Recall: E, E' elliptic curves on a perfect field k.

Isogeny: Non constant morphism $f: E \to E'$ s.t. $f(O_E) = O_{E'}$.

$H^0(\Omega_E) = k\omega$

$H^0(\Omega_{E'}) = k\omega'$

For any morphism $f: E \to E'$

$f^*\omega' = \lambda_f \omega$ for some $\lambda_f \in k$.

($f^*\omega'$: diff form on E)

Th: 1) if $x \in E(k)$, $t_x : E \to E$, $y \mapsto x+y$, then

$t_x^* \omega = \omega$ i.e. $\lambda_{t_x} = 1$ $\quad (E = E',\ \omega = \omega')$.

2) $\varphi, \psi : E \to E'$ then $\lambda_{\varphi+\psi} = \lambda_\varphi + \lambda_\psi$.

Lemma 1.
Let $\mu : E \times_k E \to E$ be the group law.
$pr_1, pr_2 : E \times E \to E$ the two projections. Then

$$\mu^*\omega = pr_1^*\omega + pr_2^*\omega.$$

Rmk: $d\mu : \mu^*\Omega_{E/k} \longrightarrow \Omega_{E\times E/k} = pr_1^*\Omega_{E/k} \oplus pr_2^*\Omega_{E/k}$.

$\mu^*\omega \longmapsto f_1 pr_1^*\omega + f_2 pr_2^*\omega$ with $f_1, f_2 \in \mathcal{O}(E\times E)$.

$E \times E$ is projective, geometrically irreducible, it has a k-rational point:

$$\mathcal{O}(E\times E) = k. \implies f_1, f_2 \in k.$$

$$\underbrace{(id,e)^*\mu^*\omega}_{\omega} = f_1 \underbrace{(id,e)^* pr_1^*\omega}_{\omega} + f_2 \underbrace{(id,e)^* pr_2^*\omega}_{0}$$

$\mu \circ (id,e) = id$ (e neutral element) $\qquad pr_1 \circ (id,e) = id$ $\qquad$ because $pr_2 \circ (id,e)$ is constant.

$$\implies \omega = f_1\omega \Rightarrow f_1 = 1. \qquad \square$$

Lemma 2. Let A, B be finitely generated k-algebras. Then

$$\Omega_{A\otimes_k B} = \left(A \otimes_k B\right) \otimes_A \Omega_{A/k} \oplus \left(A \otimes_k B\right) \otimes_B \Omega_{B/k}.$$

Pf: Exercise. $\square$

Proof of Lemma 1. The algebraic variety $E \times E$ is covered by open subsets of the form $V_1 \times V_2$ with $V_1, V_2 \subseteq E$ open and affine. Take $V \subseteq E$ open subset

$$\mu^{-1}(V) = \bigcup_{i=1}^{n} \mu^{-1}(V) \cap \left(V_{i1} \times V_{i2}\right) \quad \text{with } V_{i1}, V_{i2} \subseteq E \text{ affine.}$$

$E \times_k E$

$\mu^* \omega \mid_{V_1 \times V_2} \in \Omega_{V_1/k} \otimes \mathcal{O}(V_1 \times V_2) \oplus \Omega_{V_2/k} \otimes \mathcal{O}(V_1 \times V_2)$ ← Lemma 2.

$V_1, V_2 \subseteq E$ affine

$\mu^* \omega \mid_{V_1 \times V_2} = f_1 \, pr_1^* \omega + f_2 \, pr_2^* \omega$ $\quad f_1, f_2 \in \mathcal{O}(V_1 \times V_2)$ are unique.

If we have an affine cover $E \times E = \bigcup_{i=1}^{n} V_{i1} \times V_{i2}$

$\mu^* \omega \mid_{V_{i1} \times V_{i2}} = f_{i1} \, pr_1^* \omega + f_{i2} \, pr_2^* \omega$ $\quad f_{i1}, f_{i2} \in \mathcal{O}(V_{i1} \times V_{i2})$

By uniqueness $(f_{i1})_{i=1}^n$, $(f_{i2})_{i=1}^n$ glue to elements $f_1, f_2 \in \mathcal{O}(E \times E)$.

