LÁTICES CON MULTIPLICACIÓN COMPLEJA

MATÍAS BRUNA

1. Motivación

Dado un látice L fijo, consideremos $\wp(z;L) = \wp(z)$, $g_2(L) = g_2$ y $g_3(L) = g_3$. Vimos en CM 6 que si $2z \notin L$ entonces

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

y más aún, también vimos que

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \quad \text{y} \quad \wp''(z) = 6\wp(z)^2 - \frac{1}{2}g_2$$

por lo que reemplazando arriba obtenemos que

$$\wp(2z) = -2\wp(z) + \frac{(12\wp(z)^2 - g_2)^2}{16(4\wp(z)^3 - g_2\wp(z) - g_3)}$$

y vemos que $\wp(2z)$ es una función racional en $\wp(z)$. Siguiendo esta misma idea, se puede probar por inducción que $\wp(nz)$ es una función racional en $\wp(z)$ $\forall n \in \mathbb{N}$. De aqui una pregunta natural es, ¿Existen otros $\alpha \in \mathbb{C}$ para los cuales $\wp(\alpha z)$ es una función racional en $\wp(z)$?. La respuesta está dada por el siguiente teorema, pero antes definamos lo siguiente

Definición 1.1. Decimos que $\wp$ tiene *multiplicación compleja* por $\alpha \in \mathbb{C}$ si $\wp(\alpha z)$ es una función racional en $\wp(z)$.

2. Teorema Principal

Teorema 2.1. *Sea L un látice y $\wp(z)$ la función $\wp$ del látice L. Para $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ las siguientes afirmaciones son equivalentes:*

(i) $\wp$ tiene multiplicación compleja por α.
(ii) $\alpha L \subseteq L$
(iii) Existe un orden $\mathcal{O}$ en un cuerpo cuadrático imaginario K tal que $\alpha \in \mathcal{O}$ y L es homotético a un ideal fraccionario propio de $\mathcal{O}$.

Más aún, si se cumplen estas condiciones, entonces $\wp(\alpha z)$ se escribe de la forma

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}$$

con $A(x)$ y $B(x)$ polinomios coprimos tales que

$$\deg(A(x)) = \deg(B(x)) + 1 = [L : \alpha L] = N(\alpha) \tag{2.1}$$

Antes de demostrar esto, probemos el siguiente lema

Lema 2.2. *Toda función elíptica par para L es una función racional en $\wp(z)$. Más aún, toda función elíptica g para L es de la forma*

$$g(z) = \frac{A(\wp(z))}{B(\wp(z))} + \frac{C(\wp(z))}{D(\wp(z))}\wp'(z)$$

con $A(x)$, $B(x)$, $C(x)$ y $D(x)$ polinomios.

Demostración: Primero notemos lo siguiente:

(a) Si f es una función elíptica par y holomorfa en $\mathbb{C}\setminus L$, su expansión de Laurent cerca de $z=0$ es

$$f(z)=\sum_{k=-m}^{\infty}a_{2k}z^{2k}=\frac{a_{-2m}}{z^{2m}}+\frac{a_{-2m+2}}{z^{2m-2}}+\cdots+\frac{a_{-2}}{z^2}+F(z)$$

con $F(z)$ holomorfa, y como

$$\wp(z)=\frac{1}{z^2}+\sum_{k=1}^{\infty}b_kz^{2k}$$

vemos que

$$f(z)-a_{-2m}(\wp(z))^m=\frac{a'_{-2m+2}}{z^{2m-2}}+\frac{a'_{-2m+4}}{z^{2m-4}}+\cdots$$

tiene sólo términos z^l con $l\geq -(2m-2)$, y similarmente

$$f(z)-a_{-2m}(\wp(z))^m-a'_{-2m+2}(\wp(z))^{m-1}$$

tiene sólo términos z^l con $l\geq -(2m-4)$. Inductivamente, encontramos $A(x)$ polinomio tal que $f(z)-A(\wp(z))$ es holomorfa cerca de $z=0$ y elíptica, y por periodicidad es holomorfa en todo $\mathbb{C}$ y elíptica, por lo tanto $f(z)-A(\wp(z))=c$ y así $f(z)=A(\wp(z))+c=B(\wp(z))$.

(b) Si f es una función elíptica par con un polo de orden m en $w\in\mathbb{C}\setminus L$, entonces $(\wp(z)-\wp(w))$ tiene un cero de orden al menos 1 en $z=w$, y por lo tanto $(\wp(z)-\wp(w))^m f(z)$ es holomorfa en w.

