EL PROBLEMA DE CONJUGACIÓN PARA MATRICES ENTERAS

GUIDO ARNONE

Teorema 1 ([3, Theorem]). *Sea α un entero algebraico y $\mathcal{O} = \mathbb{Z}[\alpha]$. Existe una correspondencia biyectiva entre ideales fraccionarios de $\mathcal{O}$ y clases de conjugación de matrices enteras con polinomio característico $m(\alpha, \mathbb{Q})$.*

1. Órdenes e ideales fraccionarios

Sea K una extensión finita de $\mathbb{Q}$ y $\mathcal{O}_\mathrm{K}$ su anillo de enteros. Un ***orden*** de K es un subanillo que como $\mathbb{Z}$-módulo tiene rango $[\mathrm{K} : \mathbb{Q}]$. Notar que $\mathsf{Frac}(\mathcal{O}) = \mathrm{K}$, ya que el primer cuerpo está contenido en el segundo y ambos tienen la misma $\mathbb{Q}$-dimensión. Un ***$\mathcal{O}$-ideal fraccionario*** es un $\mathcal{O}$-módulo $\mathrm{I} \subset \mathrm{K}$; siempre existe $x \in \mathcal{O}$ y un ideal $\mathrm{J} \trianglelefteq \mathcal{O}$ tal que $\mathrm{I} = \frac{1}{x}\mathrm{J}$.

Ejemplo 1.1. *Si α es un entero algebraico y $\mathrm{K} = \mathbb{Q}(\alpha)$, entonces $\mathbb{Z}[\alpha]$ es un orden de $\mathcal{O}_\mathrm{K}$. En particular $\mathbb{Z}[\sqrt{-5}]$ es un orden de $\mathbb{Q}(\sqrt{-5})$ que está contenido propiamente en su anillo de enteros $\mathbb{Z}[\frac{1+\sqrt{-5}}{2}]$.*

Dos $\mathcal{O}$-ideales fraccionarios I y J se dicen ***equivalentes*** si $\mathrm{I} = x\mathrm{J}$ para algún $x \in \mathrm{K} \setminus \{0\}$. Esta es una relación de equivalencia; notamos $\mathrm{ICM}(\mathcal{O})$ al conjunto de clases de equivalencia de ideales fraccionarios. La multiplicación de ideales define una estructura de monoide en este conjunto; notamos $\mathrm{Pic}(\mathcal{O})$ al grupo de elementos inversibles de $\mathrm{ICM}(\mathcal{O})$. En general, si $\mathcal{O} \neq \mathcal{O}_\mathrm{K}$, no todo ideal fraccionario es inversible.

Precisaremos los siguientes lemas sobre ideales fraccionarios más adelante.

Lema 1.2. *Sea K una extensión finita de $\mathbb{Q}$ y $\mathcal{O}$ un orden de K. Dos $\mathcal{O}$-ideales fraccionarios I y J son equivalentes si y sólo si son isomorfos como $\mathcal{O}$-módulos. Más aún, isomorfismo $\mathcal{O}$-lineal $\mathrm{I} \to \mathrm{J}$ está dado por la multiplicación por un elemento de $\mathrm{K} \setminus \{0\}$.*

Demostración. Si $\mathrm{I} = x\mathrm{J}$ para cierto $x \in \mathrm{K} \setminus \{0\}$, el morfismo $j \in \mathrm{J} \mapsto xj \in \mathrm{I}$ resulta un isomorfismo $\mathcal{O}$-lineal. Recíprocamente, supongamos que tenemos un isomorfismo $\mathcal{O}$-lineal $\varphi \colon \mathrm{I} \to \mathrm{J}$. Por la implicación ya demostrada, podemos suponer que $\mathrm{I}, \mathrm{J} \subset \mathcal{O}$, es decir que I y J son ideales de $\mathcal{O}$. Ahora, dado $x \in \mathrm{I}$ no nulo, para cada $i \in \mathrm{I}$ es

$$\varphi(x)i = \varphi(xi) = x\varphi(i).$$

Esto implica que φ coincide con el morfismo dado por la multiplicación por $\varphi(x)/x$. En particular tomando imágenes es $\mathrm{J} = \frac{\varphi(x)}{x}\mathrm{I}$. ⋇

