§ Morphisms between EC/k.

Fact: (rigidity thm) ① any Morphism $E_1 \to E_2$ is a translate of gp homophism.

② any gp homophism $E_1 \to E_2$ is either trivial, or an isogeny.

Properties of isogenies. between EC over a field k. $f: E \to E'$

① finite. (projective + finite fiber)

② flat (miraculous flatness theorem).

③ ker f is a finite flat group scheme. (①+②)

④ f is étale ⟺ ker f is an étale group scheme.

base change; unramified at 0, group translate.

⑤ f is étale. ⟺ iff $f^*\Omega_{E'} \to \Omega_E$ is $\frac{\text{inj}}{\text{bij}}$, $(\Omega_{E'/E} = 0)$.

both $\simeq \mathcal{O}_E$

$T_{E',x} \xrightarrow{\sim} T_{E,f(x)}$ is iso

⑥ $(\deg f, \operatorname{char} k) = 1 \overset{\times}{\longleftarrow} \Rightarrow$ f is étale.

(since $f\check{f} = [\deg f]$. it suffices to show $[m]$ is étale. Now $[m]$ induces multiplication by m map. which is inj if $(\operatorname{char} k, m) = 1$)

⑦ when $p = \operatorname{char} k > 0$, $k = \bar{k}$, ker f can be weird

Say $|\ker[p]|$ can be $\underset{\overset{\uparrow}{ss}}{1}$ or $\underset{\nwarrow}{p}$. (It can not be p^2. since otherwise $\ker[p]$ is étale.)

ordinary. $\underline{\mathbb{Z}/p} \propto \underline{\mu_p}$.

$|\ker[p^r]| = 1$ or p^r

§ ℓ-adic & p-adic realizations.

E/k. write $E[m]$ for the m-torsion of E.

$(\mathbb{Z}/\ell^3)^{\oplus 2} \to (\mathbb{Z}/\ell^2)^{\oplus 2} \dashrightarrow (\mathbb{Z}/\ell)^{\oplus 2}$

Def (ℓ-adic Tate module) $T_\ell E = \varprojlim \left(\cdots \xrightarrow{\times\ell} E_{\bar{k}}[\ell^3] \xrightarrow{\times\ell} E_{\bar{k}}[\ell^2] \xrightarrow{\times\ell} E_{\bar{k}}[\ell] \to 0 \right)$

$= \mathbb{Z}_\ell^{\oplus 2} \circlearrowleft \operatorname{Gal}(\bar{k}/k)$.

$(\to x_3 \xrightarrow{\ell} x_2 \xrightarrow{\ell} x_1 \xrightarrow{\ell} 0$

$V_\ell E = T_\ell E \otimes \mathbb{Q}_\ell$

Def (p-div group) If $p = \operatorname{char} k > 0$. p

let $E[p^\infty] = \varinjlim \left(\ker[p] \hookrightarrow \ker[p^2] \hookrightarrow \ker[p^3] \hookrightarrow \cdots \right)$

$\circlearrowright$ Frob & Verschiebung.

$\mathbb{D}(E[p^\infty])_{\mathbb{Q}}$: F-Isocry

Dieu-module : $\mathbb{D}(E[p^\infty]) = \varprojlim (\mathbb{D}(\ker[p^k])) = W^{\oplus 2} \circlearrowleft F, V$ semi-linear action

Rmk ① If $p = \operatorname{char} k > 0$. $T_p E$ does not capture enough information ✓

Rmk ② $T_\ell E$ is "ℓ-adic étale homology" ⟶ $H^1(E_{\bar{k}}, \mathbb{Z}_\ell) = (T_\ell E)^\vee$

$E[p^\infty]$ is "Crystalline homology" — $H^1_{cris}(E/W) = \mathbb{D}(E[p^\infty])$ ⟷

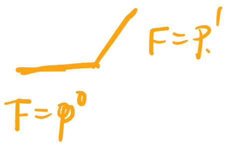
Crystalline coh captures deformation of E. while étale not

Example: $k = \overline{\mathbb{F}}_p$. $W = W(k)$. $\mathbb{D}(E[p^\infty])$ has two types.