Ahora, dada f una función elíptica par, consideramos el paralelogramo fundamental

$$\mathbf{P}=\{s\omega_1+t\omega_2\mid 0\leq s,t\leq 1\}$$

Como f es meromorfa, solo tiene finitos polos en $\mathbf{P}\setminus L$, digamos $z_1,\ldots,z_m$, de ordenes $\alpha_1,\ldots,\alpha_m$ respectivamente. Por (b) tenemos que

$$g(z)=f(z)\cdot\prod_{k=1}^{m}(\wp(z)-\wp(z_k))^{\alpha_k}$$

es holomorfa en $\mathbf{P}\setminus L$, y por periodicidad g es holomorfa en $\mathbb{C}\setminus L$. Finalmente, por (a) tenemos que existe $A(x)$ polinomio tal que $g(z)=A(\wp(z))$, y por lo tanto

$$f(z)=\frac{A(\wp(z))}{\prod_{k=1}^{m}(\wp(z)-\wp(z_k))^{\alpha_k}}=\frac{A(\wp(z))}{B(\wp(z))}$$

con $B(x)$ un polinomio, mostrando así que f es una función racional en $\wp(z)$. Por último, notamos que toda función elíptica h se escribe como

$$h(z)=\underbrace{\frac{h(z)+h(-z)}{2}}_{\text{par}}+\underbrace{\frac{h(z)-h(-z)}{2}}_{\text{impar}}=\underbrace{\frac{h(z)+h(-z)}{2}}_{\text{par}}+\underbrace{\left(\frac{h(z)-h(-z)}{2\wp'(z)}\right)}_{\text{par}}\wp'(z)$$

de donde se sigue que existen polinomios $A(x)$, $B(x)$, $C(x)$ y $D(x)$ tales que

$$h(z)=\frac{A(\wp(z))}{B(\wp(z))}+\frac{C(\wp(z))}{D(\wp(z))}\wp'(z)$$

□

Demostremos ahora el Teorema 2.1

Demostración:

(i) ⇒ (ii): Si $\wp(\alpha z)$ es racional en $\wp(z)$, entonces existen polinomios $A(x)$, $B(x)$ tales que

$$B(\wp(z))\wp(\alpha z)=A(\wp(z)) \tag{2.2}$$

y como $\wp(z)$ y $\wp(\alpha z)$ tienen polos dobles en el origen, si $\deg(A(x))=m$ y $\deg(B(x))=n$, entonces comparando las expansiones de Laurent en la igualdad de arriba vemos que

$$\left(\frac{b}{z^{2n}}+\cdots\right)\left(\frac{1}{\alpha^2z^2}+\cdots\right)=\frac{a}{z^{2m}}+\cdots$$

y concluimos que $\deg(A(x))=\deg(B(x))+1$. Ahora, dado $\omega\in L$, por la igualdad (2.2) tenemos que $\wp(\alpha z)$ tiene un polo en ω, y por lo tanto $\wp(z)$ tiene un polo en $\alpha\omega$, y como los polos de $\wp(z)$ son exactamente L, concluimos que $\alpha\omega\in L$ y por ende $\alpha L\subseteq L$.

$(ii) \Rightarrow (i)$: Si $\alpha L \subseteq L$, entonces $\wp(\alpha z)$ es meromorfa y tiene a L como su látice de periodos, y como $\wp(\alpha z)$ es par, por el Lema 2.2 tenemos que $\wp$ tiene multiplicación compleja por α.

$(ii) \Rightarrow (iii)$: Supongamos que $\alpha L \subseteq L$. Eligiendo $\lambda \in \mathbb{C}^\times$ conveniente, tenemos que $L' = \lambda L = [1, \tau]$ para algún $\tau \in \mathbb{C} \setminus \mathbb{R}$, y por Lema 2.11 de CM 3, existe un orden $\mathcal{O}$ del cuerpo cuadrático imaginario $K = \mathbb{Q}(\tau)$ tal que L' es un ideal fraccionario propio de $\mathcal{O}$ y $\alpha \in \mathcal{O}$ (ya que $\alpha L' \subseteq L'$).

$(iii) \Rightarrow (ii)$: Es directo, ya que si $L' = \lambda L$ es ideal fraccionario propio de $\mathcal{O}$ y $\alpha \in \mathcal{O}$ entonces

$$\alpha \in \mathcal{O} = \{\beta \in K \mid \beta L' \subseteq L'\}$$

por definición de ideal fraccionario propio.

