§1 The pairing E/S EC

Recall $\hat{E}/S$:= dual EC, represents functor

$$\mathrm{Pic}^0_{E/S} : T \longmapsto \mathrm{Pic}^0(T \times_S E) / p_T^* \mathrm{Pic}(T).$$

Aim $E_n \times \hat{E}_n \longrightarrow \mu_n$ bilinear

First $S = \mathrm{Spec}\, k$, $k = \bar{k}$

$x \in E_n(k)$, $L \in \mathrm{Pic}^0(E)_n$ i.e. $L^{\otimes n} \cong \mathcal{O}_E$.

Write $L \cong \mathcal{O}([y] - [e])$

$L^{\otimes n} \cong \mathcal{O}_E$ means $\exists\, f \in k(E)$ s.th.

$$\mathrm{div}(f) = [n]^{-1}([y] - [e])$$

Then $t_x^*([n]^* L) = ([n] \circ t_x)^* L = [n]^* L$

$$\Longrightarrow \mathrm{div}(f) = \mathrm{div}(t_x^*(f))$$

Def $e_n(x, y) := \dfrac{f}{t_x^*(f)}$

Now general case: (Nach $T^{\times}_{S}$ — schreibe S für T.)

$x \in E_n(S)$, $\mathcal{L} \in \hat{E}_n(S)$

Locally on S, fix $\psi : \mathcal{O}_E \xrightarrow{\cong} [n]^*\mathcal{L}$.

(unique up to $\mathcal{O}_S^{\times}$)

Apply t_x^*:

$$\begin{tikzcd}
\psi_x : \mathcal{O}_E \arrow[r, "\cong"] & t_x^*\mathcal{O}_E \arrow[r, "t_x^*\psi"] & t_x^*\left([n]^*\mathcal{L}\right) \arrow[d, equal] \\
 & & {[n]^*\mathcal{L}}
\end{tikzcd}$$

canonical iso, part of defn of t_x^* as scheme morphism

canonical iso from fact $[n] = [n] \circ t_x$.

Then ψ_x & ψ are non-vanishing sections of $[n]^*\mathcal{L}$,

hence differ by scalar:

$$\psi_x = e_n(x, \mathcal{L}) \cdot \psi .$$

Prop 1) $e_n(x, \mathcal{L})$ independent of ψ. In partic, def globalizes to all of S. (ψ exists only locally)

2) Linear in x and $\mathcal{L}$

3) Values lie in $\mu_n(S) = \{ \zeta \in \mathcal{O}_S^\times(S) \;\; \zeta^n = 1 \}$

4) $e_n(x, x) = 0$. (alternating)

5) $e_{nm}(x, y) = e_n(m x, y)$ (compatibility)

$nmx = 0 \;,\; ny = 0$

Proof 1) $t_x^*(\lambda \cdot \psi) = \lambda \cdot t_x^*(\psi)$

$= e_n(x, z)\,(\lambda \cdot \psi)$

$\Longrightarrow$ Independence & globalization.

Remaining statements reduce to alg closed field in char 0, e.g. $\mathbb{C}$.

a) 2) – 5) are identities of sections of $\mathcal{O}_S$,

so enough to show for all $\mathcal{O}_{S,s}$

$\Longrightarrow$ wlog $S = \operatorname{Spec} R$ local

b) The def of e_n is functorial in S, i.e. if

$E = S \times_{S_0} E_0$, x, y, L etc. all via b.c. from x_0, y_0, L_0 etc. $/S_0$, then suffices to prove statements for $x_0, y_0, L_0, \ldots$

c) S local $\Rightarrow$ ω_E trivial

$\Rightarrow$ $E: \quad y^2 + a_1 xy + a_3 y \qquad \subseteq \mathbb{P}^2_S$.

$= x^3 + a_2 x^2 + a_4 x + a_6$

Thus comes via pull back from

$$S \longrightarrow \underbrace{\operatorname{Spec} \mathbb{Z}[a_1, \dots, a_6][\Delta^{-1}]}_{=: B}$$

Over B, have universal Weierstraß family $\mathcal{E}$,

$$\tilde{B} := \mathcal{E}[n] \times_B \hat{\mathcal{E}}[n] \longrightarrow B.$$

Then (E, x, y) via pull back from $S \to \tilde{B}$.

d) $\tilde{B} \longrightarrow B$ is finite + loc free, smooth flat

Thus $\tilde{B}/\mathbb{Z}$ flat (i.e. $\mathcal{O}_{\tilde{B}}$ torsion-free)

$$\Rightarrow \mathcal{O}_{\tilde{B}} \hookrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_{\tilde{B}} \hookrightarrow \prod_{\substack{\eta \in \tilde{B} \\ \text{gen points}}} \kappa(\eta)$$

All these $\kappa(\eta)$ fin gen $/\mathbb{Q}$ + char 0, hence $\hookrightarrow \mathbb{C}$.

