Recall: We defined a pairing

$$e_m : E[m](\bar{k}) \times E[m](\bar{k}) \longrightarrow \mu_m(\bar{k}) = \{x \in \bar{k} : x^m = 1\}$$

under the following assumptions:

- $\mathrm{char}(k) \nmid m$.
- $\deg([m]) = m^2$.

From now on: $E[m] := E[m](\bar{k})$

$x \in E[m]$ $\quad [m]^*([x]-[e]) \equiv 0$ in $\mathrm{Pic}^0(\bar{E})$.

$$\Longrightarrow \quad [m]^*([x]-[e]) = \mathrm{div}(g_x)$$

$g_x \in K(\bar{E})$ unique up to scalar factor.

- g_x^m is invariant under translation by $y \in E[m]$

$$e_m(y,x) = \frac{t_y^* g_x}{g_x} \in \mu_m(\bar{k})$$

Thm: e_m is a bilinear, alternating, non-degenerate Galois equivariant pairing.

Pf: Linearity in 1st variable: ✓

Linearity in 2nd variable: ✓

Alternating: it suffices to show $e_m(x,x) = 1$.

$$\mathrm{div}(t_x^* g_y) = t_x^* [m]^*([y]-[e])$$

$$= [m]^* \underbrace{t_{mx}^*([y]-[e])}_{[y-mx]-[-mx]}$$

Pick $x' \in E(\bar{k})$ s.t. $mx' = x$.

$$\mathrm{div}\left(\prod_{i=0}^{m-1} t_{ix'}^* g_x\right) = [m]^*\left(\sum_{i=0}^{m-1} [x - imx'] - [-imx']\right)$$

$$x \qquad x$$

$$(1-i)x \qquad -ix$$

$$= [m]^*\left(\sum_{i=0}^{m-1} [(1-i)x] - [-ix]\right) = 0 \text{ in}$$

telescopic sum

$mx = e$

$$\Longrightarrow \prod_{i=0}^{m-1} t_{ix}^* g_x \text{ is constant.}$$

$$1 = \frac{t_x^*\left(\prod_{i=0}^{m-1} t_{ix}^* g_x\right)}{\prod_{i=0}^{m-1} t_{ix}^* g_x} = \frac{\prod_{i=1}^{m} t_{ix}^* g_x}{\prod_{i=0}^{m-1} t_{ix}^* g_x} = \frac{t_{mx}^* g_x}{g_x} = \frac{t_x^* g_x}{g_x}$$

$$= e_m(x,x).$$

(Non-degenerate): Suppose $e(x,y) = 1$ for all x.

$\Longrightarrow$ $t_x^* g_y = g_y$ $\Longrightarrow$ g_y is invariant under translation by $E[m]$.

$\Longrightarrow$ $g_y = \tilde{g}_y \circ [m]$ | $E \xrightarrow{[m]} E$ is also the quotient map by $E[m]$

$[m]^* \operatorname{div}(\tilde{g}_y) = [m]^*([x]-[e])$ $\Longrightarrow$ $\operatorname{div}(\tilde{g}_y) = [x]-[e]$.

$\operatorname{div}(g_y)$

$\Downarrow$

$[x]-[e] \equiv 0$ in $\mathrm{Pic}^0(\bar{E})$.

but $E(\bar{k}) \longrightarrow \mathrm{Pic}^0(\bar{E})$ is injective

$x \longmapsto [x]-[e]$

[Rmk: $\varphi: E \to E'$ is a separable isogeny

$K(E') \xrightarrow{-\circ\varphi} K(E)$

$K(E') \xrightarrow{\sim} K(E)^{\ker\varphi}$]

Rmk: X smooth proj curve, $\{f \in K(X)\} \xleftrightarrow{1:1} \{f: X \to \mathbb{P}^1_k\}$

(Galois equivariance) $\quad \dfrac{t_{\sigma x}^* g_{\sigma y}}{g_{\sigma y}} = \sigma\left(\dfrac{t_x^* g_y}{g_y}\right)$.

$\sigma \in \mathrm{Gal}(\bar{k}/k)$

σ acts on $E[m]$

[Rmk: Let X be a smooth projective curve over k. $\quad K(\bar{X}) = K(X) \otimes_k \bar{k}$

$\bar{X}$ = smooth proj. curve w/ function field $K(X) \otimes_k \bar{k}$.

$\Gamma = \mathrm{Gal}(\bar{k}/k)$ acts on $K(\bar{X})$ by

$\sigma\left(\sum f_i \otimes \lambda_i\right) = \sum f_i \otimes \sigma(\lambda_i)$.