Por último, para probar la igualdad (2.1), supongamos que

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))} \tag{2.3}$$

Vimos que $\deg(A(x)) = \deg(B(x)) + 1$, y por la observación hecha en CM 10 tenemos que $[L : \alpha L] = N(\alpha)$, por lo que basta probar que $\deg(A(x)) = [L : \alpha L]$. Para esto usaremos el siguiente lema:

Lema 2.3.

(i) Si $A(x)$ y $B(x)$ son polinomios coprimos, entonces el polinomio $A(x) - \lambda B(x)$ tiene raíces múltiples solo para finitos $\lambda \in \mathbb{C}$.

(ii) Para todo $u \in \mathbb{C}$ existe $w \in \mathbb{C}$ tal que $\wp(w) = u$.

Demostración:

(i) Como $A(x)$ y $B(x)$ son coprimos, $\operatorname{disc}(A(x) - \lambda B(x))$ es un polinomio en λ de grado al menos 1, y como $A(x) - \lambda B(x)$ tiene raíz múltiple si y sólo si $\operatorname{disc}(A(x) - \lambda B(x)) = 0$ se tiene lo pedido.

(ii) La demostración es la misma que ($\Rightarrow$) del Lema 2.5 de CM 6, cambiando $f(z) = \wp(z) - \wp(z_2)$ por $f(z) = \wp(z) - u$.

□

Fijemos ahora $z \in \mathbb{C}$ tal que $2z \notin (1/\alpha)L$, y que además el polinomio $A(x) - \wp(\alpha z)B(x)$ no tenga raíces múltiples (que existe por el Lema 2.3). Este polinomio tiene el mismo grado que $A(x)$, por lo que lo usaremos para encontrar $\deg(A(x))$. Consideremos los látices $L \subseteq (1/\alpha)L$, y sean $\{w_i\}$ representantes de $(1/\alpha)L/L$. Afirmamos que $\{\wp(z + w_i)\}$ son todas las raíces de $A(x) - \wp(\alpha z)B(x)$. Si demostramos esto, tendremos que $\deg(A(x)) = [(1/\alpha)L : L] = [L : \alpha L]$, que es lo que queríamos probar. Para esto, notemos primero que $\wp(z + w_i) \neq \wp(z + w_j)$ si $i \neq j$, pues en caso contrario tendríamos que $\wp(z + w_i) = \wp(z + w_j)$ para algunos $i \neq j$, y por el Lema 2.5 de CM 6 eso implica que $z + w_i \equiv \pm(z + w_j) \mod L$.

- Si $z + w_i \equiv (z + w_j) \mod L$ entonces $w_i \equiv w_j \mod L$, lo que contradice que $i \neq j$.
- Si $z + w_i \equiv -(z + w_j) \mod L$ entonces $2z \equiv -w_i - w_j \mod L$, lo que contradice que $2z \notin (1/\alpha)L$.

por lo que concluimos que los $\wp(z + w_i)$ son distintos. De la igualdad (2.3) vemos que

$$A(\wp(z + w_i)) = \wp(\alpha(z + w_i))B(\wp(z + w_i))$$

pero $w_i \in (1/\alpha)L$, por lo que $\alpha(z + w_i) \equiv \alpha z \mod L$, y por ende $\wp(\alpha(z + w_i)) = \wp(\alpha z)$, luego los $\wp(z + w_i)$ son raíces de $A(x) - \wp(\alpha z)B(x)$. Para ver que estas son todas las raíces, consideremos u una raíz cualquiera. Notemos que $B(u) \neq 0$ pues $B(u) = 0$ implicaría $A(u) = 0$, pero $A(x)$ y $B(x)$ son coprimos. Por Lema 2.3 existe $w \in \mathbb{C}$ tal que $\wp(w) = u$, y por lo tanto

$$\wp(\alpha z) = \frac{A(u)}{B(u)} = \frac{A(\wp(w))}{B(\wp(w))} = \wp(\alpha w)$$

y usando nuevamente el Lema 2.5 de CM 6 concluimos que $\alpha w \equiv \pm \alpha z \mod L$. Cambiando w por $-w$ de ser necesario (esto no afecta la relación encontrada antes, ya que $\wp$ es par), podemos asumir que $w \equiv z \mod (1/\alpha)L$. Esto implica que $w = z + (1/\alpha)k$ para algún $k \in L$, y como los w_i son representantes, $(1/\alpha)k \equiv w_i \mod L$ para algún i, y por lo tanto $w \equiv z + w_i \mod L$ y así $u = \wp(w) = \wp(z + w_i)$ es una de las raíces que ya conocíamos, concluyendo así la demostración del Teorema 2.1. □

Esto muestra que si una función elíptica tiene multiplicación compleja por algún $\alpha \in \mathbb{C} \setminus \mathbb{Z}$, entonces tiene multiplicación compleja por un orden completo $\mathcal{O}$ en un cuerpo cuadrático imaginario. Además, por la caracterización de los ordenes vista en CM 3 vemos que todos los elementos de $\mathcal{O} \setminus \mathbb{Z}$ son genuinamente complejos, es decir $(\mathcal{O} \setminus \mathbb{Z}) \cap \mathbb{R} = \emptyset$, asi que esto justifica el nombre "multiplicación compleja".

