Math 6170 C, Lecture on March 25, 2020

Yongchang Zhu

Plan

(1) Review of III § 6. Isogeny and Dual Isogeny

(2) Review of Chapter III § 7. The Tate Module

(3) Chapter III § 8. The Weil Pairing

Review of Chapter III, §6. Isogeny and Dual Isogeny.

Let E_1, E_2 be elliptic curves over $\bar{K}$. A morphism $\phi : E_1 \to E_2$ with $\phi(O_1) = O_2$ is called an **isogeny**.

An isogeny is a group homomorphism. The set $\mathrm{Hom}(E_1, E_2)$ is a $\mathbb{Z}$-module. $\mathrm{End}(E) \stackrel{\mathrm{def}}{=} \mathrm{Hom}(E, E)$ is a ring.

For an non-constant isogeny $\phi : E_1 \to E_2$, the **dual isogeny** is the unique isogeny $\hat{\phi} : E_2 \to E_1$ such that

$$\hat{\phi} \circ \phi = [\deg \phi].$$

The dual isogeny of [0] is defined to be [0].

The properties of dual isogeny:

Let $\phi : E_1 \to E_2$ and $\lambda : E_2 \to E_3$ be isogenies. Then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$$

Let $\phi, \psi : E_1 \to E_2$ be isogenies. Then

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$$

$$\hat{\hat{\phi}} = \phi$$

Corollary III 6.3.

Let E_1, E_2 be elliptic curves. The degree map

$$\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form.

Corollary III 6.4.

Let E be an elliptic curve and $m \in \mathbb{Z}$, $m \neq 0$. Let $E[m] = \ker[m]$.

(a) $\deg[m] = m^2$.

(b) If $\mathrm{char}(K) = 0$ or if m is relatively prime to $\mathrm{char}\, K$, then $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

(c) If $\mathrm{char}\, K = p$, then
$E[p^e] = \{O\}$ for all $e = 1, 2, \dots$ or
$E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ for all $e = 1, 2, \dots$.

Review of Chapter III. § 7. The Tate Module.

If E is defined over K, then $G_{\bar{K}/K}$ acts on $E(\bar{K})$ as automorphisms of abelian groups. So $G_{\bar{K}/K}$ acts on the group of m-torsion points $E[m]$ for each positive integer m.

Assume $\mathrm{char}\, K = 0$ or m is relatively prime to $\mathrm{char}\, K$, so we have a group homomorphism

$$G_{\bar{K}/K} \to \mathrm{Aut}(E[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z}).$$

We take the inverse limit of $E[l^n]$ (l is a prime) to get a l-adic representation of $G_{\bar{K}/K}$.

Let E be an elliptic curve, l be a prime, we have map

$$E[l^n] \to E[l^{n-1}], \quad P \mapsto [l]P$$

The inverse limit $T_l(E) \stackrel{\text{def}}{=} \varprojlim E[l^n]$ is an abelian group, and moreover the inverse is a $\mathbb{Z}_l$-module, because of the commutative diagram

$$\begin{array}{ccc}
\mathbb{Z}/l^n\mathbb{Z} \times E[l^n] \to & & \mathbb{Z}/l^{n-1}\mathbb{Z} \times E[l^{n-1}] \\
\downarrow & & \downarrow \\
E[l^n] & \to & E[l^{n-1}]
\end{array}$$

Proposition III 7.1.

As a $\mathbb{Z}_l$-module, the Tate module has the following structure.

(a)

$$T_l(E) \simeq \mathbb{Z}_l \times \mathbb{Z}_l \quad \text{if } l \neq \mathrm{char}(K)$$

(b)

$$T_l(E) \simeq \mathbb{Z}_l \ \text{ or } \ \{0\} \quad \text{if } l = \mathrm{char}(K)$$

Assume E is defined over K. The action of $G_{\bar{K}/K}$ on $E[l^n]$ commutes with the maps $[m]$, so $G_{\bar{K}/K}$ acts on the Tate module $T_l(E)$.

Definition. The l-adic representation of $G_{\bar{K}/K}$ on E is the map

$$\rho_l : G_{\bar{K}/K} \to \mathrm{Aut}(T_l(E))$$

given above.

A similar but simpler construction is the following:

Let $U(l^n) \subset \bar{K}^*$ be the subgroup given by

$$U(l^n) = \{a \in \bar{K}^* \mid a^{l^n} = 1\}.$$

We have group homomorphism

$$U(l^n) \to U(l^{n-1}), \quad a \mapsto a^l$$

The inverse limit $T_l(U) \stackrel{\text{def}}{=} \varprojlim E[l^n]$ is a $\mathbb{Z}_l$ module and a l-adic representation of $G_{\bar{K}/K}$. So we have 1-dimensional representation

$$G_{\bar{K}/K} \to \mathrm{Aut}(T_l(U)) \simeq \mathbb{Z}_l^*$$

(Assume $l \neq \mathrm{char}\, K$)

