RETICULADOS CON MULTIPLICACIÓN COMPLEJA

DANIEL HEIMLICH LÓPEZ

El objetivo de este apunte es es explicar el concepto de reticulados con multiplicación compleja. Primero es necesario revisar algunos resultados sobre órdenes en cuerpos de números, específicamente en cuerpos cuadráticos imaginarios.

1. Órdenes en cuerpos de números

Definición 1.1. Sea K un cuerpo de números. Un orden de K es un subanillo $\mathcal{O}$ de K tal que

(i) $\mathcal{O}$ contiene al 1.
(ii) $\mathcal{O}$ es un $\mathbb{Z}$-módulo finitamente generado.
(iii) $\mathcal{O}$ contiene una $\mathbb{Q}$-base de K.

Observemos que las condiciones (ii) y (iii) son equivalentes a que $\mathcal{O}$ sea un $\mathbb{Z}$-módulo libre de rango $[K : \mathbb{Q}]$.

Además, notemos que $\mathcal{O}_K$, el anillo de enteros de K, es un orden. De hecho, todo orden $\mathcal{O}$ de K es un subanillo de $\mathcal{O}_K$, de manera que $\mathcal{O}_K$ es el orden maximal. Esto es por la siguiente caracterización de enteros algebraicos.

Lema 1.1. Un elemento $\alpha \in K$ es un entero algebraico si y solo si $\mathbb{Z}[\alpha]$ es finitamente generado como $\mathbb{Z}$-módulo.

Notemos que para todo $\alpha \in \mathcal{O}$, el $\mathbb{Z}$-módulo $\mathbb{Z}[\alpha]$ es un $\mathbb{Z}$-submódulo de $\mathcal{O}$ (porque $\mathcal{O}$ es un anillo). Luego, $\mathbb{Z}[\alpha]$ es finitamente generado. Así, la caracterización anterior muestra que todo $\alpha \in \mathcal{O}$ es un entero algebraico, y por lo tanto $\mathcal{O} \subset \mathcal{O}_K$.

El índice $f = [\mathcal{O}_K : \mathcal{O}]$ es finito, pues ambos $\mathcal{O}_K$ y $\mathcal{O}$ son $\mathbb{Z}$-módulos del mismo rango. Se llama conductor de f.

Sea M un $\mathbb{Z}$-submódulo de K de rango $[K : \mathbb{Q}]$. El conjunto

$$\mathcal{O}_M := \{\alpha \in K : \alpha M \subset M\}$$

se llama anillo de multiplicación (o anillo de multiplicadores) de M en K . La siguiente proposición será importante.

Proposición 1.1. Si M es un $\mathbb{Z}$-submódulo de K de rango $n = [K : \mathbb{Q}]$, entonces su anillo de multiplicación

$$\mathcal{O}_M = \{\alpha \in K : \alpha M \subset M\}$$

es un orden de K.

Demostración. Es claro que $\mathcal{O}_M$ es subanillo de K, y que $1 \in \mathcal{O}_M$. Sea $\gamma \in M$ un elemento no nulo. Se tiene $\alpha\gamma \in M$ para todo $\alpha \in \mathcal{O}_M$. Es decir, $\gamma\mathcal{O}_M \subset M$, y por lo tanto $\mathcal{O}_M$ es un $\mathbb{Z}$-módulo finitamente generado (libre de rango $\leq n$).

Veamos que contiene una $\mathbb{Q}$-base. Sea $\alpha_1, \dots, \alpha_n$ una $\mathbb{Z}$-base de M, que es por fuerza una $\mathbb{Q}$-base de K. Luego, para cada α_i, $i = 1, \dots, n$, se tiene

$$\alpha_i \alpha_j = \sum_{k=1}^{n} c_{jk}^{(i)} \alpha_k, \quad j = 1, \dots, n,$$

donde los coeficientes $c_{jk}^{(i)} \in \mathbb{Q}$. Sea $c^{(i)}$ el denominador común de los $c_{jk}^{(i)}$. Entonces se tiene $(c^{(i)}\alpha_i)\alpha_j \in M$ para cada $j = 1, \dots, n$. Es decir, $(c^{(i)}\alpha_i)M \subset M$, y por lo tanto $\mathcal{O}_M$ contiene a la $\mathbb{Q}$-base $\{c^{(i)}\alpha_i\}$, de modo que $\mathcal{O}_M$ es un orden de K. □

1.1. Ideales en $\mathcal{O}$. Un **ideal fraccionario** de $\mathcal{O}$ es un subconjunto $\mathfrak{a}$ de K que es un $\mathcal{O}$-módulo finitamente generado. Esta definición es equivalente a que $c\mathfrak{a}$ sea una ideal de $\mathcal{O}$ para algún $c \in K^*$.

Decimos que un ideal fraccionario $\mathfrak{a}$ de $\mathcal{O}$ es invertible si existe un ideal fraccionario $\mathfrak{b}$ de $\mathcal{O}$ tal que $\mathfrak{ab} = \mathcal{O}$. En general, no todos los ideales fraccionarios son invertibles. La siguiente es una condición necesaria.

