Math 6170 C, Lecture on March 23, 2020

Yongchang Zhu

Plan

(1) Review of Chapter III § 5. The Invariant Differentials

(2) Chapter III § 6. The Dual Isogeny (continued)

(3) Chapter III § 7. The Tate Module

Review of III. § 5. The Invariant Differentials

Let E/K be an elliptic curve given by the usual Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then

$$\omega = \frac{dx}{2y + a_1x + a_3} \in \Omega_E$$

has neither zeros nor poles. Any other differential with this property is a $\bar{K}^*$-multiple of ω.

Proposition III 5.1

For ω as above, for every $Q \in E$,

$$\tau_Q^* \omega = \omega.$$

Theorem III 5.2. Let E, E' be elliptic curves, let ω be an invariant differential on E, and let $\phi, \psi : E' \to E$ be isogenies. Then

$$(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$$

Proof.

Consider the variety $E \times E$, its function field is

$$\bar{K}(E \times E) = \mathrm{Frac}\ \bar{K}[x_1, y_1, x_2, y_2]/(F(x_1, y_1),\ F(x_2, y_2))$$

where

$$F(x_1, y_1) = y_1^2 + a_1 x_1 y_1 + a_3 y_1 - (x_1^3 + a_2 x_1^2 + a_4 x_1 + a_6)$$

$$F(x_2, y_2) = y_2^2 + a_1 x_2 y_2 + a_3 y_2 - (x_2^3 + a_2 x_2^2 + a_4 x_2 + a_6).$$

The space of meromorphic differentials on $E \times E$, $\Omega_{E \times E}$ is defined similarly as Ω_E.

Proof (continued).
$\Omega_{E\times E}$ is 2-dimensional vector over $\bar{K}(E\times E)$.

It has basis

$$\omega_1 = \frac{dx_1}{2y_1 + a_1x_1 + a_3}, \quad \omega_2 = \frac{dx_2}{2y_2 + a_1x_2 + a_3}$$

Proof (continued).

We have projection maps:

$$\mathrm{pr}_1 : E \times E \to E, \quad (P, Q) \mapsto P$$

$$\mathrm{pr}_2 : E \times E \to E, \quad (P, Q) \mapsto Q$$

We have

$$\omega_1 = \mathrm{pr}_1^* \omega, \qquad \omega_2 = \mathrm{pr}_2^* \omega$$

Consider the addition map

$$\mu : E \times E \to E, \quad (P, Q) \mapsto P + Q$$

$$\mu^*(\omega) = f\omega_1 + g\omega_2$$

Proof (continued).

Because ω has no poles, so are ω_1, ω_2 and $\mu^*(\omega)$. So f and g are regular functions on $E \times E$. Since $E \times E$ is projective, so $f, g \in \bar{K}$.

Proof (continued).

For a fixed $Q \in E$. Let $i_Q : E \to E \times E$ be the map $P \mapsto (P, Q)$. So we have the map

$$i_Q^* : \Omega_{E \times E} \to \Omega_E$$

Apply this to the equation

$$\mu^*(\omega) = f\omega_1 + g\omega_2$$

we get (note that $\mu \circ i_Q = \tau_Q, \mathrm{Pr}_1 \circ i_Q = Id, \mathrm{Pr}_2 \circ i_Q = Q$),

$$\tau_Q^* \omega = f\omega$$

This proves $f = 1$. Similarly $g = 1$.
So

$$\mu^*(\omega) = \omega_1 + \omega_2$$

Proof (continued).

Consider the map $\alpha : E \to E \times E, \alpha(P) = (\phi(P), \psi(P))$, Then

$$\phi + \psi = \mu \circ \alpha, \quad \mathrm{pr}_1 \circ \alpha = \phi, \quad \mathrm{pr}_2 \circ \alpha = \psi$$

Apply α^* to

$$\mu^*(\omega) = \omega_1 + \omega_2$$

we get

$$(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$$

Corollary III 5.3.

Let ω be an invariant differential on an elliptic curve E. Let $m \in \mathbb{Z}$. Then

$$[m]^*\omega = m\omega$$

Theorem III 6.1. Let $\phi : E_1 \to E_2$ be a non-constant isogeny with $\deg \phi = m$.
(a) There exists a unique isogeny

$$\hat{\phi} : E_2 \to E_1$$

satisfying

$$\hat{\phi} \circ \phi = [m]$$

(b) as a group homomorphism, $\hat{\phi}$ equals to the composition

$$E_2 \xrightarrow{\kappa} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\kappa^{-1}} E_1$$

Let $\phi : E_1 \to E_2$ be a non-constant isogeny. The **dual isogeny** to ϕ is the unique isogeny $\hat{\phi} : E_2 \to E_1$ such that

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

We define the dual isogeny of [0] to be [0].

Theorem III 6.2.

Let $\phi : E_1 \to E_2$ be an isogeny.
(a) Let $m = \deg \phi$. Then

$$\hat{\phi} \circ \phi = [m] \quad \text{on } E_1$$

$$\phi \circ \hat{\phi} = [m] \quad \text{on } E_2$$

(b) Let $\lambda : E_2 \to E_3$ be an isogeny. Then

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

Theorem III 6.2 (continued).