Recall a non-constant morphism $\phi : C_1 \to C_2$ induces

$$\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$$

$$\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\,(P).$$

ϕ also induces an embedding of fields

$$\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$$

$$(\phi^* f)(P) = f(\phi(P)).$$

The two ϕ^*'s are compatible:

$$\mathrm{div}(\phi^* f) = \phi^*(\mathrm{div}(f)).$$

Let m be a positive integer, assume $\mathrm{char}\, K = 0$ or m is relatively prime to $\mathrm{char}\, K > 0$. E be an elliptic curve over K. The Weil pairing is a skew-symmetric non-degenerate bilinear map

$$E[m] \times E[m] \to \mu_m(\bar{K})$$

Lemma

For every $T \in E[m]$, there is $f \in \bar{K}(E)^*$ such that

$$\mathrm{div}(f) = m(T) - m(O)$$

and $[m]^* f = f \circ [m] = g^m$ for some $g \in \bar{K}(E)$.

Proof. Recall that a divisor $\sum_{i=1}^n N_i(P_i) \in \mathrm{Div}^0(E)$ is principal iff $\sum_{i=1}^n [N_i]P_i = O$. $m(T) - m(O)$ is principal, because$[m]T - [m]O = O$.
There exists $f \in \bar{K}(E)^*$ such that

$$\mathrm{div}(f) = m(T) - m(O)$$

$[m]^* f(X) = f([m]X)$,

Proof (continued).

$$
\begin{aligned}
&\mathrm{div}([m]^* f) = [m]^* \mathrm{div}(f) \\
&= [m]^*(m(T) - m(O)) = m\,[m]^*((T) - (O)) \\
&= m \left(\sum_{P \in [m]^{-1}(T)} (P) - \sum_{R \in [m]^{-1}(O)} (R) \right) \\
&\quad \text{(we used the fact that } [m] \text{ is unramified)} \\
&= m \sum_{R \in E[m]} \big((R + T') - (R) \big)
\end{aligned}
$$

where $T' \in [m]^{-1}(T)$.

Proof (continued).

The addition map $\mathrm{Div}^0(E) \to E$ sends

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

to 0. So there is $g \in \bar{K}(E)^*$ such that

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

$[m]^* f = f \circ [m]$ and g^m have the same divisor. So

$$f \circ [m] = C\, g^m$$

for some $C \in \bar{K}^*$. Replace f by $C^{-1} f$, $C^{-1} f$ satisfies the properties in Lemma. $\square$

Now we define a pairing

$$e_m : E[m] \times E[m] \to \mu_m(\bar{K}) = \{u \in \bar{K} \mid u^m = 1\}.$$

by

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

$$e_m(S, T)^m = \frac{g(X+S)^m}{g(X)^m} = \frac{f([m](X+S))}{f([m]X)} = \frac{f([m]X)}{f([m]X)} = 1.$$

So $e_m(S, T) \in \mu_m(\bar{K})$.

g depends on S, a different choices g are related by a scalar: $g_1 = Cg_2$. It is easy to see e_m is independent of the choices of g.

Proposition III 8.1.

The m-th Weil pairing e_m satisfies the following properties:
(a) Bilinear:

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2)$$

(b) Skew Symmetric:

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

(c) Non-degeneracy: If $e_m(S, T)$ for all $S \in E[m]$, then $T = O$.

Proposition III 8.1. (continued)

(d) Galois invariance: For all $\sigma \in G_{\bar{K}/K}$,

$$e_m(S, T)^\sigma = e_m(S^\sigma, T^\sigma)$$

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

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

Proof of (a).

$$
\begin{aligned}
& e_m(S_1 + S_2, T) \\
&= \frac{g(X + S_1 + S_2)}{g(X)} \\
&= \frac{g(X + S_1 + S_2)}{g(X + S_1)} \frac{g(X + S_1)}{g(X)} \\
&= e_m(S_2, T) e_m(S_1, T)
\end{aligned}
$$

Proof of (a) (continued).

Let $T_1, T_2 \in E[m]$, $T_3 \stackrel{\mathrm{def}}{=} T_1 + T_2$. Choose $f_1, f_2, f_3 \in \bar{K}(E)^*$ such that

$$\mathrm{div}(f_i) = m(T_i) - m(O), \quad f_i \circ [m] = g_i^m$$

Because $(T_3) - (T_1) - (T_2) + (O)$ is a principal divisor, there is $h \in \bar{K}(E)^*$ such that

$$\mathrm{div}(h) = (T_3) - (T_1) - (T_2) + (O)$$

$$\mathrm{div}(\frac{f_3}{f_1 f_2}) = m\,\mathrm{div}(h)$$

$$f_3 = c\, f_1 f_2 h^m$$

Proof of (a) (continued).

$$g_3 = c' \, g_1 g_2 (h \circ [m])$$

$$\begin{aligned} e_m(S, T_1 + T_2) \qquad &= \frac{g_3(X+S)}{g_3(X)} \\ &= \frac{g_1(X+S)}{g_1(X)} \frac{g_2(X+S)}{g_2(X)} \frac{h([m](X+S))}{h([m]X)} \\ &= e_m(S, T_1) e_m(S, T_2) \end{aligned}$$

Proposition III 8.2.

