1 Isogenies between Elliptic Curves and the Tate Module

1.1 The Tate Module

1.1 Definition. Let E be an elliptic curve and ℓ a prime. The (ℓ-*adic*) *Tale module* of E is the inverse limit of $E[\ell^n]$, where the inverse limit is taken with respect to the natural maps

$$E[\ell^{n+1}] \to E[\ell^n].$$

The Tate module of E is denoted by $\mathrm{T}_\ell(E)$.

Since each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module, and $\mathbb{Z}_\ell$ is the inverse limit of $\mathbb{Z}/\ell^n\mathbb{Z}$, we see that the Tate module has a natural structure as a $\mathbb{Z}_\ell$-module,

1.2 Proposition. *Let E be an elliptic curve. Then, as a $\mathbb{Z}_\ell$-module, the Tate module of E has the following structure:*

(i) *if $\ell \neq \mathrm{char}(\Bbbk)$, then $\mathrm{T}_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$;*
(ii) *if $\ell = \mathrm{char}(\Bbbk) > 0$, then $\mathrm{T}_\ell(E) \cong \{0\}$ or $\mathrm{T}_\ell(E) \cong \mathbb{Z}_\ell$.*

PROOF: This follows immediately from Corollary III.6.4 (c) in Silverman. □

The preceding proposition shows that as a $\mathbb{Z}_\ell$-module, $\mathrm{T}_\ell(E)$ is free of degree at most 4. We will use the Tate module to show that the same thing is true of $\mathrm{Hom}(E_1, E_2)$ as a $\mathbb{Z}$-module for any pair of elliptic curves E_1 and E_2. The important idea here is that isogenies of elliptic curves can be extended to homomorphisms of their Tate modules. Indeed, let $\varphi : E_1 \to E_2$ be an isogeny of elliptic curves. We know from our work on isogenies that φ induces natural maps from $E_1[\ell^n] \to E_2[\ell^n]$ for all primes $\ell \in \mathbb{Z}$, and these in turn induce a $\mathbb{Z}_\ell$-linear map $\varphi_\ell : \mathrm{T}_\ell(E_1) \to \mathrm{T}_\ell(E_2)$. Therefore, we obtain a homomorphism from $\mathrm{Hom}(E_1, E_2)$ to $\mathrm{Hom}(\mathrm{T}_\ell(E_1), \mathrm{T}_\ell(E_2))$. By Proposition 1.2, both $\mathrm{T}_\ell(E_1)$ and $\mathrm{T}_\ell(E_2)$ are free $\mathbb{Z}_\ell$-modules of rank at most 2. Hence $\mathrm{Hom}(\mathrm{T}_\ell(E_1), \mathrm{T}_\ell(E_2))$ is a free $\mathbb{Z}_\ell$-module of rank at most 4. We would like to use this fact to conclude that $\mathrm{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module of rank at most 4, but this will require more work than it seems it should.

1.3 Proposition. *Let E_1 and E_2 be elliptic curves. Then the degree map* deg : $\mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ *is a positive-definite quadratic form.*

PROOF: We only need to show that the pairing $\langle \cdot, \cdot \rangle$ given by

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

is bilinear. This is clear, as

$$\begin{aligned}
[\langle \varphi, \psi \rangle] &= [\deg(\varphi + \psi)] - [\deg(\varphi)] - [\deg(\psi)] \\
&= \widehat{(\varphi + \psi)} \circ (\varphi + \psi) - \hat{\varphi} \circ \varphi - \hat{\psi} \circ \psi \\
&= \hat{\varphi} \circ \psi + \hat{\psi} \circ \varphi.
\end{aligned}$$

□

By Proposition III.4.2 (b) of Silverman, we know that $\mathrm{Hom}(E_1, E_2)$ is torsion-free. Therefore, $\mathrm{Hom}(E_1, E_2)$ naturally injects into $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$. If M is a submodule of $\mathrm{Hom}(E_1, E_2)$, we define

$$M^{\mathrm{div}} = (M \otimes \mathbb{Q}) \cap \mathrm{Hom}(E_1, E_2),$$

or equivalently

$$M^{\mathrm{div}} = \{\varphi \in \mathrm{Hom}(E_1, E_2) : n \cdot \varphi = [n] \circ \varphi \in M \text{ for some } n \in \mathbb{N}\}.$$

1.4 Proposition. *Let E_1 and E_2 be elliptic curves. Then if M is a finitely generated submodule of $\mathrm{Hom}(E_1, E_2)$, then M^{div} is also finitely generated.*

