Pontificia Universidad Católica de Chile
Facultad de Matemáticas
Departamento de Matemática

El teorema principal CM
Francisco Gallardo
03/05/2024

1 Introducción

Antes que nada, dado un orden imaginario $\mathcal{O}$, por "campo de clases" de $\mathcal{O}$ me referiré al ring class field de $\mathcal{O}$.

El teorema principal de este documento es el siguiente:

Teorema 1.1 (Teorema principal de la teoría de multiplicación compleja)**.** Sea $\mathcal{O}$ un orden en un campo cuadrático imaginario K, y sea $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionario propio. Luego el complejo $j(\mathfrak{a})$ es un entero algebraico y $K(j(\mathfrak{a}))$ es el campo de clases del orden $\mathcal{O}$.

2 Preliminares

Partimos con un teorema probado en la charla pasada.

Teorema 2.1 (Primos que escinden, Parte I)**.** Sea $n > 0$ un entero y L el campo de clases del orden $\mathbb{Z}[\sqrt{-n}] \subset \mathbb{Q}(\sqrt{-n})$. Si p es primo impar que no divide a n, entonces

$$p = x^2 + ny^2 \iff p \text{ escinde completamente en } L.$$

Proof. [C, Teorema 9.4]. □

Resulta que algo parecido sigue valiendo cuando estudiamos los primos de la forma $x^2 + xy + \frac{1+n}{4}y^2$. El ejercicio 9.3 del libro de Cox nos pide formular y probar este resultado. Obedientemente obtenemos:

Teorema 2.2 (Primos que escinden, Parte II)**.** Sea $n > 0$ entero con $-n \equiv 1 \bmod 4$. Sea L el campo de clases del orden $\mathcal{O}$ de discriminante $-n$ en $K = \mathbb{Q}(\sqrt{-n})$ (si n es libre de cuadrados, $\mathcal{O} = \mathcal{O}_K$). Si p es un primo impar que no divide a n, entonces

$$p = x^2 + xy + \left(\frac{1+n}{4}\right)y^2 \iff p \text{ escinde completamente en } L.$$

Proof. Sabemos que $-n = f^2 d_K$ donde f es el conductor de $\mathcal{O}$. Sea p un primo que no divide a n. Luego $p \nmid d_K$ así que p no ramifica y $p \nmid f$. Probaremos las mismas equivalencias que en la demostración del Teorema 2.1 en Cox, i.e, probaremos

$$\begin{aligned} p = x^2 + xy + \left(\frac{1+n}{4}\right)y^2 &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}},\ \mathfrak{p} \text{ principal en } \mathcal{O}_K \\ &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}},\ \mathfrak{p} \in P_{K,\mathbb{Z}}(f) \\ &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}},\ ((L/K)/\mathfrak{p}) = 1 \\ &\iff p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}},\ \mathfrak{p} \neq \overline{\mathfrak{p}},\ \mathfrak{p} \text{ escinde completamente en } L \\ &\iff p \text{ escinde completamente en } L. \end{aligned}$$

Veamos la primera equivalencia. Sea $w = \frac{1+\sqrt{-n}}{2}$. Si $p = x^2 + xy + \left(\frac{1+n}{4}\right)$, entonces $p = (x + wy)(x + \overline{w}y)$. Sea $\mathfrak{p} = (x + wy)\mathcal{O}$. Este ideal es primo pues tiene norma igual a p. Luego $\mathfrak{p}\overline{\mathfrak{p}}$ es la factorización prima de p en $\mathcal{O}_K$ y $\mathfrak{p} \neq \overline{\mathfrak{p}}$ pues p no ramifica en K. Por último, $\mathfrak{p}$ es principal por construcción. Para el converso, escribimos $\mathfrak{p} = (x + wy)\mathcal{O}_K$ y entonces

$$p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}} = (x + wy)(x + \overline{w}y)\mathcal{O}_K = (x^2 + xy + \left(\frac{1+n}{4}\right) y^2)\mathcal{O}_K.$$

Así, $pu = x^2 + xy + \left(\frac{1+n}{4}\right) y^2$ para una unidad $u \in \mathcal{O}_K$. Pero el lado derecho es un número real positivo, así que $u = 1$ y obtenemos lo pedido.

Las siguientes equivalencias siguen igual que en el caso del Teorema 9.4 del Cox. □

Seguimos con un resultado que permite comparar extensiones de un campo de números mediante el conjunto de los primos que ramifican en las respectivas extensiones.