(Rmk: $\{p\text{-div gp}\} \simeq \{$Dieudonné module $/W(k)$ free$\}$ over k perfect

Rmk 2. $k = \overline{\mathbb{F}}_p$, through classification of Dieu-modules up to isogeny (DM-class)

① (ordinary) $E[p^\infty] \cong \underbrace{\mathbb{Q}_p/\mathbb{Z}_p}_{\varinjlim_n \frac{1}{p^n}\mathbb{Z}_p} \oplus \underbrace{\mu_{p^\infty}}_{\varinjlim_n \mu_{p^n}}$ $\mathbb{D}(E[p^\infty]) \cong We_1 \oplus We_2$



$$F\begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} 1 & \\ & p \end{bmatrix}\begin{bmatrix} e_1 \\ e_2 \end{bmatrix}$$

$$V\begin{bmatrix} e_1 \\ e_2 \end{bmatrix} = \begin{bmatrix} p & \\ & 1 \end{bmatrix}\begin{bmatrix} e_1 \\ e_2 \end{bmatrix}$$

② (supersingular) $\mathbb{D}(E[p^\infty]) \cong We_1 \oplus We_2$

$F = \begin{pmatrix} & 1 \\ p & \end{pmatrix}$, $V = \begin{pmatrix} & 1 \\ p & \end{pmatrix}$ $FV = \begin{pmatrix} & 1 \\ p & \end{pmatrix}\begin{pmatrix} & 1 \\ p & \end{pmatrix} = p \cdot \mathrm{id}$.

If $f = [m]$ then $T_\ell f = [m]$ iso.

§ Functoriality of realizations.

Notation: $E_1, E_2/k$.

Example: If $f \in \mathrm{End}(E)$, $f \neq 0$, then $T_\ell E \xrightarrow{T_\ell f} T_\ell E$ is inj of torsion coker $\Rightarrow V_\ell E \to V_\ell E$

$(x_n, x_{n-1}, \cdots, x_1, 0) \xrightarrow{f} (f(x_n), \cdots, f(x_1), 0)$

$\overset{\shortparallel}{0}$ $f(x_1) = 0$ $\Downarrow$ $f = 0$

Ⓐ $\mathrm{Hom}_k(E_1, E_2) \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\bar{k}/k)}(T_\ell(E_1), T_\ell(E_2))$ are injective.

$f \longrightarrow T_\ell f$

$\longrightarrow \mathrm{Hom}_{F,V}(E_1[p^\infty], E_2[p^\infty])$.

Have natural maps.

Pf: If $f \longrightarrow 0$, then f is 0 on every ℓ-torsion pts. $\Rightarrow$ "$\deg f = \infty$" $\Rightarrow f = 0$

Ⓑ If $\ell^m \mid T_\ell(f)$ then $\ell^m \mid f$.

Similarly if $p^m \mid f[p^\infty]$ then $p^m \mid f$.

Pf: $\ell^m \mid T_\ell f \Rightarrow f$ kills $E[\ell^m]$.

$\Rightarrow f$ factors through $E \xrightarrow{[\ell^m]} E/E[\ell^m] \overset{\shortparallel}{E}$

$\Rightarrow \ell^m \mid f$.

Ⓒ $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(\bar{k}/k)}(T_\ell(E_1), T_\ell(E_2))$ are injective.

$\otimes \mathbb{Z}_p$ or $\mathrm{Hom}_{F,V}(E_1[p^\infty], E_2[p^\infty])$ with torsion free Cokernel.

Sketch: to simplify things. let $E_1 = E_2 = E$ (general treatment: let $A = E_1 \times E_2$. and prove this for abelian var).

Suppose. $\exists$ $\mathbb{Z}$- ~~linearly~~ indep elements $f_1, \cdots, f_r \in \mathrm{End}(X)$ and $c_1, \cdots c_r \in \mathbb{Z}_\ell$. s.t.

$c_1 T_\ell f_1 + \cdots c_r T_\ell f_r = 0$. assume r is minimal.