Proposición 1.2. Si $\mathfrak{a}$ es un ideal invertible de $\mathcal{O}$, entonces su anillo de multiplicación en K es $\mathcal{O}$. Es decir,

$$\{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}.$$

Demostración. Para cualquier ideal fraccionario de $\mathcal{O}$ se tiene $\mathcal{O} \subset \{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\}$, por la definición de ideal fraccionario. Si $\mathfrak{a}$ es invertible, $\mathfrak{ab} = \mathcal{O}$ para algún ideal fraccionario $\mathfrak{b}$, y dado β tal que $\beta\mathfrak{a} \subset \mathfrak{a}$, entonces

$$\beta\mathcal{O} = \beta\mathfrak{ab} \subset \mathfrak{ab} = \mathcal{O},$$

de modo que $\beta \in \mathcal{O}$. □

Un ideal que satisface la condición $\{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}$ se llama **ideal propio**.

Ejemplo 1.1. Para $K = \mathbb{Q}(\sqrt{-3})$ y $\mathcal{O} = \mathbb{Z}[\sqrt{-3}]$, el ideal $\mathfrak{a} = (2, 1 + \sqrt{-3})$ no es propio (y por ende no invertible) ya que $\mathcal{O} \subsetneq \{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\} = O_K$. Para verificar esto, observemos primero lo siguiente.

Lema 1.2. Sea $\mathcal{O}$ un orden de K, sea $\mathfrak{a} = (\alpha_1, \dots, \alpha_m)$ el ideal generado por $\{\alpha_1, \dots, \alpha_m\} \subset \mathcal{O}$, y sea $M = \mathbb{Z}\mu_1 + \cdots + \mathbb{Z}\mu_n$ un $\mathbb{Z}$-submódulo de K. Entonces son equivalentes

(i) $\mu\mathfrak{a} \subset \mathfrak{a}$ para todo $\mu \in M$.
(ii) $\mu_i\alpha_j \in \mathfrak{a}$ para todo $i = 1, \dots, n$, y para todo $j = 1, \dots, m$.

Demostración. Claramente (i) $\Longrightarrow$ (ii). Para ver que (ii) $\Longrightarrow$ (i), sea $\mu = k_1\mu_1 + \cdots + k_n\mu_n \in M$, $k_i \in \mathbb{Z}$ para cada i, y sea $\alpha = \beta_1\alpha_1 + \cdots + \beta_m\alpha_m \in \mathfrak{a}$, con $\beta_j \in \mathcal{O}$ para cada j. Entonces

$$\mu\alpha = \sum_{i,j} (k_i\mu_i)(\beta_j\alpha_j) = \sum_{i,j} (k_i\beta_j)(\mu_i\alpha_j) \in \mathfrak{a},$$

pues $\mu_i\alpha_j \in \mathfrak{a}$, $k_i\beta_j \in \mathcal{O}$, y $\mathfrak{a}$ es un ideal de $\mathcal{O}$. □

En el ejemplo, sabemos que $\{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\}$ es un orden de K, así que es subanillo de $\mathcal{O}_K$. Luego, basta ver que $\beta\mathfrak{a} \subset \mathfrak{a}$ para todo $\mathfrak{a} \in \mathcal{O}_K$.

Una $\mathbb{Z}$-base de $\mathcal{O}_K$ es $\{1, (1+\sqrt{-3})/2\}$, y es fácil verificar que los cuatro productos

$$1 \cdot 2, \quad 1 \cdot (1+\sqrt{-3}), \quad \frac{1+\sqrt{-3}}{2} \cdot 2, \quad \frac{1+\sqrt{-3}}{2} \cdot (1+\sqrt{-3})$$

pertenecen a $\mathfrak{a}$. El lema implica entonces que $\{\beta \in K \mid \beta\mathfrak{a} \subset \mathfrak{a}\} = \mathcal{O}_K$.

En cuerpos cuadráticos imaginarios (que serán el objeto de interés) también se cumple que los ideales propios son invertibles. Es decir, un ideal es invertible si y solo si es propio. Para la demostración, véase [Cox22, p. 107].

Sea K un cuerpo cuadrático imaginario, y $\mathcal{O}$ un orden de K. Sea $I(\mathcal{O})$ el grupo de ideales invertibles (i.e. propios), y $P(\mathcal{O})$ el grupo de ideales principales. Al igual que en $\mathcal{O}_K$, el grupo de clases de $\mathcal{O}$ se define por $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$. Se puede demostrar que es finito, y el número de clases de $\mathcal{O}$ se define por $h(\mathcal{O}) = \#C(\mathcal{O})$.

Observación 1.1. Para expresar el grupo de clases $C(\mathcal{O})$ en el lenguaje de la teoría de cuerpos de clase es necesario considerar el subgrupo de ideales primos al conductor de $\mathcal{O}$ (ver el apéndice).

2. Multiplicación compleja

Un reticulado L en $\mathbb{C}$ es un subgrupo aditivo de $\mathbb{C}$ generado por dos elementos ω_1 y ω_2 linealmente independientes sobre $\mathbb{R}$. Es decir, $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ con $\omega_1/\omega_2 \notin \mathbb{R}$. Lo denotamos por $L = [\omega_1, \omega_2]$. Decimos que dos reticulados L y L' son homotéticos si $L' = \lambda L$ para algún $\lambda \in \mathbb{C}^*$.

