Previously...

- Isogenies, the dual isogeny
- Inverse limits and the Tate module

$$T_p(\mu) = \varprojlim \mu_{p^n}, \quad T_p(E) = \varprojlim E[p^n]$$

$$\varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}, \quad T(\mu) = \varprojlim \mu_n, \quad T(E) = \varprojlim E[n]$$

Today...

- The Weil pairing

André Weil

(1906 - 1998)

Recall: $\sigma : \mathrm{Pic}^0(E) \xrightarrow{\sim} E$, $[D] \longmapsto P$ s.t. P is the unique pt on E w/ $D \sim (P) - (\mathcal{O})$.

Corollary Let E be an elliptic curve, and let $D = \sum_{P \in E} n_P \cdot (P)$ be a divisor of degree 0. Then D is principal iff $\sum_{P \in E} [n_P] \cdot P = \mathcal{O}$. (addition on E.)

Pf.

$$D \sim \mathcal{O} \text{ (principal)} \iff \sigma(D) = \mathcal{O}$$

$$\iff \sigma\left(\sum_{P \in E} n_P \cdot (P)\right) = \mathcal{O}$$

$$\iff \sigma\left(\sum_{P \in E} n_P \cdot (P) - \left(\sum_{P \in E} n_P\right)\cdot(\mathcal{O})\right) = \mathcal{O} \qquad \left(\deg D = 0 \Rightarrow \left(\textstyle\sum n_P = 0\right)\right)$$

$$\iff \sigma\left(\sum_{P \in E} n_P \cdot \big((P) - (\mathcal{O})\big)\right) = \mathcal{O}$$

$$\iff \sum [n_P] \cdot \underbrace{\sigma\big((P) - (\mathcal{O})\big)}_{P} = \mathcal{O} \iff \sum [n_P] \cdot P = \mathcal{O}. \qquad \blacksquare$$

Construction of the Weil pairing.

E elliptic curve $/K$. Let $T \in E[m]$. Consider $m\cdot(T) - m\cdot(\mathcal{O})$.

NOTE: $[m]\cdot T - [m]\cdot\mathcal{O} = \mathcal{O} - \mathcal{O} = \mathcal{O}$, and $\deg(\nearrow) = m - m = 0$.

COR $\Rightarrow \exists\, f \in \bar{K}(E)$ s.t. $\operatorname{div}(f) = m\cdot(T) - m\cdot(\mathcal{O})$.

Let $T' \in E$ be s.t. $[m]T' = T$. ($[m]$ is a non-ct. isog $\Rightarrow$ surjective)

NOTE: $[m]^*(T) - [m]^*\mathcal{O}$

(Recall: $\phi^*((Q)) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\cdot(P)$)

$$= \sum_{R \in E[m]} (T' + R) - \sum_{R \in E[m]} (R)$$

$\deg = 0 - m^2 - m^2$

$\sum_{R \in E[m]} T' + R - \sum_{R \in E[m]} R = \sum_{R \in E[m]} T' = [m^2]T' = [m]T = \mathcal{O}$

COR $\Rightarrow \exists\, g$ s.t.

$$\operatorname{div}(g) = \sum_{R \in E[m]} (T' + R) - \sum_{R \in E[m]} (R)$$

f s.t. $\operatorname{div}(f) = m\cdot(T) - m\cdot(O)$ w/ $T \in E[m]$

g s.t. $\operatorname{div}(g) = \sum_{R\in E[m]} (T'+R) - \sum (R)$

NOTE: $\operatorname{div}(g^m) = m\cdot\operatorname{div}(g) = \sum_{R\in E[m]} m(T'+R) - m\cdot(R)$

$$\operatorname{div}(f([m])) = m\cdot\left(\sum_{R\in E[m]} (T'+R) - (R)\right)$$

$f([m])(Q) = 0 \Rightarrow f([m]Q) = 0$

$\Rightarrow f([m])$ and g^m differ by a factor of $\overline{K}^*$

$\Rightarrow$ Pick f so that $\boxed{f\circ[m] = g^m.}$

$f_T \circ [m] = g_T^m$ $\rightsquigarrow$ $T \in E[m]$

Let $S \in E[m]$, for any $X \in E$:

$$g(X+S)^m = f([m](X+S)) = f([m]X + [m]S)$$

$$= f([m](X)) = g(X)^m$$

$$\Rightarrow \left(\frac{g(X+S)}{g(X)}\right)^m = 1. \quad \Rightarrow \frac{g(X+S)}{g(X)} \in \mu_m \subseteq \overline{K}$$

Moreover, $E \longrightarrow \mathbb{P}^1$ (smooth)

$X \longmapsto \dfrac{g(X+S)}{g(X)}$ } a morphism with values in $\mu_m \subsetneq \overline{K}$

$\Rightarrow$ NOT surjective $\Rightarrow$ constant!

$\dfrac{g(X+S)}{g(X)}$ constant wrt X.