Now $S = \mathrm{Spec}\, k$ $k = \bar{k}$ char $k = 0$.

$\mathrm{div}(f) = [n]^{-1}([y] - [e])$ as before.

2) Linearity in x: $t^*_{x_1+x_2}(f)/f = t^*_{x_1+x_2}(f) / t^*_{x_1}(f) \cdot t^*_{x_1}(f)/f$.

$= t^*_{x_1}\left(t^*_{x_2}(f)/f \right) \cdots$

$= e_n(x_1, y) \cdot e_n(x_2, y)$ since any constant is translation invariant.

Linearity in L: Clear from def.

3) Bilinearity implies $e_n(x, y)^n = e_n(nx, y) = 0$,

so $e_n \in \mu_n$

4) Alternating: $e_n(y, y) = e_n(y, \mathcal{O}([y] - [e])) = 1$.

Take g s.th. $\mathrm{div}(g) = n[y] - n[e]$.

$\Rightarrow \mathrm{div}\left(\prod_{i=0}^{n-1} t^*_{iy} g \right) = n \sum_{i=0}^{n-1} [(1-i)y] - [-iy]$

$= 0$, hence fct. constant.

Now f and g are related by $f^n = g \circ [n]$ (up to const.)

Let $ny' = y$. Then

$$\left(\prod_{i=0}^{n-1} t_{iy'}^* f \right)^n = \left(\prod_{i=0}^{n-1} t_{iy}^* g \right) \circ [n]$$

is also constant.

$$\Rightarrow \quad h = \prod_{i=0}^{n-1} t_{iy'}^* f \quad \text{constant}$$

In other words, for all t, $h(t) = h(t+y')$

$$\Rightarrow \quad \prod_{i=0}^{n-1} f(t + iy') = \prod_{i=0}^{n-1} f(t + (i+1)y')$$

Cancellation $\Rightarrow$ $f(t) = f(t + \underbrace{ny'}_{=y})$

i.e. $e_n(y,y) = \dfrac{f(t+y)}{f(y)} = 1$.

5) f as above. Then $\mathrm{div}(f \circ [m]) = [nm]^{-1}([y] - [e])$

$$\Rightarrow \quad e_{nm}(x,y) = \frac{f \circ [m]}{t_x^*(f \circ [m])} = \left(\frac{f}{t_{mx}^* f} \right) \circ [m]$$

$$= e_n(mx, y) \quad \square$$

Further properties

6) $e_n(x,y) = e_n(y,x)^{-1}$

Proof $1 = e_n(x+y, x+y)$

$$= \cancel{e(x,x)}\, e(x,y)\, e(y,x)\, \cancel{e(y,y)} \qquad \square$$

7) $\operatorname{char} k \nmid n$, $k = \bar{k}$. Then

$$e_n : E_n(k) \times \hat{E}_n(k) \to \mu_n(k)$$

is non-degenerate.

Proof Assume $e_n(x,y) = 1 \quad \forall x$.

This means f invariant under $E_n(k)$.

Thus $f = h \circ [n]$.

Then $\operatorname{div}(h) = [y] - [e]$

Then $[y] = [e]$. $\square$

Example Assume E/k has a level-n-str. α

Then $\zeta_n \in k$.

Proof $e_n(\alpha_1, \alpha_2)$ is such root of unity. $\square$

Example Have $\mathcal{M}_n \longrightarrow \operatorname{Spec} \mathbb{Z}[\frac{1}{n}, T]/_{T^n - 1}$

$$(E, \alpha) \longmapsto e_n(\alpha_1, \alpha_2).$$

This map is smooth of rel dim 1, its fibers are geometrically connected.

Its image is the conn. comp $\operatorname{Spec} \mathbb{Z}[\frac{1}{n}, T]/_{\Phi_n(T)}$ by non-degeneracy

8) $k = \bar{k}$, char $k \nmid n$, $\zeta_n \in \mu_n(k)$ primitive.

Then $\exists$ symplectic basis:

$\alpha_1 \in E[n](\bar{k})$ of order n any.

e_n non-degen $\rightarrow \exists\, \alpha_2$ s.th. $e_n(\alpha_1, \alpha_2) = \zeta_n$

Since e_n alternating, α_1, α_2 $\mathbb{Z}/n$-basis for $E[n](\bar{k})$.