(c) Let $\psi : E_1 \to E_2$ be an isogeny. Then

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

(d) For all $m \in \mathbb{Z}$,

$$\widehat{[m]} = [m], \quad \deg [m] = m^2$$

(e)

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

(f)

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

Definition.

Let A be an abelian group. A function

$$d : A \to \mathbb{R}$$

is called a **quadratic form** if
(1)

$$d(-v) = d(v)$$

(2) The pairing $A \times A \to \mathbb{R}$ given by

$$(u, v) \mapsto d(u+v) - d(u) - d(v)$$

is bilinear.

Example. $A = \mathbb{Z}^n$ column vectors with entries in $\mathbb{Z}$

M: an $n \times n$ symmetric matrix with entries in $\mathbb{R}$.

$$d(v) = v^T M v$$

is a quadratic form.

$$d(u+v) - d(u) - d(v) = u^T M v + v^T M u$$

A quadratic form d is **positive definite** if

$$d(v) \geq 0 \quad \text{for all } v \in A, \quad \text{and } q(v) = 0 \text{ iff } v = 0.$$

In the above example, if M is positively definite, the corresponding quadratic form is positive definite.

Corollary III 6.3.

Let E_1, E_2 be elliptic curves. The degree map

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

is a positive definite quadratic form.

Proof. Using $[\deg \phi] = \hat{\phi} \circ \phi$, we have

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

$$[\langle \phi, \psi \rangle] = (\widehat{\phi + \psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi = \hat{\phi} \circ \psi + \hat{\psi} \circ \phi$$

which is bilinear in ϕ and ψ.

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 $e = 1, 2, \ldots$ or
$E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ for all $e = 1, 2, \ldots$.

Proof.

(a) is in Theorem 6.2. (b) Since $\mathrm{char}\bar{K} = 0$ or $\mathrm{char}\,\bar{K}$ is relatively prime to m, $|E[m]| = \deg([m]) = m^2$.

For a prime p satisfying the condition of the Corollary, $|E[p]| = p^2$ and every element $a \in E[p]$ satisfies $pa = 0$, this forces

$$E[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Proof (continued).

For general m, for each prime divisor p of m,

$$\{a \in E[m] \mid pa = 0\} = E[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

This and the classification Theorem for finite abelian groups implies

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(c) omitted.

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 $G_{\bar{K}/K}$.

Inverse Limits of Groups and Rings.

If we have a chain of surjective group (ring) homomorphisms

$$\cdots \to A_n \to A_{n-1} \to \cdots \to A_2 \to A_1$$

The inverse limit

$$\lim_{\leftarrow} A_n$$

is a subgroup (subring) of $\Pi_{i=1}^{\infty} A_i$ that consists of elements

$$(\ldots, a_n, a_{n-1}, \ldots, a_2, a_1)$$

such that $a_n \mapsto a_{n-1}$ for $n = 2, 3, \ldots$.

The operation on $\varprojlim A_n$ is the pointwise operation:

$$(\ldots, a_n, a_{n-1}, \ldots) + (\ldots, b_n, b_{n-1}, \ldots) = (\ldots, a_n + b_n, a_{n-1} + b_{n-1}, \ldots)$$

$$(\ldots, a_n, a_{n-1}, \ldots) \cdot (\ldots, b_n, b_{n-1}, \ldots) = (\ldots, a_n \cdot b_n, a_{n-1} \cdot b_{n-1}, \ldots)$$

Example. $A_n = k[t]/(t^n) = \{c_{n-1}t^{n-1} + \cdots + c_1 t + c_0\}$.

$A_n \to A_{n-1}$ be the obvious ring homomorphism:

$$c_{n-1}t^{n-1} + c_{n-2}t^{n-2} \cdots + c_1 t + c_0 \mapsto c_{n-2}t^{n-2} + \cdots + c_1 t + c_0$$

We have a chain of ring homomorphisms:

$$\cdots \to A_n \to A_{n-1} \to \cdots \to A_2 \to A_1$$

The inverse limit ring $\varprojlim A_n$ is just the ring of formal power series over k:

$$k[[t]] = \{\sum_{i=0}^{\infty} c_i t^i\}.$$

Example. Let l be a prime. $A_n = \mathbb{Z}/l^n\mathbb{Z}$, We have a chain of rings

$$\cdots \to \mathbb{Z}/l^n\mathbb{Z} \to \mathbb{Z}/l^{n-1}\mathbb{Z} \to \cdots \to \mathbb{Z}/l^2\mathbb{Z} \to \mathbb{Z}/l\mathbb{Z}$$

The inverse limit ring

$$\lim_{\leftarrow} \mathbb{Z}/l^n\mathbb{Z}$$

is called the ring of l-adic integers, denoted by $\mathbb{Z}_l$.

An element in $\mathbb{Z}_l$ can be expressed as an infinite sum

$$c_0 + c_1 l + c_2 l^2 + \dots$$

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 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

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

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

Theorem III 7.9 (Serre)

Let K be a number field and E/K an elliptic curve without complex multiplication (i.e., $\mathrm{End}(E) = \mathbb{Z}$). Then

(a) $\rho_l(G_{\bar{K}/K})$ is of finite index in $\mathrm{Aut}(T_l(E))$ for all primes l.

(b) For almost all primes l,

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

End