$K(X)$ $\quad \overline{k}$

This gives a map $\alpha_\tau : \overline{X} \to \overline{X}$

but $\alpha_{\tau\tau'} = \alpha_{\tau'} \alpha_\tau$. Define an action of Γ on $\overline{X}$

by $\quad \tau . x = \alpha_{\tau^{-1}}(x)$.

$t_{\tau x} = \tau \circ t_x \circ \tau^{-1}$

$\tau^* g_{\tau y} = g_y \qquad$ (up to scalar factor).

$$(t_{\tau x})^* g_{\tau y} = (\tau \circ t_x \circ \tau^{-1})^* g_{\tau y} = (\tau^{-1})^* t_x^* \underbrace{\tau^* g_{\tau y}}_{g_y}$$

$$= (\tau^{-1})^* \left(e(x,y)\, g_y \right)$$

$$= \underbrace{\left((\tau^{-1})^* e(x,y) \right)}_{\tau(e(x,y))} \underbrace{(\tau^{-1})^* g_y}_{g_{\tau y}}$$

Rmk: Suppose $k = \overline{k}$. Let $\varphi : E \to E'$ be an isogeny. Set-theoretically the map $\hat{\varphi}$ is given by

$$\begin{array}{ccc} E' & \xrightarrow{\sim} & \mathrm{Pic}^\circ(E') \\ \hat{\varphi} \downarrow & & \downarrow \varphi^* \\ E & \xrightarrow{\sim} & \mathrm{Pic}^\circ(E) \end{array} \qquad \begin{array}{c} [x'] - [e'] \\ \downarrow \\ \end{array}$$

This is because there is a unique set-theoretical map $f : E' \to E$ s.t. $f \circ \varphi = [\deg \varphi]$.

The uniqueness is clear because φ is surjective. Let $x' \in E'$ and $x \in E$ s.t. $\varphi(x) = x'$. Then

$$\varphi^* \left([x'] - [e'] \right) = \sum_{t \in \ker \varphi} \deg_i \varphi \left([x+t] - [t] \right) \equiv \sum_{t \in \ker \varphi} \deg_i \varphi \left([x] - [e] \right)$$

$$= (\deg \varphi) \left([x] - [e] \right).$$

This shows the existence. By uniqueness f is the set-theoretic map underlying $\hat{\varphi}$.

Prop An isogeny and its dual are adjoint w.r.t. Weil's Pairing.

Let $\varphi: E \to E'$ be an isogeny, let $\hat{\varphi}: E' \to E$. Then

$$e_m(\varphi(x), x') = e_m(x, \hat{\varphi}(x')) \qquad x \in E[m],\ x' \in E'[m].$$

Proof: $e_m(\varphi(x), Y) = \dfrac{t_{\varphi(x)}^* g_Y}{g_Y} = \varphi^*\left(\dfrac{t_{\varphi(x)}^* g_Y}{g_Y}\right) = \dfrac{\varphi^* t_{\varphi(x)}^* g_Y}{\varphi^* g_Y}$

$$= \frac{t_x^* \varphi^* g_Y}{\varphi^* g_Y}$$

$$e_m(x, \hat{\varphi}(Y)) = \frac{t_x^* g_{\hat{\varphi}(Y)}}{g_{\hat{\varphi}(Y)}}$$

$$\operatorname{div}(\varphi^* g_Y) = \varphi^*\left([m]^*([Y] - [e'])\right) = [m]^*\left(\varphi^*([Y] - [e'])\right)$$

$$\equiv [m]^*\left([\hat{\varphi}(Y)] - [e]\right) = \operatorname{div}\left(g_{\hat{\varphi}(Y)}\right).$$

$\equiv$ in $\mathrm{Pic}^\circ(\bar{E})$

$$[\varphi]^*([Y] - [e']) \equiv [\hat{\varphi}(Y)] - [e] \quad \text{in } \mathrm{Pic}^\circ(\bar{E}).$$

$$\Longrightarrow \exists f \in K(\bar{E})^* \text{ s.t. } \operatorname{div}(f) = \varphi^*([Y] - [e']) - ([\hat{\varphi}(Y)] - [e])$$

$$\Longrightarrow \operatorname{div}\left(\frac{\varphi^* g_Y}{g_{\hat{\varphi}(Y)}}\right) = [m]^* \operatorname{div}(f) = \operatorname{div}(f \circ [m])$$