Otra consecuencia importante del Teorema 2.1 es que la multiplicación compleja es una propiedad intrínseca del látice, por lo que en vez de hablar de funciones elípticas con multiplicación compleja, hablaremos de látices con multiplicación compleja. Y como cambiar un látice por uno homotético no afecta la multiplicación compleja, trabajaremos con clases de homotecias de látices.

Más aún, la caracterización (iii) del Teorema 2.1 nos permite encontrar la siguiente correspondencia:

Corolario 3.1. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático imaginario. Existe una correspondencia uno a uno entre el grupo de clases $C(\mathcal{O})$ y las clases de homotecia de látices que tienen a $\mathcal{O}$ como su anillo de multiplicación compleja.*

Demostración: Si L es un látice con $\mathcal{O}$ como su anillo de multiplicación compleja, por (iii) del Teorema 2.1 tenemos que $L' = \lambda L$ es un ideal fraccionario propio de $\mathcal{O}$, y recíprocamente, todo ideal fraccionario propio de $\mathcal{O}$ es un látice con $\mathcal{O}$ como su anillo de multiplicación compleja (por definición de ideal fraccionario propio). Por último, vemos que dos ideales fraccionarios propios de $\mathcal{O}$, $\mathfrak{a}$ y $\mathfrak{b}$, son homotéticos como látices si y sólo si están en la misma clase de $C(\mathcal{O})$:

$$\mathfrak{a}P(\mathcal{O}) = \mathfrak{b}P(\mathcal{O}) \iff \mathfrak{a}\mathfrak{b}^{-1} \in P(\mathcal{O}) \iff \mathfrak{a}\mathfrak{b}^{-1} = \alpha\mathcal{O} \iff \mathfrak{a} = \alpha\mathfrak{b}\mathcal{O} = \alpha\mathfrak{b}$$

□

De esto se concluye que el número de clase $h(\mathcal{O})$ nos dice las cantidad de clases de homotecia de látices con $\mathcal{O}$ como su anillo de multiplicación compleja, por lo que, usando la correspondencia vista en CM 4, podemos encontrar todas estas clases usando la teoría de reducción de formas cuadráticas vista en CM 1.

Ejemplo 3.2 (Cálculo de clases de látices con multiplicación compleja prefijada)**.**

(1) Consideremos todos los látices que tienen multiplicación compleja por $\sqrt{-3}$. En este caso estamos trabajando con un orden $\mathcal{O}$, que contiene a $\sqrt{-3}$, en $K = \mathbb{Q}(\sqrt{-3})$. Como $D = -3 \equiv 1 \mod 4$, $w_k = \frac{1+\sqrt{-3}}{2}$, por lo que $\mathcal{O} = \mathbb{Z} + \mathbb{Z}(f \cdot \frac{1+\sqrt{-3}}{2})$ para algún $f \in \mathbb{N}$, pero vemos que $\sqrt{-3} \in \mathcal{O} \iff f$ es 1 o 2.

Si $f = 1$ entonces $\mathcal{O} = \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, con $\omega = e^{2\pi i/3}$, y como $D = -3 \equiv 1 \mod 4$, $D_{\mathcal{O}} = D = -3$. Busquemos ahora las formas cuadráticas reducidas de discriminante $D_{\mathcal{O}} = -3$. Sabemos que $a \leq \sqrt{\frac{-(-3)}{3}} = 1$, por lo que $a = 1$, y como D es impar, b debe ser impar. De aqui $b \in \{-1, 1\}$, pero si $b = -1$ entonces $|b| = a$ y por lo tanto b debe ser positivo. Si $b = 1$ entonces $1^2 - 4c = -3$, por lo que $c = 1$, y así la única forma cuadrática reducida de discriminante -3 es $x^2 + xy + y^2$, que corresponde al látice $[1, \frac{-1+\sqrt{-3}}{2}] = [1, \omega]$.