(Consider positive definite bilinear pairing: $\langle f, g \rangle = \deg(f+g) - \deg f - \deg g$. $\underset{\sim}{\deg 2f - 2\deg f} > 0$ $(B(f,f) > 0)$

Change basis, can assume $f_1 \perp f_j$ $(j > 1)$. (Schmidt orthogonalization and scaling.)

let $m \in \mathbb{Z}^+$. choose integers $n_i \equiv c_i \pmod{\ell^m}$.

~~then~~ let $g = n_1 f_1 + \cdots + n_r f_r$. then $\ell^m \mid T_\ell g - \underset{\sim}{T_\ell(c_1 f_1 + \cdots c_r f_r)}$ $\overset{\shortparallel}{0}$.

So $\ell^m \mid g$. so $\ell^m \mid \langle f_1, g \rangle = n_1 \langle f_1, f_1 \rangle \Rightarrow \ell^m \mid c_1 \langle f_1, f_1 \rangle$

So c_1 is divisible by arbitrary ℓ^n. $\Rightarrow c_1 = 0$ ※.

Coker tor-free: Say $\phi \in \mathrm{Hom}(T_\ell(E), T_\ell(E_2))$ is s.t. $\phi = \ell \psi$ & $\phi \in \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$, then

let $\phi = \alpha_1 \phi_1 + \cdots \alpha_r \phi_r$, $\alpha_1, \cdots \alpha_r \in \mathbb{Z}_\ell$. $\psi_i \in \mathrm{Hom}(E_1, E_2)$ & $\phi_1 \cdots \phi_r$ $\mathbb{Z}$-independent

Not divisible by ℓ.

let $n_i \equiv \alpha_i \pmod{\ell}$.

then $\phi' = n_1 \phi_1 + \cdots + n_r \phi_r$

$\ell \mid \phi' - \phi \Rightarrow \ell \mid \phi' \Rightarrow \ell \mid n_i \ \forall i \Rightarrow \ell \mid \alpha_i \ \forall i$

Ⓓ Cor: $\mathrm{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module with rank ≤ 4

Pf: $\mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) = \mathbb{Z}_\ell^{\oplus 4}$.

Ⓖ (Isogeny thms). k is a finitely gen field (finite field / # field. function field over fin or # field)

$$\mathrm{Hom}_k(E_1, E_2)\otimes\mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_{G}(T_\ell(E_1), T_\ell(E_2))$$ ← also

$$\otimes\mathbb{Z}_p \xrightarrow{\sim} \mathrm{Hom}_{F,V}(E_1[p^\infty], E_2[p^\infty])$$

if $E_1 = E_2$ also G acts semi-simplely on $V_\ell(E)$.

Sketch ① reduce to case $E = E_1 = E_2$ $(A = E_1\times E_2)$.

☆ ② Finiteness of isogeny class over k.

k finite: trivial.

k # field — Faltings height

function field > Heights — Zarhin.

③ purely algebraic manipulation;

Ⓕ Characteristic polynomial: let $f\in \mathrm{End}(E)$.

get $T_\ell f \in \mathrm{End}(V_\ell E)$. the characteristic polynomial is of form $x^2 - \mathrm{tr}(T_\ell f)x + \det(T_\ell f) = 0$. ⊛

thm: ① $\det(T_\ell f) = \deg f$

② $\mathrm{tr}(T_\ell f) = 1 + \deg f - \deg(1-f)$.

③ (⊛) is ℓ-independent. is called the char poly of f. In fact, it is the polynomial $P(x)$ s.t. $P(n) = \deg(n-f)$.

Sketch: ① ⇒ ② since for any matrix A, we have

$$\mathrm{tr}(A) = 1 + \det(A) - \det(1-A),$$

so $\mathrm{tr}(T_\ell f) = 1 + \det(T_\ell f) - \det(T_\ell(1-f))$.

① ⇒ ③.

$\deg(n-f) = \det(T_\ell(n-f))$

$= \det(n - T_\ell f)$,

$= \mathrm{Char\,poly}(T_\ell f)$

proof of ① ?

