§1 Some properties of ECs

k field.

E/k EC, i.e. curve/k w/ group law $+ : E \times E \longrightarrow E$.

(Recall: Commutative, genus 1, cubic in $\mathbb{P}^2_k$.)

1) Weierstraß Eqn

char $k \neq 2, 3$. Then $\exists\, a, b \in k$ and an isom

$$E \cong V(y^2 = x^3 + ax + b)^{\text{closure}} \subseteq \mathbb{P}^2_k.$$

$$e \longmapsto [0:1:0].$$

Conversely, pick $a, b \in k$. Then

$$V(y^2 = x^3 + ax + b)^{\text{closure}}$$

is <u>smooth</u> cubic

$\Leftrightarrow$ $x^3 + ax + b$ separable over k

$\Leftrightarrow$ discriminant $\Delta \neq 0$,

$$\Delta := 4a^3 + 27b^2.$$

Reference: [Silverman $\overline{\text{III}}$]

2) Classification

To E, may associate <u>j-invariant</u> $j(E) \in k$.

If $k = \overline{k}$, classifies E up to isom.

If char $k \neq 2, 3$ & E as above, $j(E) = 108 \cdot \frac{(4a)^3}{\Delta}$

3) **Homomorphisms** [Silverman §III.9]

$\mathrm{Hom}(E_1, E_2)$ means Hom of k-group schemes

$\{ f : E_1 \longrightarrow E_2$ k-scheme morph s.t.

$m_{E_2} \circ (f \times f) = f \circ m_{E_1} \}$

Put $\mathrm{Hom}^\circ := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{Hom}$, same w/ End°.

Thm 1) Hom is finite free $\mathbb{Z}$-mod of

rank 0, 1, 2 or 4.

2) Three possibilities for $\mathrm{End}^\circ(E)$

$\mathbb{Q}$

K imag-quad ext of $\mathbb{Q}$

B quaternion division alg/$\mathbb{Q}$ (only char $\neq 0$)

Example $k = \mathbb{C}$, $E_i(\mathbb{C}) \cong \mathbb{C}/\Lambda_i$

$$\mathrm{Hom}(E_1, E_2) = \{ x \in \mathbb{C} \mid x\Lambda_1 \subseteq \Lambda_2 \}$$

$$= \mathbb{C} \cap \mathrm{Hom}_{\mathbb{Z}}(\Lambda_1, \Lambda_2) \hookrightarrow \mathrm{Hom}_{\mathbb{R}}(\Lambda_{1,\mathbb{R}}, \Lambda_{2,\mathbb{R}})$$

is of rank ≤ 2.

E.g. $\mathrm{rk}\, \mathrm{End}(E) = 2$ occurs if and only if

$E(\mathbb{C}) \simeq \mathbb{C}/2\mathbb{Z}2\tau$ w/ $\tau \in K$, $K/\mathbb{Q}$ quadratic

Then $\mathrm{End}(E) \subseteq \mathcal{O}_K$ is an order.

4) Degree $f: E_1 \longrightarrow E_2$ map $\neq 0$.

As the E_i smooth proper curves, f is automatically finite loc free.

$$\deg f := \text{its degree} \in \mathbb{Z}_{>0}.$$

E.g. $\deg [n] = n^2$

Extends naturally to $\mathrm{Hom}^0(E_1, E_2) \xrightarrow{\deg} \mathbb{Q}_{\geq 0}$

$$\frac{a}{b} \cdot f \longmapsto \frac{a^2}{b^2} \cdot \deg f.$$

5) Rosati involution [Silverman Thm III.6.1]

Thm There is an isomorphism

$$\begin{array}{ccc} \mathrm{Hom}(E_1, E_2) & \xrightarrow{*} & \mathrm{Hom}(E_2, E_1) \\ f & \longmapsto & f^* \end{array}$$

characterized uniquely by $f^* \circ f = [\deg f]_{E_1}$.

It satisfies $(g \circ f)^* = f^* \circ g^*$

$$(f^*)^* = f$$

$$(f_1 + f_2)^* = f_1^* + f_2^*.$$

Alternative characterizing property:

$$f^* \underbrace{\mathcal{O}([e] - [x])}_{\in \mathrm{Pic}^0(E_2)} \cong \underbrace{\mathcal{O}([e] - [f^* x])}_{\in \mathrm{Pic}^0(E_1)}$$

§2 The Frobenius

R rng w/ $p \cdot R = 0$. Then $x \overset{F}{\longmapsto} x^p$ is rng endo.