Si $f = 2$ entonces $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\sqrt{-3}$, y como $D = -3 \equiv 1 \mod 4$, $D_{\mathcal{O}} = 2^2 \cdot D = -12$. Busquemos ahora las formas cuadráticas reducidas de discriminante $D_{\mathcal{O}} = -12$. Sabemos que $a \leq \sqrt{\frac{-(-12)}{3}} = 2$, por lo que $a \in \{1, 2\}$, y como $D_{\mathcal{O}}$ es par, b debe ser par. Si $a = 1$, entonces $b = 0$ y así $0^2 - 4c = -12$, por lo que $c = 3$, encontrando así la forma $x^2 + 3y^2$. Si $a = 2$, entonces $b \neq -2$ porque $|b| = a \Rightarrow b \geq 0$. Si $b = 0$ entonces $0^2 - 8c = -12$ lo cual es imposible, y si $b = 2$ entonces $2^2 - 8c = -12$, lo que implica que $c = 2$, pero $(a, b, c) > 1$ por lo que no es reducida, y así la única forma cuadrática reducida de discriminante -12 es $x^2 + 3y^2$, que corresponde al látice $[1, \frac{\sqrt{-12}}{2}] = [1, \sqrt{-3}]$.

De aqui vemos que los únicos látices con multiplicación compleja por $\sqrt{-3}$ salvo homotecia son $[1, \sqrt{-3}]$ y $[1, \omega]$.

(2) Consideremos ahora multiplicación compleja por $\sqrt{-5}$. Aqui $K = \mathbb{Q}(\sqrt{-5})$ y el único orden que contiene a $\sqrt{-5}$ es $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. Como $D = -5 \not\equiv 1 \mod 4$, $D_{\mathcal{O}} = 4D = -20$, por lo que debemos buscar las formas cuadráticas reducidas de discriminante $D_{\mathcal{O}} = -20$, pero el ejemplo (2) de CM 1 muestra que las únicas son $x^2 + 5y^2$ y $2x^2 + 2xy + 3y^2$, que corresponden a los látices $[1, \frac{\sqrt{-20}}{2}] = [1, \sqrt{-5}]$ y $[2, \frac{-2+\sqrt{-20}}{2}] = [2, -1 + \sqrt{-5}] =$

$[2, 1+\sqrt{-5}]$ respectivamente, por lo que esos serán los únicos látices con multiplicación compleja por $\sqrt{-5}$ salvo homotecia.

El Teorema 2.1 también nos permite calcular $j(L)$ para L un látice con multiplicación compleja por α, pero antes veamos el siguiente lema:

Lema 3.3. *Si tenemos el siguiente producto de expansiones de Laurent:*

$$\left(a_2z^2 + a_4z^4 + a_6z^6 + \cdots\right)\left(b_{-2}z^{-2} + b_0 + b_2z^2 + \cdots\right) = 1$$

entonces $b_{-2} = 1/a_2$, $b_0 = -a_4/a_2^2$ *y* $b_2 = a_4^2/a_2^3 - a_6/a_2^2$.

Demostración: Comparando coeficientes de z^l vemos que:

- $l = 0 : a_2b_{-2} = 1$, por lo que $b_{-2} = 1/a_2$.
- $l = 2 : a_2b_0 + a_4b_{-2} = 0$, por lo que $b_0 = -a_4b_{-2}/a_2 = -a_4/a_2^2$.
- $l = 4 : a_4b_0 + a_2b_2 + a_6b_{-2} = 0$, por lo que $b_2 = (-a_6b_{-2} - a_4b_0)/a_2 = a_4^2/a_2^3 - a_6/a_2^2$.

□

Ejemplo 3.4 (Cálculo de $j(L)$ para L con multiplicación compleja)**.**

(1) Consideremos multiplicación compleja por i. Siguiendo la misma idea que antes, se puede ver que $L = [1, i]$ es el único látice salvo homotecia, y como $iL = L$ vemos que

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

por lo que $g_3(L) = 0$ y así $j(L) = j(i) = 1728$.

(2) Si $L = [1, \omega]$, con $\omega = e^{2\pi i/3}$ entonces, como $\omega L = L$, tenemos que

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

por lo que $g_2(L) = 0$ y así $j(L) = j(\omega) = 0$.

(3) Un caso más interesante se consigue considerando multiplicación compleja por $\sqrt{-2}$. Siguiendo la misma idea que antes, se puede ver que $L = [1, \sqrt{-2}]$ es el único látice involucrado salvo homotecia, y usando el Teorema 2.1 mostraremos que $j(\sqrt{-2}) = 8000$.

