COMPLEX MULTIPLICATION: LECTURE 15

Proposition 0.1. *Let $\phi : E_1 \to E_2$ be a non-constant isogeny, then $\#\phi^{-1}(0) = \deg_s \phi$ where $\deg_s$ is the separable degree of ϕ.*

Proof. Silverman III 4.10 □

Exercise: i) Consider the elliptic curve E over $\mathbb{C}$ defined by $y^2 = x^3 + x$. Compute j invariant, and show that it has an endomorphism (actually an automorphism) $[i]$ given by

$$(x, y) \mapsto (-x, iy)$$

.

ii) Show that $g_3(i) = 0$ (use translation property), hence deduce that $j(i) = 1728$. This should be the j-invariant obtained from part i. What is the homomorphism of complex tori corresponding to i?

0.1. **Dual isogenies and Tate Modules.** Given a complex torus $\mathbb{C}/\Lambda_1$, and an isogeny $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ of degree m, we know from the theory of Riemann surfaces that for almost all $P \in \mathbb{C}/\Lambda_2$, $\phi^{-1}(x)$ has m elements. But since these Riemann surfaces have a group structure, it follows that this is true for all $P \in \mathbb{C}/\Lambda_2$ by translating preimages by group elements. Thus $\ker \phi$ is a finite subgroup of order m in $\mathbb{C}/\Lambda_1$, in particular, it is contained in the m torsion $\mathbb{C}/\Lambda_1[m]$ of $\mathbb{C}/\Lambda_1$. Since there are m^2 m-torsion points, the image of $\ker[m]$ in $\mathbb{C}/\Lambda_2$ is a subgroup of order m, thus we may quotient out this group by to obtain another isogeny of degree m

$$\hat{\phi} : \mathbb{C}/\Lambda_2 \to /\Lambda_3$$

It is easy to see that the composition $\hat{\phi} \circ \phi$ is the the isogeny $[m] : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_1$.

This construction generalises to the cases of an elliptic curve defined over an arbitrary field using the Riemann Roch theorem, the isogeny $\hat{\phi}$ constructed is called the dual isogeny to ϕ and it satsifes the following properties.

Proposition 0.2. *Let $\phi : E_1 \to E_2$ be a non-constant isogeny of elliptic curves of degree m, then exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ of degree m such that*

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

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

We have the following properties of $\hat{\phi}$:

a) If $\psi : E_2 \to E_2$ is another isogeny, we have

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

b) If $\psi : E_1 \to E_2$ is another isogeny, we have

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

c) $\widehat{[m]} = [m]$ and $\deg[m] = m^2$

d) $\hat{\hat{\phi}} = \phi$

Proof. See Silverman, for the proof of the existence and uniqueness of ϕ, and the proof of b). a) c) and d) then follow easily. □

Corollary 0.3. *Let m be coprimes to char(K), then*

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

Proof. Since $\deg[m] = m^2$ is coprime to char$K$, we have that $[m]$ is a separable map. Thus it follows from 0.1 that $\#E[m] = m^2$, similarly we have $\#E[d] = d^2$ for all $d|m$. From this it follows that

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

is the only possibility. □

The following construction is hugely important in the theory of elliptic curves and in general number theory. It was the first example of Galois represention "coming from geometry," its properties have provided an endless source of intuition for theorems and conjectures that have been made since Tate first studied these objects.

Let m be an integer coprime to char$K$, we have seen above that $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. However this group has considerably more structure if E is defined over K. In fact if $\sigma \in G_{\overline{K}/K}$, it is easy to check that for $P \in E[m](\overline{K})$, we have $\sigma(P) \in E[m]$. Therefore we obtain a representation

$$G_{\overline{K}/K} \to \mathrm{Aut}E[m] \cong GL_2(\mathbb{Z}/m\mathbb{Z})$$

The l-adic Tate module will be defined by patching together these representations over powers of l to obtain a representation over $\mathbb{Z}_l$, much in the same way that $\mathbb{Z}_l$ is constructed as the inverse limit of $\mathbb{Z}/l^n\mathbb{Z}$.

Definition 0.4. Let l be a prime number which is coprime to $mboxcharK$. The l-adic Tate module of E, $T_l(E)$ is the set given by

$$\lim_{\to n} E[l^n]$$

where the transition maps are given by

$$[l] : E[l^{n+1}] \to E[l^n]$$

The structure of $\mathbb{Z}/l^n\mathbb{Z}$ modules are compatible with the transition maps and the actions of $G_{\overline{K}/K}$, hence $T_l(E)$ has a natural structure of $\mathbb{Z}_l$-module. We obtain a representation

$$G_{\overline{K}/K} \to \mathrm{Aut}T_l(E)$$

.

It follows from 0.3 that the $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ as $\mathbb{Z}_l$ modules, thus picking a basis for $T_l(E)$, we obtain a representations

$$G_{\overline{K}/K} \to GL_2(\mathbb{Z}_l)$$

well defined up to conjugation.