(equalities in $\mathrm{Div}^\circ(\bar{E})$)

$$\Longrightarrow \frac{\varphi^* g_Y}{g_{\hat{\varphi}(Y)}} = \lambda\, f \circ [m] \qquad \lambda \in \bar{k}$$

invariant under $E[m]$

$$\Longrightarrow \frac{t_x^* \varphi^* g_Y}{t_x^* g_{\hat{\varphi}(Y)}} = \frac{\varphi^* g_Y}{g_{\hat{\varphi}(Y)}} \qquad x \in E[m]. \qquad \square$$

Thm: Let $\varphi, \psi: E \to E'$ be isogenies. Then,

$$(\varphi + \psi)^\wedge = \hat{\varphi} + \hat{\psi}.$$

Proof. Suppose $\mathrm{char}(k) \neq 2$. We know that $[2^n]$ is separable of degree $(2^n)^2$. So Weil's pairing exist for $m = 2^n$ for all n.

Let $x \in E[2^n]$, $y \in E'[2^n]$

$$\frac{e_{2^n}(x, (\varphi+\psi)^\wedge(y))}{e_{2^n}(x, \hat{\varphi}(y)\,|\,e_{2^n}(x, \hat{\psi}(y))} \cdot \frac{e_{2^n}((\varphi+\psi)(x), y)}{e_{2^n}(\varphi(x), y)\; e_{2^n}(\psi(x), y)} = 1.$$

($\varphi(x)+\psi(y)$ " $e_{2^n}(\varphi(x), y)\, e_{2^n}(\psi($)

Now we know that $\bigcup_{n \in \mathbb{N}} E[2^n] = E[2^\infty]$ is infinite, thus it is dense in E. Since E, E' are geometrically irreducible and reduced, it follows that $(\varphi+\psi)^\wedge = \hat{\varphi} + \hat{\psi}$.

When $\mathrm{char}(k) = 2$, one can do the argument as soon as we know that $\# E[3] = 9$ and one 3^n-torsion points.

The Hessian argument only works for $\mathrm{char}(k) \geq 5$. But one can compute explicitely the multiplication by 3-map and see that it is of degree 9. Unfortunately the computation is hard. □

Cor: $[m]^\wedge = [m]$ and $[m]$ has degree m^2.

1) $\mathrm{char}(k) \nmid m \Rightarrow E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$.

2) $\mathrm{char}(k) = p \Rightarrow$ either $E[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z}$ for all n
or $E[p^n] = 0$. for all n.

Pf: Because of the previous Theorem, we get $[m]^\wedge = [m]$ by induction on m. Then

$$[m]^\wedge \circ [m] = [m] \circ [m] = [m^2]$$
$$[\deg[m]] \Longrightarrow \deg([m]) = m^2.$$

1) Reduce to m = power of a prime by

$$E[m] = \prod_{p \mid m} E[p^{v_p(m)}].$$

Then, $\mathrm{char}(k) \nmid p$,

$$0 \to \underbrace{E[p]}_{\simeq (\mathbb{Z}/p\mathbb{Z})^2} \to E[p^n] \to \underbrace{E[p^{n-1}]}_{\simeq (\mathbb{Z}/p^{n-1}\mathbb{Z})^2} \to 0$$

because it is a $\mathbb{F}_p$-vector space of dimension 2.

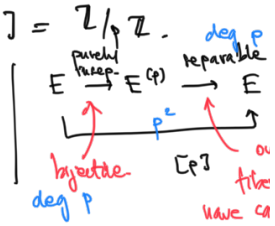
by induction

$$\#E[p^n] \overset{[p^n] \text{ separable}}{=} \deg[p^n] = (p^n)^2 \longrightarrow E[p^n] = (\mathbb{Z}/p^n\mathbb{Z})^2.$$

2) $\mathrm{char}(k) = p$. $\quad [p] = F_p \circ \hat{F}_p$

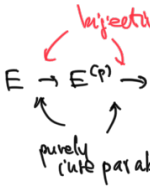
- $\hat{F}_p$ separable $\Rightarrow \#E[p] = p \rightarrow E[p] = \mathbb{Z}/p\mathbb{Z}$.

  $\Rightarrow$ by induction $E[p^i] = \mathbb{Z}/p^i\mathbb{Z}$.



- $\hat{F}_p$ inseparable $\Rightarrow E[p] = 0 \longrightarrow E[p^i] = 0$ by induction. $\square$

  $[p^i]$ purely inseparable.



Def: An elliptic curve over a field of char p is

- **supersingular** if $E[p] = 0$. ($\Leftrightarrow \hat{F}_p$ is separable.)
- **ordinary** otherwise.

Cor: $\deg : \mathrm{Hom}(E, E') \to \mathbb{N}$ is a positive-definite quadratic form.

