mathbb{R}^2$ que pertenecen a dicha curva. La idea es sustituir el cuerpo $\mathbb{R}$ por un cuerpo F. Así, los puntos de una curva algebraica C están en el espacio afín $\mathbb{A}^2(F)$ (tienen sus coordenadas en F) y vendrán dados por una ecuación de la forma

$$C\colon\ g(x,y)=0,$$

donde pedimos que $g\in F[x,y]$ sea un polinomio. Esta ecuación se llama **ecuación afín de la curva** C. Pero debemos, además, admitir que una curva pueda tener (o no) por punto cualquiera de los puntos de la *recta del infinito* del espacio proyectivo $\mathbb{P}^2(\mathbb{R})$. Para poder definir esto, debemos expresar los puntos de la curva con coordenadas proyectivas (u homogéneas), es decir, como elementos de $\mathbb{P}^2(\mathbb{R})$. Esto lo podemos hacer mediante una ecuación

$$C\colon\ G(x_0,x_1,x_2)=0,$$

donde $G\in F[x_0,x_1,x_2]$ es un polinomio homogéneo. Esta ecuación se llama **ecuación proyectiva de la curva** C.

Así, una curva algebraica es esencialmente el conjunto de puntos dados por una ecuación afín o proyectiva. Para pasar de la afín a la proyectiva, hacemos $G(x_0,x_1,x_2)=g(\frac{x_0}{x_1},\frac{x_2}{x_1})$. Este proceso se conoce como *proyectivización*. Por el contrario, para pasar de la proyectiva a la afín, hacemos $g(x,y)=G(x,1,y)$. Este proceso se conoce como *deshomogeneización*.

Definición 12. Sea F un cuerpo con característica distinta de 2 y 3. Una **curva elíptica** E definida sobre F es una curva algebraica con ecuación afín

$$E\colon\ y^2=4x^3-g_2x-g_3,$$

donde $g_2,g_3\in F$ y $g_2^3-27g_3^2\neq 0$. ◂

El conjunto de puntos de una curva elíptica definida sobre F, denotado por $E(F)$, viene dado por los puntos afines (x,y) con coordenadas en F y un punto en la recta del infinito, con coordenadas homogéneas $[0,1,0]$, que denotamos por ∞ (en adelante llamado **punto del infinito**). El motivo es que si proyectivizamos la ecuación de la curva veremos que el punto del infinito la satisface.

Está bastante claro que una curva elíptica no viene dada por una única ecuación, pues podemos hacer cambios de variables que transformen la ecuación de la definición anterior en otra ecuación de la forma $g(x,y)=0$ con $g\in F[x,y]$. Pero una curva elíptica sí que tiene una única ecuación en la forma de la que aparece en la definición 12, que se llama **ecuación de Weierstrass** de la curva elíptica.

A continuación introducimos el concepto de j-invariante de una curva elíptica, que es un objeto que va a ser fundamental en nuestros propósitos.

Definición 13. Sea E una curva elíptica definida sobre F con ecuación de Weierstrass

$$E\colon\ y^2=4x^3-g_2x-g_3.$$

Se define el j**-invariante** de E como el número

$$j(E)=1728\,\frac{g_2^3}{g_2^3-27g_3^2}.$$ ◂

Nótese que $j(E)$ está bien definido porque, por definición de curva elíptica, $g_2^3-27g_3^2\neq 0$.

Sea E una curva elíptica definida sobre un cuerpo F. Podemos definir una operación binaria sobre el conjunto de puntos $E(F)$ de la curva E que lo dota de **estructura de grupo abeliano**. El elemento neutro

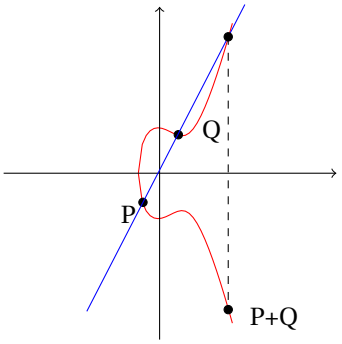

Figura 1: Suma de puntos en una curva elíptica.

de $E(F)$ es el punto del infinito. Para ver como se suman dos puntos, vamos a considerar el caso en que nuestra curva elíptica tiene coeficientes reales. Entonces podemos representarla gráficamente, como en la figura 1.

Para sumar dos puntos P y Q, seguimos el procedimiento indicado en la figura: trazamos la recta que pase por los puntos P y Q, que cortará a la curva elíptica en un tercer punto, y $P+Q$ es el simétrico de este punto respecto del eje horizontal.

