* COMPUTING ISOMORPHISM CLASSES OF ABELIAN VARIETIES OVER FINITE FIELDS.

§ INTRODUCTION

Let k be a field.

Remember: quote D. T. Z
+ extra stuff I did

Q: is every order C. Macaulay
typo: λ missing in the slides
Q: Alexey...

- An abelian variety A over k is a connected and complete gr. Var.
  ↘ ("compact" / $\mathbb{C}$)

- Facts: an ab. var. A is projective, smooth and the group structure is abelian.

Ex

ab. var. of dimension 1 = elliptic curve E

- if $\mathrm{char}\, k \neq 2, 3$ we can describe E by

$$Y^2Z = X^3 + AXZ + BZ^3 \quad \text{with} \quad 4A^3 + 27B^2 \neq 0$$

- " - if $\mathrm{char}\, k = 2$ or 3 we also have an equation, with more coefficients.
  - given the eq. we can check effectively if two curves are isomorphic. "
- "In dimension > 1, it is very hard to produce the equations (Mumford eg, living in a huge space)."
- (" we need a different object to describe our ab. var's"
- $\boxed{k = \mathbb{C}}$ We have an equivalence of categories:

$$\left\{\begin{array}{l}\text{ab varieties over } \mathbb{C} \\ \text{of dim } g\end{array}\right\} \quad \circledast \quad \longleftrightarrow \quad \left\{\begin{array}{l}\text{complex tori } \mathbb{C}^g/L, \\ L \text{ a full lattice } (\simeq \mathbb{Z}^{2g}) \\ + \text{ Riemann form}\end{array}\right\}$$

$$A \longmapsto A(\mathbb{C})$$

$\left\{\begin{array}{l} E(iv, iv) = E(v,v) \\ E(v,v) + iE(v,v) \\ \text{is pos def}\end{array}\right.$

(" we can describe A's in terms of L's "

§ $k = \mathbb{F}_q$, $q = p^{nd}$

- "Serre: the equivalence ⊛ does not work in positive char. There are supersingular ell. curves, whose end. alg is quaternionic and does not admit a 2-dim rep."

- Recall that a morphism

$$\varphi : A \to B$$

is called an isogeny if

- φ is surjective and $\dim A = \dim B$

- Eg $A / \mathbb{F}_q$

$$\pi_A : A \longrightarrow A$$

Frobenius endomorphism: { - identity on the top. space
- $\mathcal{O}_A \to \mathcal{O}_A : f \mapsto f^q$

π_A is an isogeny.

- Let $\ell \neq p = \mathrm{char}\, k$.

We have an action

$$\pi_A \curvearrowright T_\ell A = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2 \cdot \dim A}$$

Let $h_A(x)$ be the characteristic poly.

- - $h_A(x)$ does not depend on ℓ
- $h_A \in \mathbb{Z}[x]$, monic, with roots of complex abs value $\sqrt{q}$
  $\deg h_A = 2 \cdot \dim A$
  i.e. h_A is a q-Weil polynomial

- **Thm (Honda-Tate)**

  A, B / $\mathbb{F}_q$.

  1 If $A \sim B$ then $P_A = P_B$

  (2 For every irreducible q-Weil poly P, there are an integer e (uniq. det by P) and an ab. var C over $\mathbb{F}_q$ st $P_C = P^e$)

- " Using q-Weil poly we can count ab var / isogeny ".

- **Thm (Deligne 69)** (Centeleghe-Stix 2015)

  There is an anti eq. of categories b/w:

  { abelian varieties A / $\mathbb{F}_q$ s.t. exactly half of the roots of P_A are p-adic units (ordinary) } — no real roots

  $\downarrow$

  { pairs (T, F) where T is a free fin. gen. $\mathbb{Z}$-module, $F: T \to T$ such that:
  - $F \otimes \mathbb{Q}$ is semisimple with eigenvalues of complex abs. value $\sqrt{q}$ ($\sqrt{p}$)
  - half of them are p-adic units
  - $\exists\, V: T \to T$ st $F \circ V = V \circ F = q$ } — no real roots

  $A \mapsto (T(A), F(A))$ — different functor.

- "Pf"

  $A/\mathbb{F}_q \rightsquigarrow \tilde{A} / W(\bar{\mathbb{F}}_q) \rightsquigarrow A_{\mathbb{C}} := \tilde{A} \otimes_{\varepsilon} \mathbb{C}$

  canonical lift

  $\varepsilon: W(\bar{\mathbb{F}}_q) \hookrightarrow \mathbb{C}$

  Put $T(A) := H_1(A_{\mathbb{C}}, \mathbb{Z})$

  and $F(A) :=$ map induced by π_A

- Note: $T(A) \cong \mathbb{Z}^{2 \cdot \dim(A)}$

Thm (M.)

- Let h be a char. poly of an ordinary abelian variety over $\mathbb{F}_q$ $\mathbb{F}_p$ $h(\sqrt{p}) \neq 0$
- Assume h is square-free.