Then $e_n(a\alpha_1 + b\alpha_2, c\alpha_1 + d\alpha_2)$

$$= (ad - bc) \cdot \zeta_n$$

agrees with determinant pairing.

g.) k any, char $k \nmid n$. Pairing may be defined on Tate module:

$$T_\ell E \times T_\ell E \xrightarrow{e} \mathbb{Z}_\ell(1) =: \varprojlim_{[\ell]} \mu_{\ell^i}(\bar{k})$$

$$e((\alpha_i),(\beta_i)) := (e_{\ell^i}(\alpha_i, \beta_i))$$

Works since $e_{\ell^{i+1}}(\alpha_{i+1}, \beta_{i+1})^\ell = e_{\ell^{i+1}}(\alpha_{i+1}, \ell\beta_{i+1})$

$$\overset{5)}{=} e_{\ell^i}(\ell\alpha_{i+1}, \ell\beta_{i+1})$$

$$= e_{\ell^i}(\alpha_i, \beta_i). \qquad \square$$

§2 Application: Structure of $M_n(\mathbb{C})$

$$\mathcal{H}^{\pm} := \mathbb{C} \setminus \mathbb{R} = \left\{ E/\mathbb{C} \quad + \quad \tau_1, \tau_2 \in \pi_0(E, e) \right\}/\cong$$

basis

$$\tau_1/\tau_2 \longmapsto \mathbb{C}/\Lambda$$

$$\tau \longmapsto \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$$

$\mathcal{H}^{\pm}_n := \{ (E, \tau_1, \tau_2, \alpha) \quad \alpha$ additional level-n str $\}$

Then $\quad GL_2(\mathbb{Z}/n) \times \mathcal{H}^{\pm} \xrightarrow{\cong} \mathcal{H}^{\pm}_n \quad$ @

$$(h, \tau) \longmapsto \left(\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, \tau, 1, h \begin{pmatrix} n^{-1}\tau \\ n^{-1} \end{pmatrix} \right)$$

$$\in n^{-1}\Lambda/\Lambda^{\oplus 2}$$

$GL_2(\mathbb{Z})$ acts on $\mathcal{H}^{\pm}_n$ as

$$g \cdot \left(E, \begin{pmatrix} \tau_1 \\ \tau_2 \end{pmatrix}, \alpha\right) = \left(E, g\begin{pmatrix} \tau_1 \\ \tau_2 \end{pmatrix}, \alpha\right)$$

Would like express this action in description of @ :

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \left(\mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}, \begin{pmatrix} a\tau + b \\ c\tau + d \end{pmatrix}, n^{-1} \cdot h\begin{pmatrix} \tau \\ 1 \end{pmatrix} \right)$$

$$\xrightarrow[\cong]{\cdot(c\tau+d)^{-1}} \left(\mathbb{C}/\mathbb{Z}\cdot g\tau + \mathbb{Z},\ \begin{pmatrix} g\tau \\ 1 \end{pmatrix},\ n^{-1}\cdot hg^{-1}\begin{pmatrix} g\tau \\ 1 \end{pmatrix} \right)$$

$$g\tau := \frac{a\tau+b}{c\tau+d}$$

$$\Rightarrow \quad g\bullet(h,\tau) = (hg^{-1}, g\tau)$$

Aim Determine $M_n(\mathbb{C}) = {}_{GL_2(\mathbb{Z})}\backslash GL_2(\mathbb{Z}/n)\times\mathcal{H}^{\pm}$

$$\Gamma(n) := \ker\left(GL_2(\mathbb{Z}) \longrightarrow GL_2(\mathbb{Z}/n) \right)$$
$$= \mathrm{Stab}(h) \quad \forall\ h \in GL_2(\mathbb{Z}/n) \circlearrowleft GL_2(\mathbb{Z})$$

$$M_n(\mathbb{C}) = \coprod_{h\in GL_2(\mathbb{Z})\backslash GL_2(\mathbb{Z}/n)} {}_{\Gamma(n)}\backslash\mathcal{H}^{\pm}$$

Claim Image $\left(GL_2(\mathbb{Z}) \longrightarrow GL_2(\mathbb{Z}/n) \right)$

$= \{ h \text{ s.t. } \det h \in \{\pm 1 \bmod n\}\}$

Proof $\det\begin{pmatrix} -1 & \\ & 1 \end{pmatrix} = -1$, so enough to show image contains $SL_2(\mathbb{Z}/n)$.