Sea K un campo de números y sea $\mathcal{P}_K$ el conjunto de todos los primos finitos de K, i.e, ideales primos de $\mathcal{O}_K$. Dada una extensión finita L/K definimos el conjunto

$$\mathcal{S}_{L/K} = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ escinde completamente en } L\}.$$

Si L no es Galois, con $\mathfrak{p}$ escinde completamente nos referimos a que $e_{\mathfrak{P}|\mathfrak{p}} = f_{\mathfrak{P}|\mathfrak{p}} = 1$ para todo $\mathfrak{P}$ en la factorización prima de $\mathfrak{p}\mathcal{O}_L$.

Por último, dados dos conjunto S y T, decimos que $S \mathrel{\dot{\subset}} T$ si $S \subset T \cup \Sigma$ para algún conjunto finito Σ, y decimos que $S \doteq T$ si $S \mathrel{\dot{\subset}} T$ y $T \mathrel{\dot{\subset}} S$.

Proposición 2.3. Sean L y M extensiones finitas de K.

(a) Si M/K es Galois, entonces $L \subset M \iff \mathcal{S}_{M/K} \mathrel{\dot{\subset}} \mathcal{S}_{L/K}$.

(b) Si L/K es Galois, entonces $L \subset M \iff \tilde{\mathcal{S}}_{M/K} \mathrel{\dot{\subset}} \mathcal{S}_{L/K}$ donde

$$\tilde{\mathcal{S}}_{M/K} := \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ no ramifica en } M \text{ y } f_{\mathfrak{P}/\mathfrak{p}} = 1 \text{ para algún } \mathfrak{P} \supset \mathfrak{p}\mathcal{O}_M\}$$

Proof. [C, Proposición 8.20]. □

Notemos que si L y M son Galois sobre K, entonces $L = K$ si y solo si $\mathcal{S}_{M/K} \doteq \mathcal{S}_{L/K}$.

Uno de los ingredientes principales en la demostración es la *ecuación modular*. La construcción de esta y sus propiedades están explicadas en el libro de Cox. Sin embargo, es harto trabajo y no la incluiré en este documento. Enunciaremos sus propiedades a continuación.

Empezamos definiendo un conjunto particular matrices. Dado m un entero positivo, definimos

$$C(m) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : ad = m,\ a > 0,\ 0 \leq b < d,\ \gcd(a, b, d) = 1 \right\}.$$

Además, recordemos que para un complejo $\tau \in \mathfrak{h}$ (semiplano superior complejo), definimos $j(\tau) := j([1, \tau])$.

Teorema 2.4. Dado un entero $m > 0$, existe un polinomio $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$ tal que:

(a) Si $\tau \in \mathfrak{h}$, entonces $\Phi_m(X, j(\tau)) = \prod_{\sigma \in C(m)} (X - j(\sigma\tau))$.

(b) $\Phi_m(X, Y)$ es irreducible como polinomio en X.

(c) $\Phi_m(X, Y) = \Phi_m(Y, X)$ si $m > 1$.

(d) Si m no es un cuadrado perfecto, entonces $\Phi_m(X, X)$ es un polinomio de grado superior a 1 cuyo coeficiente líder es ± 1.

(e) Si $m = p$ es primo, entonces

$$\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \bmod p\mathbb{Z}[X,Y]$$

Proof. [C, §11]. □

La *ecuación modular de peso* m es la ecuación

$$\Phi_m(X,Y) = 0.$$

En la siguiente sección estudiaremos las soluciones de la ecuación modular.

3 Subretículos cíclicos

Dado un retículo $L \subset \mathbb{C}$, decimos que un subretículo $L' \subset L$ es *cíclico de índice* m si $L/L' \cong \mathbb{Z}/m\mathbb{Z}$. El resultado principal de esta sección es el siguiente:

Teorema 3.1 (Soluciones de la ecuación modular)**.** Sea m un entero positivo. Si $u, v \in \mathbb{C}$, entonces $\Phi_m(u,v) = 0$ si y solo si existe un retículo L y un subretículo $L' \subset L$ cíclico de índice m tales que $u = j(L')$ y $v = j(L)$.

Antes de la demostración necesitamos el siguiente lema.

Lemma 3.2. Sea $\tau \in \mathfrak{h}$ y considere el retículo $[1,\tau]$. Sea $L' \subset [1,\tau]$ un subretículo. Las siguientes son equivalentes:

(a) $L' \subset [1,\tau]$ es cíclico de índice m.

(b) Existe un único $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$ tal que $L' = d[1, \sigma\tau]$.

Proof. Un subretículo $L' \subset L$ se puede escribir como $[a\tau + b, c\tau + d]$. Por el Corolario 5.3 del apéndice de álgebra lineal tenemos que L' es cíclico de índice m si y solo si $\gcd(a,b,c,d) = 1$ y $|ad - bc| = m$.