Si utilizamos coordenadas afines, podemos calcular las coordenadas de $P+Q$ en función de las coordenadas de P y Q. Estas expresiones son las que utilizamos para definir la suma de puntos de una curva elíptica definida sobre un cuerpo arbitrario (véase el libro de Silverman [11, capítulo 3, sección 2]). Podemos deducir también gráficamente que el opuesto de un punto P de E es el simétrico de P respecto del eje horizontal, y que la suma es conmutativa. Por supuesto, esto no es una demostración general porque no todas las curvas elípticas tienen una representación como la de la figura 1.

4.2. Curvas elípticas con multiplicación compleja

En esta sección vamos a establecer qué significa que una curva elíptica definida sobre el cuerpo $\mathbb{C}$ de los números complejos tenga multiplicación compleja. Esta familia de curvas tienen algunas buenas propiedades que aprovecharemos para llevar a cabo la construcción explícita que buscamos.

Empezaremos esta sección introduciendo el concepto de isogenia. Sean E y E' curvas elípticas definidas sobre un mismo cuerpo F. Un **morfismo de curvas elípticas** $\phi\colon E \longrightarrow E'$ es, esencialmente, una aplicación entre los conjuntos de puntos $\phi\colon E(F) \longrightarrow E'(F)$ tales que, para cada $(x,y) \in E(F)$, las coordenadas de $\phi(x,y)$ vienen dadas por funciones racionales de x e y (o sea, sumas, restas, multiplicaciones y divisiones de x e y). Esto solo sirve como idea y no como definición rigurosa porque tiene algunos problemas técnicos (se puede ver una definición rigurosa y más general en el libro de Silverman [11, pág. 12]). Habitualmente la notación para estos morfismos será $\phi\colon E \longrightarrow E'$, y estaremos entendiendo que hay una aplicación bien definida entre los conjuntos de puntos de E y E'. Una isogenia es un caso particular de morfismo de curvas elípticas.

Definición 14. Sean E y E' curvas elípticas definidas sobre un mismo cuerpo F. Una **isogenia** de E a E' es un morfismo de curvas elípticas $\phi\colon E \longrightarrow E'$ que manda el punto del infinito de E al punto del infinito de E'. ◂

Por ejemplo, si E es una curva elíptica, el morfismo $\phi\colon E \longrightarrow E$ que manda cada punto a sí mismo es una isogenia, porque en particular manda el punto del infinito a sí mismo.

Veamos un ejemplo más interesante. Sea E una curva elíptica definida sobre un cuerpo F de característica 0 y sea $m \in \mathbb{Z}$. Recordemos que $E(F)$ tiene estructura de grupo, por lo que dado $P \in E(F)$, podemos sumar P consigo mismo un número arbitrario de veces. Así, tenemos definido un morfismo de curvas elípticas dado por

$$[m]\colon E(F) \longrightarrow E(F)$$

de forma que, para $P \in E(F)$, $[m](P)$ es la suma de P m veces si m es positivo o la suma de P $-m$ veces si m es negativo. Si $m = 0$, parece lógico convenir que *la suma de P* 0 *veces* es el neutro del grupo, o sea ∞. Por definición de elemento neutro, $[m]$ es una isogenia. La llamaremos **multiplicación por** m.

Definición 15. Sea E una curva elíptica. Se define el anillo de endomorfismos de E como el conjunto

$$\mathrm{End}(E) = \{\phi \colon E \longrightarrow E \mid \phi \text{ es isogenia}\}. \qquad \blacktriangleleft$$

El anillo de endomorfismos de una curva elíptica tiene, en efecto, estructura de anillo con las operaciones

$$(\phi + \psi)(P) \coloneqq \phi(P) + \psi(P),$$
$$(\phi\,\psi)(P) \coloneqq \phi \circ \psi(P).$$

Por ejemplo, los morfimos *multiplicación por m* son endomorfismos de una curva elíptica E.

Definición 16. Sea E una curva elíptica definida sobre $\mathbb{C}$. Decimos que E tiene **multiplicación compleja** si $\mathrm{End}(E)$ tiene más elementos aparte de los morfismos *multiplicación por m*. $\blacktriangleleft$

Para curvas elípticas definidas sobre otros cuerpos no hemos definido qué significa que una curva elíptica tenga multiplicación compleja. Por tanto, cada vez que digamos que una curva elíptica tiene multiplicación compleja obviaremos que está definida sobre $\mathbb{C}$ (o un subcuerpo de $\mathbb{C}$).