En efecto, notemos que $L = [1, \sqrt{-2}]$ no tiene multiplicación compleja por i ni por ω, pues $i, \omega \notin \mathbb{Z} + \mathbb{Z}\sqrt{-2}$, por lo tanto $g_2(L)$ y $g_3(L)$ son distintos de cero. Además, como

$$\frac{g_2(\lambda L)}{g_3(\lambda L)} = \frac{\lambda^{-4}g_2(L)}{\lambda^{-6}g_3(L)} = \lambda^2 \cdot \frac{g_2(L)}{g_3(L)}$$

y $\frac{g_2(L)}{g_3(L)}$ es un número fijo distinto de 0, existe $\lambda \in \mathbb{C}$ tal que $\frac{g_2(\lambda L)}{g_3(\lambda L)} = \frac{20}{28}$, y por lo tanto $g_2(\lambda L) = 20g$ y $g_3(\lambda L) = 28g$ para algún $g \in \mathbb{C}^\times$. Además, considerando $L' = \lambda L$, como $N(\sqrt{-2}) = 2$, el Teorema 2.1 nos dice que

$$\wp(\sqrt{-2}z; L') = \frac{A(\wp(z; L'))}{B(\wp(z; L'))}$$

donde $A(x)$ es un polinomio cuadrático y $B(x)$ es lineal. Haciendo la división de polinomios llegamos a que

$$\wp(\sqrt{-2}z; L') = a\wp(z; L') + b + \frac{1}{c\wp(z; L') + d}$$

con a, b, c, $d \in \mathbb{C}$, y tanto a como c son distintos de cero. Consideremos ahora la expansión de Laurent de $\wp(z; L')$ cerca de $z = 0$:

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

donde usamos que $a_3 = \frac{a_1^3}{3} = \frac{g_2^2}{1200}$ por el Lema 0.1 de CM 7.

Así, usando que $g_2(L') = 20g$ y $g_3(L') = 28g$ tenemos que

$$\wp(z; L') = \frac{1}{z^2} + gz^2 + gz^4 + \frac{g^2}{3}z^6 + \cdots$$

y por lo tanto

$$\wp(\sqrt{-2}z; L') = \frac{-1}{2z^2} - 2gz^2 + 4gz^4 - \frac{8g^2}{3}z^6 + \cdots$$

y como sabíamos que $\wp(\sqrt{-2}z;L') = a\wp(z;L')+b+\frac{1}{c\wp(z;L')+d}$, comparando los coeficientes de z^{-2} y z^0 vemos que $a=-1/2$ y $b=0$. De esto concluimos que

$$\left(\wp(\sqrt{-2}z;L')+\frac{1}{2}\wp(z;L')\right)^{-1} = \left(-\frac{3g}{2}z^2+\frac{9g}{2}z^4-\frac{5g^2}{2}z^6+\cdots\right)^{-1}$$
$$= -\frac{2}{3gz^2}-\frac{2}{g}+\left(\frac{10}{9}-\frac{6}{g}\right)z^2+\cdots$$

donde la segunda igualdad es por el Lema 3.3, ya que aqui $a_2=-3g/2$, $a_4=9g/2$ y $a_6=-5g^2/2$, por lo que

$$b_{-2}=-\frac{2}{3g}\quad,\quad b_0=-\frac{\frac{9g}{2}}{\left(-\frac{3g}{2}\right)^2}=-\frac{2}{g}\quad,\quad b_2=\frac{\left(\frac{9g}{2}\right)^2}{\left(-\frac{3g}{2}\right)^3}-\frac{-\frac{5g^2}{2}}{\left(-\frac{3g}{2}\right)^2}=\frac{10}{9}-\frac{6}{g}$$

y como $(\wp(\sqrt{-2}z;L')+(1/2)\wp(z;L'))^{-1}=c\wp(z)+d$, comparando coeficientes de z^{-2} y z^0 vemos que $c=-2/(3g)$ y $d=-2/g$, y comparando coeficientes de z^2 en esta última igualdad vemos que

$$\frac{10}{9}-\frac{6}{g}=\frac{-2}{3g}g$$

y despejando g obtenemos $g=27/8$, por lo que $g_2(L')=20g=\frac{5\cdot 27}{2}$ y $g_3(L')=28g=\frac{7\cdot 27}{2}$, de donde concluimos que

$$j(\sqrt{-2})=1728\frac{\left(\frac{5\cdot 27}{2}\right)^3}{\left(\frac{5\cdot 27}{2}\right)^3-27\left(\frac{7\cdot 27}{2}\right)^2}=1728\frac{5^3}{5^3-2\cdot 7^2}=20^3=8000$$

Observación 3.5. Notemos que el cálculo hecho en 3.4 (3) se puede hacer de manera abstracta para α con $N(\alpha)=2$, y tal que exista un látice L con multiplicación por α.