I want to see that f_1, f_2 are constant. Up to passing to an algebraic closure of k, we may assume $k = \bar{k}$. Take $p \in E$.

$$E \xrightarrow{(id,p)} E \times E \xrightarrow{\mu} E$$
$$x \longmapsto (x, p) \longmapsto x + p.$$

$$\underbrace{(id,p)^* \mu^* \omega}_{t_p^* \omega} = f_1|_{E \times \{p\}} \underbrace{(id,p)^* pr_1^* \omega}_{\omega} + f_2|_{E \times \{p\}} \underbrace{(id,p)^* pr_2^* \omega}_{0}$$

$pr_1 \circ (id, p) = id$

because $pr_2 \circ (id, p)$ is the constant morphism with value p.

$$\Longrightarrow t_p^* \omega = f_1|_{E \times \{p\}} \, \omega$$

$f_1|_{E \times \{p\}} \in \mathcal{O}(E) = k$

$t_p^* \omega = \lambda_{t_p} \omega$ does not depend on x

Look at the map $p \mapsto \lambda_p$. This can be written as

$$E \longrightarrow E \times E \xrightarrow{f_1} \mathbb{A}^1$$
$$p \longmapsto (e, p) \longmapsto \lambda_p.$$

So this is a morphism of algebraic varieties.

$\Longrightarrow$ $p \mapsto \lambda_p$ is constant.

Moreover, $\lambda_e = 1$ because $t_e = id$. Therefore $f_1 = 1$.

By arguing in the same way for f_2 we get the result. □

Proof of the Theorem. 1) Consider the morphism

$$E \xrightarrow{(x,id)} E \times E$$
$$y \longmapsto (x, y)$$

Pull-back the equality

$$(*) \qquad \mu^* \omega = pr_1^* \omega + pr_2^* \omega$$

by (x, id) :

$$\underbrace{(id,x)^* \mu^* \omega}_{t_x^* \omega} = \underbrace{(id,x)^* pr_1^* \omega}_{\omega} + \underbrace{(id,x)^* pr_2^* \omega}_{0 \;\; pr_2 \circ (id,x) \text{ is constant.}}$$

$$\Longrightarrow \lambda_{t_x} = 1.$$

2) $\varphi, \psi : E' \longrightarrow E$ morphisms of elliptic curves.

$$\varphi + \psi \; : \; E' \xrightarrow{(\varphi,\psi)} E \times E \xrightarrow{+} E$$

Pull-back $(*)$ by (φ, ψ) we get

$$\underbrace{(\varphi,\psi)^* \mu^* \omega}_{(\varphi+\psi)^* \omega} = \underbrace{(\varphi,\psi)^* pr_1^* \omega}_{\varphi^* \omega} + \underbrace{(\varphi,\psi)^* pr_2^* \omega}_{\psi^* \omega}$$

□

DUAL ISOGENIES

Let $\varphi : E \to E'$ be an isogeny between elliptic curves.

$$\varphi^* : Div^0(E') \longrightarrow Div^0(E)$$

$$\underset{\| \; \Sigma m_i [x_i]}{D} \longmapsto \varphi^* D = \sum_i \Big(\sum_{x_i' \mapsto x_i} ord_{x_i'}(\pi) \, m_i [x_i'] \Big)$$

- $\deg(\varphi^* D) = \deg \varphi \cdot \deg D$
- $\varphi^* \, div(f) = div(\underset{f \circ \varphi}{\varphi^* f})$

$$\rightsquigarrow \varphi^* : Pic^0(E') \longrightarrow Pic^0(E).$$

For $k = \bar{k}$

$$\begin{array}{ccc} x' & \longmapsto & [x'] - [e'] \\ E' & \xrightarrow{\sim} & Pic^0(E') \\ \vdots & & \downarrow \varphi^* \\ E & \xrightarrow{\sim} & Pic^0(E) \\ & & \varphi^*([x'] - [e']) \end{array}$$

this is a group morphism.