Let $S \in E_1[m]$, $T \in E_2[m]$, and $\phi : E_1 \to E_2$ an isogeny. Then

$$e_m(\phi(S), T) = e_m(S, \hat{\phi}(T)).$$

Note that $\phi : E_1[m] \to E_2[m]$ because ϕ is a group homomorphism.
Similarly $\hat{\phi} : E_2[m] \to E_1[m]$.

The proof uses
Claim.

$$\phi^*(T) - \phi^*(O) - (\hat{\phi}T) + (O)$$

is a principal divisor on E_1.

Proof of Claim.
Because ϕ is an isogeny, so all $e_\phi(P)$ are equal for all P, we denote it by e.

$$\begin{aligned}
\phi^*(T) - \phi^*(O) \quad &= e(\sum_{P \in \phi^{-1}(T)} (P) - \sum_{R \in \phi^{-1}(O)} (R)) \\
&= e(\sum_{R \in \phi^{-1}(O)} (R + T') - \sum_{R \in \phi^{-1}(O)} (R))
\end{aligned}$$

where T' is a point in $\phi^{-1}(T)$. Under the map $\mathrm{Div}^0(E_1) \to E_1$, the above element goes to

$$[\deg \phi]T' = \hat{\phi}(\phi(T')) = \hat{\phi}(T)$$

Proof of Claim (continued).

So

$$\phi^*(T) - \phi^*(O) - (\hat{\phi} T) + (O)$$

goes to O under the map $\mathrm{Div}^0(E_1) \to E_1$. This proves Claim.

Proof of $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$:

$$
\begin{aligned}
& e_m(S, (\hat{\phi} + \hat{\psi})(T)) \\
&= e_m(S, \hat{\phi}(T)) e_m(S, \hat{\psi}(T)) \\
&= e_m(\phi(S), T) e_m(\psi(S), T) \\
&= e_m((\phi + \psi)(S), T) \\
&= e_m(S, \widehat{\phi + \psi}(T))
\end{aligned}
$$

By the non-degeneracy of e_m, we have

$$\widehat{\phi + \psi}(T) = (\hat{\phi} + \hat{\psi})(T)$$

This holds for all $T \in E_2[m]$.

Proof of $\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$ (continued):

So the two maps $\widehat{\phi+\psi}$ and $\hat{\phi} + \hat{\psi}$ are equal on $\cup_m E_2[m]$. The union $\cup_m E_2[m]$ is an infinite set. Any infinite set in a curve is dense. So

$$\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}.$$

Let l be a prime number different from $\operatorname{char} K$. The pairings

$$e_{l^n} : E[l^n] \times E[l^n] \to \mu_{l^n}$$

are compatible for different n's in the sense that

$$\begin{array}{ccc} E[l^{n+1}] \times E[l^{n+1}] & \xrightarrow{e_{l^{n+1}}} & \mu_{l^{n+1}} \\ \downarrow [l] \times [l] & & \downarrow [l] \\ E[l^n] \times E[l^n] & \xrightarrow{e_{l^n}} & \mu_{l^n} \end{array}$$

is commutative

We take the inverse limit to get the Weil pairing

$$e : T_l(E) \times T_l(E) \to T_l(\mu)$$

which is a $\mathbb{Z}_l$-bilinear pairing of $\mathbb{Z}_l$-modules.

Proposition III 8.3.

The Weil pairing

$$e : T_l(E) \times T_l(E) \to T_l(\mu)$$

is $\mathbb{Z}_l$-bilinear, alternating (=skew symmetric), non-degenerated, Galois invariant. If $\phi : E_1 \to E_2$ is an isogeny, $\hat{\phi} : E_2 \to E_1$ is the dual isogeny, then

$$e(\phi(u), v) = e(u, \hat{\phi}(v)).$$

Let E/K be an elliptic curve. The $\mathrm{End}(E)$ has the following properties:

(1) $\mathrm{End}(E)$ is a characteristic 0 integral domain, and $\mathrm{rank}_{\mathbb{Z}} \mathrm{End}(E) \leq 4$.

(2) There is an anti-involution on $\mathrm{End}(E)$, $\phi \mapsto \hat{\phi}$.

(3) $\phi\hat{\phi} \in \mathbb{Z}_{\geq 0}$, $\phi\hat{\phi} = 0$ iff $\phi = 0$.

The above properties implies that $\mathrm{End}(E)$ is isomorphic to one of the following rings:

(1) $\mathbb{Z}$.
(2) An order in a quadratic imaginary field $\mathbb{Q}(\sqrt{-d})$.
(3) An order in a quaternion algebra over $\mathbb{Q}$.

End