Supongamos que $L' \subset L$ es cíclico de índice m. Afirmo que L' se puede escribir de la forma $[d, a\tau + b]$ donde d es el entero positivo más pequeño en L'. Como $m \in L'$, $L' \cap \mathbb{Z}$ es no trivial y entonces $L' \cap \mathbb{Z} = d\mathbb{Z}$. Es claro que d es el entero más pequeño en L'. Ahora, L' tiene rango 2 así que $L'/d\mathbb{Z}$ tiene rango 1. Probemos que además dicho cociente es libre de torsión. Si $m \neq 0$ y $\alpha = a\tau + b \in L'$ cumple $m\alpha \in d\mathbb{Z}$, entonces $ma\tau + mb \in d\mathbb{Z}$ y se deduce que $a = 0$. Pero luego $\alpha = b \in L' \cap \mathbb{Z} = d\mathbb{Z}$ y prueba que $L'/d\mathbb{Z}$ es libre de torsión. Esto implica que $L'/d\mathbb{Z} \cong \mathbb{Z}$. Finalmente, si escogemos $\alpha \in L'$ que se mapee al generador de $\mathbb{Z} \cong L'/d\mathbb{Z}$, entonces obtenemos $L' = d\mathbb{Z} + \alpha\mathbb{Z}$, i.e, $L' = [d, \alpha]$. Como $L' \subset [1,\tau]$ podemos escoger $\alpha = a\tau + b$ para algún $a, b \in \mathbb{Z}$.

Podemos asumir $a > 0$ y entonces $ad = |ad| = |ad - b \cdot 0| = m$. Restando un múltiplo apropiado de d a $a\tau + b$ podemos asumir que $0 \le b < d$. Además, $\gcd(a,b,d) = 1$ puesto que $L' \subset L$ es cíclico. Esto muestra que $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in C(m)$. Luego

$$L' = [d, a\tau + b] = d\left[1, \frac{a\tau + b}{d}\right] = d[1, \sigma\tau].$$

Ahora supongamos que $L' = d[1,\sigma\tau] = d'[1,\sigma'\tau]$ para $\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $\sigma' = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \in C(m)$. Luego $[d, a\tau + b] = L' = [d', a'\tau + b']$. Esta igualdad implica inmediatamente que $d = d'$, puesto que d es el entero más pequeño en $[d, a\tau + b] = L'$ y d' también. Como $a'd' = ad = m$, sigue que $a = a'$. Luego

$$[d, a\tau + b] = [d, a\tau + b'].$$

Pero entonces
$$b' - b = a\tau + b' - (a\tau + b) \in [d, a\tau + b].$$
Como d es el entero más pequeño en L', $d \mid (b' - b)$ y como $0 \leq b, b' < d$ se deduce que $b' = b$. Con esto terminamos (a) $\Longrightarrow$ (b).

(b) $\Longrightarrow$ (a) es evidente por el primer párrafo, ya que una matriz en $C(m)$ satisface las propiedades necesarias para ser un subretículo cíclico de índice m. $\square$

Ahora sí vamos a la demostración del Teorema 3.1.

Proof. Por el lema anterior, si $L' = d[1, \sigma\tau] \subset [1, \tau] = L$ es un subretículo cíclico de índice m, entonces
$$j(L') = j(d[1, \sigma\tau]) = j([1, \sigma\tau]) = j(\sigma\tau).$$
Por el Teorema 2.4.(a), $\Phi_m(j(L'), j(L)) = \Phi_m(j(\sigma\tau), j(\tau)) = 0$ y deducimos que las soluciones de $\Phi_m(X, j(\tau))$ son exactamente los $j(L')$ para subretículos $L' \subset [1, \tau]$ cíclicos de índice m.

Si $u, v \in \mathbb{C}$ son tales que $\Phi_m(u, v) = 0$, usamos la sobreyectividad de $j\colon \mathfrak{h} \to \mathbb{C}$ para encontrar $\tau \in \mathfrak{h}$ tal que $v = j(\tau) = j([1, \tau])$. Luego $u = j(L')$ para un subretículo cíclico de índice m en $[1, \tau]$ por la parte anterior y el teorema está demostrado. $\square$

Para probar el Teorema Principal 1.1 aplicaremos la ecuación modular a retículos con multiplicación compleja. El punto clave es que dicho retículos tienen subretículos cíclicos especialmente interesantes. Necesitaremos la noción de ideal primitivo.