This will be the dual isogeny.

Quotients by finite subgroups. Back to arbitrary perfect k.

Let E be an elliptic curve over k. Let $\bar{k}$ be an algebraic closure of k and $\bar{E}$ the elliptic curve on $\bar{k}$ obtained by extending scalars.

Def: A finite subset $\Gamma \subseteq E$ is a subgroup if its pre-image via $\pi: \overline{E} \longrightarrow E$ is a subgroup of $\overline{E}$.

$$\uparrow$$

$$K(\overline{E}) = K(E) \otimes_k \overline{k}$$

the map $\uparrow$ just the restriction of valuations

$$K(E) \hookrightarrow K(E) \otimes_k \overline{k}$$

it has finite fibers. ($E = \overline{E}/\mathrm{Gal}(\overline{k}/k)$.)

Example: 1) if $\varphi : E \to E'$ is an isogeny, then

$\ker(\varphi) := \varphi^{-1}(O_{E'})$ is a subgroup in this sense.

2) A finite subgroup $\overline{\Gamma} \subseteq \overline{E}$ comes from a subgroup of E iff it is stable under the action of $\mathrm{Gal}(\overline{k}/k)$.

Lemma: Let $\Gamma \subseteq E$ be a subgroup. Then there exists an elliptic curve E/Γ together with an isogeny $\varphi: E \to E/\Gamma$ with kernel $\varphi^{-1}(0) = \Gamma$. If $\psi: E \to E'$ is an isogeny with $\Gamma \subseteq \ker(\psi) = \psi^{-1}(0)$, then there exits a unique isogeny $\tilde{\psi}: E/\Gamma \to E'$ s.t.

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E/\Gamma \\ {\scriptstyle\psi}\downarrow & \swarrow_{\tilde{\psi}} & \\ E' & & \end{array}$$

Proof: Suppose first $k = \overline{k}$. For $\gamma \in \Gamma$,

$$t_\gamma : E \longrightarrow E \qquad x \longmapsto x. \quad \text{(on the left)}$$

$$t_\gamma : K(E) \longrightarrow K(E) \qquad f \longmapsto f \circ t_\gamma$$

Therefore Γ acts on $K(E)$ by

$$\gamma . f = f \circ t_{\gamma^{-1}}.$$

Take $K = K(E)^\Gamma$. By Galois theory, the extension $K(E)/K$ is a Galois extension of degree $|\Gamma|$.

$\Longrightarrow K$ is a function field of a smooth projective C.

Since the induced morphism $\varphi: E \to C$ is separable, we can apply Hurwitz formula:

$$\underbrace{2g(E) - 2}_{0} = |\Gamma| \left(2g(C) - 2\right) + \deg(R_\varphi).$$

We want to conclude that $\deg R_\varphi$. To do this remark the following:

[illegible] take t

for $x \in E$ and $\gamma \in \Gamma$, $\varphi(x) = \varphi(x+\gamma)$. It not have

on C which has a pole on $\varphi(x)$ and a zero on $\varphi(x+\gamma)$.

this is not possible because meromorphic functions on C are invariant under translation by Γ. Therefore the fibers of φ have at least cardinality $|\Gamma|$, but the degree is $|\Gamma|$, so the map must be unramified.

$\Longrightarrow$ φ is unramified and $g(C) = 1$.

If $\varphi: E \to E'$ is an isogeny with $\Gamma \subseteq \varphi^{-1}(0)$, then the image of $\varphi^*: K(E') \longrightarrow K(E)$ lands in the Γ-invariant functions $K(E)^\Gamma = K(C)$.