·) $F^{-1}(\mathfrak{p}) = \mathfrak{p}$ for prime $\mathfrak{p} \subseteq R$ since

$x^p \in \mathfrak{p} \rightsquigarrow x \in \mathfrak{p}$ by prime ideal property.

$\Longrightarrow \operatorname{Spec} F = id_{\operatorname{Spec} R}$

·) F commutes with all rng homomorphisms,

so given as following way:

Def X scheme w/ $p \cdot \mathcal{O}_X = 0$.

Absolute Frobenius $F : X \longrightarrow X$ is

·) $|F| = id_{|X|}$

·) $F^*(U) : \mathcal{O}_X(U) \longrightarrow \mathcal{O}_X(\underbrace{|F|^{-1}(U)}_{=U})$

$f \longmapsto f^p$.

Properties ·) Commutes w/ all scheme morphisms

·) $dF = 0$ on $\Omega^1_{X/\mathbb{F}_p}$ since

$d(Ff) = df^p = p f^{p-1} df = 0$.

·) Assume $X \longrightarrow \operatorname{Spec} \mathbb{F}_q$, $q = p^n$.

Then F^n is an $\mathbb{F}_q$-scheme endomorph of X.

Fix base $\mathbb{F}_q$, write F for q-Frobenius from now on.

Lem Let $X \longrightarrow \operatorname{Spec} \mathbb{F}_q$ and $k/\mathbb{F}_q$ any field ext.

Then $X(k)^{F=id} = X(\mathbb{F}_q)$.

Proof Let $x \in X(k)$ factor through affine open

$x : \operatorname{Spec} k \longrightarrow \operatorname{Spec} R \subseteq X$.

Then $F \cdot x$ is the point $\operatorname{Spec}\left(R \xrightarrow{F} R \xrightarrow{x^*} k\right)$

$= R \xrightarrow{x^*} k \xrightarrow{F} k$

Thus $F \cdot x = x \iff \operatorname{Im}(x^*) \subseteq \mathbb{F}_q \iff x \in X(k)$ □

To appreciate Proof shows that $F \in C^\infty X(\overline{\mathbb{F}_q})$ in

same way as Frobenius of $\operatorname{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$.

In general, $\operatorname{Gal}(k'/k)$-action on $X(k')$ for X/k

does not come from k-endomorphisms of X!

Assume now $X/\operatorname{Spec}\mathbb{F}_q$ loc. of. fin type.

Have

$$\Delta : X \longrightarrow X \underset{\mathbb{F}_q}{\times} X$$

$$x \longmapsto (x, x)$$

$$\Gamma_F : X \longrightarrow X \underset{\mathbb{F}_q}{\times} X$$

$$x \longmapsto (x, F(x))$$

$$X^F := \Delta \underset{X \times X}{\times} \Gamma_F \qquad \left(= \Delta(X) \cap \Gamma_F(X) \right)$$

are the <u>schematic</u> Frobenius fixed points

$$X^F(S) = \{ x \in X(S) \mid Fx = x \}.$$

<u>Prop</u> (Transversality of Frobenius)

$$X^F = \coprod_{X(\mathbb{F}_q)} \operatorname{Spec}\mathbb{F}_q \quad \text{"agrees" w/ } X(\mathbb{F}_q).$$

<u>Pool</u> We already know $|X^F| = |X(\mathbb{F}_q)|$

for top spaces. Hence X^F be finite type $/\mathbb{F}_q$,

$\dim X^F = 0$, all closed points $\mathbb{F}_q$-rational.

$\Longrightarrow$ Enough to show X^F reduced,

i.e. $m_x/m_x^2 = 0$ $\forall x$ i.e. $X^F(\mathbb{F}_q[\varepsilon]/\varepsilon^2) = X^F(\mathbb{F}_q)$.

This is local around each point of $X(\mathbb{F}_q)$:

R $\mathbb{F}_q$-alg

$$\begin{array}{ccc} R & \xrightarrow{\tilde{\varphi}} & \mathbb{F}_q[\varepsilon]/\varepsilon^2 \\ \varphi \downarrow & \nearrow_{\text{incl.}} & \\ \mathbb{F}_q & & \end{array}$$

Then $\tilde{\varphi} \circ F = \text{incl} \circ \varphi$ since $(a+b\varepsilon)^q = a$.