Silverman "Weil pairing" (~~Essentially~~ Pf 1: $\overset{\det H^1_{et}}{\wedge^2 H^1_{et}} = H^2_{et}$ ↺ f acts by deg f "cycle class")

Pf 2: Say char $k=0$ (char $k=p$ is similar).

let $T_{\hat{\mathbb{Z}}}E = \prod_{\ell\text{ prime}} T_\ell E$. (adelic realization).

roughly $\ker f$.

then $\deg f = \left| T_{\hat{\mathbb{Z}}}E \big/ T_{\hat{\mathbb{Z}}} f(T_{\hat{\mathbb{Z}}}E) \right|$

think of f as matrix on $\underbrace{T_{\hat{\mathbb{Z}}}E\otimes\mathbb{Q}}$. ($\hat{\mathbb{Z}}\otimes\mathbb{Q}=\mathbb{A}$

Then $\deg f = \det(T_{\hat{\mathbb{Z}}} f)$.

Now

$$\begin{tikzcd}
\mathrm{End}(E) \arrow[r, hook] \arrow[rdd] & \mathrm{End}(T_{\hat{\mathbb{Z}}}E\otimes\mathbb{Q}) \arrow[dd] \\
f \arrow[r, mapsto] \arrow[rdd, mapsto] & T_{\hat{\mathbb{Z}}}f \arrow[dd] \\
& \mathrm{End}(T_\ell E\otimes\mathbb{Q}) \\
& T_\ell f
\end{tikzcd}$$

$\det f = \det(\underbrace{T_{\hat{\mathbb{Z}}} f}) = \det(T_\ell f)$

philosophy: f, as a linear operator, is "defined over $\mathbb{Q}$"
So projecting to $T_\ell f$ loses no information

(when char $k=p$, replace T_pE by $\underline{\mathbb{D}(E[p^\infty]^\vee)}$)

§ EC : over finite field. $k=\mathbb{F}_q$

$y^2 = x^3+ax+b$
$a,b\in k.$
$\subset \mathbb{P}^2_{\bar{k}}$

Frobenius π_E : $(\text{absolute Frob})^q$ or $(\text{relative Frob})^q$ or $\begin{matrix} E \longrightarrow E \\ (x,y)\longrightarrow (x^q,y^q)\end{matrix}$

Fact : π_E is ~~a~~ group homomorphism. (rigidity). π_E is purely inseparable

tangent space argument.
$\frac{dx}{y} \to \frac{dx^p}{y^p} = \frac{p\,dx^{\cdot\cdot}}{y^{\cdot\cdot}} = 0$

charpoly(π_E) : $x^2-tx+q=0$ $(*)$

Fact : π_E, $\hat{\pi}_E$ are two roots of $(*)$. (Since π_E is a root, so is $\frac{q}{\pi_E} = \hat{\pi}_E$).

Thm: ① (counting pts) $t = q+1-\#E(\mathbb{F}_q)$

② (Hasse weil bound) $|t|\le 2\sqrt{q}$. (It can happen that $t=2\sqrt{q}$.)
then E is SS

pf: ① $t = 1+\deg\pi_E - \deg(1-\pi_E)$.

& $\deg(\underline{1-\pi_E}) = \#E(\mathbb{F}_q)$, $\deg\pi_E = q$.

étale : look at induced map on tangent spaces.

② Identify $\mathbb{Z}[1]\subseteq \mathrm{End}(E)$ with $\mathbb{Z}$.

So $0\le \deg(m1_E-n\pi_E) = (m1_E-n\pi_E)(m\hat{1}_E-n\hat{\pi}_E)$

$= m^2+n^2q-nm(\pi_E+\hat{\pi}_E)$

$= m^2+n^2q-nm.t$.

$\Delta = t^2-4q\le 0 \Rightarrow |t|\le 2\sqrt{q}$ □

Thm: TFAE

Slogan: EC/Isogeny ⟺ Trace of Frob.

① $E_1\sim E_2$ over k.