Lema 1.3. *Sea K una extensión finita de $\mathbb{Q}$. Si $\mathcal{O}$ es un orden de K, todo $\mathcal{O}$-ideal fraccionario no nulo tiene rango $[\mathrm{K} : \mathbb{Q}]$ como $\mathbb{Z}$-módulo.*

Demostración. Sea I un $\mathcal{O}$-ideal fraccionario, que salvo isomorfismo $\mathcal{O}$-lineal (en particular, $\mathbb{Z}$-lineal) podemos suponer contenido en $\mathcal{O}$. Tensorizando por $\mathbb{Q}$ a la sucesión exacta $0 \to \mathrm{I} \hookrightarrow \mathcal{O} \twoheadrightarrow \mathcal{O}/\mathrm{I} \to 0$ vemos que $\operatorname{rk} \mathrm{I} = \operatorname{rk} \mathcal{O}$ si y sólo si $\operatorname{rk} \mathcal{O}/\mathrm{I} = 0$. Para ver esto último probaremos que $\mathcal{O}/\mathrm{I}$ es finito: dado $x \in \mathrm{I}$ no nulo tenemos un epimorfismo $\mathcal{O}/x\mathcal{O} \to \mathcal{O}/\mathrm{I}$; podemos asumir entonces que $\mathrm{I} = (x)$. Finalmente, el mismo argumento que en el caso $\mathcal{O} = \mathcal{O}_\mathrm{K}$ prueba que el cociente $\mathcal{O}/x\mathcal{O}$ tiene cardinal $\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(x)$. ⋇

2. El teorema de Latimer-MacDuffee

En esta sección probamos el Teorema 1. De aquí en más fijamos α un entero algebraico con polinomio minimal f de grado n y notemos $\mathcal{O} = \mathbb{Z}[\alpha]$ y $\mathrm{K} = \mathbb{Q}(\alpha)$.

Observemos que para todo $\mathcal{O}$-ideal fraccionario I la multiplicación por α define un morfismo $\mathbb{Z}$-lineal,

$$m_{\mathrm{I}}\colon \mathrm{I} \to \mathrm{I}, \qquad x \mapsto \alpha x.$$

Por el Lema 1.3, todo tal ideal I es $\mathbb{Z}$-libre de rango n; en paticular, dada una $\mathbb{Z}$-base B de I, podemos considerar la matriz $[\mathrm{L}_{\mathrm{I}}]_{\mathrm{B}} \in \mathrm{M}_n\,\mathbb{Z}$ de L_{I} en base B. Si cambiamos la base por otra, digamos B′, entonces $[\mathrm{L}_{\mathrm{I}}]_{\mathrm{B}}$ y $[\mathrm{L}_{\mathrm{I}}]_{\mathrm{B}'}$ son conjugadas con matriz de conjugación la matriz de cambio de base $\mathrm{C}_{\mathrm{B},\mathrm{B}'}$.

Por otro lado, si J es un $\mathcal{O}$-ideal fraccionario equivalente a I, por el Lema 1.2 esto equivale a tener un isomorfismo $\mathcal{O}$-lineal $\phi\colon \mathrm{I} \to \mathrm{J}$ dado por la multiplicación por cierto elemento $\beta \in \mathrm{K}\setminus\{0\}$. Se sigue de aquí que $\varphi m_{\mathrm{I}} = m_{\mathrm{J}}\varphi$, pues

$$\varphi(m_{\mathrm{I}}(x)) = \varphi(\alpha x) = \beta\alpha x = \alpha\beta x = m_{\mathrm{J}}(\varphi(x))$$

para todo $x \in \mathrm{I}$. En particular, dadas $\mathbb{Z}$-bases B de I y B′ de J, las matrices $[\mathrm{L}_{\mathrm{I}}]_{\mathrm{B}}$ y $[\mathrm{L}_{\mathrm{J}}]_{\mathrm{B}'}$ serán conjugadas con matriz de conjugación $[\varphi]_{\mathrm{B},\mathrm{B}'}$. (También se puede observar que si $\mathrm{J} = x\mathrm{I}$ para cierto $x \in \mathrm{K}\setminus\{0\}$, entonces $[\mathrm{L}_{\mathrm{J}}]_{x\mathrm{B}} = [\mathrm{L}_{\mathrm{I}}]_{\mathrm{B}}$.)