Teorema 5. *Sea E una curva elíptica con multiplicación compleja. Entonces, el anillo* $\mathrm{End}(E)$ *de endomorfismos de E es isomorfo a un orden en un cuerpo cuadrático imaginario.*

Un orden en un cuerpo numérico es un subanillo de ese cuerpo numérico que generaliza la noción de anillo numérico. El anillo numérico de un cuerpo numérico es un orden y, además, es el maximal (para la inclusión). Así, si E es una curva elíptica con multiplicación compleja, puede suceder que $\mathrm{End}(E) \cong \mathcal{O}_K$. En tal caso, diremos que E **tiene multiplicación compleja por** $\mathcal{O}_K$. Este tipo de curvas tienen propiedades adicionales y son las que utilizaremos para resolver el caso cuadrático-imaginario.

Sea E una curva elíptica con multiplicación compleja por $\mathcal{O}_K$. Sabemos entonces que $\mathrm{End}(E)$ y $\mathcal{O}_K$ son anillos isomorfos. Resulta que podemos tomar un isomorfismo de anillos

$$[\cdot] \colon \mathcal{O}_K \longrightarrow \mathrm{End}(E)$$

de forma que la imagen de cada número entero $m \in \mathbb{Z}$ (que pertenece a $\mathcal{O}_K$) es el endomorfismo $[m]$ *multiplicación por m*. Se tiene, por tanto, que el isomorfismo $[\cdot]$ generaliza la asignación que acabamos de describir a todo el anillo $\mathcal{O}_K$. Es decir, cada elemento $\alpha \in \mathcal{O}_K$ tiene asociado un endomorfismo $[\alpha]$ de E que se puede ver como la generalización de los morfismos *multiplicación por m*. La aplicación $[\cdot]$ se llama **identificación normalizada** de E.

El grupo de puntos de una curva elíptica en general tiene parte de torsión no trivial. Así, dado $m \in \mathbb{Z}$, podemos considerar el grupo de m-torsión de E,

$$E[m] = \{P \in E(\mathbb{C}) \mid [m](P) = \infty\},$$

que es un subgrupo de $E(\mathbb{C})$. Utilizando la identificación normalizada de E, podemos generalizar esto a un ideal $\mathfrak{m}$ de $\mathcal{O}_K$ cualquiera.

Definición 17. Sea E una curva elíptica con multiplicación compleja por $\mathcal{O}_K$ y sea $\mathfrak{m}$ un ideal de $\mathcal{O}_K$. Se define el **grupo de** $\mathfrak{m}$**-torsión** de E como

$$E[\mathfrak{m}] = \{P \in E(\mathbb{C}) \mid [\alpha](P) = \infty \text{ para todo } \alpha \in \mathfrak{m}\}. \qquad \blacktriangleleft$$

Esto será importante para entender la construcción explícita que queremos llevar a cabo.

5. El caso cuadrático imaginario

Con todas las herramientas introducidas, estamos preparados para entender la respuesta al duodécimo problema de Hilbert para el caso cuadrático imaginario. La referencia utilizada en esta sección es el libro de Silverman [12, capítulo II, secciones 1-5]. En este caso el problema es el siguiente:

Problema 3. Sea K un cuerpo cuadrático imaginario. Determinar explícitamente los generadores de la extensión abeliana maximal K^{ab} de K. ◂

Lo que haremos es encontrar primero un sistema de generadores del cuerpo de clases de Hilbert H de K, y utilizaremos este resultado para encontrar un sistema de generadores del cuerpo de clases radiales $K_{\mathfrak{m}}$ de K para cualquier ideal $\mathfrak{m}$. Esto lo haremos usando la teoría de curvas elípticas introducida en la sección anterior.

Primero de todo, vamos a introducir el concepto de isomorfismo para curvas elípticas definidas sobre $\mathbb{C}$.

Definición 18. Un **isomorfismo de curvas elípticas** definidas sobre $\mathbb{C}$ es una isogenia $\phi\colon E \longrightarrow E'$ entre curvas elípticas definidas sobre $\mathbb{C}$ que es biyectiva y cuya inversa es también una isogenia. En tal caso, decimos que E y E' son isomorfas (o $\mathbb{C}$-isomorfas). ◂

Consideremos ahora el conjunto de todas las curvas elípticas con multiplicación compleja por $\mathcal{O}_K$. Definamos sobre este conjunto la relación binaria

$$E \cong E' \iff E \text{ y } E' \text{ son isomorfas.}$$

Esta relación es de equivalencia y divide al conjunto anteriormente mencionado en clases de equivalencia, de modo que las curvas elípticas de cada clase son $\mathbb{C}$-isomorfas entre sí y no lo son con las de ninguna otra clase. Denotamos la clase de equivalencia de una curva elíptica E con multiplicación compleja por $\mathcal{O}_K$ como $[E]$. El conjunto cociente, o sea, el conjunto de todas estas clases, se denota por $\mathcal{ELL}(\mathcal{O}_K)$. Se tiene el siguiente resultado:

Teorema 6. *$\mathcal{ELL}(\mathcal{O}_K)$ es finito.*

La demostración utiliza técnicas de teoría algebraica de números que no hemos visto en este artículo. Lo que se hace es establecer una aplicación biyectiva con el grupo de clases de ideales de $\mathcal{O}_K$, que es finito (véase el libro de Silverman [12, capítulo II, proposición 1.2]).