Sea L un reticulado en $\mathbb{C}$. Vamos a considerar el conjunto de números complejos α tales que $\alpha L \subset L$. Notemos que este conjunto es un subanillo de $\mathbb{C}$, pues si $\alpha L \subset L$ y $\beta L \subset L$, entonces $(\alpha+\beta)L \subset L$ y $\alpha\beta L \subset \alpha L \subset L$. Lo llamamos **anillo de multiplicación** de L. Además, si $\alpha L \subset L$, decimos que L tiene multiplicación por α. Notemos que reticulados homotéticos tienen el mismo anillo de multiplicación, pues para $\lambda \in \mathbb{C}^*$,

$$\alpha L \subset L \iff \alpha\lambda L \subset \lambda L.$$

Así, el anillo de multiplicación está definido en clases de reticulados módulo homotecia. Es claro que L tiene multiplicación por n para todo $n \in \mathbb{Z}$. La pregunta que vamos a discutir es si existen $\alpha \in \mathbb{C} - \mathbb{Z}$ tales que $\alpha L \subset L$.

Primero vamos a relacionar la condición $\alpha L \subset L$ con la función $\wp$ de Weierstrass asociada a L.

Teorema 2.1. Sea L un reticulado complejo, y $\wp = \wp(z; L)$ la función de Weierstrass. Dado $\alpha \in \mathbb{C}$, las siguientes son equivalentes:

(i) Se tiene $\alpha L \subset L$.
(ii) La función $g(z) := \wp(\alpha z)$ es una función racional de $\wp(z)$ (i.e. $g \in \mathbb{C}(\wp)$).

Demostración. Asumamos que $\wp(\alpha z)$ es una función racional de $\wp(z)$,

$$\wp(\alpha z) = \frac{P(\wp(z))}{Q(\wp(z))},$$

donde $P(X)$ y $Q(X)$ son polinomios con coeficientes en $\mathbb{C}$. Ambas $\wp(z)$ y $\wp(\alpha z)$ tienen un polo doble en $z = 0$. Luego, el orden de $P(\wp(z))$ en $z = 0$ es $-2\deg P$, y el orden de $Q(\wp(z))$ es $-2\deg Q$. Comparando ordenes en $z = 0$ obtenemos

$$-2 = -2\deg P + 2\deg Q,$$

de donde $\deg P = \deg Q + 1$. Ahora, sea $\omega \in L - \{0\}$. Como $\wp(z)$ tiene un polo doble en $z = \omega$, la relación entre los grados de P y Q implica que

$$\wp(\alpha z) = \frac{P(\wp(z))}{Q(\wp(z))}$$

tiene un polo doble en $z = \omega$. Es decir, $\wp(z)$ tiene un polo doble en $\alpha\omega$. Como el conjunto de polos de $\wp(z)$ es L, debe tenerse $\alpha\omega \in L$. Esto muestra que $\alpha L \subset L$, pues $\omega \in L$ era arbitrario.

Asumamos ahora que $\alpha L \subset L$. Entonces $\wp(\alpha z)$ es una función elíptica para L (es meromorfa, y L-periódica porque $\alpha L \subset L$). Para concluir la demostración usamos el siguiente reultado.

Lema 2.1. Toda función elíptica par es una función racional de $\wp(z)$.

Demostración. Ver [Lan87, p.9]. □

Basta entonces notar que $\wp(\alpha z)$ es una función par, pues $\wp(z)$ lo es. □

Observación 2.1. Para $n \in \mathbb{Z}$, es fácil verificar que la función $\wp(nz)$ es una función racional de $\wp(z)$. Esto es consecuencia de la ley de adición de $\wp$, que en el caso $z_1 = z_2 = z$ (con $2z \notin L$) es

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2.$$

La expresión en el lado derecho es una función racional de $\wp(z)$, pues $\wp'(z)^2$ y $\wp''(p)^2$ lo son (esto sigue de la ecuación diferencial para $\wp(z)$). Luego, usando la fórmula de adición sigue por inducción que $\wp(nz)$ es racional en $\wp(z)$.

Veremos ahora que si L tiene multiplicación por algún $\alpha \in \mathbb{C} - \mathbb{Z}$, entonces el anillo de multiplicación de L es un orden de un cuerpo cuadrático imaginario. Notemos que, dado un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario, todo ideal de $\mathcal{O}$ es un reticulado en $\mathbb{C}$.

Teorema 2.2. Si $\alpha L = L$ para algún $\alpha \in \mathbb{C} - \mathbb{Z}$, entonces el anillo de multiplicación de L es un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario K. Además, L es homotético a un ideal fraccionario propio de $\mathcal{O}$.

Demostración. Reemplazando L por un reticulado homotético, podemos asumir que $L = [1, \tau]$, con $\tau \notin \mathbb{R}$. Entonces, $\alpha L \subset L$ es equivalente a

$$\alpha = a + b\tau$$

$$\alpha\tau = c + d\tau$$

donde $a, b, c, d \in \mathbb{Z}$, con $b \neq 0$. Luego, α satisface

$$\alpha^2 - (a + d)\alpha + (ad - bc) = 0.$$

Como α no es racional, esto muestra que α es cuadrático sobre $\mathbb{Q}$, y además es un entero algebraico. Luego, $K = \mathbb{Q}(\alpha)$ es un cuerpo cudrático imaginario, y además se tiene $K = \mathbb{Q}(\tau)$, ya que $\tau = (\alpha - a)/b$.