Si I es un $\mathcal{O}$-ideal fraccionario, vamos a notar $[\mathrm{L}_{\mathrm{I}}]$ a la clase de conjugación de las matrices $[\mathrm{L}_{\mathrm{I}}]_{\mathrm{B}}$ donde B es una $\mathbb{Z}$-base de I. El conjunto de matrices de $\mathrm{M}_n\,\mathbb{Z}$ de polinomio característico f será denotado M_f; recordemos que $\mathrm{GL}_n(\mathbb{Z})$ actúa allí por conjugación. La discusión anterior prueba la siguiente proposición.

Proposición 2.1. *Se tiene una función bien definida*

$$\Lambda\colon\ \mathrm{ICM}(\mathcal{O}) \to \mathrm{M}_f/\mathrm{GL}_n(\mathbb{Z}), \qquad [\mathrm{I}] \mapsto [\mathrm{L}_{\mathrm{I}}]. \tag{2.2}$$

※

El Teorema 1 será una consecuencia de que la función Λ es biyectiva, como veremos a continuación.

Proposición 2.3. *La función* (2.2) *es sobreyectiva.*

Demostración. Sea $\mathrm{A} \in \mathrm{M}_f$ y veamos que existe un $\mathcal{O}$-ideal fraccionario tal que $\Lambda([\mathrm{I}]) = \mathrm{A}$. Como $\mathcal{O} = \mathbb{Z}[\mathrm{X}]/(f)$, y $f(\mathrm{A}) = 0$ por el teorema de Cayley-Hamilton, la multiplicación por A define una estructura de $\mathcal{O}$-módulo en $\mathrm{N} := \mathbb{Z}^n$ donde la multiplicación por α se identifica con la multiplicación por A. Más aún, esta estructura es una restricción de la estructura de K-módulo que A define sobre $\mathrm{M} := \mathbb{Q}^n$.

Observemos que

$$n = \dim_{\mathbb{Q}} \mathrm{M} = \dim_{\mathrm{K}} \mathrm{M} \cdot \dim_{\mathbb{Q}} \mathrm{K} = \dim_{\mathrm{K}} \mathrm{M} \cdot n,$$

así que $\dim_{\mathrm{K}} \mathrm{M} = 1$. En consecuencia, existe un isomorfismo K-lineal $\varphi\colon \mathrm{M} \to \mathrm{K}$, que se restringe entonces a un isomorfismo $\mathcal{O}$-lineal $\varphi|\colon \mathrm{N} \to \varphi(\mathrm{N})$. Por definición $\mathrm{I} := \varphi(\mathrm{N})$ es un $\mathcal{O}$-ideal fraccionario y la multiplicación por α en I tiene matriz A en base $\{\varphi(e_1), \dots, \varphi(e_n)\}$. En particular $\Lambda([\mathrm{I}]) = [\mathrm{A}]$. ※

Proposición 2.4. *La función* (2.2) *es inyectiva.*

Demostración. Supogamos que $[\mathrm{L}_{\mathrm{I}}] = [\mathrm{L}_{\mathrm{J}}]$, de forma que existen una matriz $\mathrm{U} \in \mathrm{GL}_n\,\mathbb{Z}$ y $\mathbb{Z}$-bases B de I y B′ de J tal que $\mathrm{U}[\mathrm{L}_{\mathrm{I}}]_{\mathrm{B}} = [\mathrm{L}_{\mathrm{J}}]_{\mathrm{B}'}\mathrm{U}$. La matriz U define un isomorfismo $\mathbb{Z}$-lineal $\mathrm{I} \to \mathrm{J}$ que, al conmutar con la multiplicación por α, es además $\mathcal{O}$-lineal. Por el Lema 1.2, se tiene entonces que $[\mathrm{I}] = [\mathrm{J}]$. ※

2.1. De matrices a ideales.

Si $\mathcal{O}_{\mathrm{K}}$ es monogenerado y $\mathrm{Cl}(\mathcal{O}_{\mathrm{K}}) = 1$, todo par de matrices con polinomio característico f son conjugadas. Hagamos un ejemplo no trivial.

