The Tate module of an elliptic curve

over $k = \bar{k}$

I. Elliptic Curve

Def: An elliptic curve is an irreducible, smooth projective curve of genus 1 with a specific point O

char $k \neq 2, 3$

Weierstrass $\wp$ function

$\{ Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3 \}$

$\subseteq \mathbb{P}^2_k$

$(k = \mathbb{C})$

$E \simeq \mathbb{C}/\Lambda$

where $\Lambda = \mathbb{Z} + \mathbb{Z}\tau \quad \tau \in \mathbb{H}^+$

Rmk: over $\mathbb{C}$

$\mathbb{C} \to \mathbb{C}/\Lambda$ is the universal covering

$\rightsquigarrow H_1^{\bullet}(E, \mathbb{Z}) \cong \Lambda \cong \mathbb{Z}^2$

Fact: • Elliptic curves have a group structure

Def: E_1, E_2 elliptic curves / k. A homomorphism b/w E_1 & E_2 is a morphism of alg variety & preserves group structure.

If ϕ is surjective, then it is called isogeny.

$\mathrm{Hom}(E_1, E_2) = \{ \phi : E_1 \to E_2 \text{ hom} \}$ $\qquad$ $\mathrm{End}(E) = \mathrm{Hom}(E, E)$

$= \{ [0] \} \cup \{ \text{isogenes} \}$

↑ zero gp hom

Ex: $[m]: E \to E$ $\quad \deg([m]) = m^2$

$P \mapsto m \cdot P$

II. Endomorphism rings / $\mathbb{C}$

Prop: $E_1 = \mathbb{C}/\Lambda_1$, $E_2 = \mathbb{C}/\Lambda_2$

then $\exists$ isom

$$\mathrm{Hom}(E_1, E_2) \xrightarrow{\sim} \{\alpha \in \mathbb{C} \mid \alpha \cdot \Lambda_1 \subseteq \Lambda_2\} \subset \mathrm{Hom}(\Lambda_1, \Lambda_2)$$

$$\text{IIS}$$

$$M_2(\mathbb{Z}^{\bullet})$$

For an elliptic curve $E/\mathbb{C}$, we have a map

$$\mathbb{Z} \hookrightarrow \to \mathrm{End}(E) \quad (n \mapsto [n])$$

Def E has complex multiplication (CM) if

$$\mathbb{Z} \subsetneq \mathrm{End}(E)$$

Thm E has CM $\Leftrightarrow \tau \in \mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{N}$

In that case, $\mathrm{End}(E) \simeq \mathbb{Z} + f \cdot \mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$

↑ some number.

Pf: E CM $\Leftrightarrow \alpha \cdot \Lambda \subseteq \Lambda$ for some α

$\Rightarrow \alpha \in \Lambda \Rightarrow \alpha = a + b\tau$, $a, b \in \mathbb{Z}$, $b \neq 0$

since $a \in \mathrm{End}(E) \Rightarrow \alpha = b\tau \in \mathrm{End}(E)$

[Multiply by $b\tau$ on $\mathbb{C} \cong \mathbb{R} \oplus \mathbb{R}\tau$ given by $\begin{pmatrix} 0 & m \\ b & n \end{pmatrix}$, $m, n \in \mathbb{Z}$

so $(b\tau)^2 - n \cdot (b\tau) + mb = 0$

hence τ is quadratic over $\mathbb{Q}$]

III. Quaternion Algebras

k field, $\operatorname{char} k \neq 2$

Def: A quaternion algebra / k is a 4-dim'l k-alg w/ v.s. base $\{1, i, j, ij\}$ and

$i^2 = a$, $j^2 = b$, $ji = -ij$ where $a, b \in k^\times$

Fact (Frobenius) If k is a local field (i.e. $\mathbb{Q}_p$, $\mathbb{R}$) then there are only 2 isom classes of quat. algebras.

- $M_2(k)$ (split case)
- unique 4-dim division algebra.

Minkowski's thm Two quat. algs / $\mathbb{Q}$ R_1 & R_2 are isomorphic iff $R_1 \otimes \mathbb{Q}_p \cong R_2 \otimes \mathbb{Q}_p$ $\forall p$ and $R_1 \otimes \mathbb{R} \cong R_2 \otimes \mathbb{R}$

IV. Serre's Observation (char $k = p > 0$)

There's no "reasonable" normal theory for variety / $k \neq 2$ w/ coeff in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{R}$

"reasonable" means functorial & $H_1(E)$ is 2-dim

Thm (Deuring) $\exists$ ell. curves E/k s.t. $\operatorname{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra which is ramified exactly at p & ∞ where $\operatorname{char} k = p$

V Tate Module

Recall: $k = \mathbb{C}$, $n \in \mathbb{Z}$

$$n\text{-torsion} = E[n] = \tfrac{1}{n}\Lambda/\Lambda$$

If ℓ is a prime, we can look at

$$\varprojlim \left(\cdots \to E[\ell^{n+1}] \xrightarrow{\ell} E[\ell^n] \to \cdots \right) \cong \Lambda \otimes \mathbb{Q}_\ell$$

Def: The Tate module of an ell curve $E/$ any k, ℓ

is $T_\ell(E) = \varprojlim_n E[\ell^n]$

Fact: $\operatorname{char} k = p > 0$, $\ell \neq p$ prime

Then $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$

$T_\ell(-)$ is functorial as $(-)[\ell]$ & inverse limits are.

E ell curve, $\ell \neq \operatorname{char} k$

$$\operatorname{End}(E) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{End}(T_\ell(E)) = \operatorname{End}(\mathbb{Z}_\ell \times \mathbb{Z}_\ell)$$

Thm $\operatorname{End}(E)$ is one of the following:

- $\mathbb{Z}$
- order in $\mathbb{Q}(\sqrt{-d})$ [$R \subset \mathbb{Q}$-alg A is an order if $R \otimes \mathbb{Q} = A$]
- order in quaternion algebra