The same construction works for the algebraic group $K^\times$ with multiplication. As a motiviating example let's see what we obtain in this case.

Example 0.5. Suppose $K = \mathbb{Q}$, and consider the group variety $\mathbb{G}_m$. Recall this was the algebraic variety $\mathbb{A}^1 - \{0\}$, so that $\mathbb{G}_m(L) = L^\times$ with group structure given by multiplication. We have for any prime l, $\mathbb{G}_m[l^n]$ is given by the l^nth roots of unity. We have a canonical isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{l^n})/\mathbb{Q}) \cong \mathbb{Z}/l^n\mathbb{Z}^\times$$

An element of $T_l\mathbb{G}_m$ is given by a compatible system of l^nth roots of unity $(\zeta_{l^n})_n$ where $\zeta_{l^{n+1}}^l = \zeta_{l^n}$, and patching together the maps $G_{\overline{\mathbb{Q}}/\mathbb{Q}} \to \mathbb{Z}/l^n\mathbb{Z}^\times$ we obtain a character

$$\chi_l : G_{\overline{\mathbb{Q}}/\mathbb{Q}} \to \mathbb{Z}_l^\times$$

known as the l-adic cyclotomic character.

Exercise: Show that the action of $g \in \mathbb{Z}_l^\times$ acts on $T_l\mathbb{G}_m$ by sending (ζ_{l^n}) to the system given by $\zeta_{l^n}^{g \bmod l^n}$.

Therefore, for the group $\mathbb{G}_m$ over $\mathbb{Q}$ this representation is easy to describe, however for elliptic curves, they can be considerably more complicated.

Tate modules provide a very useful tool for studying isogenies between elliptic curves. Suppose $\phi : E_1 \to E_2$ is an isogeny of elliptic curves over K. Then

$$\phi(E_1[l^n]) \subset E_2[l^n]$$

and we can patch these together for all n so that $\phi_l : T_l(E_1) \to T_l(E_2)$. In fact it is easy to see this is a map of $\mathbb{Z}$-modules, therefore we obtain a homomorphism:

$$\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l}(T_l E_1, T_l E_2)$$

Furthermore if ϕ is defined over K, the map ϕ_l is compatible with the Galois actions on the Tate modules so that we obtain a homomorphism

$$\mathrm{Hom}_K(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_{G_{\overline{K}/K}}(E_1, T_l E_2)$$

We have the following theorem:

Theorem 0.6. *i) The homomorphism*

$$Hom(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to Hom_{\mathbb{Z}_l}(T_l E_1, T_l E_2)$$

is injective.

ii) The homomorphism

$$Hom_K(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to Hom_{G_{\overline{K}/K}}(E_1, T_l E_2)$$

is an isomorphism when K is a finite field or a number field (it is alway injective by part i)

Proof. i) Silverman III 7

ii) The case K is a finite field is due to Tate. When K is a number field, this was proved Faltings, it was the main ingredient in his proof of the Mordell conjecture. □

Part i) of the above immediately implies the following corollary.

Corollary 0.7. *$Hom(E_1, E_2)$ has rank at most 4 over $\mathbb{Z}$.*

Important exercise: Read chapter 9 of section III in Silverman. This proves there are only 3 possibilities for the endomorphism ring of an elliptic curve. End(E) can only be $\mathbb{Z}$, an order in a quadratic imaginary extension of K or an order in a quaternion algebra over $\mathbb{Q}$.

The we refer to Chpater 8 of Silverman [AEC], for the following theorem. Although the following construction is very imporant in general, it plays only a small part in the proof of the theorems of Complex multiplication so we will only state the result that we need.

Theorem 0.8 (Weil Pairing)**.** *There exists a non-degenerate, Galois invariant pairing:*

$$T_l E \times T_l E \to T_l \mathbb{G}_m$$

Furthermore, if $\phi : E_1 \to E_2$ is an isogeny, then ϕ and $\hat{\phi}$ are adjoints for the pairing, i.e.

$$e(\phi(x), y) = e(x, \hat{\phi}(x))$$

for $x \in T_l E_1, y \in T_l(E_2)$

0.2. **The invariant differential.** Recall that to any algebraic curve C we may associate a $\overline{K}(C)$ vector space Ω_C. We appply this construction for an elliptic curve E.

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

Definition 0.9. The invariant differential ω of E is given by

$$\frac{dx}{2y + a_1 x + a_3}$$

Let P be any point in E, then we have an induced algebraic map

$$\tau_P : E \to E$$

given by

$$Q \mapsto Q + P$$

The following proposition justifies the name invariant differential.

Proposition 0.10. *i) ω is non-zero hence generates the one dimensional $\overline{K}(E)$ vectors space Ω_E*

ii) For any $P \in E$, we have $\tau_P^* \omega = \omega$

iii) The $\overline{k}$-subspace of Ω_E consisting of differentials df for which $\tau_P^* df = df$ for all $P \in E$ is one dimensional. A generator of this subspace is called an invariant differential.