Consideremos $d = -5$ y $\mathrm{K} = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O} = \mathcal{O}_{\mathrm{K}} = \mathbb{Z}[\sqrt{-5}]$. Como consecuencia de la cota de Minkowski, el grupo de clases de $\mathcal{O}$ es isomorfo a $\mathbb{Z}_2$, generado por $\mathrm{I} = (2, 1+\sqrt{5})$. Tomemos como $\mathbb{Z}$-base de (1) a $\{1, \sqrt{-5}\}$. De esta forma, la multiplicación de $\sqrt{-5}$ tiene en esta base matriz $\mathrm{A}_0 = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$. Para I tomamos la $\mathbb{Z}$-base $\{2, 1+\sqrt{5}\}$; como $2\sqrt{-5} = -2 + 2(1+\sqrt{-5})$ y

$\sqrt{-5}(1+\sqrt{-5}) = -5+\sqrt{-5} = -3\cdot 2+(1+\sqrt{-5})$, la multiplicación por $\sqrt{-5}$ en esta base tiene matriz $A_1 = \begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix}$.

Por el Teorema 1, toda matriz entera A de 2×2 que satisfaga $A^2 = -5I$ es conjugada a A_0 ó A_1, y estas dos últimas no son conjugadas.

2.2. De ideales a matrices. Vamos ahora en la dirección opuesta, consideremos la matriz $A = \begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix}$ que satisface la ecuación $A^2+5I = 0$. La multiplicación por A define una estructura de $\mathbb{Q}(\sqrt{-5})$-módulo en $\mathbb{Q}^2$ y de $\mathbb{Z}[\sqrt{-5}]$-módulo en $\mathbb{Z}^2$. Concretamente

$$(a+b\sqrt{-5})\begin{pmatrix} x \\ y \end{pmatrix} = (aI+bA)\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} (a+2b)x+3by \\ -3bx+(a-2b)y \end{pmatrix}.$$

Tomando por ejemplo $v_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, tenemos un isomorfismo mandando $\gamma\in K \mapsto \gamma v_0$, i.e.

$$\varphi\colon\, a+b\sqrt{-5}\in K \longmapsto \begin{pmatrix} a+2b \\ -3b \end{pmatrix} \in \mathbb{Q}^2.$$

Luego la preimagen de $\mathbb{Z}^2$ son los elementos $a+b\sqrt{-5}$ tales que $a+2b, 3b\in\mathbb{Z}$. Si ponemos $b = -k/3$ para cierto $k\in\mathbb{Z}$, y $a = l+2k/3$ para cierto $l\in\mathbb{Z}$, entonces $a+b\sqrt{-5} = l+k(2/3-\sqrt{-5}/3)$. Luego

$$I := \varphi^{-1}(\mathbb{Z}^2) = \mathbb{Z}+\left(\frac{2}{3}-\frac{1}{3}\sqrt{-5}\right)$$

Multiplicando por 3 obtenemos la misma clase, así que la matriz A está asociado a la clase del ideal fraccionario $3\mathbb{Z}+(2-\sqrt{-5})\mathbb{Z} = (3, 2-\sqrt{-5})$.

Para ver si A es conjugada a A_0 o a A_1, basta analizar si $(3, 2-\sqrt{-5})$ es principal. El cociente $\mathbb{Z}[\sqrt{-5}]/(3, 2-\sqrt{-5})$ es isomorfo a $\mathbb{Z}/3\mathbb{Z}$; de ser princial este ideal existiría $x\in\mathbb{Z}[\sqrt{-5}]$ de norma 3; i.e. enteros a y b tales que $a^2+5b^2 = 3$. Sin embargo, para que suceda esto debe ser $b = 0$ y luego $3 = a^2$, lo cual es absurdo pues 3 no es un cuadrado.

En definitiva, se obtuvo que $(3, 2-\sqrt{-5}) \sim (2, 1+\sqrt{5})$ y entonces A es conjugada a A_1. Más todavía, podemos explicitar la matriz de conjugación. En pos de la brevedad, referimos a [1, Example 3.5] para el resto de los cálculos.