② $V_\ell(E_1)\sim V_\ell(E_2)$ as G-modules

③ $V_\ell(E_1)\sim V_\ell(E_2)$ as $\mathbb{Q}_\ell[\phi]$-modules

④ Charpoly(π_{E_1}) = Charpoly(π_{E_2})

⑤ $\mathrm{Tr}(\pi_{E_1}) = \mathrm{Tr}(\pi_{E_2})$

⑥ $\# E_1(k) = \# E_2(k)$

ϕ acts semi-simply

by Thm above.

pf ① ⟺ ② ⟺ ③ ⟺ ④ ⟺ ⑤ ⟺ ⑥ □

Tate's isogeny thm

G topologically gen'd by ϕ

by $(*)$ explicitly

Question: ① What trace can appear? ② Can we tell SS / ordinary from trace ??

Honda-Tate style question

Overview. A simple abelian Var $/k = \mathbb{F}_q$ $q = p^a$.

- q-Weil number is an algebraic integer α s.t. $|\sigma(\alpha)| = \sqrt{q}$ for all $\sigma \in Gal(\mathbb{Q})$.
- $\pi_A \in \overset{\text{Division.}}{End^0(A)}$ π_A admits minimal poly P_A.

then By weil conjectures. roots of P_A are q weil numbers.

get a map.
$$\{\text{Simple A.V}/k\}/_{\text{isogeny}} \xrightarrow{\ \Phi\ } \{q\text{-Weil numbers}\}/_{\text{Conj}}$$

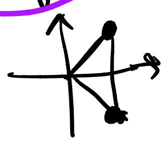
Thm (HT). Φ is bijection.

$$\begin{tikzcd}
\{\text{Simple A.V}/k\}/_{\text{isogeny}} \arrow[r, "HT"] & \{q\text{-Weil numbers}\}/_{\text{Conj}} \\
\{\text{Elliptic Curves}/k\}/_{\text{isogeny}} \arrow[u, hook] \arrow[r, hook, "HT_{EC}"] & \left\{\begin{array}{l} q\text{-weil numbers} \\ \text{of degree } 1 \text{ or } 2 \end{array}\right\}/_{\text{Conj}} \arrow[u, hook] \arrow[d, equal] \\
& \{\pm\sqrt{q}\}/_{\text{conj}} \cup \left\{\begin{array}{l}\text{roots of} \\ x^2 - tx + q = 0\end{array}\right\}/_{\text{conj}} \quad |t| < 2\sqrt{q}
\end{tikzcd}$$

real ones

imaginary ~~complex ones~~

Caveat: HT_{EC} is injective, but not surjective in general.
$|t| \le 2\sqrt{q}$



That is, there may be $x^2 - tx + q = 0$ ~~that~~ is not Char poly of (π_E) but is ~~char~~ mini- poly of (π_A).

Higher dim abelian var.

Question: describe $im(HT_{EC})$.

It suffices to find all possible $t, \in [-2\sqrt{q}, 2\sqrt{q}]$ that comes from $tr(\pi_E)$ of EC.

Thm (HT_{EC}). All $t \in [-2\sqrt{q}, 2\sqrt{q}]$ that come from trace of EC are

$q = p^a$.

① $(t, p) = 1$, $\rightarrow$ (E is ordinary)

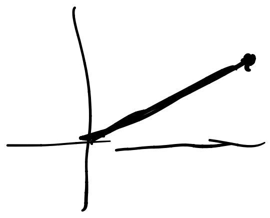
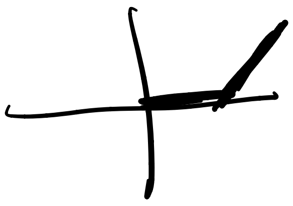
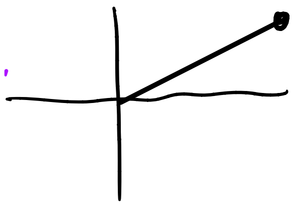
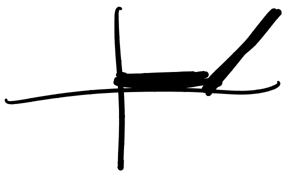
② If $2 \mid a$: $t = \pm 2\sqrt{q}$. $\longrightarrow$ (E ss, $End^0(E)$ = Quaterion)

③ $2 \mid a$ and $p \not\equiv 1 \pmod 3$. : $t = \pm\sqrt{q}$

④ $2 \nmid a$ and $p = 2$ or 3 : $t = \pm p^{\frac{a+1}{2}}$.