Proof. Silverman [AEC] II Section 5 □

Invariant differentials are useful because they allow us to linearise the complicated addition law on E.

Proposition 0.11. *Let $\phi, \psi : E_1 \to E_2$ be non-constant isogenies of elliptic curves and ω an invariant differential on E_2. Then $\phi^* \omega, \psi^* \omega \in \Omega_{E_1}$ are invariant differentials on E_1 and we have*

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

Proof. Silverman II Section 5. □

The addition on the left is induced by the addition structure on E_2 which is very complicated while the addition on the left is simply addition in $\overline{k}$ vector spaces, which is somewhat easier to understand.

The invariant differential will play a role in the definition of Elliptic curves with comples multiplication because it wil allow us to relate the endomorphism ring of R with the base field $\overline{k}$.

Corollary 0.12. *If char$K = 0$, then End(E) is commutative.*

Proof. Let $\phi \in \mathrm{End}(E)$, then since $\phi^*\omega$ is also an invariant and the space of invariant differentials is 1-dimensional, it follows that there exists an $a_\phi \in \overline{k}$ such that $\phi^*\omega = a_\phi\omega$. Then the above proposition shows that the association

$$\phi \mapsto a_\phi$$

is a ring homomorphism.

If ϕ is a non-zero isogeny, then ϕ is separable since we are working over characteristic 0, so that $a_\phi \neq 0$. Therefore the map $\phi \mapsto a_\phi$ is injective. Since $\overline{k}$ is commutative so it $\mathrm{End}(E)$. □

Combining this with the classification of endomorphism rings shows that if $\mathrm{char}K = 0$, $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order in a quadratic imaginary field K.

0.3. **Reduction of Elliptic curves.** In this section let K be a local field with ring of integers $\mathcal{O}$ and residue field k. Let π be a uniformiser of K and v the valuation associated to the discrete valuation ring $\mathcal{O}$. Given an elliptic curve E over K, we want to reduce this modulo π.

Definition 0.13. Given a Weierstrass equation for E over K, with coefficients $a_1, ..., a_6$, we say the equation is minimal if $a_1, ..., a_6 \in \mathcal{O}$ and $v(\Delta)$ is minimal among all Weierstrass equations for E subject to this condition.

It can be shown that reduced Weierstrass equations exists for all elliptic curves E. Then given a minimal Weierstrass equation for E, the reduced curve $\tilde{E}$ is given by the equation

$$y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6$$

Where $\overline{a}_i \in k$ is the reduction of the coefficients a_i modulo π.

Of course the reduced may be singular, but we have seen before that a Weierstrass equation defines a non-singular curve if and only if $\Delta \neq 0$. This leads to the following result.

Proposition 0.14. *i) Any two minimal Weierstrass equation are related by a change of variables*

$$y = u^3y' + sx' + t$$
$$x = u^2x' + r$$

where $u, r, s, t \in \mathcal{O}$ and $u \in \mathcal{O}^\times$. Consequently $v(\Delta)$ does not depend on the the minimal Weierstrass equation chosen for E.

ii) The reduced curve is non-singular (hence an elliptic curve) if and only if $v(\Delta) = 0$, for Δ the discriminant of a minimal Weierstrass equation for E.

Proof. i) Silverman Chapter VII Section I.

ii) The discriminant of the reduced curve is Δ mod π hence is non-zero if and only if $v(\Delta) = 0$. □

Definition 0.15. We say the elliptic curve E has good reduction if the curve $\tilde{E}$ is non-singular.

More generally let K be a number field and $\mathfrak{p}$ a fnite place of K. Then we say E has good reduction at $\mathfrak{p}$ if E has good reduction considered as an elliptic curve over $K_{\mathfrak{p}}$.

Given an elliptic curve over a local field K, let $(x_0 : x_1 : x_2)$ be a point in E for an embedding given by a minimal Weiersrass equation. We may scale the x_i by an element of K so that $x_0, x_1, x_2 \in \mathcal{O}_K$, and such that some $x_i \in \mathcal{O}_K^\times$. Then reducing the coefficients modulo $\mathfrak{m}$, we obtain a well defined element of $\tilde{E}(k)$. This gives a reduction map

$$\Theta : E(K) \to \tilde{E(k)}$$

Also given $\phi : E_1 \to E_2$ and isogeny defined over K, we may reduce mod π to obtain an isogeny $\tilde{\phi} : \tilde{E_1} \to \tilde{E_2}$, which is characterised by the property that

$$\tilde{\phi} \circ \Theta(x) = \phi \circ \Theta(x)$$

for any $x \in E(K)$. We obtain thus a group homomorphism

$$\mathrm{Hom}_K(E_1, E_2) \to \mathrm{Hom}_k(\tilde{E_1}, \tilde{E_2})$$

.