Siguiendo la misma idea del ejemplo, podemos elegir λ conveniente tal que $g_2(L')=20g$, $g_3(L')=28g$ para algún $g\in\mathbb{C}^\times$, donde $L'=\lambda L$. Y como $N(\alpha)=2$, $\wp(\alpha z;L')=a\wp(z)+b+\frac{1}{c\wp(z)+d}$ para algunos a, b, c, $d\in\mathbb{C}$, a y c distintos de cero. Comparando coeficientes vemos que $a=1/(\alpha^2)$ y $b=0$, y luego

$$(\wp(\alpha z)-a\wp(z)-b)^{-1} = \left(g\left(\alpha^2-\frac{1}{\alpha^2}\right)z^2+g\left(\alpha^4-\frac{1}{\alpha^2}\right)z^4+\frac{g^2}{3}\left(\alpha^6-\frac{1}{\alpha^2}\right)z^6+\cdots\right)^{-1}$$
$$= \frac{\alpha^2}{g(\alpha^2-1)z^2}-\frac{\alpha^2(\alpha^4+\alpha^2+1)}{g(\alpha^2-1)(\alpha^2+1)^2}$$
$$+\alpha^2\left(\frac{(\alpha^4+\alpha^2+1)^2}{g(\alpha^2+1)^3(\alpha^2-1)}-\frac{\alpha^4+1}{3(\alpha^4-1)}\right)z^2+\cdots$$

donde usamos el Lema 2.3, y comparando coeficientes de z^{-2} y z^0 vemos que $c=\frac{\alpha^2}{g(\alpha^2-1)}$ y $d=-\frac{\alpha^2(\alpha^4+\alpha^2+1)}{g(\alpha^2-1)(\alpha^2+1)^2}$, y comparando coeficientes de z^2 vemos que

$$\alpha^2\left(\frac{(\alpha^4+\alpha^2+1)^2}{g(\alpha^2+1)^3(\alpha^2-1)}-\frac{\alpha^4+1}{3(\alpha^4-1)}\right)=\frac{\alpha^2}{g(\alpha^2-1)}\cdot g$$

y despejando g se obtiene

$$g=\frac{3(\alpha^4+\alpha^2+1)^2}{(\alpha^2+1)^2(\alpha^4+4)}$$

Ejemplo 3.6 (Cálculo de $j(L)$ para L con multiplicación compleja 2.0)**.** Si consideramos multiplicación compleja por $\alpha=\frac{1+\sqrt{-7}}{2}$, podemos ver que el único látice involucrado salvo homotecia es $L=[1,\frac{1+\sqrt{-7}}{2}]$ y nuevamente $N(\alpha)=2$. Usando la formula encontrada arriba para g tenemos que $g=7/4$, por lo tanto $g_2(L')=(7/4)\cdot 20=35$ y $g_3(L')=(7/4)\cdot 28=49$, por lo que

$$j\left(\frac{1+\sqrt{-7}}{2}\right)=1728\frac{35^3}{35^3-27\cdot 49^2}=1728\frac{5^3}{5^3-27\cdot 7}=(-15)^3=-3375$$

En los todos los ejemplos que hemos visto $j(L)$ es un entero, pero sabemos que $j:\mathbb{H}\to\mathbb{C}$ es sobreyectiva por lo que esto claramente no ocurre siempre. Sin embargo, el siguiente teorema nos permite probar que si L es un látice con multiplicación compleja entonces $j(L)$ es un número algebraico.

Teorema 3.7. *Sea $\mathcal{O}$ un orden en un cuerpo cuadrático imaginario. Si $\mathfrak{a}$ es un ideal fraccionario propio de $\mathcal{O}$ entonces $j(\mathfrak{a})$ es un número algebraico de grado a lo más $h(\mathcal{O})$.*

Demostración: Sean $g_2 = g_2(\mathfrak{a})$ y $g_3 = g_3(\mathfrak{a})$. Por el Lema 0.1 de CM 7, la expansión de Laurent de $\wp(z)$ es