Se tiene además que el j-invariante es un invariante de la relación de isomorfía de curvas elípticas definidas sobre $\mathbb{C}$. Es decir:

Proposición 7. *Sean E y E' curvas elípticas definidas sobre $\mathbb{C}$. Entonces, E y E' son isomorfas si y solo si $j(E) = j(E')$.*

Lo que este resultado nos dice es que si tomamos una clase $[E] \in \mathcal{ELL}(\mathcal{O}_K)$ de curvas elípticas, entonces todas las curvas elípticas de dicha clase tienen el mismo j-invariante $j(E)$. Además, este valor es distinto de todos los demás j-invariantes de las curvas elípticas de otras clases de $\mathcal{ELL}(\mathcal{O}_K)$.

Combinando los dos resultados anteriores, obtenemos lo siguiente:

Corolario 8. *El conjunto $\{j(E) \mid E \in \mathcal{ELL}(\mathcal{O}_K)\}$ es finito.*

Por tanto, si tomamos $j(E)$ y hacemos variar E por el conjunto de las curvas elípticas con multiplicación compleja por $\mathcal{O}_K$, obtenemos un número finito de valores. Pero, además, se tiene el siguiente resultado.

Proposición 9. *Sean E y E' curvas elípticas con multiplicación compleja por $\mathcal{O}_K$. Entonces $j(E)$ y $j(E')$ son conjugados (es decir, raíces del mismo polinomio irreducible sobre K). Además, si fijamos E, todos los conjugados de $j(E)$ se obtienen de esta forma.*

Dicho de otra forma, obtenemos todos los conjugados de $j(E)$, que son un número finito por el corolario 8. Además, todos ellos pertenecen a $K(j(E))$, pues la extensión $K(j(E))/K$ es de Galois (véase la demostración del teorema 4.3 del capítulo II del libro de Silverman [12]). Pero en realidad podemos decir mucho más.

Teorema 10. *Sea K un cuerpo cuadrático imaginario y sea E una curva elíptica con multiplicación compleja por O_K. Entonces, el cuerpo de clases de Hilbert de K es*

$$H = K(j(E)).$$

En el lenguaje de teoría de Galois, H es el cuerpo de descomposición del polinomio mínimo (o irreducible) de $j(E)$ sobre K.

Vamos a entender la última frase del enunciado. Si L/K es una extensión de cuerpos y $f \in K[X]$ es un polinomio, decimos que L es cuerpo de descomposición de f sobre K si $L = K(S)$, donde S es el conjunto de las raíces de f en L. Así, la última frase del enunciado anterior dice que H se obtiene de adjuntar a K todas las raíces en H del polinomio irreducible de $j(E)$ sobre K. Esto será importante en los ejemplos de cálculo.

Este resultado nos da, pues, un sistema de generadores de H/K. Para demostrarlo hace falta una serie de resultados que utilizan conceptos de los que no hemos hablado aquí y con unas demostraciones muy técnicas, así que omitiremos esta parte. La demostración se puede encontrar en la referencia de Silverman [12, capítulo II, teorema 4.3].

Recuérdese que queremos encontrar un sistema de generadores de $K_{\mathfrak{m}}/K$ para cualquier ideal $\mathfrak{m}$ de O_K. El resultado que resuelve esta cuestión, y el más importante de este artículo, es el siguiente.

Teorema 11 (teorema principal). *Sea K un cuerpo cuadrático imaginario y sea $\mathfrak{m}$ un ideal de O_K. El cuerpo de clases radiales de K para $\mathfrak{m}$ es*

$$K_{\mathfrak{m}} = K(j(E), x(E[\mathfrak{m}])),$$

donde E es una curva elíptica con multiplicación compleja por O_K y definida sobre H, y x es, esencialmente, la función primera coordenada.

La función primera coordenada es aquella que envía un punto (x, y) de la curva elíptica E a su primera coordenada x. Decimos *esencialmente* porque hay un par de casos en los que la función primera coordenada no funciona. Cuando $j(E) = 0$, hay que sustituirla por la función $(x, y) \longmapsto x^3$, y cuando $j(E) = 1728$, hay que sustituirla por $(x, y) \longmapsto x^2$. Combinando el teorema principal con el corolario 4 obtenemos la solución al problema 3.