Pf: If $\varphi \neq 0$, then $\deg \varphi > 0$. We have shown that

$$(\varphi, \psi) \mapsto \deg(\varphi+\psi) - \deg\varphi - \deg\psi \text{ is bilinear.}$$

Since $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ it suffices to show that

$$(\varphi, \psi) \mapsto [\deg(\varphi+\psi)] - [\deg\varphi] - [\deg\psi] \text{ is bilinear}$$

$$\deg(\varphi+\psi) = (\varphi+\psi)^\wedge \circ (\varphi+\psi) \qquad \hat{\varphi}\circ\varphi \qquad \hat{\psi}\circ\psi$$

$$(\hat{\varphi}+\hat{\psi})(\varphi+\psi) = \hat{\varphi}\varphi + \hat{\varphi}\psi + \hat{\psi}\varphi + \hat{\psi}\varphi$$

We're done because $(\varphi, \psi) \mapsto \hat{\varphi}\psi + \hat{\psi}\varphi$ is bilinear. $\square$

Thm (Hasse): Let E be an elliptic curve over $\mathbb{F}_q$. Then

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

Pf: We saw in the exercises, $E^{(q)} = E$.

$F_q : E \to E$ is an endomorphism.

Its fixed points are exactly the $\mathbb{F}_q$-rational points.

Moreover $F_q - \mathrm{id}$ is a separable isogeny.

$$\#E(\mathbb{F}_q) = \#\ker(F_q - id) = \deg(F_q - id)$$

Cauchy-Schwarz inequality for deg:

$$\left|\tfrac{1}{2}\left(\deg(\varphi+\psi) - \deg\varphi - \deg\psi\right)\right| \leq \sqrt{\deg\varphi}\ \sqrt{\deg\psi}$$

$\varphi = F_q \qquad \psi = -id$

$\deg\varphi = q \qquad \deg\psi = 1 \qquad \deg(\varphi+\psi) = \#E(\mathbb{F}_q)$

$$\left|\tfrac{1}{2}\left(\#E(\mathbb{F}_q) - q - 1\right)\right| \leq \sqrt{q} \quad . \qquad \square$$

Tate module: $\mathrm{char}(k) \nmid m$.

(1) $\mu_m = \{x \in \bar{k} : x^m = 1\}. \simeq \mathbb{Z}/m\mathbb{Z}$.

$\Gamma = \mathrm{Gal}(\bar{k}/k)$ acts on μ_m. $\rightsquigarrow \rho_m : \Gamma \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$

- $m = \ell^n$ $\qquad \mu_{\ell^n} \longrightarrow \mu_{\ell^{n-1}}$ is Γ-equivariant
  $x \longmapsto x^\ell$

$\rightsquigarrow \quad T_\ell \mathbb{G}_m := \varprojlim_n \mu_{\ell^n} \simeq \mathbb{Z}_\ell$ (ℓ-adic)

it comes equipped with $\rho : \Gamma \longrightarrow \mathbb{Z}_\ell^*$ cyclotomic character
(continuous representation)

(2) $E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2 \rightsquigarrow \rho_m : \Gamma \longrightarrow GL(E[m])$

Γ acts on it $\qquad \left(\simeq GL_2(\mathbb{Z}/m\mathbb{Z})\right)$.

$m = \ell^n$: $\quad E[\ell^n] \longrightarrow E[\ell^{n-1}]$ $\quad \Gamma$-equivariant.
$x \longmapsto [\ell]x$

$T_\ell E := \varprojlim E[\ell^n]$ $\qquad$ ℓ-adic Tate module of E $\left(\simeq \mathbb{Z}_\ell^2\right)$

$\rightsquigarrow$ continuous representation $\rho_\ell : \Gamma \longrightarrow GL(T_\ell E) \quad (\simeq GL_2(\mathbb{Z}_\ell))$

Rmk: The construction of the Tate module is functorial

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \cup & & \cup \end{array}$$

morphism of elliptic curves defined over k.

$$E[\ell^n] \longrightarrow E'[\ell^n]$$

$$\rightsquigarrow \quad T_\ell f : T_\ell E \longrightarrow T_\ell E' \qquad \Gamma\text{-equivariant}, \ \mathbb{Z}_\ell\text{-linear}.$$

Rmk: Weil's pairing $e_{\ell^n} : E[\ell^n] \times E[\ell^n] \longrightarrow \mu_{\ell^n}$ induces a $\mathbb{Z}_\ell$-bilinear, alternating, non-degenerate, Galois-equivariant pairing

$$e : T_\ell E \times T_\ell E \longrightarrow T_\ell \mathbb{G}_m.$$

If φ is an isogeny, then $T_\ell\varphi$ and $T_\ell\hat{\varphi}$ are adjoint:

$$e(T_\ell\varphi(x), y) = e(x, T_\ell\hat{\varphi}(y)).$$

Thm: 1) The map $\mathrm{Hom}(E, E') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell E, T_\ell E')$ is injective;