3. Conjugación por $SL_n\mathbb{Z}$

Refinamos ahora nuestra pregunta inicial. Si $UA = BU$ para ciertas matrices $A, B\in M_n\mathbb{Z}$ y $U\in GL_n\mathbb{Z}$, entonces $\det U = \pm 1$.

> ¿Cuándo son dos matrices enteras conjugadas por una matriz de determinante 1?

La relación de conjugación por $SL_n\mathbb{Z}$ es igual o más fina que la conjugación por $GL_n\mathbb{Z}$. El siguiente lema muestra que para cada clase de conjugación $GL_n\mathbb{Z}$ hay a lo sumo dos clases de conjugación por $SL_n\mathbb{Z}$.

Lema 3.1. *Sea* $A\in M_n\mathbb{Z}$ *y* $D\in GL_n\mathbb{Z}$ *tal que* $\det D = -1$ *(por ejemplo* $D = \operatorname{diag}(-1, 1, \dots, 1)$*).*

(i) Si B *es conjugada a* A *por una matriz de* $GL_n\mathbb{Z}$*, está en la clase de conjugación por* $SL_n\mathbb{Z}$ *de* A *ó* DAD^{-1}.

(ii) Existe $U\in SL_n\mathbb{Z}$ *tal que* $UAU^{-1} = DAD^{-1}$ *si y sólo si existe una matriz* $C\in GL_n\mathbb{Z}$ *que conmuta con* A *y tiene determinante* -1.

Demostración. Si $A = UBU^{-1}$ para cierta U inversible, entonces o bien $\det U = 1$ y entonces B está en la clase de $SL_n\mathbb{Z}$-conjugación de A o bien $\det U = -1$ y luego $\det(DU) = 1$, $(DU)B(DU)^{-1} = DAD^{-1}$. Esto prueba (i).

Para ver (ii), obserevemos que $DAD^{-1} = U^{-1}AU$ para cierta matriz de determinante 1 si y sólo si $(U^{-1}D)A = A(U^{-1}D)$. La multiplicación a derecha por D establece una biyección entre

$\mathrm{SL}_n\mathbb{Z}$ y $-\mathrm{SL}_n\mathbb{Z}$, por tanto, la ecuación de arriba se satisface sólo si existe $C \in -\mathrm{SL}_n\mathbb{Z}$ tal que $CA = AC$. ⁂

Observación 3.2. *Como $I_n \in \mathbb{Z}(M_n\mathbb{Z})$ y $\det I_n = -1$ si $2 \nmid n$, para n impar el problema de conjugación para $\mathrm{SL}_n\mathbb{Z}$ coincide con el problema para $\mathrm{GL}_n\mathbb{Z}$.*

Podemos caracterizar precisamente cuándo las clases de conjugación de $\mathrm{SL}_n\mathbb{Z}$ y $\mathrm{GL}_n\mathbb{Z}$ coinciden.

3.1. El *narrow-class group*.

Un elemento $x \in K$ se dice ***positivo*** si $N_{K/\mathbb{Q}}(x) > 0$ y ***totalmente positivo*** si $\sigma(x) > 0$ para todo embedding real $\sigma\colon K \to \mathbb{R}$. Notamos $K^+ \subset K$ al conjunto de elementos totalmente positivos y $\mathcal{O}^+ = \mathcal{O} \cap K^+$. Se define el ***narrow-class group*** de $\mathcal{O}$ como el grupo $\mathrm{Cl}^+(\mathcal{O})$ de $\mathcal{O}$-ideales fraccionarios inversibles módulo la relación de equivalencia $I \sim J \iff I = xJ$ para cierto $x \in K$ totalmente positivo.

