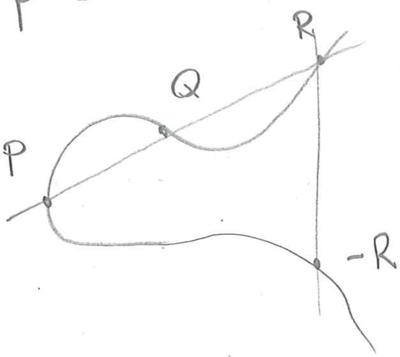
Isomorphism Classes of Abelian Varieties over Finite Fields

variety: $\operatorname{Spec}\left(\dfrac{k[x_1,\dots,x_m]}{I}\right)$

Ex $k[x,y]$, char $k \neq 2,3$

$y^2 = x^3+ax+b$ $4a^3+27b^2 \neq 0$

$+$ pt at $\infty = O$



$P+Q+R=O$

abelian variety: connected, complete group variety $/k$

" Nice prop: - projective (no equations in gen)"
- non-sing
- commutative

" EC ⇝ AB   polarization: extra structure that encodes how it embeds in a projective sp".

Goal:

Count principally polarized abelian varieties $/\mathbb{F}_q$ ($q=p^d$) with their group of automorphism.

- Over $\mathbb{C}$

$A/\mathbb{C}$, $\dim A = g$

then: $A(\mathbb{C}) = V/L$ complex torus

$V \simeq \mathbb{C}^g$ vector space

$L \subseteq V$, $L \simeq \mathbb{Z}^{2g}$

"Not every complex torus arises from an abelian variety"

- Need: $E : V/L \times V/L \to \mathbb{R}$ Riemann form

"skewsymmetric + conditions"

- $\{\text{abelian Var}/\mathbb{C}\} \longrightarrow \{\text{complex tori} + \text{Riemann form}\}$

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

is an equivalence of categories

- (principal) polarization

$$\lambda_E : A \xrightarrow{(\simeq)} A^\vee := V^* / L^*$$

$V^* = \{\text{antilinear functionals } V \to \mathbb{R}\}$

$L^* = \{f \in V^* : \mathrm{Im}(f(L)) \subseteq \mathbb{Z}\}$

$$v \longmapsto E(iv, -) + i E(v, -)$$

- "In general, we cannot attach to an abelian variety a full rank lattice on the whole category of ab. var. over an arbitrary field k."

"• Pb/Ex over a finite field $\mathbb{F}_q$ there are object"
such as supersingular elliptic curves.

- "So we need to restrict to a smaller category"
i.e. we cannot consider all the ab. var. / $\mathbb{F}_q$.

§ Ordinary ab. variety over $\mathbb{F}_q$ $\quad q = p^d$, p

- To every abelian variety A of dim g over $\mathbb{F}_q$ we can associate a monic polynomial $h_A \in \mathbb{Z}[x]$ of degree $2g$ called the characteristic poly.
- h_A encodes the # of points of A over finite fields ext,
- "it is an invariant"
  the roots of h_A have $\mathbb{C}$-size $= \sqrt{q}$
- A is called ordinary if:
  - the middle coeff. (of x^g) of h_A is coprime with p;

  $\Updownarrow$
  - A has exactly p^g points of order divisible by p

Def

$\mathcal{L}_q$ category of pairs (T, F) where T is a free and fin. gen $\mathbb{Z}$-modules with an endomorphism $F : T \to T$ such that

(*) "
- $F \otimes \mathbb{Q}$ on $T \otimes \mathbb{Q}$ is semisimple with eigenvalues of size $\sqrt{q}$.
- the middle coeff of the char. poly of F is coprime w/ p.
- there exist $V : T \to T$ st $FV = q$
"

Thm (Deligne '69)

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

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

- if $\dim A = g$, then $\mathrm{rank}_{\mathbb{Z}}\, T(A) = 2g$
- Frob $(A) \mapsto F(A)$ (char poly)
- Howe '95 defined a notion of dual variety and polarization in $\mathcal{L}_q$ which are compatible w/ the equivalence.

add ordinary to Goal

§ Count

- We look at $\mathcal{L}_q$.
- we fix an irreducible characteristic poly h
- Let F be a root of h and $VF = q$
- Then Delige's theorem means that

$$A \longleftrightarrow I \text{ fractional ideal}$$

ab var / $\mathbb{F}_q$ w/ char poly h — of $\mathbb{Z}[F, V] = R$

$K = \mathrm{Frac}(\mathbb{Z}[F, V])$

" Pb we know how to deal w/ invertible fractional ideals, but not much is known about the non-inv. ones "

" This is a number theoretical question "

" Moreover I can translate a lot of interesting geometric properties of A into number theoretical objects "

Thm

a) If $A \longleftrightarrow I$ then $A^\vee \longleftrightarrow \bar{I}^t$

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

$\mathrm{Aut}(A) \longleftrightarrow (I:I)^*$

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

d) A (princ) polarization of A corresponds to a $\lambda \in K^*$ st

- $\lambda I \subseteq \bar{I}^t$ ("=")
- $\bar{\lambda} = -\lambda$ (tot imaginary)