Además, si $\beta L \subset L$, entonces $\beta = a' + b'\tau$ con $a', b' \in \mathbb{Z}$, así que $\beta \in K$. Es decir, el anillo de multiplicación de L es en realidad subconjunto de K. Luego, la proposición 1,1 implica que es un orden $\mathcal{O}$ de K. Notemos que L es un ideal

fraccionario de $\mathcal{O}$, pues es un $\mathbb{Z}$-módulo libre de rango 2, y $\beta L \subset L$ para todo $\beta \in \mathcal{O}$. Por último, L es propio, pues se tiene $\{\beta \in K : \beta L \subset L\} = \mathcal{O}$. □

Si L tiene multiplicación por algún $\alpha \in \mathbb{C} - \mathbb{Z}$, decimos que L tiene **multiplicación compleja** por α. El término viene del hecho de que α es necesariamente complejo, i.e., no real. Esto es una consecuencia del teorema anterior.

Fijemos ahora un cuerpo cuadrático imaginario K y un orden $\mathcal{O}$ de K. Vamos a describir las clases de reticulados con anillo de multiplicasción $\mathcal{O}$. Hay una conexión entre estas y el grupo de clases de $\mathcal{O}$.

Proposición 2.1. Sea K un cuerpo cuadrático imaginario y $\mathcal{O}$ un orden de K. Hay una biyección entre las clases de reticulados cuyo anillo de multiplicación es $\mathcal{O}$, y el grupo de clases $C(\mathcal{O})$.

Demostración. Sea L un reticulado cuyo anillo de multiplicación es $\mathcal{O}$. Por el teorema anterior, L es homotético a un ideal propio de $\mathcal{O}$. Además, dos ideales propios en $\mathcal{O}$ definen la misma clase módulo homotecia si y solo si definen la misma clase en $C(\mathcal{O})$. Esto es porque para $\lambda \in K^*$,

$$\mathfrak{a} = \lambda\mathfrak{b} \iff \mathfrak{a} = (\lambda)\mathfrak{b},$$

donde la primera igualdad es en el sentido de reticulados, y la segunda en el sentido de ideales (con $(\lambda) = \lambda\mathcal{O}$). Esto nos da la biyección deseada. □

2.1. Ejemplos. La proposición anterior es útil para calcular ejemplos explícitos. Vamos a encontrar las clases de reticulados que tienen multiplicación compleja por $i, \sqrt{-5}$ y $\sqrt{-3}$.

Ejemplo 2.1 (Multiplicación compleja por $\sqrt{-1}$)**.** Sea L un reticulado que tiene multiplicación compleja por i. Entonces la clase de L (módulo homotecia) es la clase de un ideal propio en un orden de $K = \mathbb{Q}(i)$ que contiene a i. El único orden de K que contiene a i es $\mathbb{Z}[i] = \mathcal{O}_K$, cuyo número de clase es 1. Así, la clase de $[1, i]$ es la única que tiene multiplicación compleja por i.

Ejemplo 2.2 (Multiplicación compleja por $\sqrt{-5}$)**.** Aquí, $K = \mathbb{Q}(\sqrt{-5})$, y el único orden que contiene a $\sqrt{-5}$ es $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Su número de clase es 2, y los ideales (1) y $(2, 1+\sqrt{-5})$ son representantes. Es fácil verificar que $(1) = [1, \sqrt{-5}]$, y también se puede verificar que $(2, 1 + \sqrt{-5}) = [2, 1 + \sqrt{-5}]$.

Así, $[1, \sqrt{-5}]$ y $[2, 1 + \sqrt{-5}]$ representan a las únicas clases de reticulados que tienen multiplicación compleja por $\sqrt{-5}$.

Ejemplo 2.3 (Multiplicación compleja por $\sqrt{-3}$)**.** Aquí, $K = \mathbb{Q}(\sqrt{-3})$, y $\mathcal{O}$ es un orden de K que contiene a $\sqrt{-3}$. Los únicos órdenes que cumplen esto son $[1, (1+\sqrt{-3})/2] = \mathcal{O}_K$, y $[1, \sqrt{-3}]$ (esto es porque $\mathcal{O}$ debe estar entre $\mathcal{O}' = [1, \sqrt{-3}]$ y $\mathcal{O}_K$, pero $[O_K : \mathcal{O}'] = 2$).

Ambos tienen número de clase 1. Luego, las únicas clases de reticulados que tienen multiplicación compleja por $\sqrt{-3}$ son las clases de $[1, (1 + \sqrt{-3})/2]$ y $[1, \sqrt{-3}]$. Notar, sin embargo, que sus anillos de multiplicación son órdenes distintos, a diferencia de los ejemplos anteriores.

2.2. Invariante j en reticulados con multiplicación compleja. Probaremos que el invariante j en reticulados con multiplicación compleja es algebraico sobre $\mathbb{Q}$. Además, daremos algunos ejemplos.

Teorema 2.3. Sea K un cuerpo cuadrático imaginario, $\mathcal{O}$ un orden de K, y $\mathfrak{a}$ un ideal propio de $\mathcal{O}$. Entonces $j(\mathfrak{a})$ es algebraico de grado a lo más $h(\mathcal{O})$.