Dado un orden imaginario $\mathcal{O}$, un $\mathcal{O}$-ideal propio es *primitivo* si no es de la forma $d\mathfrak{a}$ para un entero $d > 1$ y un $\mathcal{O}$-ideal propio $\mathfrak{a}$. La relación entre ideales primitivos y subretículos cíclicos viene dada por el siguiente lema:

Lemma 3.3 (Subretículos de un $\mathcal{O}$-ideal fraccionario propio)**.** Sea $\mathcal{O}$ un orden imaginario y sea $\mathfrak{b}$ un $\mathcal{O}$-ideal fraccionario propio. Luego dado un $\mathcal{O}$-ideal propio $\mathfrak{a}$, $\mathfrak{a}\mathfrak{b}$ es un subretículo de $\mathfrak{b}$ de índice $N(\mathfrak{a})$, y es cíclico si y solo si $\mathfrak{a}$ es primitivo.

Proof. Podemos asumir $\mathfrak{b} \subset \mathcal{O}$ reemplazando posiblemente por un múltiplo de $\mathfrak{b}$. Luego la secuencia exacta
$$0 \longrightarrow \mathfrak{b}/\mathfrak{a}\mathfrak{b} \longrightarrow \mathcal{O}/\mathfrak{a}\mathfrak{b} \longrightarrow \mathcal{O}/\mathfrak{b} \longrightarrow 0$$
implica que $[\mathfrak{b} : \mathfrak{a}\mathfrak{b}]N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$, de modo que $[\mathfrak{b} : \mathfrak{a}\mathfrak{b}] = N(\mathfrak{a})$.

Supongamos que $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ no es cíclico. Ahora, por el teorema de clasificación de grupos abelianos finitos debe ocurrir que $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ contiene un subgrupo isomorfo a $(\mathbb{Z}/d\mathbb{Z})^2$ para un entero $d > 1$, es decir, existe un subretículo $\mathfrak{b}'$ que cumple $\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}' \subset \mathfrak{b}$ y $\mathfrak{b}'/\mathfrak{a}\mathfrak{b} \cong (\mathbb{Z}/d\mathbb{Z})^2$. Nótese que $d\mathfrak{b}' \subset \mathfrak{a}\mathfrak{b}$ y como $\mathfrak{b}'$ es libre de rango 2, $\mathfrak{b}'/d\mathfrak{b}' \cong (\mathbb{Z}/d\mathbb{Z})^2$. Esto implica que $d\mathfrak{b}' = \mathfrak{a}\mathfrak{b}$ y entonces $\mathfrak{a} = d\mathfrak{b}'\mathfrak{b}^{-1}$. Como $\mathfrak{b}' \subset \mathfrak{b}$, $\mathfrak{b}'\mathfrak{b}^{-1} \subset \mathfrak{b}\mathfrak{b}^{-1} = \mathcal{O}$ y entonces $\mathfrak{a}$ no es primitivo (es igual a $d > 1$ veces el ideal $\mathfrak{b}'\mathfrak{b}^{-1}$).

Ahora supongamos que $\mathfrak{a}$ no es primitivo y sea $d > 1$ entero tal que $\mathfrak{a} = d\mathfrak{a}'$ para un $\mathcal{O}$-ideal propio $\mathfrak{a}'$. Como $\mathfrak{a}'\mathfrak{b}$ el libre de rango 2, $\mathfrak{a}'\mathfrak{b}/\mathfrak{a}\mathfrak{b} = (\mathfrak{a}'\mathfrak{b})/d(\mathfrak{a}'\mathfrak{b}) \cong (\mathbb{Z}/d\mathbb{Z})^2$ y entonces la contención $\mathfrak{a}'\mathfrak{b}/\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}/\mathfrak{a}\mathfrak{b}$ implica que $\mathfrak{b}/\mathfrak{a}\mathfrak{b}$ no es cíclico. $\square$

Cuando apliquemos este lema, $\mathfrak{a}$ solerá ser un ideal principal $\alpha\mathcal{O}$. En este caso, $\alpha\mathcal{O}$ es primitivo si y solo si el elemento α es primitivo, i.e, no es divisible por $d > 1$ en $\mathcal{O}$. Usando además que $N(\alpha\mathcal{O}) = N(\alpha)$ obtenemos el siguiente corolario de nuestro lema:

Corolario 3.4. Sea $\mathcal{O}$ un orden imaginario y $\mathfrak{b}$ un $\mathcal{O}$-ideal fraccionario propio. Luego, dado $\alpha \in \mathcal{O}$, $\alpha\mathfrak{b}$ es un subretículo de índice $N(\alpha)$ y es cíclico si y solo si α es primitivo.

4 Demostración

Ha llegado la hora de la demostración del Teorema Principal 1.1.

Proof. Sea $\mathfrak{a}$ un $\mathcal{O}$-ideal fraccionario propio, donde $\mathcal{O}$ es un orden en campo cuadrático imaginario K. Debemos probar que

(i) $j(\mathfrak{a})$ es un entero algebraico.