Corolario 12. *Sea K un cuerpo cuadrático imaginario. Entonces,*

$$K^{\mathrm{ab}} = K(j(E), x(E_{\mathrm{tors}})),$$

donde E es una curva elíptica con multiplicación compleja por O_K y definida sobre H, y x es, esencialmente, la función primera coordenada.

Esto resuelve completamente el caso cuadrático-imaginario del duodécimo problema de Hilbert. La demostración del teorema 11 es también muy técnica y requiere de otros resultados que no vamos a presentar aquí (el lector la puede consultar en la referencia de Silverman [12, capítulo II, teorema 5.6]).

Una posible pregunta es, ¿para qué nos sirve el teorema 10? Si lo que queríamos era saber una expresión explícita de $K_{\mathfrak{m}}$ para cada ideal $\mathfrak{m}$ de O_K, podríamos haberla enunciado sin decir que $K(j(E))$ es el cuerpo de clases de Hilbert de K. Lo que sucede es que este hecho es teóricamente crucial para la demostración del teorema principal. Sin ir más lejos, el saber que $H = K(j(E))$ nos asegura que toda clase de curvas elípticas $[E] \in \mathcal{ELL}(O_K)$ tiene algún representante definido sobre H. Por tanto, existe alguna curva elíptica definida sobre O_K y definida sobre H, que es la que nos sirve para el teorema principal.

6. Ejemplos de cálculo

Ya sabemos, para cada cuerpo cuadrático imaginario K, la expresión explícita de K^{ab}. Pero, si nos dan un cuerpo cuadrático imaginario concreto, ¿cómo calcularíamos K^{ab}? En esta sección vamos a tratar de responder a esta pregunta siguiendo el capítulo 7 del artículo de Kedlaya [6].

6.1. Cuerpo de clases de Hilbert

No tan rápido, primero vamos a tratar de calcular el cuerpo de clases de Hilbert H de K. Por el teorema 10, $H = K(j(E))$, con $E \in \mathcal{ELL}(\mathcal{O}_K)$ definida sobre H. Podemos hallar cómo son todos los elementos de $\mathcal{O}_K$, pero en principio no parece fácil hallar una curva elíptica con multiplicación compleja por $\mathcal{O}_K$ y calcular su j-invariante.

Aún si hubiésemos conseguido calcular una tal curva E y su j-invariante $j(E)$, probablemente lo tendríamos como una expresión decimal aproximada. Pero esto es algebraicamente insuficiente. De poco nos serviría saber, por ejemplo, que $j(E) \approx 1{,}0003$, pues no tendríamos información de la estructura de $K(j(E))$ (más allá de que está generada por $j(E)$). Lo que nos interesa es saber el polinomio irreducible de $j(E)$, pues esto nos permite conocer todos sus conjugados y poder describir algebraicamente $K(j(E))$.

Pero lo que hacemos realmente en la práctica es al revés: calculamos todos los conjugados de $j(E)$ y, una vez sabiendo esto, podemos calcular el polinomio irreducible de $j(E)$ como

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i),$$

donde $\alpha_1, \ldots, \alpha_n$ son los conjugados de $j(E)$. Así, si calculamos f, por el teorema 10, H es el cuerpo de descomposición de f sobre K y habremos acabado.

Calculemos, pues, el polinomio f. Por la proposición 9, los conjugados de $j(E)$ son los elementos del conjunto

$$\{j(E) \mid [E] \in \mathcal{ELL}(\mathcal{O}_K)\}.$$

Así, tenemos que

$$f(X) = \prod_{[E] \in \mathcal{ELL}(\mathcal{O}_K)} (X - j(E)).$$

Por tanto, ahora la pregunta que cabe hacerse es, ¿cómo calculamos $j(E)$ para cada curva elíptica E con multiplicación compleja por $\mathcal{O}_K$? En este punto, introducimos una nueva herramienta que vamos a necesitar: el grupo de clases de ideales de $\mathcal{O}_K$. La idea es la siguiente: definimos en el conjunto de todos los ideales de $\mathcal{O}_K$ la relación

$$I \sim J \iff \text{existe } \alpha \in K \text{ tal que } I = \alpha J.$$

Esta relación es de equivalencia y las clases de equivalencia son las clases de homotecias de ideales de $\mathcal{O}_K$ (es decir, las clases de múltiplos por elementos de K). A la clase de un ideal $\mathfrak{a}$ de $\mathcal{O}_K$ la denotaremos por $\overline{\mathfrak{a}}$.