\+ (condition on the p-adic valuation of λ)

(e) $A \simeq A^\vee \Rightarrow (I:I) = \overline{(I:I)}$)

f) (A, λ) princ. pol, $S = (I:I)$ Then

$\left\{ \begin{array}{l} \text{non-isomorphic} \\ \text{polarizations of } A \end{array} \right\} \longleftrightarrow \dfrac{\{\text{tot. positive } u \in S^\times\}}{\{ v\bar{v} : v \in S^\times \}}$

and $\mathrm{Aut}(A, \lambda) \longleftrightarrow \{\text{torsion units of } S\}$

" From the computational pov everything is quite easy but ICM because there are NON - inv. ideals "

- K a # field, that is a finite ~~dic~~ extension of $\mathbb{Q}$
- If R is a Dedekind domain, that is $R = \mathcal{O}_K$, then every ideal is invertible and so

$$ICM(R) = \mathrm{Pic}(\mathcal{O}_K) = Cl_K$$

- If $R \subsetneq \mathcal{O}_K$ we can compute the invertible ideal classes using

$$0 \to \mathcal{O}_K^\times / R^\times \to \left(\mathcal{O}_K/f\right)^\times / \left(R/f\right)^\times \to \mathrm{Pic}(R) \to \mathrm{Pic}(\mathcal{O}_K) \to 0$$

where $f = (R : \mathcal{O}_K) = \{x \in K : x\mathcal{O}_K \subseteq R\}$ <u>conductor</u> of R

- ~~To each fractional ideal I of R we can attach a specific over-order: the multiplicator ring~~

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

~~Note $R \subseteq S \subseteq \mathcal{O}_K$~~

- ~~Moreover if a fractional R-ideal is invertible in an overorder S, that is $\exists\ J$ st $I \cdot J = S$, then $(I:I) = S$.~~
- In general:

$$ICM(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathcal{O}_K \\ \text{over-orders}}} \mathrm{Pic}(S)$$

<u>Ex</u>

- If $[K:\mathbb{Q}] = 2$ then $(*)$ is an equality for every order R.

Ex: $f = x^3 + 10x^2 - 8$, α a root of f.

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

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

there is a 3rd overorder: $S = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \frac{\alpha^2}{2}\mathbb{Z}$

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

We have, $\mathrm{Pic}(\mathcal{O}_K) = \{\overline{\mathcal{O}_K}\}$

$\mathrm{Pic}(R) = \{\overline{R}\}$

$\mathrm{Pic}(S) = \{\overline{S}\}$

but $\mathrm{ICM}(R) = \{\overline{R}, \overline{S}, \overline{\mathcal{O}_K}, \overline{I}\}$

$$I = 2\mathbb{Z} \oplus \frac{\alpha}{2}\mathbb{Z} \oplus \frac{\alpha^2+4}{2}\mathbb{Z}$$

$$\| $$

$$S^\vee = \{x \in K \text{ st } \mathrm{Tr}(xS) \subseteq \mathbb{Z}\}$$ trace dual of S

"$S^\vee$ not invertible $\Leftrightarrow$ S not Gorenstein"

"all the overorders of R are Gorenstein

$\Updownarrow$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \mathrm{Pic}(S)$$ "ICM(R) is a clifford monoid"

"easy to compute"

" Where do look for these extra-non-inv. classes" (8)
" Minkowsi Bound"

- " Simpler Problem " (DADE - TAUSSKY - ZASSENHAUS 1962)

<u>Def</u> I is weakly equivalent to J if

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

$\Updownarrow$

2) $1 \in (I:J)\cdot(J:I)$ ⟵ "easy to check"

$\Updownarrow$

(3) $I_p \simeq J_p \quad \forall\, p$ maximal S-ideal)

$$\mathcal{W}(R) = \{\text{fractional } R\text{-id}\}/_{\text{wk eq}}$$

<u>Thm</u> [D. T. Z]

$$\{\text{fract. } R\text{-ideals } I \text{ st } I\mathcal{O}_K = \mathcal{O}_K\} \subseteq \{R\text{-submodules of } \mathcal{O}_K/f\}$$

finite and "small"

$$\Downarrow$$

$$\mathcal{W}(R)$$

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

Fix an over-order S of R.

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

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

and

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

<u>Thm</u>
- $Pic(S)$ acts freely on $\overline{ICM}(S)$
- $\overline{\mathcal{W}}(S) = \overline{ICM}(S)^{Pic(S)}$ ⇝ Compute $ICM(R)$

* Conclusion :

We were able to count the number of all iso classes of ppav dimonany ab var $\mathbb{F}_q$ w/ irreducible char polynomial w/ autom.

of dim	2	(a lot of q)
	3	(some)
	4	(few)