Observación 3.3. *Observemos que $N_{K/\mathbb{Q}}(x)$ se puede ver como el producto de las imagenes de x a través de cada embedding $\sigma\colon K \to \mathbb{C}$. Algunos de ellos se pueden correstringir a $\mathbb{R}$. Si σ es un embedding complejo, también lo es $\overline{\sigma}$, y entonces $\sigma(x)\overline{\sigma}(x) = |\sigma(x)|^2 \geq 0$. El signo de la norma depende entonces únicamente de los embeddings reales; en particular, un elemento totalmente positivo es positivo.*

Proposición 3.4. *Se tiene una sucesión exacta corta*

$$1 \to \mathcal{O}^\times/\mathcal{O}^+ \to K^\times/K^+ \to \mathrm{Cl}^+(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}) \to 1.$$

Demostración. Toda clase $[I]$ de ideal fraccionario en $\mathrm{Cl}(\mathcal{O})$ es imagen de la clase de igual representante en $\mathrm{Cl}^+(\mathcal{O})$; esto define un epimorfismo $\pi\colon \mathrm{Cl}^+(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O})$. El núcleo consiste de las clases $[x\mathcal{O}]$ donde $x \in K^\times$. En particular se tiene un morfismo $x \in K^\times/K^+ \mapsto [x\mathcal{O}] \in \mathrm{Cl}^+(\mathcal{O})$. Su núcleo son las clases $[x] \in K^\times/K^+$ que satisfacen $[x\mathcal{O}] = [\mathcal{O}]$, esto es, que existe $y \in K_+$ tal que $x\mathcal{O} = y\mathcal{O}$; en particular $x/y \in \mathcal{O}$ y de forma simétrica $y/x \in \mathcal{O}$. Por lo tanto $x = y \cdot z$ con $z \in \mathcal{O}^\times$ y la clase de x en $K^\times/K^+$ pertenece a $\mathcal{O}^\times$. Finalmente el núcleo del morfismo $\mathcal{O}^\times \to K^\times/K^+$ inducido por la inclusión $\mathcal{O}^\times \subset K^\times$ es $\mathcal{O}^\times \cap K^+ = \mathcal{O}^+$. ⁂

Observación 3.5. *Observemos que si $x \in K^\times$, entonces $x^2 \in K^+$. En particular $K^\times/K^+$ y $\mathcal{O}^\times/O^+$ son 2-grupos.*

3.2. Ejemplos en el caso cuadrático.

De aquí en más fijamos la siguiente notación: sea d un entero positivo libre de cuadrados y $d \not\equiv 1 \pmod 4$. Tomando $K = \mathbb{Q}(\sqrt{d})$, es $\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Los *embedding* reales $\sigma_1, \sigma_2\colon K \to \mathbb{R}$ son

$$\sigma_1(a + b\sqrt{d}) = a + b\sqrt{d}, \qquad \sigma_2(a + b\sqrt{d}) = a - b\sqrt{d}.$$

Por el teorema de unidades de Dirichlet, sabemos que $\mathcal{O}^\times = \langle \pm 1 \rangle \times \langle u \rangle$ con u una unidad fundamental. Podemos suponer, cambiando u por $-u$, que $\sigma_1(u) > 0$; de aquí se seguirá también que $\sigma_1(u)^n > 0$ para todo $n \in \mathbb{Z}$.

Proposición 3.6. *El cociente $\mathcal{O}^\times/\mathcal{O}^+$ es isomorfo a $\mathbb{Z}/2\mathbb{Z}$ si $N(u) = 1$ e isomorfo a $(\mathbb{Z}/2\mathbb{Z})^2$ si $N(u) = -1$.*

Demostración. Notar que $N(u) = 1$ si y sólo si u es totalmente positiva - es decir, si $\sigma_2(u) > 0$. Observemos que

$$\sigma_i(\pm u^n) = \pm\sigma_i(u)^n.$$

Si $i = 1$, esta expresión es positiva sólo si $\pm = 1$. Para que además la expresión sea positiva si $i = 2$, debe ser o bien $\sigma_2(u) > 0$ o bien n par. Si $N(u) = 1$, entonces $\sigma_2(u) > 0$ y $\mathcal{O}^+ = \langle 1 \rangle \times \langle u \rangle$, en cambio si $N(u) = -1$ entonces $\mathcal{O}^+ = \langle 1 \rangle \times \langle u^2 \rangle$. ⁂

Proposición 3.7. *El morfismo*

$$K^\times \xrightarrow{(\sigma_1,\sigma_2)} \mathbb{Q}^\times \times \mathbb{Q}^\times \xrightarrow{\mathrm{sgn}} \{\pm 1\}^2$$

es sobreyectivo y su núcleo es K^+. En particular $K^\times/K^+ \simeq (\mathbb{Z}/2\mathbb{Z})^2$.

