# ISOMORPHISM CLASSES OF ABELIAN VARIETIES OVER $\mathbb{F}_q$ 

Goal: Count isomorphism classes of (ordinary) principally polarized abelian var. $/\mathbb{F}_q$ w/ their group of automorphisms.

$k = \mathbb{C}$

We have an equiv. of categories:

$$\left\{ \begin{array}{c} \text{ab var over} \\ \mathbb{C} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{complex tori} \\ \text{admitting a Riemann form} \end{array} \right\}$$

"skew symm form +"

$$A \longmapsto A(\mathbb{C}) \simeq V/L \qquad V \simeq \mathbb{C}^g, \quad L \simeq \mathbb{Z}^{2g}, \ L \subset V$$

$\dim A = g$ — full rank lattice.

**Point**: we have a concrete object to look at $L$.

$k = \mathbb{F}_q \quad q = p^a$

Serre: We cannot functorially attach to the whole category of ab. var $/\mathbb{F}_q$ a full rank lattice

b/c: $\exists$ supersingular ell. curves, whose Endomorphism algebra is a quat. algebra which does not admit a 2-dim representation

• "Need to restrict to a subcategory."

• $\ell \neq p$; $A/\mathbb{F}_q$ with Frobenius endomorphism $\pi_A$

$T_\ell A := \varprojlim A[\ell^n](\overline{\mathbb{F}_p})$ "$\ell$-Tate module"

is a free $\mathbb{Z}_\ell$-module of rank $2g$. ($g = \dim A$)

Def $h_A :=$ char poly of $T_\ell \pi_A$ acting on $T_\ell A$

Facts: $h_A \in \mathbb{Z}[X]$, monic, $\deg h_A = 2g$, roots of $\mathbb{C}$-size $\sqrt{q}$

$A$ is <u>ordinary</u> if the middle coefficient of $h_A$ (coeff of $x^g$ if $\dim A = g$) is coprime w/ $p$. $\Leftrightarrow$ max $p$-rank

<u>Thm</u> (Deligne '69)

There is an equivalence between the category of ordinary ab. var. $/\mathbb{F}_q$ and the category $\mathcal{L}_q$:

- obj $(\mathcal{L}_q)$ $\div$ pairs $(T, F)$ where
  - . $T$ is a free fin. gen. $\mathbb{Z}$-module of even rank
  - . $F : T \to T$ $\mathbb{Z}$-linear satisfying:

    1) $F \otimes \mathbb{Q}$ acts semisimply on $T \otimes \mathbb{Q}$ and its eigenvalues have $\mathbb{C}$-size $\sqrt{q}$

    2) the char poly of $F$ is ordinary "middle coeff* coprime with $p$"

    3) $\exists\ V : T \to T$ st $FV = q$

- morphisms $\mathcal{L}_q$:

$$\begin{tikzcd} T \arrow[r, "F"] \arrow[d] \arrow[dr, phantom, "\circlearrowright"] & T \arrow[d] \\ T' \arrow[r, "F'"] & T' \end{tikzcd}$$

"This is concrete : free ab groups and $\mathbb{Z}$-matrices!"

The functor:

$$A \longmapsto (T(A), F(A))$$

$$\begin{array}{l} A \quad / \mathbb{F}_q \\ \Big\downarrow \text{ Serre-Tate can. lift} \\ A^{\#} \quad W(\mathbb{F}_q) \text{ ring of Witt-vectors } / \mathbb{F}_q \\ \Big\downarrow \end{array}$$

$\tilde{A} = A^{\#} \otimes_{\varepsilon} \mathbb{C}$ where $\varepsilon : W(\mathbb{F}_q) \hookrightarrow \mathbb{C}$ fixed

$T(A) := H^1(\tilde{A})$

$F(A) :=$ induced by the Frobenius $\pi_A$

- $\dim(A) = g \rightsquigarrow \mathrm{rk}_{\mathbb{Z}} T(A) = 2g$ (3)
- Howe '95 : defined "dual" and "polarization" in $\mathcal{L}_q$

<u>Count</u> : - dimension $g$;
- fix a characteristic poly $h$;

Need : $h$ <u>irreducible</u>.