(ii) $K(j(\mathfrak{a}))$ es el campo de clases de $\mathcal{O}$.

Para (i) usaremos la ecuación modular. Sea f el conductor de $\mathcal{O}$, de modo que $\mathcal{O} = [1, fw_K]$. Luego $\alpha := fw_K \in \mathcal{O}$ es primitivo (obviamente) y $N(\alpha) = \frac{f^2 d_K(d_K-1)}{4}$ no es cuadrado. Ciertamente, si $N(\alpha) = c^2$, entonces

$$f^2 d_K(d_K - 1) = (2c)^2.$$

Como $f^2 \mid (2c)^2$, $f \mid 2c$ y entonces

$$d_K(d_K - 1) = \left(\frac{2c}{f}\right)^2.$$

Pero al menos alguno entre $|d_K|$ y $|d_K - 1|$ no es un cuadrado y además son coprimos, así que su producto no es un cuadrado, contradicción.

Como nuestro α es primitivo, se sigue que $\alpha\mathfrak{a} \subset \mathfrak{a}$ es un subretículo cíclico de índice $m := N(\alpha)$.

Luego por el Teorema 3.1 sigue que

$$\Phi_m(j(\mathfrak{a}), j(\mathfrak{a})) = \Phi_m(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = 0$$

donde usamos que $j(\alpha\mathfrak{a}) = j(\mathfrak{a})$ ($\mathfrak{a}$ y $\alpha\mathfrak{a}$ son evidentemente homotéticos).

Por el Teorema 2.4, $\Phi_m(X, X) \in \mathbb{Z}[X]$ y es mónico pues $m = N(\alpha)$ no es un cuadrado (ahá!). Esto prueba que $j(\mathfrak{a})$ es un entero algebraico.

Ahora pasaremos a la demostración de (ii). Sea L el campo de clases de $\mathcal{O}$ y sea $M = K(j(\mathfrak{a}))$. Para probar $L = M$ estudiaremos los conjuntos $\mathcal{S}_{L/\mathbb{Q}}$ y $\mathcal{S}_{M/\mathbb{Q}}$ en vista de la Proposición 2.3.

Partimos afirmando que

$$\mathcal{S}_{L/\mathbb{Q}} \doteq \{p \text{ primo} : p = N(\alpha) \text{ para algún } \alpha \in \mathcal{O}\}. \tag{1}$$

Demostración de (1): Sea f el conductor de $\mathcal{O}$ y $D = f^2 d_K < 0$ su discriminante. Supongamos primero que $D \equiv 0 \bmod 4$. Afirmo que $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ para un entero positivo n. Ciertamente, si $4 \mid d_K$, entonces $\mathcal{O}_K = \mathbb{Z}[\sqrt{d_K/4}]$ y luego $\mathcal{O} = \mathbb{Z}[\sqrt{f^2 d_K/4}]$. Haciendo $n = -f^2 d_K/4$ obtenemos la afirmación. Si $4 \nmid d_K$, entonces $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{d_K})/2]$. La condición $4 \mid D$ obliga entonces a que f sea par y esto obliga a su vez a que $\mathcal{O} = \mathbb{Z}[\sqrt{(f/2)^2 d_K}]$. Nuevamente, haciendo $n = -f^2 d_K/4$ obtenemos la afirmación. Prosigamos. Por el Teorema 2.1, salvo que p divida a n o $p = 2$, p escinde completamente en L si y solo si $p = x^2 + ny^2 = N(\alpha)$, con $\alpha = x + y\sqrt{-n} \in \mathcal{O}$. Esto prueba nuestra afirmación en este caso.

Si $D \equiv 1 \bmod 4$, entonces $n := -D$ es positivo, congruente a 3 módulo 4 y $\mathcal{O}$ es el orden de discriminante $-n$ en $\mathbb{Q}(\sqrt{-n})$. Luego aplicamos el Teorema 2.2 y obtenemos que, salvo que $p \mid -n$ o $p = 2$, p escinde completamente en L si y solo si $p = x^2 + xy + \left(\frac{1+n}{4}\right) y^2 = N(\alpha)$, donde $\alpha = x + \left(\frac{1+\sqrt{-n}}{2}\right) y \in \mathcal{O}$. Esto demuestra la afirmación en el caso que faltaba.

Sigamos con la demostración. En la charla pasada vimos que $L/\mathbb{Q}$ es Galois, así que la Proposición 2.3 nos dice que $L \subset M$ si y solo si $\mathcal{S}_{L/\mathbb{Q}} \dot{\subset} \mathcal{S}_{M/\mathbb{Q}}$.