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} a_k(g_2, g_3) z^{2k}$$

donde los $a_k(g_2, g_3)$ son polinomios en g_2 y g_3 con coeficientes racionales. Para enfatizar esta dependencia de g_2 y g_3, escribiremos $\wp(z) = \wp(z; g_2, g_3)$. Como $\mathfrak{a}$ es ideal fraccionario propio de $\mathcal{O}$, para cada $\alpha \in \mathcal{O}$ tenemos que $\wp(\alpha z; g_2, g_3)$ es una función racional en $\wp(z; g_2, g_3)$:

$$\wp(\alpha z; g_2, g_3) = \frac{A(\wp(z; g_2, g_3))}{B(\wp(z; g_2, g_3))} \tag{3.4}$$

y por lo tanto su expansión de Laurent es

$$\wp(\alpha z; g_2, g_3) = \frac{1}{\alpha^2 z^2} + \sum_{k=1}^{\infty} a_k(g_2, g_3) \alpha^{2k} z^{2k}$$

por lo que podemos trabajar la igualdad (3.4) como una identidad en $\mathbb{C}((z))$. Ahora, dado σ un automorfismo de $\mathbb{C}$, este induce un automorfismo en $\mathbb{C}((z))$ actuando en los coeficientes, por lo que si aplicamos σ en la igualdad (3.4), como $a_k(g_2, g_3)$ son polinomios en g_2 y g_3, obtenemos que

$$\wp(\sigma(\alpha) z; \sigma(g_2), \sigma(g_3)) = \frac{A^\sigma(\wp(z; \sigma(g_2), \sigma(g_3)))}{B^\sigma(\wp(z; \sigma(g_2), \sigma(g_3)))} \tag{3.5}$$

donde $A^\sigma(x)$ y $B^\sigma(x)$ son los polinomios obtenidos al aplicar σ a los coeficientes de $A(x)$ y $B(x)$ respectivamente. Notemos también que, por Teorema 0.2 de CM 7, $g_2^3 - 27 g_3^2 \neq 0$, por lo que $\sigma(g_3)^3 - 27\sigma(g_3)^2 \neq 0$, y por Corolario 1.6 de CM 8 esto implica que existe un látice L tal que

$$g_2(L) = \sigma(g_2) \quad \text{y} \quad g_3(L) = \sigma(g_3)$$

Así, la igualdad (3.5) nos dice que

$$\wp(\sigma(\alpha) z; L) = \frac{A^\sigma(\wp(z; L))}{B^\sigma(\wp(z; L))}$$

y por lo tanto L tiene multiplicación compleja por $\sigma(\alpha)$, y como esto se cumple para todo $\alpha \in \mathcal{O}$, si llamamos $\mathcal{O}'$ al anillo de multiplicación compleja de L, tenemos que

$$\mathcal{O} = \sigma(\mathcal{O}) \subseteq \mathcal{O}'$$

y repitiendo el argumento, reemplazando σ por σ^{-1} y $\mathfrak{a}$ por L, vemos que $\mathcal{O}' \subseteq \mathcal{O}$, y por lo tanto $\mathcal{O} = \mathcal{O}'$ es el anillo de multiplicación compleja tanto de $\mathfrak{a}$ como de L. De aqui vemos que, por como encontramos L, $j(L) = \sigma(j(\mathfrak{a}))$, y como $\mathcal{O}$ es el anillo de multiplicación compleja de L, el Corolario 3.1 implica que hay $h(\mathcal{O})$ clases de látices con $\mathcal{O}$ como su anillo de multiplicación compleja, en particular hay a lo más $h(\mathcal{O})$ valores posibles para $j(L)$, y por ende para $\sigma(j(\mathfrak{a}))$. Por último, como σ era un automorfismo arbitrario de $\mathbb{C}$, tenemos que el conjunto

$$\{\sigma(j(\mathfrak{a})) \mid \sigma \text{ automorfismo de } \mathbb{C}\} \tag{3.6}$$

es finito, y por lo tanto $j(\mathfrak{a})$ debe ser un número algebraico, pues en caso contrario $j(\mathfrak{a})^n$ sería trascendental para todo $n \in \mathbb{N}$. De aqui podríamos encontrar un automorfismo σ_n de $\mathbb{C}$ tal que $\sigma_n(j(\mathfrak{a})) = j(\mathfrak{a})^n$ para todo n, y por ende el conjunto de (3.6) sería infinito. Esto prueba que $j(\mathfrak{a})$ es un número algebraico con polinomio minimal sobre $\mathbb{Q}$ de grado a lo más $h(\mathcal{O})$, que es lo que queríamos probar. □

Referencias

[1] David A. Cox *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication.* Wiley, second edition, 2013.

[2] H. M. Stark *Class numbers of complex quadratic fields*, in *Modular Functions of One Variable I*, Lecture Notes in Math. **320**, Springer-Verlag, Berlin, Heidelberg, and New York, 1973, pp. 153 – 174.

Email address: mebruna@uc.cl