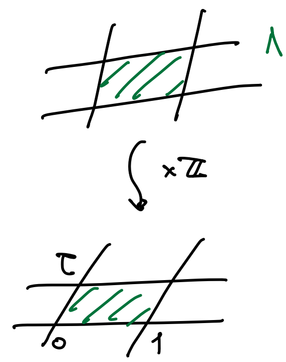
Lecture 0: Introduction to Abelian Variety

by Liang Xiao, Sept 9

§1 Elliptic Curves

"Abelian variety" = n-dim'l elliptic curve.

Ⓐ Elliptic curve $/\mathbb{C}$:



$\mathbb{Z}^{\oplus 2} \approx \Lambda \subseteq \mathbb{C}$ s.t. $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{C}$.

$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda \simeq (\mathbb{C},+)/(\Lambda,+)$.

Up to multiplication by an elt $z \in \mathbb{C}^\times$,

may assume $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\tau$,

$\tau \in \mathfrak{h} = \{\tau \in \mathbb{C} \mid \operatorname{Im} \tau > 0\}$.

* Can check that $E(\mathbb{C}) = \mathbb{C}/\Lambda_\tau$ is an algebraic variety

$\leadsto$ $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{C}$ with $\operatorname{Disc} = 4A^3 + 27B^2 \neq 0$.

$E^\circ := \operatorname{Spec} \mathbb{C}[x,y]/(y^2 - x^3 - Ax - B) \subseteq \mathbb{A}^2_{\mathbb{C}} \subseteq \mathbb{P}^2_{\mathbb{C}}$.

Equivalently, E = closure of E° in $\mathbb{P}^2_{\mathbb{C}} = \underset{[x:y:1]}{E^\circ} \cup \underset{[1:0:0]}{\{\infty\}}$

And $E(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}/\Lambda_\tau$

$\infty \longmapsto$ "0".

Ⓑ Elliptic curves / finite fields $\mathbb{F}_q$, where $q = p^r$.

E = closure of $\operatorname{Spec} \mathbb{F}_q[x,y]/(y^2 - x^3 - Ax - B)$ inside $\mathbb{P}^2_{\mathbb{F}_q}$.

$\Rightarrow$ In particular, $E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + Ax + B\} \cup \{\infty\}$.

as a finite additive group.

<u>Theorem</u> (Hasse) $a_q = q + 1 - \#E(\mathbb{F}_q)$ (error term)

Then $\boxed{|a_q| \leq 2\sqrt{q}}$.

<u>Sketchy Proof</u>. Consider ($\ell \neq p$ prime) $E[\ell^n] := \{x \in E(\overline{\mathbb{F}}_q) : \overbrace{x +_E \cdots +_E x}^{\ell^n} = \underset{\text{"0" on } E_{grp}}{\infty}\}$.

$\Rightarrow E[\ell^n] \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{\oplus 2}$.

$\rightsquigarrow T_\ell(E) := \varprojlim_n E[\ell^n] \simeq \mathbb{Z}_\ell^{\oplus 2}$ ℓ-adic Tate module of E

$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \circlearrowright$. $\mathbb{Z}_\ell$-linear action.

$\rightsquigarrow$ Gal rep'n $\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \longrightarrow GL_2(\mathbb{Z}_\ell)$.

$ \qquad \qquad \qquad \qquad \qquad \quad \overline{\phi_q}^{\hat{\mathbb{Z}}}$, $\phi_q :=$ arithmetic Frob.

$$\phi_q \longmapsto \begin{pmatrix} \alpha & \\ & \beta \end{pmatrix}$$

well-def'd up to conjugation

<u>Fact</u> $\mathrm{Tr}(\rho_{E,\ell}(\phi_q)) = a_q \; (= \alpha + \beta)$, $\det(\rho_{E,\ell}(\phi_q)) = q \; (= \alpha\beta)$. $\Big\{$ α, β are zeros of $x^2 - a_q x + q = 0$. (<u>Rmk</u> α, β are alg integers)