2) For $\varphi : E \to E$, $\det(T_\ell\varphi) = \deg\varphi$.

$$\mathrm{tr}(T_\ell\varphi) = t(\varphi) := 1 + \deg\varphi - \deg(\mathrm{id} - \varphi)$$

3) The polynomial $X^2 - t(\varphi)X + \deg\varphi$ vanishes on φ (in $\mathrm{End}(E)$) and has negative discriminant.

Proof: 1) Pick $x \in \mathrm{Hom}(E,E') \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and write it $x = \sum_{i=1}^{r} \lambda_i \otimes \varphi_i$

$\lambda_i \in \mathbb{Z}_\ell$ and $\varphi_i \in \mathrm{Hom}(E, E')$.

Φ = subgroup of $\mathrm{Hom}(E, E')$ generated by $\varphi_1, \dots, \varphi_r$.

$$\mathrm{Hom}(E, E') \supseteq \Phi_{\mathrm{sat}} = \{\psi \in \mathrm{Hom}(E,E') : \psi \circ [m] \in \Phi, \ \exists m \in \mathbb{Z} \setminus \{0\}\}.$$

Claim: Φ_{sat} is a free abelian group of finite rank.

Pf of the Claim: Since $\mathrm{Hom}(E, E')$ is torsion-free, it suffices to prove that Φ_{sat} is finitely generated.

$$\Phi_{\mathrm{sat}} \subseteq \underbrace{\Phi \otimes_{\mathbb{Z}} \mathbb{Q}}_{\text{finite dim. } \mathbb{Q}\text{-vector space}} \subseteq \Phi \otimes_{\mathbb{Z}} \mathbb{R}.$$

↑ extend deg here: it is a positive definite quadratic form.

Moreover, if $\varphi \in \Phi_{\mathrm{sat}} \setminus \{0\}$, then $\deg\varphi \geq 1$.

$\longrightarrow$ Φ_{sat} is discrete in $\Phi \otimes_{\mathbb{Z}} \mathbb{R}$

$\Longrightarrow$ Φ_{sat} is finitely generated. $\square$

Let $\psi_1, \dots, \psi_s$ be a basis of Φ_{sat}. Write

$$x = \sum_{i=1}^{s} \beta_i \otimes \psi_i \qquad \beta_1, \dots, \beta_s \in \mathbb{Z}.$$

Suppose that the image of x in $\mathrm{Hom}(T_\ell E, T_\ell E')$ is 0, i.e.

$$\sum_{i=1}^{s} \beta_i \, T_\ell \psi_i = 0$$

Fix $n \in \mathbb{N}$. Take $b_1, \dots, b_s \in \mathbb{Z}$ s.t. $v_\ell(b_i - \beta_i) \geq n$.

$$\psi = \sum_{i=1}^{s} b_i \psi_i. \quad \in \mathrm{Hom}(E, E').$$

$$\psi \longmapsto \sum_{i=1}^{s} b_i \, T_\ell \psi_i = \sum_{i=1}^{s} (b_i - \beta_i) \, T_\ell \psi_i$$

$$\uparrow \quad \sum \beta_i T_\ell \psi_i = 0$$

$\Longrightarrow$ ℓ^n divides $T_\ell \psi$.

$$\begin{array}{ccc} T_\ell E & \xrightarrow{T_\ell \psi} & T_\ell E' \\ \downarrow & & \downarrow \\ E[\ell^n] & \xrightarrow{0} & E'[\ell^n] = T_\ell E' / \ell^n T_\ell E' \end{array}$$

This means that ψ vanishes on $E[\ell^n]$. Therefore it is of the form $\psi = \tilde{\psi} \circ [\ell^n]$ with $\tilde{\psi} \in \mathrm{Hom}(E, E')$.

$$\tilde{\psi} \circ [\ell^n] \in \Phi_{sat} \quad \Rightarrow \quad \tilde{\psi} \in \Phi_{sat}$$

Since $\psi_1, \dots, \psi_r$ is a basis of Φ_{sat}, ℓ^n divides b_i for each i. So ℓ^n divides β_i for each i.

$\Longrightarrow$ $v_\ell(\beta_i) \geq n$ for each i for each n

$\Longrightarrow$ $\beta_1, \dots, \beta_s = 0$. $\square$