Demostración. La demostración se basa en probar que el conjunto de valores $\sigma(j(\mathfrak{a}))$, donde σ recorre los automorfismos de $\mathbb{C}$, es finito, de cardinalidad $\leq h(\mathcal{O})$. Esto implica que $j(\mathfrak{a})$ es algebraico, pues, si $\sigma_1(j(\mathfrak{a})), \ldots, \sigma_r(j(\mathfrak{a}))$ son los valores distintos que puede tomar $\sigma(j(\mathfrak{a}))$, el polinomio

$$f(x) = \prod_{i=1}^{r} \big(X - \sigma_i(j(\mathfrak{a})\big)$$

es invariante bajo la acción de cualquier automorfismo de $\mathbb{C}$, y por lo tanto sus coeficientes son racionales.

Veremos que el conjunto de valores distintos de $\sigma(j(\mathfrak{a}))$ para $\sigma \in \mathbb{C}$ es exactamente

$$\{j(\mathfrak{b})\colon \mathfrak{b} \text{ ideal propio de } \mathcal{O}\}$$

que tiene cardinalidad $h(\mathcal{O})$ (así que el grado de $j(\mathfrak{a})$ es a lo más $h(\mathcal{O})$).

Fijemos entonces $\sigma \in \mathcal{O}$. Para probar que $\sigma(j(\mathfrak{a}) \in \{j(\mathfrak{b})\colon \mathfrak{b} \text{ ideal propio de } \mathcal{O}\}$, necesitamos probar primero que $\sigma(j(\mathfrak{a})) = j(L)$ para algún reticulado L. Para eso usaremos lo siguiente:

Lema 2.2. Si $u^3 - 27v^2 \neq 0$, entonces existe un único reticulado L (módulo homotecia) tal que tal que $g_2(L) = u$ y $g_3(L) = v$.

Demostración. La demostración es consecuencia de la sobreyectividad del invariante j. Ver [Cox22, p.176]. □

Sean $g_2 = g_2(\mathfrak{a})$ y $g_3 = g_3(\mathfrak{a})$. Como $\Delta(\mathfrak{a}) = g_2^3 - 27g_3^2 \neq 0$, se tiene $\sigma(g_2)^3 - 27\sigma(g_3)^3 \neq 0$. Luego, el lema implica que existe un reticulado L tal que $\sigma(g_2) = g_2(L)$ y $\sigma(g_3) = g_3(L)$, y por lo tanto

$$j(L) = \frac{g_2(L)^3}{g_2(L)^3 - 27g_3(L)^2} = \frac{\sigma(g_2)^3}{\sigma(g_2)^3 - 27\sigma(g_3)^2} = \sigma(j(\mathfrak{a})).$$

Para concluir la demostración, solo nos falta probar que L es homotético a un ideal propio de $\mathcal{O}$. Probaremos que el anillo de multiplicación de L es $\mathcal{O}$ (que es equivalente a lo anterior). Para eso, usaremos la relación con la función $\wp$ de Weierstrass (proposición 2.1).

Sea $\alpha \in \mathcal{O}$. Como $\mathfrak{a}$ tiene multiplicación por α, la función $\wp(\alpha z; \mathfrak{a})$ es una función racional de $\wp(z; \mathfrak{a})$:

$$\wp(\alpha z; \mathfrak{a}) = \frac{P(\wp(z; \mathfrak{a}))}{Q(\wp(z; \mathfrak{a}))}.$$

También sabemos que, cerca de $z = 0$, $\wp(\alpha z, \mathfrak{a})$ tiene la expansión de Laurent (ver apéndice)

$$\begin{aligned}\wp(\alpha z; \mathfrak{a}) &= \frac{1}{\alpha^2 z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(\mathfrak{a}) \alpha^{2n} z^{2n} \\ &= \frac{1}{\alpha^2 z^2} + \sum_{n=1}^{\infty} a_n(g_2, g_3) \alpha^{2n} z^{2n},\end{aligned}$$

donde $g_2 = g_2(\mathfrak{a}), g_3 = g_3(\mathfrak{a})$, y los coeficientes $a_n(g_2, g_3)$ son expresiones racionales de g_2 y g_3 (i.e., pertenecen a $\mathbb{Q}(g_2, g_3)$). Luego, cerca de 0 se tiene

$$\frac{P(\wp(z; g_2, g_3))}{Q(\wp(z; g_2, g_3))} = \frac{1}{\alpha^2 z^2} + \sum_{n=1}^{\infty} a_n(g_2, g_3) \alpha^{2n} z^{2n} \tag{1}$$

y por lo tanto los coeficientes de ambas expresiones (la expresión en el lado izquierdo vista como serie de Laurent) son los mismos. Es decir, hay igualdad en $\mathbb{C}((z))$ (series formales de Laurent). Notemos que σ actúa en $\mathbb{C}((z))$ al hacerlo en los coeficientes. Así,

$$\frac{P^\sigma(\wp(z; \sigma(g_2), \sigma(g_3)))}{Q^\sigma(\wp(z; \sigma(g_2), \sigma(g_3)))} = \frac{1}{\sigma(\alpha)^2 z^2} + \sum_{n=1}^{\infty} a_n(\sigma(g_2), \sigma(g_3)) \sigma(\alpha)^{2n} z^{2n}, \tag{2}$$

donde P^σ y Q^σ son los polinomios que se obtienen al aplicar σ en los coeficientes, y $\sigma(a_n(g_2, g_3)) = a_n(\sigma(g_2), \sigma(g_3))$, ya que σ fija $\mathbb{Q}$. Como $\sigma(g_2) = g_2(L)$ y $\sigma(g_3) = g_3(L)$, obtenemos

$$\frac{P^\sigma(\wp(z; L))}{Q^\sigma(\wp(z; L))} = \frac{1}{\sigma(\alpha)^2 z^2} + \sum_{n=1}^{\infty} a_n(g_2(L), g_3(L)) \sigma(\alpha)^{2n} z^{2n}.$$