If k is not necessarily alg closed, take an alg closure $\bar{k}$ of k, and consider $\pi: \bar{E} \longrightarrow E$ defined above.

$$\bar{\Gamma} = \pi^{-1}(\Gamma)$$

Now the field $K(\bar{E})^{\bar{\Gamma}} = \left(\bar{k} \underset{k}{\otimes} K(E)\right)^{\bar{\Gamma}}$ is stable under the action of $\mathrm{Gal}(\bar{k}/k)$. Set

$$K(E/\Gamma) = \left(K(\bar{E})^{\bar{\Gamma}}\right)^{\mathrm{Gal}(\bar{k}/k)}.$$

Exercise: This does the job. □

Let's go back to the construction of the dual isogeny.

Thm: Let $\varphi: E \to E'$ be an isogeny of degree d. There exists a unique isogeny $\hat{\varphi}: E' \to E$ s.t. $\hat{\varphi} \circ \varphi = [d]_E$. Moreover:

1) $\varphi \circ \hat{\varphi} = [d]$

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

Proof: Uniqueness is clear: suppose having α, β s.t. $\alpha \circ \varphi = \beta \circ \varphi = [d]$

$$K(E') \underset{\beta}{\overset{\alpha}{\rightrightarrows}} K(E') \xrightarrow{\varphi^*} K(E), \qquad [d]^*: K(E') \to K(E)$$

Since φ^* is injective, $\alpha = \beta$.

- If $\hat{\varphi}$ exists, then

$$\varphi \circ \hat{\varphi} \circ \varphi = \varphi \circ [d] = [d] \circ \varphi \overset{\varphi \text{ isogeny}}{\Longrightarrow} \varphi \circ \hat{\varphi} = [d].$$

- If $\hat{\varphi}, \hat{\psi}$ exist, then

$$(\hat{\varphi}\circ\hat{\psi})\circ(\psi\circ\varphi) = \hat{\varphi}\circ\underbrace{(\hat{\psi}\circ\psi)}_{[\deg\psi]}\circ\varphi = [\deg\psi]\cdot\underbrace{\hat{\varphi}\circ\varphi}_{[\deg\varphi]} = [\deg\varphi\cdot\deg\psi]$$

We can treat separately the separable and the purely inseparable case.

(φ separable)

$$\begin{array}{ccc} K(E') & \xrightarrow{\varphi^*} & K(E) \\ & \searrow^{2} & \uparrow \\ & & K(E)^{\ker\varphi} \end{array} \qquad \deg\varphi = [d] \Rightarrow \ker\varphi \subseteq \ker[d] = E[d].$$

$$\Longrightarrow \quad \begin{array}{ccc} E & \longrightarrow & E' = E/\ker\varphi \\ {\scriptstyle [d]}\downarrow & \swarrow_{\hat{\varphi}} & \\ E & & \end{array}$$

by the property of the quotient

$\hat{\varphi}$ is the dual isogeny.

(φ purely inseparable) $\Longrightarrow$ $\mathrm{char}(k) = p > 0$, $d = p^r$.

$$E \xrightarrow{F_{E,p}} E^{(p)} \xrightarrow{F_{E^{(p)},p}} E^{(p^2)} \to \cdots \to E^{(p^r)} = E'$$

It suffice to treat the case of $\varphi = F_p : E \to E^{(p)}$.

We know that $[p]$ is inseparable (because $\lambda_{[p]} = 0$)

$$\begin{array}{ccc} E & \xrightarrow{F_p} & E^{(p)} \\ {\scriptstyle [p]}\downarrow & \swarrow_{\hat{F}_p} & \\ E & & \end{array}$$

therefore $\hat{F}_p$ is the wanted isogeny. □

Rmk: $\hat{F}_p$ is called the Verschiebung.

WEIL'S PAIRING

Let E be an elliptic curve over a perfect field k.