  Put $K := \frac{\mathbb{Q}[x]}{(h)}$ (finite prod of number fields)

  ω
  $F := x \pmod{(h)}$

  $R := \mathbb{Z}[F, q/F]$ ($\subseteq \mathcal{O}_K$ ring of integers of K)

- There is an anti- equiv. of categories :

$$\left\{ \begin{array}{l} \text{ab. var. } / \mathbb{F}_q \text{ with} \\ h_A = h \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{fractional } R\text{-ideals} \\ + R\text{-linear maps} \end{array} \right\}$$

$AV(h)$

Recall: A fractional R-ideal I is a sub-R-module of K such that $\mathrm{rk}_{\mathbb{Z}} I = \mathrm{rk}_{\mathbb{Z}} R$ (full lattice of K)

Idea: - In Deligne one focus on the different endomorphi $F \curvearrowright \mathbb{Z}^{2g}$
- there we "fix F" as a root of h and look at the different R-module structures"

Cor:

$$AV(h)/\cong \longleftrightarrow \text{ideal class monoid } \boxed{ICM(R)}$$

§ ICM

K = finite product of number fields

$\cup$

R = order, i.e. a full lattice in K which is a ring

Def $ICM(R) := \{\text{fractional } R\text{-ideals}\} / \tilde{=}_R$

- **Recall** :- Two fractional R-ideals I and J are
  - isomorphic $\iff \exists\, x \in K^\times : xI = J$
  - I is invertible in R if $\exists\, J$ st $IJ = R$
  - $Pic(R) := \{\text{inv. fract } R\text{-ideals}\} / \tilde{=}_R$

"well known alg. to compute"

- **Lemma** :

$$ICM(R) \cong \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K \text{ over orders}} Pic(S)$$

"eq cff R is Bass $\iff \forall S$ is Gorenstein ring"

Weak equiv. (Dade, Taussky, Zassenhaus) '62

- **Def** $I \sim_{wk} J$ if

$$I_p \cong_{R_p} J_p \quad \forall\, p \in \mathrm{MSpec}(R)$$

- **Prop**: $I_p \sim_{wk} J_p \iff 1 \in (I:J)(J:I)$

- { poly time "

- **Def** Set of wk classes $\mathcal{W}(R)$

- **Prop** All representatives of $\mathcal{W}(R)$ can be found in

$$\mathcal{H} = \{ \text{sub-}R\text{-modules of } \mathcal{O}_K/f_R \}$$

f_R = conductor of R

$:= (R : \mathcal{O}_K)$

("$\mathcal{H}$ is finite & most of the time not-too-big")

• Partition: $\mathcal{W}(R) = \bigsqcup_{R \subseteq S \subseteq \Theta_K} \overline{\mathcal{W}}(S)$

↖ Wk classes w/ mult ring S

$\overline{\mathcal{W}}(S)$ ← iso cl. — " —

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

• Thm (M.)

For every over-order S of R, $\mathrm{Pic}(S)$ acts freely on $\overline{ICM}(S)$ and

$$\overline{\mathcal{W}}(S) = \overline{ICM}(S) / \mathrm{Pic}(S)$$

Repeat $\forall S \rightsquigarrow \overline{ICM}(R)$.

" Cor We have an algorithm to compute the iso cl. of (square free) do var / $\mathbb{F}_q$ ordinary / $\mathbb{F}_p$ no real roots "

§ back to ab. var.

- h, ordinary, char poly, over $\mathbb{F}_q$, square-free
- Howe '95 describes dual varieties and polarizations in Deligne's category

Thm (M.)

- $K = \mathbb{Q}[x]/(h) = \mathbb{Q}(F)$, $R = \mathbb{Z}[F, q/F]$

1) If $A \leftrightarrow I$ then $A^\vee \leftrightarrow \bar{I}^t$

2) If $(\mu: A \to A^\vee) \leftrightarrow (\lambda: I \to \bar{I}^t)$

then μ is a polarization iff:

- $\lambda \otimes \mathbb{R}$ is invertible
- $\bar{\lambda} = -\lambda$
- λ is Φ-positive, where Φ is a specific CM-type of K.

Also $[\deg \mu] = \#\left(\bar{I}^t / \lambda I\right)$

3) If $A \leftrightarrow I$ then

$$\left\{\begin{matrix}\text{non-isomorphic} \\ \text{pol's of } A\end{matrix}\right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{V\bar{V} \,:\, V \in S^\times\}}$$

where $S = (I : I)$.

Also:

$$\mathrm{Aut}(A, \mu) = \{\text{torsion units of } S\}$$

(μ: pol)

§ Final Remarks

- I can handle the case when the char poly has the form

$$h = g^s$$

with g square-free and ordinary (over $\mathbb{F}_q$)
or " + no real roots (over $\mathbb{F}_p$)

when $\mathbb{Z}[F, q/F]$ is Bom

$F = x \bmod (g)$ in $\frac{\mathbb{Q}[x]}{(g)}$

" modules will be direct sum of fr. ideals"

- $A \overset{\mathbb{F}_q}{\mapsto} A \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$

- period matrices