PROOF: We will view M^{div} as a subgroup of $M \otimes \mathbb{R}$. We will show it is a discrete subgroup, which implies that it is finitely generated. Since the degree map is a quadratic form on $\mathrm{Hom}(E_1, E_2)$, it is a quadratic form on M. Since M is finitely generated, we can think of it being given by a quadratic polynomial in the coefficients of each generator. Therefore, it extends naturally to a quadratic form on $M \otimes \mathbb{R}$, which is automatically continuous. Hence

$$U = \{\varphi \in M \otimes \mathbb{R} : \deg(\varphi \otimes x) < 1\}$$

is a neighbourhood of the origin in $M \otimes \mathbb{R}$, but it clearly only intersects M^{div} at 0, so M^{div} must be a discrete subgroup of $M \otimes \mathbb{R}$. □

1.5 Theorem. *Let E_1 and E_2 be elliptic curves, and let ℓ be a prime distinct from* $\mathrm{char}(\Bbbk)$. *Then the map*

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(\mathrm{T}_\ell(E_1), \mathrm{T}_\ell(E_2))$$

given by $\varphi \otimes a \mapsto a \cdot \varphi_\ell$ is injective.

PROOF: Suppose that

$$\varphi = a_1(\varphi_1)_\ell + \cdots + a_k(\varphi_k)_\ell = 0,$$

where $a_1, \ldots, a_k \in \mathbb{Z}_\ell$ and $\varphi_1, \ldots, \varphi_k \in \mathrm{Hom}(E_1, E_2)$. Let M be the submodule of $\mathrm{Hom}(E_1, E_2)$ generated by $\varphi_1, \ldots, \varphi_k$. By Proposition 1.4, M^{div} is finitely generated, and hence free. Let $\psi_1, \ldots, \psi_m$ be a basis for M^{div}. Then there exist $b_1, \ldots, b_m \in \mathbb{Z}_\ell$ such that

$$\varphi = b_1(\psi_1)_\ell + \cdots + b_m(\psi_m)_\ell = 0.$$

We will show that each b_i is zero by showing that its $\mathbb{Z}/\ell^n\mathbb{Z}$ part is zero for each n. If $n \in \mathbb{N}$, there is a $c_i \in \mathbb{Z}$ such that $b_i \equiv c_i \pmod{\ell^n}$. Hence,

$$\psi = c_1(\psi_1)_\ell + \cdots + c_m(\psi_m)_\ell$$

agrees with

$$\varphi = b_1(\psi_1)_\ell + \cdots + b_m(\psi_m)_\ell$$

up to the level of ℓ^n. Since φ acts as 0 on $T_\ell(E_1)$, ψ acts as 0 on $E_1[\ell^n]$. Since $\ell \neq \mathrm{char}(\Bbbk)$, $[\ell^n]$ is a separable morphism, and since its kernel is contained in the kernel of ψ, we can factor ψ as $[\ell^n] \circ \psi'$. Since $\psi \in M^{\mathrm{div}}$, $\psi' \in M^{\mathrm{div}}$ also, so

$$\psi' = d_1(\psi_1)_\ell + \cdots + d_m(\psi_m)_\ell$$

for some $d_1, \ldots, d_m \in \mathbb{Z}$. But the ψ_i are a basis for M^{div}, so $c_i = d_i\ell^n$. Hence $b_i \equiv 0 (\mathrm{mod} \ell^n)$. Since $n \in \mathbb{N}$ was chosen arbitrarily, the b_i are 0 in $\mathbb{Z}_\ell$, so $\varphi = 0$ as desired. □

1.6 Corollary. *Let E_1 and E_2 be elliptic curves. Then* $\mathrm{Hom}(E_1, E_2)$ *is a free $\mathbb{Z}$-module of rank at most* 4.

PROOF: Let ℓ be a prime distinct from $\mathrm{char}(\Bbbk)$. By Theorem 1.5 and Proposition 1.2, $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$ is free of rank at most 4, so

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}_\ell \cong (\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

is as well. Since $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$ is a vector space, it is automatically free, and it has rank at most 4, since

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}_\ell \cong (\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell.$$

We may choose generators for $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$ that lie in $\mathrm{Hom}(E_1, E_2)$ by clearing denominators, and these generators will generate a finitely generated submodule M of $\mathrm{Hom}(E_1, E_2)$. Since they generate all of $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}$ over $\mathbb{Q}$,

$$\begin{aligned} M^{\mathrm{div}} &= (M \otimes \mathbb{Q}) \cap \mathrm{Hom}(E_1, E_2) \\ &\cong (\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Q}) \cap \mathrm{Hom}(E_1, E_2) \\ &\cong \mathrm{Hom}(E_1, E_2), \end{aligned}$$

so by Proposition 1.4, we know that $\mathrm{Hom}(E_1, E_2)$ is finitely generated. Since $\mathrm{Hom}(E_1, E_2)$ is torsion-free, this implies that it is free. Therefore, by Theorem 1.5 and Proposition 1.2, the rank of $\mathrm{Hom}(E_1, E_2)$ is at most 4. □