Talk 4: Tate Module and the Weil Pairing

Anish Ray
University of Muenster

18 May 2022

Aim of the talk

(*i*) Define the Tate module and explain its properties.
(*ii*) Explain the relation between the Tate module and the isogenies between two elliptic curves.
(*iii*) Explain the construction of the Weil pairing.
(*iv*) Explain how the automorphism group of an elliptic curve looks like.

Notations and some definitions

- K perfect field, i.e., every algebraic extension of K is separable,
- $\bar{K}$ a fixed algebraic closure of K,
- K^* group of units of K,
- E a smooth curve,
- E/K E is defined over K,
- $K(E)$ the function field of E over K,
- If $\bar{K}/K$ is a Galois extension, then $G_{\bar{K}/K}$ is the Galois group of $\bar{K}/K$,
- (Categorical definition of the Projective/Inverse limit) Given a diagram

$$A_0 \xleftarrow{f_0} A_1 \xleftarrow{f_1} A_2 \xleftarrow{f_2} A_3 \xleftarrow{f_3} \cdots$$

where $(A_i)_{i\in\mathcal{I}}$ is a family of objects indexed by a poset $(\mathcal{I}, \leq)$ and morphisms $f_i : A_i \to A_{i-1}$, we define the projective limit $\varprojlim A_i$ to be the categorical limit of the diagram.
For groups and modules we can give an explicit construction of such an object,

$$\varprojlim_n A_n = \left\{ (a_n) \in \prod_n A_n \mid \forall n \in \mathbb{N} \quad \text{where} \quad f(n) = a_{n-1} \right\}$$

- (Definition of the ℓ-adic topology) For a given prime number ℓ, the field $\mathbb{Q}_\ell$ of ℓ-adic numbers is a completion of the rational numbers. The field $\mathbb{Q}_\ell$ is also given a topology, called the ℓ-adic topology which is derived from a metric, which is itself derived from the ℓ-adic order, an alternative valuation on the rational numbers.

§1 The Tate Module

Definition 1.1. *Let E/K be an elliptic curve and let $l \in \mathbb{Z}$ be a prime. The ℓ-adic Tate module of E is the group*

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

the inverse limit being taken with repsect to the natural maps

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

Since each $E[\ell^n]$ is a $\mathbb{Z}/\ell^n\mathbb{Z}$-module we see that the Tate module has a natural structure as $\mathbb{Z}_\ell$-module (here, $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers). Further since the multiplication-by-ℓ maps are surjective, the inverse limit topology on $T_\ell(E)$ is equivalent to the ℓ-adic topology that it gains by being a $\mathbb{Z}_\ell$-module.

Proposition 1.1. *As a $\mathbb{Z}_\ell$-module, the Tate module has the following structure:*
(a) $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ if $l \neq \mathrm{char}(K)$,
(b) $T_p(E) \cong 0$ or $\mathbb{Z}_p$ if $p = \mathrm{char}(K) > 0$.

Proof. Using [Si] corollary 6.4$(b), (c)$ and the fact that $\mathbb{Z}_\ell \cong \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$ ([Neu] Chapter 2 Proposition 2.5), we obtain the desired result. □

Definition 1.2. *The ℓ-adic representation of $G_{\bar{K}/K}$ associated to E is the homomorphism*

$$\rho_\ell : G_{\bar{K}/K} \to \mathrm{Aut}(T_\ell(E))$$

induced by the action of $G_{\bar{K}/K}$ on ℓ^n-torsion points of E.

Note. From here on, we consider $\ell \in \mathbb{Z}$ to be a prime number.

Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Then ϕ induces maps

$$\phi : E_1[\ell^n] \to E_2[\ell^n]$$

and hence it induces a $\mathbb{Z}_\ell$-linear map

$$\phi_\ell : T_\ell(E_1) \to T_\ell(E_2).$$

We thus obtain a natural homomorphism

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)).$$

Further, if $E_1 = E_2 = E$, then the map

$$\mathrm{End}(E) \to \mathrm{End}(T_\ell(E))$$

is a homomorphism of rings.

Theorem 1.2. *Let E_1 and E_2 be two elliptic curves and let $\ell \neq \mathrm{char}(K)$. Then the natural map*

$$\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)), \quad \phi \mapsto \phi_\ell,$$

is injective.