Definición 19. Se define el **grupo de clases de ideales** de $\mathcal{O}_K$, y se denota por $C(\mathcal{O}_K)$, como el conjunto cociente para la relación de equivalencia anterior. ◂

El grupo de clases de ideales, como su propio nombre indica, tiene estructura de grupo con la operación $\overline{I}\,\overline{J} := \overline{IJ}$. El neutro es la clase del ideal trivial $\mathcal{O}_K$ (también llamada clase trivial), que de hecho es la clase de todos los ideales principales de $\mathcal{O}_K$.

Y, ¿para qué queremos el grupo de clases de ideales? Resulta que *hay una correspondencia biunívoca* entre el grupo de clases de ideales $C(\mathcal{O}_K)$ y el conjunto de clases $\mathcal{ELL}(\mathcal{O}_K)$. Más concretamente:

Proposición 13. *Hay una aplicación biyectiva*

$$\begin{array}{ccc} C(\mathcal{O}_K) & \longrightarrow & \mathcal{ELL}(\mathcal{O}_K) \\ \overline{\mathfrak{a}} & \longmapsto & [E_{\mathfrak{a}}]. \end{array}$$

La demostración se deduce del teorema 10.14 y el ejercicio 14.2 del libro de Cox [2]. Esto nos permite hacer la siguiente definición:

Definición 20. Sea $\mathfrak{a}$ un ideal de $\mathcal{O}_K$. Definimos el j-invariante de $\mathfrak{a}$ como

$$j(\mathfrak{a}) := j(E_{\mathfrak{a}}).$$ ◂

En otras palabras, el j-invariante de un ideal de O_K es el j-invariante de la clase de curvas elípticas $[E_{\mathfrak{a}}]$ que corresponde a su clase de ideales $\overline{\mathfrak{a}}$. Nótese que esta definición no depende de representantes por la proposición 7.

Combinando la proposición 13 y la definición 20, tenemos que hay una aplicación biyectiva

$$\begin{array}{ccc} C(O_K) & \longrightarrow & j(\mathcal{ELL}(O_K)) \\ \overline{\mathfrak{a}} & \longmapsto & j(E_{\mathfrak{a}}). \end{array}$$

Por tanto, el polinomio f que queríamos calcular se puede escribir como

$$f(X) = \prod_{\overline{\mathfrak{a}} \in C(O_K)} (X - j(\mathfrak{a})).$$

Hemos **trasladado el problema** de calcular las clases de curvas elípticas de $\mathcal{ELL}(O_K)$ a calcular las clases de ideales de $C(O_K)$. Y esto último lo podemos hacer utilizando Sage [9].

Así, el procedimiento a seguir es el siguiente:

1. Calculamos un sistema de representantes de $C(O_K)$ (el conjunto que forman un representante de cada clase).
2. Calculamos el j-invariante de cada ideal del sistema anterior.
3. Calculamos $f(X) = \prod_{\overline{\mathfrak{a}} \in C(O_K)} (X - j(\mathfrak{a}))$.

Veámoslo con un ejemplo concreto. Calculemos el cuerpo de clases de Hilbert de $K = \mathbb{Q}(\sqrt{-15})$. En Sage ponemos la instrucción

```
K=QuadraticField(-15).
```

Para calcular el grupo de clases de ideales, ponemos la instrucción

```
C=K.class_group().
```

Entonces, C será una lista cuyos elementos son representantes de distintas clases de ideales de $C(O_K)$, justo como queríamos. Así, las instrucciones

```
C[0],
```

```
C[1]
```

tendrán *outputs*

```
Trivial principal fractional ideal class,
```

```
Fractional ideal class (2, 1/2*a - 1/2).
```

El grupo de clases de ideales tiene, pues, dos elementos: la clase trivial y la clase $\overline{\langle 2, \frac{\sqrt{-15}-1}{2} \rangle}$.

Ahora toca calcular los j-invariantes. Por supuesto, Sage nos devolverá valores aproximados de los mismos. En realidad, el j-invariante induce una función analítica, que es la que está implementada en Sage bajo el nombre de *elliptic_j*. En general, se tiene que $j(\langle a, b \rangle) = j(\frac{b}{a})$. Así que para calcular el j-invariante de un ideal en Sage lo que haremos será *dividir el segundo generador por el primero*.

Aquí hacemos un inciso. En general, cuando estemos trabajando con el cuerpo cuadrático imaginario $K = \mathbb{Q}(\sqrt{-n})$, existen dos posibilidades:

- $n \equiv 1, 2 \pmod 4$, en cuyo caso un representante de la clase trivial es $\langle 1, \sqrt{-n}\rangle$.
- $n \equiv 3 \pmod 4$, en cuyo caso un representante de la clase trivial es $\langle 2, 1 + \sqrt{-n}\rangle$.