Demostración. Basta notar que las imagenes de $\sqrt{d}$ y $\sqrt{-d}$ son $(1,-1)$ y $(1,-1)$ respectivamente. ⁂

Observación 3.8. *En general para todo cuerpo de números el cociente* $\mathrm{K}^\times/\mathrm{K}^+$ *es isomorfo a un producto de tantas copias de* $\mathbb{Z}/2\mathbb{Z}$ *como embeddings* $\mathrm{K} \to \mathbb{R}$, *ver* [2, II.2.14].

Recordemos que se definen $h_\mathrm{K} = |\mathrm{Cl}(\mathcal{O}_\mathrm{K})|$ y $h_\mathrm{K}^+ = |\mathrm{Cl}^+(\mathcal{O}_\mathrm{K})|$.

Corolario 3.9. *Si* $\mathrm{N}(u) = -1$, *entonces* $\mathrm{Cl}(\mathcal{O}) = \mathrm{Cl}^+(\mathcal{O})$. *En caso contrario el subgrupo de* $\mathrm{Cl}^+(\mathcal{O})$ *generado por los ideales fraccionario principales tiene órden 2, y* $|\mathrm{CL}^+(\mathcal{O})| = 2|\mathrm{Cl}(\mathcal{O})|$. ⁂

n	unidad fundamental u de $\mathrm{K} = \mathbb{Q}(\sqrt{n})$	$\mathrm{N}_{\mathrm{K}/\mathbb{Q}}(u)$	h_K	h_K^+
2	$1+\sqrt{2}$	-1	1	1
3	$2+\sqrt{3}$	-1	1	1
6	$5+2\sqrt{6}$	1	1	2
7	$8+3\sqrt{7}$	1	1	2
10	$3+\sqrt{10}$	-1	2	2

3.3. Un refinamiento del teorema de Latimer-MacDuffee. Fijemos un conjunto de representantes $\{\mathrm{I}_1,\ldots,\mathrm{I}_k\}$ de elementos de $\mathrm{Cl}(\mathcal{O})$ por ideales de $\mathcal{O}$. Todo $\mathcal{O}$-ideal fraccionario es de la forma $r\mathrm{I}_j$ para cierto $r \in \mathrm{K}$ $j \in \{1,\ldots,k\}$.

Para cada j, fijamos dos $\mathbb{Z}$-bases $\mathrm{B}_j^+, \mathrm{B}_j^+$ tales que la matriz de cambio de base entre estas tenga determinante -1. Dado J un $\mathcal{O}$-ideal fraccionario equivalente a I_j, fijamos $r_\mathrm{J} \in \mathrm{K}^\times$ tal que $\mathrm{I}_j = r\mathrm{J}$ y $\mathrm{N}(r_\mathrm{J}) > 0$ si I_j y J son estrechamente equivalentes. Vamos a asociarle a J una $\mathbb{Z}$-base B_J; si $\mathrm{N}(r) > 0$ tomamos $\mathrm{B}_\mathrm{J} = r\mathrm{B}_j^+$, en caso contrario $\mathrm{B}_\mathrm{J} = r\mathrm{B}_j^-$.

De esta manera, tenemos una aplicación bien definida

$$\Xi\colon \mathrm{Cl}^+(\mathcal{O}) \to \mathrm{M}_f/\mathrm{SL}_n\mathbb{Z}, \qquad [\mathrm{J}] \mapsto [\mathrm{L}_\mathrm{J}]_{\mathrm{B}_\mathrm{J}}. \tag{3.10}$$

Para terminar, veremos que Ξ es una biyección.