⑤ $2 \nmid a$. or $2 \mid a$ & $p \not\equiv 1 \pmod 4$: $t = 0$.

(E ss, $End^0(E) = \mathbb{Q}(\pi_E)$)

Thm:	SS. EC /k	Ord EC / k
TFAE ① $E[p^\infty]$	loc-loc type.	$\frac{\mathbb{Q}_p}{\mathbb{Z}_p} \oplus \mu_{p^\infty}$.
② $\mathbb{D}(E[p^\infty])$. p-adic realization	 $F = V = \begin{bmatrix} \cdot & 1 \\ p & \cdot \end{bmatrix}$ $F^2 = p$.	
③ Char poly (π_E)	NP. 	
④ π_E	$\pi_E \in \mathbb{Z}$ or $\pi_E^2 \in \mathbb{Z}$.	p splits in $\mathbb{Q}(\pi_E)$ ← imaginary quadratic
④' $t = Tr(\pi_E)$	$v_q(t) \geq \frac{1}{2}$.	$v_q(t) = 0$ i.e. $(q, t) = 1$
⑤ $End^0(E_E)$	Quaternion	$\mathbb{Q}(\pi_E)$.

Pf ① ⇔ ② easy. ② ⇔ ③ : p-adic realization.

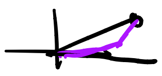
③ ⇔ ④. for ss, say $\pi_E \in \mathbb{Z}$, then Char poly$(\pi_E) = (x - \pi_E)^2 = x^2 \pm 2\sqrt{q}\, x + q$,

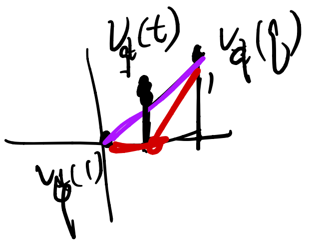
$q = p^{even}$

for ord : $\mathbb{Q}(\pi_E)$ im quad, p splits since

$$\mathbb{Z}[\pi_E] \curvearrowright E[p^\infty] = \underbrace{\mathcal{G}_{\acute{e}t}}_{1\,dim} \oplus \underbrace{\mathcal{G}_{loc}}_{1\,dim.} \Rightarrow \mathbb{Z}[\pi_E] \hookrightarrow End(\mathcal{G}_{\acute{e}t}) = \mathbb{Z}_p.$$

So p must be split.

⑤ ⇔ ④'. SS ⇔  ⇔ $v_p(t) \geq \frac{1}{2}$.



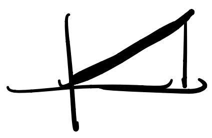
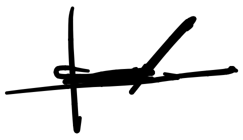
④ ⇔ ⑤ Tate isogeny thm.

diagonal matrix

Say if $\pi_E \in \mathbb{Z}$ then $End^0(E)_{\mathbb{Q}_l} = End_{\pi_{E,l}}(V_l E) \cong M_2(\mathbb{Q}_l)$.

So E is quaternion.

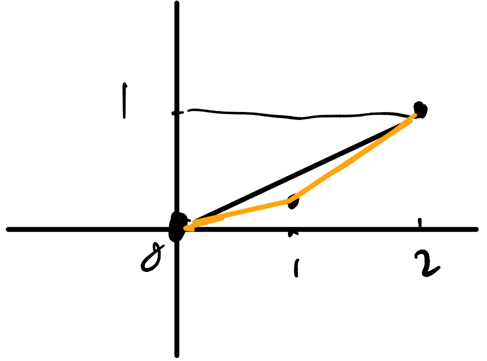
Cor: A nesserary condition for a q-Weil number to be elliptic is its charact

has Newton polygon ~~as~~  or  □

Example: let $p=2$. Consider $x^2-2x+8=0$. it yields

8-Weil number, but it can not be elliptic.. since

Newton polygon:



$v_8(2)=\frac{1}{3}$.