# THE IDEAL CLASS MONOID OF AN ORDER

- Motivation: Conjugacy matrices (over $\mathbb{Z}$)
- $A, B \in M_n(R)$, $R$ a ring,
  ? $\exists\, U \in GL_n(R)$ s.t. $UAU^{-1} = B$
  $\Leftrightarrow$
  ~~$\det U \in R^\times$~~
- Invariants: characteristic poly $f_A(x) := \det(A - xI_n)$
- Not a complete invariant:
  Ex $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ are not conj over every ring $R$!
  $(x^2-1)^2$
- In Linear algebra 1:
- Thm A $F$ a field, $f(x) \in F[x]$ irreducible, monic, $\deg f = n$. Then:
  1) for $A \in M_n(F)$: $f_A(x) = f(x) \Leftrightarrow f(A) = 0$
  2) all matrices in $M_n(F)$ w/ char poly $f(x)$ are conjugates.
- Over $\mathbb{Z}$: A 1) is true
  A 2) is NOT true

- Recall some terminology

- A number field is a finite extension of $\mathbb{Q}$

- $f = x^3 + 10x^2 - 8$, $f(\alpha) = 0$

$K = \mathbb{Q}[x]/(f) \cong \mathbb{Q}(\alpha)$

$K = 1\cdot\mathbb{Q} \oplus \alpha\mathbb{Q} \oplus \alpha^2\mathbb{Q}$

- An order Ring $K$ is a subring $R \subseteq K$ st $\operatorname{Frac} R = K$ $(K = R \otimes \mathbb{Q})$

$R = \mathbb{Z}[\alpha] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z}$

$\mathcal{O}_K = \mathbb{Z} \oplus \frac{\alpha}{2}\mathbb{Z} \oplus \frac{\alpha^2}{4}\mathbb{Z}$

$S = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \frac{\alpha^2}{2}\mathbb{Z}$

$R \subseteq S \subseteq \mathcal{O}_K$.

- A fractional $R$-ideal $I$ is a $\neq 0$ fin. gen. $R$-submodule of $K$ $(I \otimes \mathbb{Q} = K)$

$\Leftrightarrow \exists\, x \in K^*$ st $xI$ is an $R$-ideal

$I = (3, \alpha+2) = 3\mathbb{Z} \oplus (\alpha+2)\mathbb{Z} \oplus (\alpha^2+2)\mathbb{Z}$

$J = 3\mathbb{Z} \oplus (\alpha+2)\mathbb{Z} \oplus \frac{\alpha^2+2\alpha}{8}\mathbb{Z}$

$(\alpha+\alpha^2)J = I$

- $I \simeq J$ if $\exists\, x \in K^*$ st $xJ = I$ (i.e. iso as $R$-modules)

**Def** Ideal class monoid of $R$

$$ICM(R) := \{\text{fract } R\text{-id}\}/\simeq \quad \ni \overline{I},$$

monoid with Ideal multiplication, unit is $\overline{R}$

$$ICM(R) = \left\{ \overline{R},\ \overline{S},\ \underbrace{\overline{\mathcal{O}_K}}_{2\mathbb{Z} \oplus \frac{\alpha}{2}\mathbb{Z} \oplus \frac{\alpha^2+4}{2}\mathbb{Z}} \right\}$$

$S$ is not Gorenstein $\overset{!!}{\Rightarrow} S^\vee$

- **Thm B** [Latimer, MacDuffe, 1933]

  $f(x)$ monic, irreducible, $\deg f = n$ $\in \mathbb{Z}[x]$

  $\alpha$ a root of $f$.

$$\left\{ \begin{array}{l} \text{matrices in } M_n(\mathbb{Z}) \\ \text{w/ char poly } f(x) \end{array} \right\} \Big/ \text{conj.} \longleftrightarrow ICM(\mathbb{Z}[\alpha])$$

$$[m_{\alpha, I}]_{conj} \longleftarrow \overline{I}$$

"

- $I$ is $\underset{\mathbb{Z}}{\cong} \mathbb{Z}^n$
- $\alpha I \subseteq I$
- if we change $J \in \overline{I}$ we "change the base"

  so take a conjugate matrix

How to compute $ICM(R)$? $R$ an order in $K$

- a fnac. $R$-ideal $I$ is $R$-invertible if $\exists$ a fn. id $J$ s.t.
$$I \cdot J = R$$
- Def: $Pic(R) = \{\text{inv. fn. } R\text{-ideals}\}/\text{iso}$
- If $I$ is $R$-invertible then we can write (unique)
$$I = \prod_{i<\infty} \mathfrak{p}_i^{e_i}$$
where $\mathfrak{p}_i$ are maximal ideals of $R$ and $e_i \geq 1$
- "Note that the $\mathfrak{p}_i$ are invertible."
- In general not all fn. ideals are invertible.
- (Among all the orders in $K$ there is a maximal "$\subseteq$" one $\mathcal{O}_K$ "the ring of integers of $K$")
- Every fractional $\mathcal{O}_K$-ideal is invertible
i.e. $ICM(\mathcal{O}_K) = Pic(\mathcal{O}_K)$ "$= cl(K)$"
- Well known algorithms to compute $Pic(\mathcal{O}_K)$

and

$$0 \longrightarrow \frac{\mathcal{O}_K^\times}{R^\times} \longrightarrow \frac{(\mathcal{O}_K/f)^\times}{(R/f)^\times} \longrightarrow Pic(R) \longrightarrow Pic(\mathcal{O}_K) \longrightarrow 0$$

where $f = (R : \mathcal{O}_K) = \{x \in K : x\mathcal{O}_K \subseteq R\}$
"the conductor".