El lado derecho corresponde a la serie de Laurent de la función $\wp(\sigma(a)z; L)$ en $z = 0$. Luego,

$$\wp(\sigma(\alpha)z; L) = \frac{P^\sigma(\wp(z; L))}{Q^\sigma(\wp(z; L))},$$

y por lo tanto L tiene multiplicación por $\sigma(\alpha)$. Esto se cumple para todo $\alpha \in \mathcal{O}$, de modo que L tiene multiplicación por $\sigma(\mathcal{O})$. Pero $\sigma(\mathcal{O}) = \mathcal{O}$, pues $\mathcal{O}$ es un orden de un cuerpo cuadrático.

Así, L tiene multiplicación por $\mathcal{O}$. Es decir, si $\mathcal{O}'$ es el anillo de multiplicación de L, se tiene $\mathcal{O} \subset \mathcal{O}'$. Pero podemos intercambiar los roles de $\mathfrak{a}$ y L (mediante σ^{-1}) para obtener $\mathcal{O}' \subset \mathcal{O}$, y luego $\mathcal{O}' = \mathcal{O}$. Por lo tanto, L es homotético a un ideal de $\mathcal{O}$, como se quería. Esto muestra que $\sigma(j(\mathfrak{a})) = j(L)$ puede tomar a lo más $h(\mathcal{O})$ valores. □

Observación 2.2. Notemos que una consecuencia del teorema anterior es que si $h(\mathcal{O}) = 1$, entonces $j(\mathfrak{a}) \in \mathbb{Q}$. Por ejemplo, esto se cumple para el anillo de enteros en todos los cuerpos cuadráticos imaginarios con número de clase igual a 1.

2.3. Cálculos explícitos. Vamos a calcular el invariante j para algunos de los ejemplos descritos arriba.

Ejemplo 2.4 (Cálculo de $j(i)$)**.** Sea $L = [1, i]$. Como $iL = L$,

$$g_3(L) = g_3(iL) = i^{-6} g_3(L) = -g_3(L),$$

de donde $g_3(L) = 0$, y por lo tanto $j(i) = j(L) = 1728$.

Ejemplo 2.5 (Cálculo de $j(\omega)$)**.** Sea $\omega = e^{2\pi i/3}$, y $L = [1, \omega]$. Como $\omega L = L$,

$$g_2(L) = g_2(\omega L) = \omega^{-4} g_2(L),$$

de donde $g_2(L) = 0$. Por lo tanto $j(\omega) = j(L) = 0$.

Ejemplo 2.6 (Cálculo de $j(\sqrt{-2})$.)**.** El único reticulado (módulo homotecia) que tiene multiplicación por $\sqrt{-2}$ es $L = [1, \sqrt{-2}]$. Aquí, $\sqrt{-2}L = [2, \sqrt{-2}] \subsetneq L$, y $[L\colon \sqrt{-2}L] = 2$, así que no podemos proceder igual que en los ejemplos anteriores. Pero se tiene lo siguiente:

Lema 2.3. Sea L un reticulado complejo, y $\alpha \in \mathbb{C}$ tal que $\alpha L \subset L$. Sea

$$\wp(\alpha z) = \frac{P(\wp(z))}{Q(\wp(z))}$$

donde P, Q son coprimos con $\deg P = \deg Q + 1$. Entonces se tiene $\deg P = [L\colon \alpha L] = N_{K/\mathbb{Q}}(\alpha)$, donde $K = \mathbb{Q}(\alpha)$.

Demostración. Probemos primero que $[L\colon \alpha L] = N_{K/\mathbb{Q}}(\alpha)$. Podemos asumir sin pérdida de generalidad que $L = [1, \tau]$. Sea

$$\alpha = a + b\tau$$
$$\alpha\tau = c + d\tau$$

Entonces α es raíz del polinomio $x^2 - (a + d)x + (ad - bc) = 0$, de modo que $N(\alpha) = ad - bc$, que es positiva pues K es cuadrático imaginario. Por otro lado, $\alpha L = [a + b\tau, c + d\tau]$, y luego $[L\colon \alpha L]$ es el valor absoluto del determinante de la matriz

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

i.e. $[L\colon \alpha L] = |ad - bc| = N(\alpha)$.

Veamos ahora que $\deg P = N_{K/\mathbb{Q}}(\alpha)$. Fijemos z tal que $2z \notin \frac{1}{\alpha}L$, y consideremos el polinomio $F(X) = P(X) - \wp(\alpha z)Q(X)$, que tiene el mismo grado que $P(X)$. Notemos que si r es una raíz de $F(X)$, entonces $Q(r) \neq 0$, porque esto implica $P(r) = 0$, lo que no puede ser porque P y Q son coprimos.