Proposición 3.11. *La función* (3.10) *es inyectiva.*

Demostración. Basta ver que si existen r de norma negativa e I_j que no sea estrechamente equivalente a $r\mathrm{I}_j$, entonces $\Xi([\mathrm{I}_j]) \neq \Xi([r\mathrm{I}_j])$. Por el contrarrecíproco, si Ξ emvía ambas clases a la misma clase de conjugación, existe $\mathrm{U} \in \mathrm{SL}_n\mathbb{Z}$ y un isomorfismo $\mathcal{O}$-lineal $\phi\colon \mathrm{I}_j \to r\mathrm{I}_j$ que es bases B_j^+ y $r\mathrm{B}_j^-$ se representa por U. Recordemos además que ϕ está dado por la multiplicación por cierto $x \in \mathrm{K}^\times$. Se tiene luego el siguiente diagrama

$$\begin{tikzcd}
\mathrm{I}_j \arrow[r, "\cdot x"] & r\mathrm{I}_j \arrow[r, "\cdot r^{-1}"] & \mathrm{I}_j \\
\mathbb{Z}^n \arrow[u, "\mathrm{B}_j^+"] \arrow[r, "\mathrm{U}"] & \mathbb{Z}^n \arrow[u, "r\mathrm{B}_j^-"] \arrow[r, "\mathrm{C}_{\mathrm{B}_j^+,\mathrm{B}_j^-}"] & \mathbb{Z}^n \arrow[u, "\mathrm{B}_j^+"]
\end{tikzcd}$$

La composición de la fila superior define el morfismo de multiplicación por x/r de I_j en sí mismo. Como se representa en base B_j^+, debe ser $\mathrm{N}(x/r) = \det\phi = \det\mathrm{U}\det\mathrm{C}_{\mathrm{B}_j^+,\mathrm{B}_j^-} = -1$ y por lo tanto $\mathrm{N}(x) = -\mathrm{N}(r) > 0$. Esto muestra que I_j y $r\mathrm{I}_j$ son estrechamente equivalentes, concluyendo la prueba. ⁂

Proposición 3.12. *La función* (3.10) *es sobreyectiva.*

Demostración. Sabemos que si $\mathrm{A} \in \mathrm{M}_f$, existe un $\mathcal{O}$-ideal fraccionario I y una $\mathbb{Z}$-base B de I tal que $[\mathrm{L}_\mathrm{I}]_\mathrm{B} = \mathrm{A}$. Escribiendo $\mathrm{I} = r_\mathrm{I}\mathrm{I}_j$, tenemos que alguna de las dos matrices $\mathrm{C}_{\mathrm{B},r_\mathrm{I}\mathrm{B}_j^+}$ ó $\mathrm{C}_{\mathrm{B},r_\mathrm{I}\mathrm{B}_j^-}$ pertenece a $\mathrm{SL}_n\mathbb{Z}$; por lo tanto la clase de $[\mathrm{L}_\mathrm{I}]_\mathrm{B}$ coincide con $[\mathrm{L}_{\mathrm{I}_j}]_{\mathrm{B}_j^+}]$ o $[\mathrm{L}_{\mathrm{I}_j}]_{\mathrm{B}_j^-}$. Si existe un ideal equivalente a I_j pero no de forma estrecha, tanto $[\mathrm{L}_{\mathrm{I}_j}]_{\mathrm{B}_j^+}]$ como $[\mathrm{L}_{\mathrm{I}_j}]_{\mathrm{B}_j^+}]$ están en la imagen de Ξ y entonces [A] lo está.

En caso contrario, todo ideal equivalente a I_j tiene por imagen via Ξ a $[\mathrm{L}_{\mathrm{I}_j}]_{\mathrm{B}_j^+}]$. Para terminar la prueba, veremos que bajo estas hipótesis $[\mathrm{L}_{\mathrm{I}_j}]_{\mathrm{B}_j^+}]$ y $[\mathrm{L}_{\mathrm{I}_j}]_{\mathrm{B}_j^-}]$ son conjugadas por una matriz de $\mathrm{SL}_n\mathbb{Z}$. ⋇

Referencias

[1] K. Conrad, *Ideal classes and matrix conjugation over* $\mathbb{Z}$, available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/matrixconj.pdf. ↑3

[2] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. ↑5

[3] Claiborne G. Latimer and C. C. MacDuffee, *A correspondence between classes of ideals and classes of matrices*, Ann. of Math. (2) **34** (1933), no. 2, 313–316, DOI 10.2307/1968204. ↑1