EL PROBLEMA DE CONJUGACIÓN PARA MATRICES ENTERAS

GUIDO ARNONE

Teorema 1 ([1, 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 $\mathcal{O}_K$ su anillo de enteros. Un ***orden*** de K es un subanillo que como $\mathbb{Z}$-módulo tiene rango $[K : \mathbb{Q}]$. Notar que $\mathsf{Frac}(\mathcal{O}) = K$, 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 $I \subset K$; siempre existe $x \in \mathcal{O}$ y un ideal $J \trianglelefteq \mathcal{O}$ tal que $I = \frac{1}{x}J$.

Ejemplo 1. *Si α es un entero algebraico y $K = \mathbb{Q}(\alpha)$, entonces $\mathbb{Z}[\alpha]$ es un orden de $\mathcal{O}_K$. 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 $I = xJ$ para algún $x \in K \setminus \{0\}$. 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 $\mathcal{O} \neq \mathcal{O}_K$, no todo ideal fraccionario es inversible.

Precisaremos los siguientes lemas sobre ideales fraccionarios más adelante.

Lema 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 $I \to J$ está dado por la multiplicación por un elemento de $K \setminus \{0\}$.*

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

Lema 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 $[K : \mathbb{Q}]$ 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 $0 \to I \hookrightarrow \mathcal{O} \twoheadrightarrow \mathcal{O}/I \to 0$ vemos que $\operatorname{rk} I = \operatorname{rk} \mathcal{O}$ si y sólo si $\operatorname{rk} \mathcal{O}/I = 0$. Para ver esto último probaremos que $\mathcal{O}/I$ es finito: dado $x \in I$ no nulo tenemos un epimorfismo $\mathcal{O}/x\mathcal{O} \to \mathcal{O}/I$; podemos asumir entonces que $I = (x)$. Finalmente, el mismo argumento que en el caso $\mathcal{O} = \mathcal{O}_K$ prueba que el cociente $\mathcal{O}/x\mathcal{O}$ tiene cardinal $N_{K/\mathbb{Q}}(x)$. ⋇

2. El teorema de Latimer-MacDuffee

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

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 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 $[\mathrm{L_I}]_{\mathrm{B}} \in \mathrm{M}_n\mathbb{Z}$ de $\mathrm{L_I}$ en base B. Si cambiamos la base por otra, digamos B′, entonces $[\mathrm{L_I}]_{\mathrm{B}}$ y $[\mathrm{L_I}]_{\mathrm{B'}}$ son conjugadas con matriz de conjugación la matriz de cambio de base $\mathrm{C_{B,B'}}$.

Por otro lado, si J es un $\mathcal{O}$-ideal fraccionario equivalente a I, por el Lema 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 $[\mathrm{L_I}]_{\mathrm{B}}$ y $[\mathrm{L_J}]_{\mathrm{B'}}$ serán conjugadas con matriz de conjugación $[\varphi]_{\mathrm{B,B'}}$. (También se puede observar que si $\mathrm{J} = x\mathrm{I}$ para cierto $x \in \mathrm{K} \setminus \{0\}$, entonces $[\mathrm{L_J}]_{x\mathrm{B}} = [\mathrm{L_I}]_{\mathrm{B}}$.)

Si I es un $\mathcal{O}$-ideal fraccionario, vamos a notar $[\mathrm{L_I}]$ a la clase de conjugación de las matrices $[\mathrm{L_I}]_{\mathrm{B}}$ 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 4. *Se tiene una función bien definida*

$$\Lambda\colon\ \mathrm{ICM}(\mathcal{O}) \to \mathrm{M}_f/\mathrm{GL}_n(\mathbb{Z}), \qquad [\mathrm{I}] \mapsto [\mathrm{L_I}]. \tag{5}$$

※

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

Proposición 6. *La función* (5) *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 7. *La función* (5) *es inyectiva.*

Demostración. Supogamos que $[\mathrm{L_I}] = [\mathrm{L_J}]$, 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 $\mathrm{U}[\mathrm{L_I}]_{\mathrm{B}} = [\mathrm{L_J}]_{\mathrm{B'}}\mathrm{U}$. 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 2, se tiene entonces que $[\mathrm{I}] = [\mathrm{J}]$. ※

3. Ejemplos

3.1. 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 $\mathrm{A} = \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$. 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 $B = \begin{pmatrix} -1 & -3 \\ 2 & 1 \end{pmatrix}$.

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

3.2. De ideales a matrices.

3.3. Una matriz que no es conjugada a su transpuesta.

4. Conjugación por $\mathrm{SL}_n\mathbb{Z}$

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

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

Ejemplo 2.

Cuando n es impar, esta relación no es más estricta que la ya considerada: si $\det U = -1$ entonces $\det -U = -1$ y $(-U)A = B(-U)$.

4.1. 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 8. *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 9. *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 10. *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.*

4.2. Ejemplos en el caso cuadrático. Sea d un entero positivo libre de cuadrados y $d \not\equiv 1 \pmod 4$. Tomando $K = \mathbb{Q}(\sqrt{d})$, es $\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$.

Referencias

[1] 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