So $X(\mathbb{F}_q[\varepsilon]/\varepsilon^2)^F = id = X(\mathbb{F}_q)$. $\square$

Rmk $\{ \operatorname{Spec} \mathbb{F}_q[\varepsilon]/\varepsilon^2 \xrightarrow{\tilde{y}} Y \}$ for x fixed

$$\begin{array}{ccc} \operatorname{Spec}\mathbb{F}_q[\varepsilon]/\varepsilon^2 & \xrightarrow{\tilde{y}} & Y \\ \uparrow & \nearrow_{y} & \\ \operatorname{Spec}\mathbb{F}_q & & \end{array}$$

$$= \operatorname{Hom}_{\mathbb{F}_q\text{-Vsp}}(y^*\Omega^1_{Y/\mathbb{F}_q}, \mathbb{F}_q \cdot \varepsilon)$$

by universal property of Kähler differentials.

So above argument shows $\Omega^1_{X^F/\mathbb{F}_q} = 0$.

This is related to $df = 0$ on $\Omega^1_{X/\mathbb{F}_q}$ of course.

§3 Thm of Hasse

$E \longrightarrow \operatorname{Spec} \mathbb{F}_q$ EC, $q = p^n$

write F for q-Frobenius (instead of F^n)

Lem F is an isogeny of degree q.

Pf For two $\mathbb{F}_q$-alg R, S: $(r \otimes s)^q = r^q \otimes s^q$.

Thus $F_{E \times E} = F_E \times F_E$.

Since F commutes w/ any $\mathbb{F}_q$-scheme morph,

if commutes w/ $+ : E \times E \longrightarrow E$.

$\longrightarrow F_E$ group homom, isogeny since $\neq 0$.

E is smooth of dimension 1 over a field,

hence regular. So $\mathcal{O}_{E,e}$ is a DVR

with residue field $\mathbb{F}_q$. Then

$\mathcal{O}_{E,e} \longrightarrow \mathcal{O}_{E,e}$, $f \longmapsto f^q$ is of degree q.

Since $|F|^{-1}(e) = \{e\}$ since $|F| = id_E$,

this shows $\deg F = q$. $\square$

Rmk :) $X/\mathbb{F}_q$ smooth of dim d.

Then $F: X \to X$ fin. loc free of deg q^d.

:) $G/\mathbb{F}_q$ group scheme $\Longrightarrow$ $F: G \to G$ group scheme homom.

Prop The difference $\psi = 1 - F \in End(E)$ is an étale isogeny.

Proof Isogeny since $\neq 0$.

Claim ψ étale $\Leftrightarrow$ $\ker(\psi) \to \operatorname{Spec} \mathbb{F}_q$ étale

Indeed: Étale is fpqc local

$$\begin{array}{ccc} E \times \ker(\psi) & \overset{h}{\simeq} & E \times_{\psi, E, \psi} E \longrightarrow E \\ & \searrow^{p_1} & \downarrow \qquad\qquad \downarrow \psi \\ & & E \xrightarrow{\psi} E \end{array}$$

where $h(e,k) = (e, e+k)$, $h^{-1}(e_1, e_2) = (e_1, e_2 - e_1)$

So ψ étale $\overset{\text{descent}}{\Longleftrightarrow}$ $E \times \ker(\psi) \to E$ étale

$\overset{\text{descent}}{\Longleftrightarrow}$ $\ker(\psi) \to \operatorname{Spec} \mathbb{F}_q$ étale.

□ Claim.

Now $\ker(\pi) = E^F$ sub of Frobenius fixed points.

Now apply transversality from §2 $\square$

Thm (Hasse) $\left| \#E(\mathbb{F}_q) - q - 1 \right| \leq 2\sqrt{q}$.

Pf $\#E(\mathbb{F}_q) = \deg(1-F)$ by prev result.

$$[\deg(1-F)] = (1-F)(1-F^*)$$

$$= 1 + FF^* - (F + F^*)$$

$$= 1 + q - (F + F^*)$$

1st case If $q = p^n$ w/ n even, can happen $F = [\pm\sqrt{q}]$.

Then $F + F^* = \pm 2\sqrt{q}$ and result is correct. $\square$

2nd case $F \neq [\pm p^{n/2}]$.