<u>So</u> Hasse's thm $\Leftrightarrow |a_q| \le 2\sqrt{q} \Leftrightarrow a_q^2 - 4q \le 0$

$\Leftrightarrow \mathrm{disc}(x^2 - a_q x + q) \le 0$

$\Leftrightarrow$ either α, β complex or $\alpha = \beta$

$\Leftrightarrow |\alpha|_{\mathbb{C}} = |\beta|_{\mathbb{C}} = |q|^{1/2}$. $\square$

<u>Rmk</u> This will later be generalized to Hasse-Weil thm for abelian varieties.

For E/k general field k (e.g. $k = \mathbb{F}_q, \mathbb{Q}, \mathbb{F}_q(t)$) & $\ell \ne \mathrm{char}(k)$,

$\rightsquigarrow$ $\boxed{\rho_{E,\ell} : \mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)) \simeq GL_2(\mathbb{Z}_\ell)}$.

This is a very important Galois rep'n.

© Elliptic curve / $\mathbb{Q}$ or a number field K

$(E(K), +_E)$ is an abelian grp.

<u>Theorem</u> (Mordell-Weil) $E(K)$ is a finitely generated abelian group.

Known that $(E(K), +) \simeq \mathbb{Z}^r \times E(K)_{tor}$

$r =$ Mordell-Weil rank of E/K.

Remark	proj. sm curves $C/\mathbb{Q}$	genus $=0$	genus $=1$	genus >1
	Assume $C(\mathbb{Q}) \neq \emptyset$	$C \simeq \mathbb{P}^1_{\mathbb{Q}}$ (so $C(\mathbb{Q})$ very "infinite")	$C(\mathbb{Q}) = \mathbb{Z}^r \oplus$ finite	$\# C(\mathbb{Q}) < \infty$ (Faltings)
	Positivity of AG	$(\Omega^1_C)^\vee$ ample	$\Omega^1_C \simeq \mathcal{O}_C$	Ω^1_C ample
	Diff Geometry	curvature >0 $\tilde{C} = \mathbb{S}$	curvature $=0$ $\tilde{C} = \mathbb{H}$	curvature <0 $\tilde{C} = \mathbb{D}$

* Hope to generalize the above to AVs.

§2 Abelian Varieties

Definition k any field. An abelian variety A/k is a proj var $/k$

with ① $m : A \longrightarrow A$ k-morphism

② $0 \in A(k)$ k-point of A

$$\begin{tikzcd} A \arrow[d] \\ \operatorname{Spec} k \arrow[u, bend right, "\text{“}0\text{”}"'] \end{tikzcd}$$

③ $i : A \longrightarrow A$ k-isomorphism

s.t. the induced map $m : A(\bar{k}) \times A(\bar{k}) \longrightarrow A(\bar{k})$

gives a group structure on $A(\bar{k})$ with identity $0 \in A(k)$

& the inverse map $i : A(\bar{k}) \to A(\bar{k})$.

Fact ① A is smooth $/k$

② The group law is commutative

③ dim 1 AV = Elliptic curve.

§3 Content of this Seminar (follow Mumford's book)

Chap I Complex analytic story

<u>Chap I</u> Variety language

<u>Chap II</u> Scheme language (refines Chap I; also deals with char $k = p > 0$).

Consider $A[p] := \ker(A \xrightarrow{\times p} A)$

"var language": $A[p](\bar{k}) := \{x \in A(\bar{k}) \mid [p]\cdot x = 0\}$

$$\text{e.g. } A = E,\quad E[p](\bar{k}) = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{ordinary} \\ \{0\}, & \text{supersingular.} \end{cases}$$

$\dim_k R = p^{2\dim A}$.

$$\begin{tikzcd} A \arrow[r, "\times p"] & A \\ \operatorname{Spec} R = \ker = (\times p)^{-1}(\text{"}0\text{"}) \arrow[u] \arrow[r] \arrow[ur, phantom, "\square"] & \operatorname{Spec} k \arrow[u, "\text{"}0\text{"}"'] \end{tikzcd}$$

finite flat of $\deg = p^{2\dim A}$.