Def. $e_m : E[m] \times E[m] \longrightarrow \mu_m = \{\text{m-th roots of unity}\} \subseteq \bar{K}$

$$(S, T) \longmapsto e_m(S,T) = \frac{g_T(X+S)}{g_T(X)}$$

is called the Weil pairing.

ex $m=2$ $\operatorname{div} f = m(T) - m(O)$, $T \in E[m]$

$y^2 = (x-e_1)(x-e_2)(x-e_3)$ $\quad T = (e_1, 0)$

$\operatorname{div}(x-e_1) = 2\cdot(T) - 2\cdot(O) \Longrightarrow f = x - e_1$

$(x-e_1)([2]) = x([2]) - e_1 = g^2$

...

Prop 8.1 (a) Bilinear: $e_m(S_1+S_2, T) = e_m(S_1,T)\cdot e_m(S_2,T)$

$$e_m(S, T_1+T_2) = e_m(S,T_1)\cdot e_m(S,T_2)$$

(b) Alternating: $e_m(T,T)=1$, and $e_m(S,T) = e_m(T,S)^{-1}$

(c) Non-deg: $e_m(S,T) = 1 \ \ \forall S\in E[m] \Rightarrow T=O$.

(d) Galois inv.: $\forall \sigma\in Gal(\bar{K}/K)$, $e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma)$.

(e) Compatible: If $S\in E[mm']$, $T\in E[m]$, then

$$e_{mm'}(S,T) = e_m([m']S, T).$$

Proof.

(a) $e_m(S_1+S_2,T) = \dfrac{g(X+S_1+S_2)}{g(X)} = \dfrac{g(X+S_1+S_2)}{g(X+S_1)}\cdot\dfrac{g(X+S_1)}{g(X)}$ $\quad X' = X+S_1$

(second part of (a) in book)

$$= \frac{g(X'+S_2)}{g(X')}\cdot\frac{g(X+S_1)}{g(X)} = e_m(S_2,T)\cdot e_m(S_1,T).$$

(b) $e_m(T,T) = 1$, so $e_m(S,T) = e_m(T,S)^{-1}$

NOTE $e_m(S+T, S+T) = e_m(S,S) \cdot e_m(S,T) \cdot e_m(T,S) \cdot e_m(T,T)$

$1 \quad 1 \quad \Rightarrow 1 \quad 1$

Pf of $e_m(T,T) = 1$:

$\tau_P : E \longrightarrow E$
$\quad Q \longmapsto P+Q$

$\operatorname{div}\left(\prod_{n=0}^{m-1} f \circ \tau_{[n]T} \right)$?

$$\operatorname{div}(f \circ \tau_{[n]T}) = m((1-n)(T)) - m((-n)\cdot(T))$$

$$\operatorname{div}\left(\prod_{n=0}^{m-1} f \circ \tau_{[n]T}\right) = m\left(\sum_{n=0}^{m-1} ((1-n)(T)) - ((-n)(T))\right) = 0$$

$\Rightarrow \prod f \circ \tau_{[n]T}$ must be constant.

$\prod f \circ \tau_{[n]T}$ is constant.

Let $T' \in E$, w/ $[m]T' = T$. Then

$$\left(\underbrace{\prod g \circ \tau_{[n]T'}}_{G}\right)^m = \prod f \circ \tau_{[n]T} = \text{constant}$$

$$\Rightarrow G^m = \text{constant} \Rightarrow G \text{ constant}$$

$$G(x) = \prod_{n=0}^{m-1} g(x + [n]T') = \prod_{n=0}^{m-1} g(x + [n+1]T') = G(x+T')$$

cancel common terms out

$$g(x) = g(x + [m]T') = g(x+T)$$

$$\Rightarrow e_m(T, T) = \frac{g(x+T)}{g(x)} = 1. \quad \blacksquare$$

Fixed T.

(c) Suppose $e_m(S,T) = 1$ for all $S \in E[m]$

so $\boxed{g_T(X+S) = g_T(X) \quad \text{for all } S \in E[m].}$

Recall $\ker [m] \longrightarrow Aut(\bar{K}(E)/[m]^*\bar{K}(E))$ is an isom.

$S \longmapsto \tau_S^*$

$\Rightarrow g \in [m]^*\bar{K}(E) \Rightarrow \exists h$ s.t. $g = h \circ [m]$

$\Rightarrow (h \circ [m])^m = g^m = f \circ [m] \Rightarrow f = h^m$.

Hence $m \cdot div(h) = div(f) = m(T) - m(O)$

$\Rightarrow div(h) = (T) - (O)$

$\Rightarrow (T) \sim (O) \longrightarrow \boxed{T = O}$ ✓

(d) Let $\sigma \in G_{\bar{K}/K}$. Let f, g fns. attached to T

$\Rightarrow f^\sigma, g^\sigma$ fns attached to T^σ

$$e_m(S^\sigma, T^\sigma) = \frac{g^\sigma(X^\sigma + S^\sigma)}{g^\sigma(X^\sigma)} = \left(\frac{g(X+S)}{g(X)}\right)^\sigma = e_m(S,T)^\sigma.$$

(e) $\operatorname{div}(f^{m'}) = mm'(T) - m \cdot m'(O)$

and $\left(g \circ ([m'])\right)^{mm'} = \left(f \circ ([mm'])\right)^{m'}$

$$e_{mm'}(S,T) = \frac{g_{\circ[m']}(X+S)}{g_{\circ[m]}(X)} = \frac{g(Y + [m']S)}{g(Y)} = e_m([m']S, T)$$

$Y = [m']X$

∎