Tomemos $p \in \mathcal{S}_{L/\mathbb{Q}}$ y asumamos que p no ramifica (solo finitos primos lo hacen así que no hay problema). Por la Proposición 5.4 (ver apéndice), tenemos que $N := [\mathcal{O}_M : \mathcal{O}_K[j(\mathfrak{a})]]$ es finito, así que excluyamos también los divisores de N.

Por la afirmación (1), $p = N(\alpha)$ para un $\alpha \in \mathcal{O}$. Luego α es primitivo pues su norma es un primo y entonces $\alpha\mathfrak{a} \subset \mathfrak{a}$ es un subretículo cíclico de índice p. Por el Teorema 3.1

$$\Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) = \Phi_p(j(\alpha\mathfrak{a}), j(\mathfrak{a})) = 0$$

y la parte (e) del Teorema 2.4 nos dice que

$$0 = \Phi_p(j(\mathfrak{a}), j(\mathfrak{a})) = -(j(\mathfrak{a})^p - j(\mathfrak{a}))^2 + pQ(j(\mathfrak{a}), j(\mathfrak{a}))$$

para $Q \in \mathbb{Z}[X, Y]$. Como $j(\mathfrak{a}) \in \mathcal{O}_M$, $Q(j(\mathfrak{a}), j(\mathfrak{a})) \in \mathcal{O}_M$.

Ahora sea $\mathfrak{P}$ un primo en M que contiene a p. Luego $p\beta \in p\mathcal{O}_M \supset \mathfrak{P}$ y entonces la última ecuación implica

$$j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{P}. \tag{2}$$

Como p escinde completamente en L, lo hace ya en M y entonces $p \in \mathfrak{p} \subset \mathfrak{P}$ para algún ideal $\mathfrak{p}$ de norma p. Esto implica $\alpha^p \equiv \alpha \bmod \mathfrak{P}$ para todo $\alpha \in \mathcal{O}_K$ y junto con (2) obtenemos que la misma congruencia vale para todo $\alpha \in \mathcal{O}_K[j(\mathfrak{a})]$. Como $p \nmid N$, la parte (b) de la Proposición 5.4 indica que la misma congruencia vale para todo $\alpha \in \mathcal{O}_M$. Luego $\alpha \mapsto \alpha^p$ es la identidad en $\mathcal{O}_M/\mathfrak{P}$, de modo que $|\mathcal{O}_M/\mathfrak{P}| = p$ y entonces $f_{\mathfrak{P}/p} = 1$. Como $\mathfrak{P}$ era cualquiera que contiene a p sigue que p escinde completamente en M. Esto muestra $\mathcal{S}_{L/\mathbb{Q}} \dot{\subset} \mathcal{S}_{M/\mathbb{Q}}$ y $M \subset L$ en última instancia.

Lo que acabamos de probar no solo muestra que $M \subset L$ sino que $j(\mathfrak{a}) \in L$ para **todos** los $\mathcal{O}$-ideales fraccionarios y propios $\mathfrak{a}$. Sea $h = h(\mathcal{O})$ y sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_h$ representantes de clases en $\mathcal{O}$. Luego $j(\mathfrak{b})$ (para cualquier $\mathfrak{b}$) es igual a algún $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$ y además los $j(\mathfrak{a}_1), \ldots, j(\mathfrak{a}_h)$ son todos distintos. De esta forma

$$\Delta := \prod_{i<j}(j(\mathfrak{a}_i) - j(\mathfrak{a}_j))$$

es elemento no nulo de $\mathcal{O}_L$ (observación que usaremos después).

Para probar la inclusión $L \subset M$ usaremos el criterio

$$\tilde{\mathcal{S}}_{M/\mathbb{Q}} \dot{\subset} \mathcal{S}_{L/\mathbb{Q}}$$

de la Proposición 2.3. Sea entonces $p \in \tilde{\mathcal{S}}_{M/\mathbb{Q}}$, i.e, p no ramifica en M y $f_{\mathfrak{P}/p} = 1$ para algún primo $\mathfrak{P}$ en $\mathcal{O}_M$ que contiene a p. Asumamos además que $p \nmid f$ y p, Δ son coprimos en $\mathcal{O}_L$. Estas suposiciones adicionales solo excluyen finitos primos, ya que pedir p, Δ coprimos en $\mathcal{O}_L$ es lo mismo que pedir $p \nmid d$ con $\Delta\mathcal{O}_L \cap \mathbb{Z} = d\mathbb{Z}$ (posiblemente $d = 0$). Tomamos un $\mathfrak{p}$ en $\mathcal{O}_K$ tal que $p \in \mathfrak{p} \subset \mathfrak{P}$ y notamos que $f_{\mathfrak{p}|p} = 1$ pues $f_{\mathfrak{P}|p} = 1$. Luego $N(\mathfrak{p}) = p$ con $\mathfrak{p} \in \mathcal{O}_K$.

