Teoría de Números: 13 diciembre

Clase pasada: $$\left|\mathrm{Pic}(\mathcal{O}_{\sqrt{d}})\right| = \left|{}^{G}/_{H}\right|$$

$$= \left|\frac{\text{ideales fraccionarios de } \mathcal{O}_{\sqrt{d}}}{\text{ideales fracc principales}}\right| < \infty$$

¡ESTE ES UN TEOREMA

Hoy: Estimar $\left|\mathrm{Pic}(\mathcal{O}_{\sqrt{d}})\right|$.

<u>Teorema</u>: $\mathcal{O}_{\sqrt{d}} \subseteq \mathbb{Q}[\sqrt{d}]$ anillo de enteros algebraicos. Entonces, existe una biyección entre

1) $\mathrm{Pic}(\mathcal{O}_{\sqrt{d}})$ &

2) $\left(\text{Matrices } 2\times 2 \text{ con entradas en } \mathbb{Z}\right) \big/ \mathbb{Z}\text{-conjugación}$

tal que $P(M) = 0$, donde $P(x) \in \mathbb{Q}[x]$ es el polinomio asociado a $\mathcal{O}_{\sqrt{d}}$.

Demostración:

$\mathcal{O}_{\sqrt{d}}$ es un $\mathbb{Z}$-módulo libre

esto implica lo siguiente:

$I \subseteq \mathcal{O}_{\sqrt{d}}$ ideal fraccionario es un $\mathbb{Z}$-submodulo de $\mathcal{O}_{\sqrt{d}}$ y por tanto

es un $\boxed{\mathbb{Z}\text{-módulo libre}}$ de rango 2.

I es un $\underbrace{\mathcal{O}_{\sqrt{d}}\text{-módulo}}$, por tanto

mult. de

$$\alpha \cdot \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = M \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

Recordar $\mathcal{O}_{\sqrt{d}} \cong \mathbb{Z}[x]/p(x)$

generador de $\mathcal{O}_{\sqrt{d}}$ como $\mathbb{Z}$-álgebra.

matriz en $GL(2,\mathbb{Z})$

i.e. $\mathcal{O}_{\sqrt{d}} \cong \mathbb{Z}[\alpha]$

$\cong \{a_0 + a_1\alpha \mid p(\alpha) = 0\}$

& $p(x) = x^2 + d$ si $d \not\equiv 1\ (4)$

$p(x) = x^2 + x + \frac{1-d}{4}$ $d \equiv 1\ (4)$

más aún, $P(M) = P(\alpha) = 0$ donde

$P(x) \in \mathbb{Q}[x]$ es irreducible$/_{\mathbb{Q}}$. $\Rightarrow P(x)$

es el polinomio característico de M.

Un cambio de base $\{e_1, e_2\} = I$

arroja una matrix M' tal que

$$M \underbrace{\sim}_{\text{conjugación}} M' = AMA^{-1}$$

$A \in GL(2, \mathbb{Z})$

$$\Rightarrow \quad Pic(\mathcal{O}_{\sqrt{d}}) \longrightarrow \left\{\begin{matrix}\text{matrices} \\ 2\times 2 \text{ en} \\ \mathbb{Z}\end{matrix}\right\} \Big/ \text{conj} \quad \text{tal que } P(M) = 0$$

$$I \longmapsto M$$

—— // ——

Recíprocamente, $M \in GL(2,\mathbb{Z})$ con P_M su polinomio característico igual a $\boxed{x^2+d}$ ($d \not\equiv 1\ (4)$) ó $\boxed{x^2+x+\frac{1-d}{4}}$ ($d \equiv 1\ (4)$).

Entonces, obtenemos un homomorfismo de anillos

$$\varphi : \mathcal{O}_{\sqrt{d}} = \mathbb{Z}[\alpha] \longrightarrow \mathrm{End}(\mathbb{Z}^2)$$

$$\boxed{\alpha \longmapsto M}$$

inducido por esta asociación.