Then $K := \mathbb{Q}[F] \subset \mathrm{End}^0(E)$

is an imaginary quadratic field :

1.) Quadratic since $\neq \mathbb{Q}$ and

$\mathrm{End}^0(E)$ either imag-quad ext or

quaternion div alg

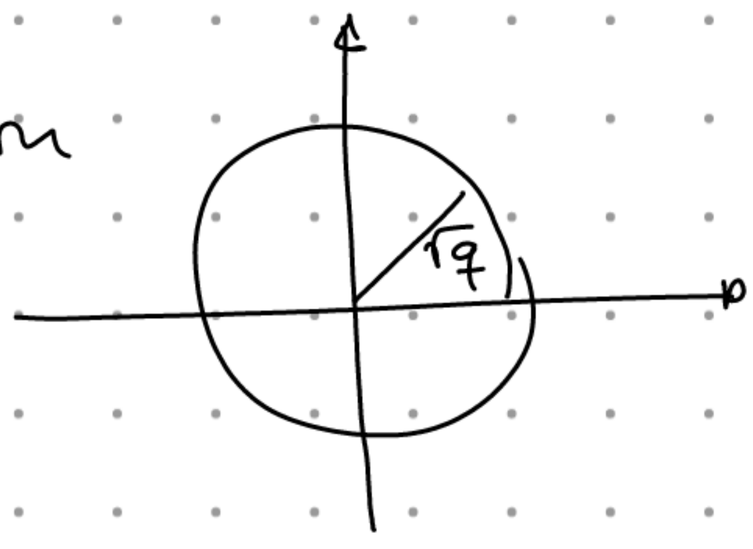
2.) imaginary since this quat div alg is

definite at ∞.

Moreover $\pi^* = \frac{[\deg \pi]}{\pi}$ is Galois conj of $K/\mathbb{Q}$

since $\pi + \pi^* = 1 + q - \deg(1-\pi) \in \mathbb{Q}$.

Then for any $K \hookrightarrow \mathbb{C}$,

π on 

& $|\alpha(\pi)| \leq 2\sqrt{q}$.

□

§4 More on Endomorphisms

1) Quaternion algebras

Def $\mathrm{char}\, k \neq 0$ **Quat alg/k** $\overline{\text{df}}$ 4-dim k-alg B

s.t. $\exists\ a,b \in k^\times$, $B \cong B_{a,b} \cong k[i,j] \Big/ \begin{matrix} i^2 = a \\ j^2 = b \\ ij = -ji \end{matrix}$.

Example $M_2(k)$ with $a = b = 1$

$$i = \begin{pmatrix} 1 & \\ & -1 \end{pmatrix} \qquad j = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$$

(**Note** $\exists$ many a,b s.th. $B_{a,b} \cong M_2(k)$:

Isomorphic $\Leftrightarrow$ $x^2 - av^2 - bt^2 - aby^2 = 0$ has non-trivial solution)

Since $B_{a,b} \cong B_{\lambda^2 a, \mu^2 b}$ $\forall\ \lambda, \mu \in k^\times$,

$i, j \longmapsto \lambda i, \mu j$

$M_2(k)$ is only quat alg/k if $k = \bar{k}$.

Thm / Example $k = \mathbb{Q}_p$ or $\mathbb{R}$. Then $\exists$ precisely 2 quat. alg / k up to iso:

$\mathbb{R}$: $M_2(\mathbb{R})$ & $\mathbb{H} = \mathbb{R}[i,j]/i^2 = j^2 = -1$
$ij = -ji$
$= B_{-1,-1}$

Hamilton quaternions

$\mathbb{Q}_p$: $M_2(\mathbb{Q}_p)$ & $B_{u,p}$ where $u \in \mathbb{Z}_p^\times - (\mathbb{Z}_p^\times)^2$.
not a square.

(Fact $B \neq M_2(k) \Longrightarrow B$ is a skew-field)

Thm $k = \mathbb{Q}$, E/k EC s.th. $\dim_{\mathbb{Q}} \mathrm{End}^\circ(E) > 2$.
Then $\mathrm{End}^\circ(E)/\mathbb{Q}$ is $\simeq$ to the unique quat. alg. B

s.th.:
$$\begin{cases} \mathbb{Q}_\ell \otimes_{\mathbb{Q}} B \simeq M_2(\mathbb{Q}_\ell) & \ell \neq p \\ \mathbb{Q}_p \otimes_{\mathbb{Q}} B \simeq B_{u,p} & \text{(cf. above)} \\ \mathbb{R} \otimes_{\mathbb{Q}} B \simeq \mathbb{H}. \end{cases}$$