Deligne functor restricted to the ab var / $\mathbb{F}_q$ w/ char poly $= h$ becomes :

$$A \longmapsto I_A$$ fractional ideal of the order $\mathbb{Z}[F, V] = R$ in the number field $\mathbb{Q}(F) = K$

- $K$ is a CM-field

<u>Thm</u>

a) $A^\vee \longmapsto \overline{I}^t$ where $I^t = \{x \in K : \mathrm{Tr}(xI) \subseteq \mathbb{Z}\}$ and $\overline{\phantom{x}}$ is the CM-conjugation

b) $\mathrm{End}(A) \leftrightsquigarrow (I:I) = \{x \in K : xI \subseteq I\}$

$\mathrm{Aut}(A) \leftrightsquigarrow (I:I)^\times$

c) $\left\{\begin{array}{l}\text{iso classes of} \\ \text{ab. var } / \mathbb{F}_q \text{ with} \\ \text{char. poly } h\end{array}\right\} \longleftrightarrow \{\text{fractional } R\text{-ideal}\} / \simeq_R = ICM(R)$ ideal class monoid of $R$.

d) a (prime) polarization of $A$

$\updownarrow$

$\lambda \in K^*$ st : 1 $\lambda I \subseteq \overline{I}^t$ $(=)$

2 $\overline{\lambda} = -\lambda$ tot. imaginary

3 $\lambda$ is $\Phi$-positive (?)

$\left(\begin{array}{l}\Phi = \{\varphi : K \hookrightarrow \mathbb{C} \text{ st } v_E(\varphi(F)) > 0\} \\ \varphi(\lambda)/i > 0 \quad \forall \varphi \in \Phi\end{array}\right)$

e) $S := (I:I)$, assume $A$ has a p.p. $\lambda$

then:

$\{$non-isom. p.p. of $A\} \longleftrightarrow \dfrac{\{\text{tot. positive } u \in S^\times\}}{\{v\bar{v} : v \in S^\times\}}$

and $Aut(A, \lambda) \hookrightarrow$ torsion units of $S$.

Rmk: Everything is "easy" to compute but ICM (R) because we have non-invertible ideals.

---

$R \subseteq K$

ICM

- $ICM(R) \supseteq Pic(R)$

  and $ICM(R) = Pic(R) \Leftrightarrow R = \mathcal{O}_K$

- Easy to prove:

$$ICM(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathcal{O}_K \\ S: \text{ order}}} Pic(S)$$

"Usually $=$": Ex: quadratic orders

Ex $f = x^3 + 10x^2 - 8$

$\alpha$ a root of $f$

$K = \mathbb{Q}(\alpha) \supseteq R = \mathbb{Z}[\alpha]$

$\mathcal{O}_K = \mathbb{Z}[\alpha/2]$

there is a 3rd over-order:

$$R \subseteq \underset{\mathbb{Z} \oplus \frac{\alpha}{2}\mathbb{Z} \oplus \frac{\alpha^2}{2}\mathbb{Z}}{\overset{\|}{S}} \subseteq \mathcal{O}_K$$

$Pic(R) = \{\bar{R}\}$

$\Rightarrow Pic(S) = \{\bar{S}\}$

and $Pic(\mathcal{O}_K) = \{\bar{\mathcal{O}}_K\}$

$ICM(R) = \{\bar{R}, \bar{S}, \bar{\mathcal{O}}_K, \bar{I}\}$ where $I = 2\mathbb{Z} \oplus \frac{\alpha}{2}\mathbb{Z} \oplus \frac{\alpha^2+4}{2}\mathbb{Z}$

$\| $

$S^t$: $S$ not Gorenst.

If $R$ is not a Bass order ($\Leftrightarrow ICM(R)$ not Clifford monoid)

where do we find the missing classes?

"Simpler problem"

Def $I \underset{wk}{\simeq} J$ if

1) $\begin{cases} (I:I) = (J:J) \text{ "} = S \text{"} \\ \exists \text{ an invertible frac. } S\text{-ideal } L \\ \text{st } LI = J \end{cases}$

$\Updownarrow$

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

[DADE, TAUSSKY, ZASSENHAUS 62]

$$\mathcal{W}(R) := \frac{\{\text{fract } R\text{-id}\}}{\simeq_{wk}}$$

Thm [DTZ]

$$\{\text{fract. } R\text{-ideal } I : I\mathcal{O}_K = \mathcal{O}_K\} \subseteq \left\{ \begin{array}{c} R\text{-submodules} \\ \text{of } \mathcal{O}_K/\mathfrak{f}_R \end{array} \right\}$$

$\Downarrow$

$\mathcal{W}(R)$

"finite"
"indep of $[K:\mathbb{Q}]$"

"Recover ICM(R) from $\mathcal{W}(R)$"



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

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

Thm

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

$\forall S \supseteq R \rightsquigarrow \mathrm{ICM}(R)$.

Conclusion

$p = 2, \dots, 31$

dim = 2 a lot of q some powers

all irreducible char poly

partial data because of bugs ...

dim = 3 $q = \underbrace{2, 3, \dots, 7}$

all cases

isolated examples

dim = 4

Nastiest example of ICM

$R = \mathbb{Z}[\alpha]$ $\alpha$ root of $f = x^3 - 1000x^2 - 1000x - 1000$

$[\mathcal{O}_K : R] = 1000$ $[\mathcal{O}_K : f_R] = 1000^2$ (?)

$\# \mathrm{ICM}(R) = 69116$