Typically R is non-reduced! e.g. $R = k[x]/(x^p)$.

A = finite flat group scheme.

<u>Beginning</u> $A/\mathbb{C}$ AV, $A(\mathbb{C}) = \operatorname{Lie}(A/\mathbb{C}) / H_1(A(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{C}^g/\Lambda$, $g = \dim A$.

<u>Analogy</u> $H_1(\mathbb{C}^\times, \mathbb{Z}) \to \mathbb{C} \simeq \operatorname{Lie}(\mathbb{C}^\times) \xrightarrow{\exp} \mathbb{C}^\times$, where $\mathbb{C}^\times = \mathbb{G}_{m,\mathbb{C}}$

$\rightsquigarrow H_1(A(\mathbb{C}), \mathbb{Z}) \to \operatorname{Lie}(A/\mathbb{C}) \xrightarrow{\text{"exp"}} A(\mathbb{C})$.

<u>Question</u> - Is every $\underbrace{\mathbb{C}^g/\Lambda}_{\text{cplx torus}}$ $(\Lambda \simeq \mathbb{Z}^{2g})$ an abelian variety?

- No!

- Missing: Embedding of $\mathbb{C}^g/\Lambda \hookrightarrow \mathbb{P}^N_{\mathbb{C}}$

$\Leftrightarrow$ find an ample line bundle on $\mathbb{C}^g/\Lambda$.

<u>Fact</u> Ample line bundles on $\mathbb{C}^g/\Lambda$

$\Leftrightarrow$ ample class in $H^2(\mathbb{C}^g/\Lambda, \mathbb{Z})$

$\Leftrightarrow$ positive Riemann form on Λ.

<u>So</u> AV = complex torus + positive Riemann form on Λ. (Chap I–III)

Application ① Help us to understand AV/other fields
② Theta theory.
③ Construct moduli spaces of AVs.

Chap IV Study $\mathrm{Hom}_{\bar{k}}(A,A) = \mathrm{End}(A)$

* Classify $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$-alg.

$\Rightarrow$ (Corollary) R-H for AV / $\mathbb{F}_q$

$\phi_q \curvearrowright T_\ell(A) \simeq \mathbb{Z}_\ell^{2g}$

$\rightsquigarrow$ $|$eigenvalues of $\phi_q|_{\mathbb{C}} = q^{1/2}$.

Comparisons

	Elliptic curves	AVs
①	$\exists$ Weierstrass eqn $y^2 = x^3 + Ax + B$	no "minimal eqns" ($\exists$ theta theory ...)
②	$\bar{k} \backslash E \simeq E^\vee = \mathrm{Pic}^0(E) = \{$all line bundles/$E$ of deg $0\}$ canonical, $x \in E \longmapsto \mathcal{O}_E(0) \otimes \mathcal{O}_E(x)$	$A \not\simeq A^\vee$ typically, $\exists$ polarization $A \to A^\vee$.
③	/ $\mathbb{F}_q$ Hasse bound	/ $\mathbb{F}_q$ R-H
④	/ $\mathbb{Q}$ Mordell-Weil $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times$ fin tor	$A(\mathbb{Q}) = \mathbb{Z}^r \times$ fin tor
⑤	B-SD conj. $\mathrm{ord}_{s=1} L(E/k, s) = r(E/k)$	$E \rightsquigarrow A$.

Modularity ⑥ $E/\mathbb{Q} \leftrightarrow f$ mod form of wt 2. $\quad A/\mathbb{Q} \longleftrightarrow \boxed{?}$

$\dim A = 2 \leftrightarrow GSp_4$ auto forms.
$(g) \quad (GSp_{2g})$