This is extended Euclidean algorithm:

given $\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in SL_2(\mathbb{Z}/n)$, pick any

Lift $\tilde{h} = \begin{pmatrix} a & b \\ \tilde{c} & \tilde{d} \end{pmatrix} \in M_2(\mathbb{Z})$.

Then $(a,b) = 1$ & $\det(\tilde{h}) \equiv 1 \mod n$.

Euclidean Alg: $\exists$ p, q s.th. $aq - bp = 1$

Now take $(c, d) = (\tilde{c}, \tilde{d}) - \underbrace{(\det \tilde{h} - 1) \cdot (p, q)}_{\equiv 0 \mod n}$.

$\square$

$$\Rightarrow M_n(\mathbb{C}) = \coprod_{\lambda \in (\mathbb{Z}/n)^\times / \{\pm 1\}} \Gamma(n) \backslash \mathcal{H}^{\pm}$$

Two cases: $n = 1$ or 2, then $\exists\, g \in \Gamma(n)$ w/ $\det g = 1$

We obtain $M_n(\mathbb{C}) = \Gamma(n) \cap SL_2(\mathbb{Z}) \backslash \mathcal{H}$

$\mathcal{H} = \{ \operatorname{Im} \tau > 0 \}$

$n \geq 3$ $\quad 1 \not\equiv -1 \mod n$, so $\Gamma(n) \subseteq SL_2(\mathbb{Z})$

preserves conn. comp. of $\mathcal{H}^{\pm}$

$$M_n(\mathbb{C}) \cong \coprod_{(\mathbb{Z}/n)^\times} \Gamma(n) \backslash \mathcal{H} \qquad (*)$$

Final observation $\mathcal{H}$ is connected, so $e_n(\alpha_1, \alpha_2)$ is constant on each of above comm. comp. But $GL_2(\mathbb{Z}/n)$ acts via

$\det : GL_2(\mathbb{Z}/n) \longrightarrow (\mathbb{Z}/n)^\times$ on π_0 of

above space + also by det on Weil pairing:

$$e_n(a\alpha_1 + b\alpha_2, c\alpha_1 + d\alpha_2) = e_n(\alpha_1, \alpha_2)^{ad-bc}$$

$$\Longrightarrow \coprod_{\zeta \in \mu_n(\mathbb{C})} \underbrace{M_{n,\zeta}(\mathbb{C})}_{e_n(\alpha_1,\alpha_2) = \zeta} = \coprod_{\lambda \in (\mathbb{Z}/n)^\times} \Gamma(n)\backslash\mathcal{H}$$

<u>Question</u> Where did $\mu_n(\mathbb{C})$ get identified w/ $(\mathbb{Z}/n)^\times$?

<u>Answer</u> Iso @ involved choice $n^{-1}\binom{\tau}{1}$ as

level-n-str over $\mathcal{H}^\pm$

$\longrightarrow$ choice of prim. root of unity $e_n(n^{-1}\tau, n^{-1})$

<u>up to inverse</u>, because we have not chosen

$\mathcal{H}^\pm = \{\mathrm{Im}\, z > 0\} \amalg \{\mathrm{Im}\, z < 0\}$ yet.

This choice is then made in $(*)$.

<u>Rapoport's lecture</u> This choice is $e^{\frac{2\pi i}{n}}$

(I don't know why currently.)

Two <u>remarks</u> 1) The surjectivity $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n)$

is called <u>strong approximation</u> for SL_2:

$$SL_2(\mathbb{Q}) \subseteq SL_2(\mathbb{A}_f) \text{ is dense.}$$

This holds for all simply connected semi-simple

alg grps $/\mathbb{Q}$. E.g. SL_n, SU_n, Sp_{2n},

$Spin_m$ $(m \geq 3)$

2) In general description of loc. sym. space

$$G(\mathbb{Q}) \backslash \Big(\underbrace{G(\mathbb{A}_f)/K_f \times G(\mathbb{A}_\infty)/K_\infty}_{=:X} \Big) \cong \coprod_{i \in I} \Gamma_i \backslash X$$

various different Γ_i will occur.

Here, normality of $\Gamma(n) \subset GL_2(\mathbb{Z})$ + fact that

$\mathbb{Q}$ has class number 1 $\left(GL_2(\mathbb{Q}) \backslash GL_2(\mathbb{A}_f) / GL_2(\hat{\mathbb{Z}}) = \{pt\} \right)$

simplified things.