Hypothesis: Let $m \in \mathbb{N}-\{0\}$ s.t. $[m]$ is of degree m^2 and $\mathrm{char}(k) \nmid m$

Let $\bar{k}$ be an algebraic closure of k. We want to construct a bilinear for on $E[m](\bar{k})$ with values in the group of m-th roots of 1 of $\bar{k}$.

$$e_m : E[m](\bar{k}) \times E[m](\bar{k}) \longrightarrow \mu_m(\bar{k}) \quad \text{“} \{\zeta \in \bar{k}^* : \zeta^m = 1\}.$$

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

$$[m]^*([x]-[0]) = \sum_{t \in E[m](\bar{k})} ([x'+t]-[t]) \overset{\text{in } \mathrm{Pic}^0}{\equiv} \sum_{t \in E[m](\bar{k})} ([x']-[0]) \overset{\text{hyp}}{\equiv} m^2([x']-[0]) \equiv m([x]-[0]) \equiv 0.$$

in $\mathrm{Div}^0(\bar{E})$

$$[x'+t]-[t] = \big([x'+t]-[0]\big)-\big([t]-[0]\big)$$

$$\equiv [x']-[0]$$

$\uparrow$ in Pic^0

Therefore the divisor $m^*([x]-[0])$ is principal, hence there exists

$g_x \in K(\bar{E})$ s.t. $\mathrm{div}(g_x) = m^*([x]-[0])$.

(Note that g_x is unique up to scalar factor.).

Claim: g_x^m is invariant under translation by $E[m](\bar{k})$.

Def: For $y \in E[m](\bar{k})$

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

Does not depend on the choice of

Proof: $\mathrm{div}(g_x^m) = [m]^*(m[x]-m[0]) \equiv [m]^*(\underbrace{[mx]-[m0]}_{0}) \equiv 0.$

This means that there is $f \in K(\bar{E})$ s.t.

$$\mathrm{div}(g_x^m) = [m]^* \mathrm{div}(f) = \mathrm{div}(f\circ[m])$$

In particular $\frac{g_x^m}{f\circ[m]}$ is constant, thus g_x^m is invariant under translation by $E[m](\bar{k})$. □

Thm: The map $e_m : E[m](\bar{k}) \times E[m](\bar{k}) \longrightarrow \mu_m(\bar{k})$

$$(x, y) \longmapsto e_m(x,y)$$

is bilinear, skew-symmetric, non-degenerate and $\mathrm{Gal}(\bar{k}/k)$-equivariant.

Proof: (Linearity 1st variable)

$$t_{x+x'}^* g_y = (t_x \circ t_{x'})^* g_y = t_x^*(t_{x'}^* g_y)$$

$$= t_x^*(e(x',y)\, g_y) = e(x,y)\, e(x',y)\, g_y.$$

$\Rightarrow$ $e(x+x',y)\, g_y.$

(Lin 2nd var)

$$[x]+[x']-[x+x']-[0] = \mathrm{div}(f)$$

$$= ([x]-[0]) + ([x']-[0]) - ([x+x']-[0]) \equiv 0 \text{ in } \mathrm{Pic}^0(\bar{E}).$$

$$\mathrm{div}\left(\frac{g_x g_{x'}}{g_{x+x'}}\right) = [m]^*\Big([x]-[0]+[x']-[0]-([x+x']-[0])\Big) = [m]^*\mathrm{div}(f).$$

$\Longrightarrow$ $\frac{g_x g_{x'}}{g_{x+x'}}$ is invariant under translation by m-torsion points.

$$t_y^*\left(\frac{g_x g_{x'}}{g_{x+x'}}\right) = \frac{t_y^* g_{x+x'}}{t_y^* g_x\, t_y^* g_{x'}}$$

$$t_Y\left(\frac{\cdot\,\cdot}{g_{x+x'}}\right) = \frac{\cdot\,\cdot}{g_{x+x'}} \iff \frac{\cdot\,\cdot}{g_{x+x'}} - \frac{\cdot\,\cdot}{g_x} \cdot \frac{\cdot\,\cdot}{g_{x'}}$$

$$\| \qquad \| \qquad \|$$

$$e(y, x+x') \qquad e(y,x) \qquad e(y,x')$$

$$\in$$