De la charla anterior sigue que $\mathfrak{p} \cap \mathcal{O}$ es primo en $\mathcal{O}$ y de igual norma a $\mathfrak{p}$, i.e, $N(\mathfrak{p} \cap \mathcal{O}) = p$ (usamos $p \nmid f$). Si logramos probar que $\mathfrak{p} \cap \mathcal{O}$ es principal estamos listos, pues en dicho caso $p = N(\alpha) = N(\alpha\mathcal{O})$ para algún $\alpha \in \mathcal{O}$ y entonces $p \in \mathcal{S}_{L/\mathbb{Q}}$ por la afirmación (1).

Sea $\mathfrak{a}' = (\mathfrak{p} \cap \mathcal{O})\mathfrak{a}$. Para mostrar que $\mathfrak{p} \cap \mathcal{O}$ es principal, mostraremos que $[\mathfrak{a}'] = [\mathfrak{a}]$ en $\mathcal{O}$. Como $\mathfrak{p} \cap \mathcal{O}$ tiene norma p, $\mathfrak{a}' \subset \mathfrak{a}$ es un subretículo cíclico de índice p. Luego $\Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = 0$. Usando nuevamente la parte (e) del Teorema 2.4 obtenemos

$$0 = \Phi_p(j(\mathfrak{a}'), j(\mathfrak{a})) = (j(\mathfrak{a}')^p - j(\mathfrak{a}))(j(\mathfrak{a}') - j(\mathfrak{a})^p) + pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \tag{3}$$

para un polinomio $Q(X, Y) \in \mathbb{Z}[X, Y]$. Sea $\tilde{\mathfrak{P}}$ un primo en L que contiene a $\mathfrak{P}$. Como $j(\mathfrak{a}')$ y $j(\mathfrak{a})$ son enteros algebraicos en L, tenemos que $pQ(j(\mathfrak{a}'), j(\mathfrak{a})) \in p\mathcal{O}_L \subset \tilde{\mathfrak{P}}$. Por (3) deducimos que

$$j(\mathfrak{a}')^p \equiv j(\mathfrak{a}) \bmod \tilde{\mathfrak{P}} \quad \text{ o } \quad j(\mathfrak{a}') \equiv j(\mathfrak{a})^p \bmod \tilde{\mathfrak{P}}. \tag{4}$$

Como $f_{\mathfrak{P}|p} = 1$, $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{P}$ y como $\mathfrak{P} \subset \tilde{\mathfrak{P}}$ obtenemos $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \tilde{\mathfrak{P}}$. Juntando esto con (4) obtenemos

$$j(\mathfrak{a}') \equiv j(\mathfrak{a}) \bmod \tilde{\mathfrak{P}} \quad \text{ o } \quad j(\mathfrak{a}')^p \equiv j(\mathfrak{a})^p \bmod \tilde{\mathfrak{P}}.$$

Como el Frobenius es inyectivo, cualquiera de estas dos condiciones implica

$$j(\mathfrak{a}) \equiv j(\mathfrak{a}') \bmod \tilde{\mathfrak{P}}.$$

Si $[\mathfrak{a}] \neq [\mathfrak{a}'] \in \mathcal{O}$, luego $j(\mathfrak{a}) - j(\mathfrak{a}')$ sería un factor de Δ y entonces p y Δ no sería coprimos. Esto contradice nuestra elección de p. Por ende, $[\mathfrak{a}'] = [\mathfrak{a}] \in \mathcal{O}$ y esto era lo que mataba la demostración así que ganamos. $\square$

5 Apéndice

5.1 Álgebra Lineal

Proposición 5.1 (Forma normal de Smith)**.** Sea $A \in \mathrm{Mat}_{n\times n}(R)$ donde R un dominio de ideales principales. Luego existen $S, T \in \mathrm{GL}_n(R)$ tales que SAT es diagonal con entradas $d_1, \ldots, d_n$ que satisfacen:

(i) Los d_i son únicos salvo multiplicar por una unidad de R.

(ii) $d_1 \mid d_2 \mid \cdots \mid d_n$.

(iii) $d_i = \frac{D_i(A)}{D_{i-1}(A)}$ donde $D_0 = 1$ y D_i es el máximo común divisor de todos los determinantes de los $i \times i$-menores de A.

Proposición 5.2 (Cardinalidad del cokernel)**.** Sea $\phi \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^n)$ con $\det\phi \neq 0$ (o equivalentemente, inyectivo). Luego $|\operatorname{coker}\phi| = |\det\phi|$.