Como

$$\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/q(x) \qquad q(x) = \begin{cases} x^2+d \ ; & d \not\equiv 1(4) \\ x^2+x+\frac{1-d}{4} & d \equiv 1(4) \end{cases}$$

necesitamos que

$d \not\equiv 1(4)$ $\quad 0 = \alpha^2 + d \longmapsto M^2 + d\,\mathrm{Id} = 0$

Teorema de Cayley-Hamilton.

φ hace $\mathbb{Z}^2$ un $\mathcal{O}_{\sqrt{d}}$-módulo.

Este es el ideal fraccional buscado.

Eg: $d=-41$ $\quad \mathcal{O}_{\sqrt{d}} \subseteq \mathbb{Q}[\sqrt{-41}]$

Para estimar $|\mathrm{Pic}(\mathcal{O}_{\sqrt{d}})|$ necesitamos

encontrar matrices 2×2 en $\mathbb{Z}$ tal que

$M^2+41\,\mathrm{Id}=0$ no conjugadas (en $GL(2,\mathbb{Z})$).

Aquí hay varias $\begin{pmatrix} 0 & 1 \\ -41 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 \\ -21 & -1 \end{pmatrix}$,

$$\begin{pmatrix} \pm 1 & 3 \\ -14 & \mp 1 \end{pmatrix}, \quad \begin{pmatrix} \pm 1 & 6 \\ -7 & \mp 1 \end{pmatrix}, \quad \begin{pmatrix} \pm 2 & 5 \\ -9 & \mp 2 \end{pmatrix}$$

$\Rightarrow |\mathrm{Pic}| \geq 8$ i.e. $h_{-41} \geq 8$

$\mathbb{Z}+\mathbb{Z}[\sqrt{-41}]$ no es DIP

(Lejos de serlo)

<u>Coro</u>: hay una biyección si <u>$d<0$</u>

1) Clases de $\mathbb{Z}$-conjugación de matrices 2×2 sobre $\mathbb{Z}$. tal que

* $d\,\mathrm{Id} = (2M - \mathrm{Id})^2$ $\quad d \equiv 1\ (4)$ $\quad D = 4d$

* $d\,\mathrm{Id} = M^2$ $\quad d \not\equiv 1\ (4)$ $\quad D = 4d$

2) $SL(2,\mathbb{Z})$-órbitas de formas cuadráticas positivas definidas con discriminante D.

<u>Demostración</u>: Supongamos $d \not\equiv 1 (4)$.

1 $\quad M^2 = d\,\mathrm{Id} \Rightarrow M = \begin{pmatrix} b/2 & -a \\ c & -b/2 \end{pmatrix}$

con $\boxed{4ac - b^2 = -4d}$

$$\boxed{\begin{array}{l} tr(M) = 0 \\ det(M) = -d \end{array}}$$

Recordar de alg lineal

definimos $M' = M \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$

¡matriz simétrica! le asociamos

la forma cuadrática $\boxed{ax^2+bxy+cy^2}$

la cual tiene discriminante $\underline{4d=D}$

Observar que $A \in SL_2(\mathbb{Z})$, entonces

$$AMA^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = AM'\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}A^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$= \det(A)\, A M' A^t$$

nos indica como cambia M' bajo conjugación de $M \longmapsto AMA^{-1}$:

Eg $\quad d=-5 \quad \mathcal{O}_{\sqrt{d}} \subseteq \mathbb{Q}[\sqrt{-5}]$

Formas de discriminante 20 que no están en la misma $SL(2,\mathbb{Z})$-órbita

$$x^2+5y^2 \quad ; \quad 2x^2+2xy+3y^2$$

Matrices en $GL(2,\mathbb{Z})$ no conjugadas:

$$\begin{pmatrix} 1 & 2 \\ -3 & -1 \end{pmatrix} = M \qquad M^2 = \begin{pmatrix} -5 & 0 \\ 0 & -5 \end{pmatrix}$$

$$\begin{pmatrix} 0 & -1 \\ 5 & 0 \end{pmatrix} = L \qquad L^2 = \begin{pmatrix} -5 & 0 \\ 0 & -5 \end{pmatrix}$$

$$\Rightarrow \boxed{h_{20} \geq 2}$$