Primero, veamos que z puede escogerse de manera que $F(X)$ tenga raices distintas. En efecto, sea z tal que $F(X)$ tiene una raíz r con multiplicidad mayor que 1. Entonces r es raíz de $F'(X) = P'(X) - \wp(\alpha z)Q'(X)$, y por lo tanto también es raíz de

$$F(X)Q'(X) - F'(X)Q(X) = P(X)Q'(X) - P'(X)Q(X),$$

que no depende de z. Así, r pertenece al conjunto de raíces de $G(X) = P(X)Q'(X) - P'(X)Q(X)$. Luego, es suficiente escoger z de modo que $\wp(\alpha z)Q(s) \neq P(s)$, para cada raíz s de $G(X)$.

Bajo estos supuestos, se tiene lo siguiente.

Afirmación. El conjunto de raices de $F(X)$ es $\{\wp(z + \omega)\colon \omega \in \frac{1}{\alpha}L\}$.

Sea $\omega \in \alpha^{-1}L$. Entonces $\alpha\omega \in L$, y luego

$$\wp(\alpha z) = \wp(\alpha(z + \omega)) = \frac{P(\wp(z + \omega))}{Q(\wp(z + \omega))},$$

así que $F(\wp(z+\omega))=0$. Ahora sea r una raíz de $F(X)$, y escojamos z_0 tal que $r=\wp(z_0)$ (esto puede hacerse porque $\wp$ es sobreyectiva). Luego, como $Q(r)\neq 0$, tenemos

$$\wp(\alpha z)=\frac{P(r)}{Q(r)}=\frac{P(\wp(z_0))}{Q(\wp(z_0))}=\wp(\alpha z_0).$$

Esto ocurre si y solo si a $\alpha z_0\equiv\pm\alpha z$ (mód L), i.e. $z_0\equiv\pm z$ (mód $\alpha^{-1}L$). No puede tenerse $z_0\equiv -z$ (mód $\alpha^{-1}L$) puesto que $2z\notin\alpha^{-1}L$. Por lo tanto $z_0\equiv z$ (mód $\alpha^{-1}L$), i.e. $z_0=z+\omega$, con $\omega\in\alpha^{-1}L$. Esto demuestra la afirmación.

El último argumento muestra que dados $\omega,\omega'\in\alpha^{-1}L$, se tiene $\wp(z+\omega)=\wp(z+\omega')$ si y solo si $\omega\equiv\omega'$ (mód L), de manera que

$$\#\{\wp(z+\omega)\colon \omega\in\alpha^{-1}L\}=[\alpha^{-1}L\colon L]=[L\colon \alpha L]=N(\alpha).$$

□

Como $[L\colon\sqrt{-2}L]=N(\sqrt{-2})=2$, el lema implica que

$$\wp(\sqrt{-2}z)=\frac{P(\wp(z))}{Q(\wp(z))},$$

donde P es cuadrático y Q es lineal. Usaremos esta igualdad para encontrar los coeficientes en la serie de Laurent de $\wp(z)$. Dividiendo $P(X)$ en $Q(X)$ obtenemos

$$\wp(\sqrt{-2}z)=a\wp(z)+b+\frac{1}{c\wp(z)+d} \tag{3}$$

para algunas constantes a,b,c,d. Los primeros términos de la serie de Laurent de $\wp(z)$ son

$$\wp(z)=\frac{1}{z^2}+\frac{g_2}{20}z^2+\frac{g_3}{28}z^4+\frac{g_2^2}{1200}z^6+\dots$$

Para simplificar la expresión, reemplazamos L por un reticulado homotético de manera que

$$\frac{g_2}{20}=\frac{g_3}{28}=g$$

para alguna constante $g\neq 0$. Esto puede hacerse porque g_2 y g_3 son distintos de 0. (En efecto, si $g_2=0$ o $g_3=0$, $j(L)$ tendría el mismo valor que en los reticulados $[1,i]$ o $[1,\omega]$, lo que no puede ocurrir porque no es homotético a ninguno de los dos). Así,

$$\wp(z)=\frac{1}{z^2}+gz^2+gz^4+\frac{g^2}{3}z^6+\dots,$$

y luego

$$\wp(\sqrt{-2}z)=-\frac{1}{2z^2}-2gz^2+4gz^4-\frac{8g^2}{3}z^6+\dots \tag{4}$$

Haciendo $z\to 0$ y comparando coeficientes en 3 y 4 obtenemos (notando que $(c\wp(z)+d)^{-1}$ tiende a 0) que $a=-1/2$ y $b=0$. Así,

$$\wp\big(\sqrt{-2}z\big)+\frac{1}{2}\wp(z)\big)^{-1}=c\wp(z)+d,$$

que es lineal en $\wp(z)$. Para c y d se usa la misma idea: encontrar los primeros términos en las expansiones de Laurent para ambos lados (en el lado izquierdo es

necesario calcular los primeros términos de la inversa formal). Para más detalle, ver [Cox22, p.168]. Esto entrega $g = 27/8$, de donde

$$g_2 = \frac{5 \cdot 27}{20},\ g_3 = \frac{7 \cdot 27}{2}.$$

Luego, $j(\sqrt{-2}) = j(L) = 20^3 = 8000$.