En nuestro caso se tiene que $15 \equiv 3 \pmod 4$ y, por tanto, estamos en la segunda situación. Así, un representante de la clase trivial es $\mathfrak{a}_1 = \langle 2, 1 + \sqrt{-15}\rangle$. Por tanto, el valor de su j-invariante vendrá dado por la siguiente instrucción:

```
elliptic_j((1+sqrt(-15))/2).
```

Para la otra clase, un representante suyo es $\mathfrak{a}_2 = \langle 2, \frac{\sqrt{-15}-1}{2}\rangle$, y ponemos la instrucción

```
elliptic_j((sqrt(-15)-1)/4).
```

Observando los *outputs*, obtenemos que

$$j(\mathfrak{a}_1) \approx -191657{,}832862547 + 1{,}34213412519219 \cdot 10^{-10}\,\mathrm{i},$$
$$j(\mathfrak{a}_2) \approx 632{,}832862547208 + 1{,}06394370576499 \cdot 10^{-13}\,\mathrm{i}.$$

Por último, calculamos el polinomio $(X - j(\mathfrak{a}_1))(X - j(\mathfrak{a}_2))$. Si llamamos $j1 = j(\mathfrak{a}_1)$ y $j2 = j(\mathfrak{a}_2)$, poniendo como *input*

```
(X-j1)*(X-j2)
```

obtenemos el *output*

```
24 x^2 + (191025.000000000 - 1.34319806889795e-10*I) x
                - 1.21287375000000e8 + 6.45433435433001e-8*I.
```

Aquí podemos usar que el polinomio que buscamos *tiene coeficientes enteros* [12, capítulo II, teorema 6.1], de forma que los coeficientes que obtendremos los podemos aproximar a los números enteros más cercanos. Así, obtenemos que el cuerpo de clases de Hilbert de K es el cuerpo de descomposición de

$$f(x) = x^2 + 191025\,x + 121287375$$

sobre K.

6.2. Cálculo del cuerpo de clases radiales

En virtud del corolario 4, K^{ab} es la composición de todos los cuerpos de clases radiales $K_{\mathfrak{m}}$. En esta sección vamos a ver cómo calcular los cuerpos de clases radiales $K_{N\,O_K}$, donde N es un entero positivo (en realidad, esto es suficiente para poder calcular K^{ab}, pues todos los cuerpos de clases radiales de K están contenidos en alguno de la forma $K_{N\,O_K}$).

Según el teorema 11,

$$K_{N\,O_K} = K(j(E), x(E[N])),$$

donde E es una curva elíptica definida sobre H y con multiplicación compleja por O_K.

Recuérdese que $K(j(E))$ es el cuerpo de clases de Hilbert de K, que ya sabemos calcular. Por tanto, todo lo que tenemos que hacer es añadir al cuerpo de clases de Hilbert las primeras coordenadas de los puntos de N-torsión de E. El cálculo de puntos de torsión de una curva elíptica en general es complicado, pero para este caso podemos utilizar una herramienta adicional: los **polinomios de división** asociados a una curva elíptica. Se trata de una familia de polinomios $\{D_N\}_{N\in\mathbb{Z}_{>0}}$ con coeficientes en el cuerpo de definición de la curva elíptica elegida (véase el ejercicio 3.7 del libro de Silverman [11]). En nuestro caso, el interés de estos polinomios reside en el siguiente resultado.

Teorema 14. *Sea $E \in \mathcal{ELL}(\mathcal{O}_K)$ definida sobre H. Las raíces del N-ésimo polinomio de división D_N de E son las primeras coordenadas de los puntos de $E[N]$.*

Se deduce, por tanto, que $K_{N\,\mathcal{O}_K}$ es el cuerpo de descomposición de D_N sobre H.

El procedimiento a seguir en este caso es:

1. Calcular el polinomio f que define el cuerpo de clases de Hilbert utilizando el procedimiento anterior.
2. Tomar una raíz α de f y calcular una curva elíptica E tal que $j(E) = \alpha$.
3. Calcular el N-ésimo polinomio de división asociado a E.

Trabajemos nuevamente sobre el ejemplo de $K = \mathbb{Q}(\sqrt{-15})$. Vamos a calcular $K_{3\,\mathcal{O}_K}$. Partimos de que tenemos el polinomio f que define el cuerpo de clases de Hilbert de K y que hemos calculado en el ejemplo anterior.