- $R \subsetneq \mathcal{O}_K \iff Pic(R) \subsetneq ICM(R)$

Compute what we are missing!

## OVERORDERS

- $\mathcal{O}_K/R$ is a finite abelian group.

- An over-order $S$ of $R$ is an order in $K$ s.t $R \subseteq S (\subseteq \mathcal{O}_K)$

- There is a finite number of over-orders.

- To every fr. $R$-ideal $I$ we can attach an over-order of $R$ :

$$(I:I) = \{ x \in K : xI \subseteq I \}$$

"the multiplicator ring of $I$"

Note : $R \subseteq (I:I)$

- If a fractional $R$-ideal $I$ is invertible in an over-order $S$ of $R$ then $S = (I:I)$

- We just proved that

$$I \subset M(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathcal{O}_K \\ \text{overorders}}} \mathrm{Pic}(S)$$

- Unfortunately sometimes "$\neq$". How often?

Whenever at least one of the $S$ is not Gorenstein.

- Fact : if $[K:\mathbb{Q}] = 2$ : "$=$"

- $ICM(R)$ is always finite

"Minkowsi Bound" is very bad:

$$M_K = \sqrt{|\Delta_K|}\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$$

$$M_R = [\mathcal{O}_K : R]\, M_K$$

- exponential in the degree
- testing if two ideals are isomorphic is slow!

- First we make the problem simpler:

**Def** $I$ is weakly equivalent to $J$ if
- $(I:I) = (J:J) =: S$
- $\exists$ an invertible fr. $S$-ideal $L$ such that $I = LJ$.

[DADE - TAUSSKY - ZASSENHAUS 1962]

locally at every closed pt $\longrightarrow$ ~~$I_\mathfrak{p} \cong J_\mathfrak{p}$ $\forall \mathfrak{p}$ maximal $S$-ideal~~

$\Updownarrow$

$1 \in (I:J)(J:I)$

$(I:J) = \{x \in K : xJ \subseteq I\}$

$(J:I) = \ldots$

easy to verify !!!

**Def** $W(R) := \{\text{fractional } R\text{-ideals}\} / \text{wk eq.}$

**Thm** [D-T-Z] $\{I \text{ fr. } R\text{-ideals s.t. } I\mathcal{O}_K = \mathcal{O}_K\} \subseteq \{R\text{-submodules of } \mathcal{O}_K/f\}$

$f = (R : \mathcal{O}_K)$ finite and "small"

$\downarrow$

$W(R)$

# How to recover $ICM(R)$ from $\mathcal{W}(R)$?

For $S$ any over-order of $R$ define

$$\overline{\mathcal{W}}(S) := \{ [I]_{wk} \in \mathcal{W}(R) \text{ s.t. } (I:I) = S \}$$

$$\mathcal{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \overline{\mathcal{W}}(S)$$

$$\overline{ICM}(S) := \{ \bar{I} \in ICM(R) \text{ s.t. } (I:I) = S \} \supseteq Pic(S)$$

$$ICM(R) = \bigsqcup_{S} \overline{ICM}(S)$$

**Thm**
- $Pic(S)$ acts freely on $\overline{ICM}(S)$
- $\overline{\mathcal{W}}(S) = \overline{ICM}(S)^{Pic(S)}$

$\rightsquigarrow$ compute $ICM(R)$.

---

## Abelian Varieties over $\mathbb{F}_q$ $\quad q = p^r$, $p$ prime

$\mathcal{I}_q$ = category of pairs $(T, F)$ where
- $T$ is a free fin. gen. $\mathbb{Z}$-module
- $F \in End_{\mathbb{Z}}(T)$:
  - a) $F \otimes \mathbb{Q}$ is a semisimple endomorphism of $T \otimes \mathbb{Q}$ and its eigenvalues have absolute value $\sqrt{q}$
  - b) (at least) half of the root of the char. poly of $F$ in $\overline{\mathbb{Q}}_p$ are $p$-adic units
  - c) $\exists\ V \in End_{\mathbb{Z}}(T)$ st $FV = q$

Morphisms:

$$\begin{array}{ccc} T & \xrightarrow{\varphi} & T' \\ F \downarrow & \circlearrowleft & \downarrow F' \\ T & \xrightarrow{\varphi} & T' \end{array}$$

COMMENT THIS

a poly satisfying a) b) is an ordinary $q$-Weil poly

**Thm** [Deligne '69]

There exist an equivalence between the category of ordinary abelian varieties / $\mathbb{F}_q$ and $\mathcal{L}_q$.

So counting iso class of $^{ord}$ ab var / $\mathbb{F}_q$

$\|$

counting iso classes of objects in $\mathcal{L}_q$.

**How**: - fix an (irreducible) ordinary $q$-Weil poly $h(x)$

- call $F$ a root of $h(x)$

- $\underline{ICM\left(\mathbb{Z}[F, q/F]\right)}$

**Rmk**: it is possible to talk about dual varieties and polarizations in $\mathcal{L}_q$ [Howe 95]

Im the future: drop: irred, ordinary