Apéndice A. Ideales primos al conductor de un orden

Los siguientes resultados están explicados en [Cox22, 7.C.].

Dado un orden $\mathcal{O}$ en de conductor f en un cuerpo cuadrárico imaginario, decimos que un ideal $\mathfrak{a}$ de $\mathcal{O}$ es primo a f si $\mathfrak{a} + fO_K = O_K$. El conjunto de ideales primos a f es cerrado bajo multiplicación. Luego, en $I(\mathcal{O})$ podemos considerar el subgrupo $I(\mathcal{O}, f)$, generado por los ideales primos a f, y además, el subgrupo $P(\mathcal{O}, f) \subset I(\mathcal{O}, f)$, generado por ideales principales $\alpha\mathcal{O}_K$, donde $N(\alpha)$ es primo a f.

Se tiene lo siguiente:

Proposición A.1. La inclusión $I(\mathcal{O}, f) \subset I(\mathcal{O})$ induce un isomorfismo

$$I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I(\mathcal{O})/P(\mathcal{O}) = C(\mathcal{O}).$$

Además, el grupo de clases $C(\mathcal{O})$ se relaciona con C_K a través de

Proposición A.2. Existe un isomorfismo

$$C(\mathcal{O}) \simeq I(\mathcal{O}, f)/P(\mathcal{O}, f) \simeq I_K(f)/P_{K,\mathbb{Z}}(f),$$

donde $I_K(f)$ es el subgrupo de I_K de ideales primos a f, y $P_{K,\mathbb{Z}}(f)$ es el subgrupo de $I_K(f)$ generado por ideales de la forma αO_K, donde $\alpha \equiv a$ (mód fO_K) para algún entero a primo a f.

Esta ultima proposición muestra que $C(\mathcal{O})$ es un grupo de clases generalizado para el módulo $f\mathcal{O}_K$.

Apéndice B. Resultados básicos sobre funciones elípticas

Los siguientes resultados están explicados en [Cox22], y con más detalle en [Lan87].

USea L un reticulado en $\mathbb{C}$. Una **función elíptica** para L es una función f meromorfa en $\mathbb{C}$ tal que $f(z+\omega) = f(z)$ para todo $\omega \in L$ (esto equivale a $f(z+\omega_1) = f(z+\omega_2) = f(z)$).

Definición B.1. La función zeta de Weierstrass para un reticulado L se define por

$$\wp(z) = \sum_{\omega \in L \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Proposición B.1. La función $\wp$ de Weierstrass es una función elíptica para L. Además, se tiene

(i) En $z = 0$, $\wp(z)$ tiene la expansión de Laurent

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty} (2n+1) G_{2n+2}(L) z^n,$$

donde

$$G_r(L) = \sum_{\omega \in L'} \frac{1}{\omega^r}.$$

(ii) La función $\wp$ satisface la ecuación diferencial

$$\wp(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L),$$

donde

$$g_2(L) = 60 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^4}, \quad g_3(L) = 140 \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^6}.$$

(iii) Los coeficientes de la serie de Laurent en 1. son racionales en $g_2(L)$ y $g_3(L)$.

Demostración. La serie que define a la función $\wp$ converge uniformemente en compactos que no contienen puntos de L, pues es dominada por la serie

$$\sum_{\omega \in L'} \frac{1}{\omega^3},$$

que converge absolutamente. Así, $\wp$ define una función meromorfa en $\mathbb{C}$. Para ver que es elíptica, notamos que

$$\wp'(z) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3}.$$

La serie converge absolutamente y es claro que es L-periódica, de modo que $\wp'$ es una función elíptica. Luego, la función $\wp(z+\omega_i) - \wp(z)$ (donde $\omega_i, i = 1, 2$ son los periodos de L) tiene derivada nula, y por lo tanto $\wp(z+\omega_i) - \wp(z) \equiv C$ para alguna constante C. Evalundo en $-\omega_i/2$, que no pertence a L, obtenemos

$$\wp(\omega_i/2) - \wp(-\omega_i/2) = C.$$

Pero $\wp$ es par (dado que $\omega \mapsto -\omega$ es una biyección en L), y por lo tanto $C = 0$. La serie de Laurent alrededor de $z = 0$ sigue de expandir

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right) = \frac{1}{\omega^2} \sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^n}$$

y reordenar (lo cual es correcto por convergencia absoluta), notando además que $G_r(L) = 0$ si r es impar. Para la ecuación diferencial, calculando los términos de orden menor a 2 en las expansiones de Laurent de $\wp$ y $\wp'$ se verifica que $f := \wp'^2 - 4\wp^3 + g_2(L)\wp + g_3(L) = o(z^2)$. Esto muestra que f es una función elíptica que se anula en $z = 0$, y por periodicidad, en todo L. Pero f es holomorfa fuera de L, así que f es holomorfa en todo $\mathbb{C}$. Como es acotada, el teorema de Liouville implica que es constante, y por ende idénticamente nula. □

Proposición B.2. La función $\wp$ de Weierstrass satisface la ley de adición

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2$$

si $z_1, z_2 \notin L$ y $z_1 + z_2 \notin L$.

Referencias

[Cox22] David A. Cox. *Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication*. AMS Chelsea Publishing, Providence, RI, third edition, [2022] ©2022. With contributions by Roger Lipsett.

[Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1987. With an appendix by J. Tate.