Con la instrucción

```
H.<z> = K.extension(f)
```

estamos definiendo $H = K(z)$, donde z tiene polinomio irreducible f (o sea, H es el cuerpo de clases de Hilbert de K). Expresaremos todos los elementos de H en función de z. A continuación, con la instrucción

```
alpha=f.roots(H)[0][0]
```

definimos `alpha` como una raíz del polinomio f en H; concretamente, la primera de la lista de tales raíces, que tiene el valor de $\alpha = -z + 191025$. Después ponemos la instrucción

```
E=EllipticCurve_from_j(alpha),
```

mediante la cual definimos E como la curva elíptica con ecuación afín

$$y^2 = x^3 + (-578259\,z - 110825787600)\,x + 74550012768\,z + 14288092368961950,$$

cuyo j-invariante es α. Por último, calculamos el tercer polinomio de división asociado a E mediante la instrucción

```
E.division_polynomial(3),
```

que es

$$\begin{aligned} D_3(x) = {} & 3\,x^4 + (-3469554\,z - 664954725600)\,x^2 \\ & + (894600153216\,z + 171457108427543400)\,x \\ & - 64296415660328775\,z - 12322911690611116662375. \end{aligned}$$

Por tanto, $K_{3\,\mathcal{O}_K}$ es el cuerpo de descomposición de D_3 sobre H.

Estamos preparados para responder a la pregunta que nos hicimos al principio de la sección. Para calcular K^{ab}, calcularíamos para cada $N \in \mathbb{Z}_{>0}$ el cuerpo de clases radiales $K_{N\,\mathcal{O}_K}$ mediante el proceso que acabamos de presentar. Si adjuntamos a K las raíces de todos estos polinomios, obtenemos K^{ab}.

Como último comentario, esta manera de proceder justifica también la importancia de calcular el cuerpo de clases de Hilbert de un cuerpo cuadrático imaginario. En la práctica, se puede ver como un paso previo al cálculo de los cuerpos de clases radiales de ese cuerpo cuadrático imaginario.

Referencias

[1] Breiding, Paul y Samart, Detchat. «Kronecker's Jugendtraum». En: (2012). URL: http://www.math.psu.edu/papikian/BreidingSamart.pdf.

[2] Cox, David A. *Primes of the form $x^2 + ny^2$*. Pure and Applied Mathematics. John Wiley & Sons, Inc., 1997. https://doi.org/10.1002/9781118400722.

[3] Gil Muñoz, Daniel. *Explicit class field theory via elliptic curves*. Trabajo final de máster. Universitat de Barcelona, 2017. URL: https://hdl.handle.net/2445/121135.

[4] Hungerford, Thomas W. *Algebra*. 1.ª ed. Graduate Texts in Mathematics 73. Springer-Verlag, 1980. https://doi.org/10.1007/978-1-4612-6101-8.

[5] Janusz, Gerald J. *Algebraic number fields*. Pure and applied mathematics a series of monographs and textbooks 55. Academic Press, 1973. https://doi.org/10.1090/gsm/007.

[6] Kedlaya, Kiran S. *Complex Multiplication and Explicit Class Field Theory*. Tesis doct. Harvard University, 1996. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.49.3926.

[7] Marcus, Daniel A. *Number fields*. Universitext. Springer-Verlag, 1977. https://doi.org/10.1007/978-1-4684-9356-6.

[8] Milne, James S. *Fields and Galois Theory*. (v4.53). 2017. URL: http://www.jmilne.org/math/CourseNotes/ft.html.

[9] The Sage Developers. *SageMath, the Sage Mathematics Software System*. https://doi.org/10.5281/zenodo.593563.

[10] Schappacher, Norbert. «On the history of Hilbert's twelfth problem: a comedy of errors». En: *Matériaux pour l'histoire des mathématiques au XXe siècle - Actes du colloque à la mémoire de Jean Dieudonné*. Séminaires et Congrès 3. Société Mathématique de France, 1998, págs. 243-273.

[11] Silverman, Joseph H. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 106. Springer-Verlag, 1986. https://doi.org/10.1007/978-0-387-09494-6.

[12] Silverman, Joseph H. *Advanced Topics in the Arithmetic of Elliptic Curves*. 1.ª ed. Graduate Texts in Mathematics 151. Springer-Verlag New York, 1994. https://doi.org/10.1007/978-1-4612-0851-8.

[13] Vladut, Serge G. *Kronecker's Jugendtraum and Modular Functions*. Gordon y Breach Publishers, 1995. ISBN: 978-2-88124-754-5.

[14] Wei, Wafa. «Moduli Fields of CM-Motives Applied to Hilbert's 12th Problem». 1994. URL: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.57.5573.