2) Involutions Again char $k \neq 2$

Def B/k quat alg. Choose any $B \cong B_{a,b}$ for following

1) **Trace** $tr : B \longrightarrow k$

$$tr(z) := \frac{1}{2} \cdot trace_k(z \circ B)$$

2) **Norm** $N : B \longrightarrow k$

$$N(z) := \sqrt[n]{det_k(z \circ B)}$$

$$N(u + v\cdot i + x\cdot j + y\cdot ij)$$

$$:= u^2 - av^2 - bx^2 - aby^2$$

3) **Main involution** $* : B \longrightarrow B$ **Equivalent:**

a) Unique $*$ s.th. $(z_1 z_2)^* = z_2^* \cdot z_1^*$

& $i^* = -i$, $j^* = -j$

b) Unique $*$ s.th. $*|_K$ = Gal conj on K

$\forall$ $K/\mathbb{Q}$ quadratic, $K \hookrightarrow B$.

c) $*|_k = id$, $*|_{B^{tr=0}} = -id$

i.e. $*(z) = tr(z) - z$.

d) Unique $*$ s.th. $z \cdot z^* = N(z)$.

Conclusion E/k EC s.th. $B = \mathrm{End}^\circ(E)$ quat alg.
Then the Rosati involution is the main involution.
Namely $f \cdot f^\star = [\deg f]$ is characteristic 4).

§5 Concerning Hasse's Thm

Now E/k EC, $K \subseteq \mathrm{End}^\circ(E)$ quadratic/$\mathbb{Q}$.
Then K is imag-quad,
(i.e. $\mathbb{R} \otimes_{\mathbb{Q}} K \cong \mathbb{C}$ instead of $\mathbb{R} \times \mathbb{R}$.)

Namely $\forall f \in K$, $f \cdot \mathrm{conj}(f) = f \cdot f^\star = \deg f \in \mathbb{Q}_{\geq 0}$.

Let $\alpha \in K \setminus \mathbb{Q}$ generator, $P \in \mathbb{Q}[T]$ its char pol.
Then $\mathbb{R}[T]/(P) \cong \mathbb{C}$ means P has no real roots,
i.e. $\mathrm{tr}(\alpha)^2 < 4 \cdot \mathrm{Nm}(\alpha)$
$\iff |\mathrm{tr}(\alpha)| < 2\sqrt{\mathrm{Nm}(\alpha)}$

Setting $E/\mathbb{F}_q$ EC, $\pi \in \mathrm{End}(E)$ Frobenius.

$K = \mathbb{Q}[\pi]$ assumed quadratic/$\mathbb{Q}$.

Then $\#E(\mathbb{F}_q) = \deg(1-\pi)$

$= (1-\pi)(1-\pi^*)$

$= q+1 - \mathrm{tr}(\pi)$

Since K imag-quad, $|\mathrm{tr}(\pi)| \leq 2\sqrt{q}$ as claimed.

Closing remarks

1) Three quantities determine each other:

Char. pol. $P(T) = T^2 - (\pi+\pi^*)T + q \in \mathbb{Z}[T]$

Frobenius Trace $\pi + \pi^* \in \mathbb{Z}$

$\#E(\mathbb{F}_q) = P(1)$.

2) $\forall m$, $\#E(\mathbb{F}_{q^m}) = \deg(1-\pi^m)$

determined by computing $\mathrm{tr}(\pi^m)$ in $\mathbb{Q}[\pi]$.

3) Isogeny invariants: Given $f: E \to E'$,

$$0 = P_E(F_E) \longrightarrow 0 = f P_E(F_E) f^{-1}$$

$$= P_E(f F_E f^{-1})$$

Since F commutes w/ all maps. $\longrightarrow = P_E(F_{E'})$

Thm (Honda-Tate) This sets up a bijection

$$\left\{ \text{ECs } E/\mathbb{F}_q \right\}/\text{Isogeny} \xrightarrow{\cong} \left\{ \alpha \in \mathbb{C} \text{ alg int w/ } \alpha\bar{\alpha} = q \text{ s.th. } [\mathbb{Q}(\alpha):\mathbb{Q}] \leq 2 \right\}/\text{gal. conj.}$$

$$E \longmapsto \text{zero of } P_E.$$

4) If $E/\mathbb{Q}$ EC, may define

$$a_p(E) := F_p + F_p^* \in \mathbb{Z}$$

for almost all p.

Aim of last part of lecture is to explain why $(a_p)_p$ form Fourier coeff of a modular form.