Proof. Sea $M = \mathbb{Z}^n$ y A una matriz representante para ϕ. Queremos probar que $|M/AM| = |\det A|$. Si $B \in \mathrm{GL}_n(\mathbb{Z})$ y el resultado vale para BA, entonces vale para A. Ciertamente $B\colon M \to M$ es un isomorfismo que lleva AM a BAM. Luego

$$|M/AM| = |M/BAM| = \det(BA) = \det B \det A = \det A.$$

Análogamente, si el resultado vale para AB, entonces vale para A. Esto nos permite cambiar A por SAT con $S, T \in \mathrm{GL}_n(\mathbb{Z})$. Escogiendo S y T sabiamente podemos llevar A a su forma normal de Smith.

Pero luego el resultado es obvio, puesto que $\operatorname{coker}\phi \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}$ y $\det\phi = d_1 \cdots d_n$. □

Corolario 5.3 (Caso $n = 2$)**.** Supongamos que $\phi \in \mathrm{End}_{\mathbb{Z}}(\mathbb{Z}^2)$ con $\det\phi \neq 0$ y sea $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ una matriz representante. Luego $\operatorname{coker}\phi$ es cíclico de orden m si y solo si $\gcd(a, b, c, d) = 1$ y $|ad - bc| = m$.

Proof. La condición en el determinante viene de la proposición anterior. Además, ninguna de las condiciones que se pide depende de la matriz representante. Ciertamente, el determinante no depende, y $\gcd(a, b, c, d) \neq 1$ si y solo si existe una matriz B y un entero $e > 1$ tal que $A = eB$. Cambiar de base no quitará el e del camino así que no cambiará la condición $\gcd(a, b, c, d) \neq 1$. Habiendo dicho esto, escogemos A representante de ϕ en su forma normal de Smith. Luego $A = \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}$ con $d_1 = \gcd(a, b, c, d)$ y $d_2 = \det(A)/d_1$. Se sigue que

$$\operatorname{coker}\phi \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z},$$

y entonces $\operatorname{coker}\phi$ es cíclico si y solo si $\gcd(a, b, c, d) = d_1 = 1$. □

Proposición 5.4. Sean $K \subset L$ campos de número y $\alpha \in \mathcal{O}_L$ tal que $L = K(\alpha)$.

(a) $N := [\mathcal{O}_L : \mathcal{O}_K[\alpha]] < \infty$.

(b) Sea $\mathfrak{P}$ un primo en $\mathcal{O}_L$ y suponga que $N(\mathfrak{P}) = p^f$ para $p \nmid N$. Si $\beta^p \equiv \beta \bmod \mathfrak{P}$ para todo $\beta \in \mathcal{O}_K[\alpha]$, entonces la misma congruencia vale para todo $\beta \in \mathcal{O}_L$.

Proof. Sea $m = [L : \mathbb{Q}]$, $n = [K : \mathbb{Q}]$ y $l = [L : K]$, de modo que $m = nl$. Luego $\mathcal{O}_L$ es un $\mathbb{Z}$-módulo libre de rango m y $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango n. Sea $\beta_1, \ldots, \beta_n$ una $\mathbb{Q}$-base de K. Luego

$$\{\beta_i\alpha^j : 1 \le i \le n,\ 1 \le j \le l\}$$

es una $\mathbb{Q}$-base de L de cardinalidad m y contenido en $\mathcal{O}_K[\alpha]$.

Además, como $\mathcal{O}_L$ es un módulo finito, $\mathcal{O}_K[\alpha]$ también. La $\mathbb{Q}$-base y la finita generación implican que $\mathcal{O}_K[\alpha]$ es libre de rango m. Como $\mathcal{O}_L$ también y $\mathcal{O}_K[\alpha] \subset \mathcal{O}_L$, obtenemos la parte (a).

Como $\gcd(p, N) = 1$, multiplicación por N es un automorfismo de $\mathcal{O}_L/\mathfrak{P}$. Dado $\beta \in \mathcal{O}_L$, podemos escoger entonces un $\beta' \in \mathcal{O}_L$ tal que $N\beta' \equiv \beta \bmod \mathfrak{P}$. Notemos que $N\beta' \in \mathcal{O}_K[\alpha]$ por definición de N. Luego

$$\beta^p \equiv (N\beta')^p \equiv N^p \beta'^p \equiv N\beta \equiv \beta \bmod \mathfrak{P}$$

La tercera equivalencia viene de la hipótesis y del hecho que $\gcd(p, N) = 1$.

$\square$

Bibliography

[C] D. A. Cox, *Primes of the form $x^2 + ny^2$*, 2nd ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013. Fermat, class field theory, and complex multiplication. MR3236783