Lemma 1.3. *Let $M \subset \mathrm{Hom}(E_1, E_2)$ be a finitely generated subgroup and let $M^{\mathrm{div}} = \{\phi \in \mathrm{Hom}(E_1, E_2) \mid [m] \circ \phi \in M$ for some integer $m \geq 1\}$. Then M^{div} is finitely generated.*

Proof. There is a natural map $M^{\mathrm{div}} \to M \otimes \mathbb{R}$ defined by $\phi \mapsto [m] \circ \phi \otimes \frac{1}{m}$, where m is any integer such that $[m] \circ \phi \in M$ and $M \otimes \mathbb{R}$ is a finite-dimensional vector space equipped with the natural topology inherited from $\mathbb{R}$. Since $\mathrm{Hom}(E_1, E_2)$ is torsion-free ([Si] III.4.2(b)), so is M, so M is free since it's finitely generated. Hence $M \to M \otimes \mathbb{R}$ defined by $\phi \mapsto \phi \otimes 1$, is an injection. This means, that for each $\phi \in M^{\mathrm{div}}$, each $\phi \otimes 1 \neq 0$, hence $M^{div} \to M \otimes \mathbb{R}$ is also an injection. On the other hand, the image of M^{div} is a discrete subgroup of $M \otimes \mathbb{R}$. Indeed, from [Si] III.6.3 we know that the degree map deg defined over $\mathrm{Hom}(E_1, E_2)$ is a positive definite quadratic form so we can extend deg linearly as a quadratic form to $M \otimes \mathbb{R}$[1]. Also, deg is clearly continuous. So, the set $U = \left\{ \sum_i \phi_i \otimes a_i \in M \otimes \mathbb{R} \mid \deg \phi < 1 \right\}$ is an open neighborhood of 0. Further, since $\mathrm{Hom}(E_1, E_2)$ is a torsion-free-$\mathbb{Z}$-module, there is a natural inclusion $M^{\mathrm{div}} \subset M \otimes \mathbb{R}$ and, also $M^{\mathrm{div}} \cap U = \{0\}$ since every nonzero isogeny has degree at least one. Hence M^{div} is finitely generated. □

Proof of Theorem 1.2. Let $\phi \in \mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$, and suppose that $\phi_\ell = 0$. Let $M \subset \mathrm{Hom}(E_1, E_2)$ be some finitely generated subgroup with the property that $\phi \in M \otimes \mathbb{Z}_\ell$. Then, from lemma 1.3 it follows that, M^{div} is finitely generated, so it is also free, since it is torsion-free. Let $\psi_1, \psi_2, \cdots, \psi_t \in \mathrm{Hom}(E_1, E_2)$ be a basis for M^{div}, and write

$$\phi = \alpha_1 \psi_1 + \alpha_2 \psi_2 + \cdots + \alpha_t \psi_t$$

with $\alpha_1, \alpha_2, \ldots, \alpha_t \in \mathbb{Z}_\ell$. Now fix some $n \geq 1$ and choose $a_1, a_2, \ldots, a_t \in \mathbb{Z}$ such that $a_i \equiv \alpha_i (\mod \ell^n)$, $i = 1, 2, \ldots, t$. Then the assumption that $\phi_\ell = 0$ implies that the isogeny

$$\psi = [a_1] \circ \psi_1 + [a_2] \circ \psi_2 + \cdots + [a_t] \psi_t \in \mathrm{Hom}(E_1, E_2)$$

annihilates $E_1[\ell^n]$. It follows from [Si] III.4.11, that ψ factors through $[\ell^n]$, so there is an isogeny $\lambda \in \mathrm{Hom}(E_1, E_2)$ satisfying $\psi = [\ell^n] \circ \lambda$. Further, $\lambda \in M^{\mathrm{div}}$, so there are integers $b_i \in \mathbb{Z}$ such that

$$\lambda = [b_1] \circ \psi_1 + [b_2] \circ \psi_2 + \cdots + [b_t] \circ \psi_t.$$

Then, since the ψ_i's form a $\mathbb{Z}$-basis for M^{div}, the act that $\psi = [\ell^n] \circ \lambda$ implies that $a_i = \ell^n b_i$, and hence $\alpha_i \equiv 0 (\mod \ell^n)$. This holds true for all $n \geq 1$, so we conclude that $\alpha_i = 0$, and hence that $\phi = 0$. □

Corollary 1.4. *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.

Remark 1.1. *By definition, an isogeny is defined over K if it commutes with the action of $G_{\bar{K}/K}$. Similarly, we can define* $\mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$ *to be the group of $\mathbb{Z}_\ell$-linear maps from $T_\ell(E_1)$ to $T_\ell(E_2)$ that commute with the action of $G_{\bar{K}/K}$ as given by the ℓ-adic representation.*

[1] A rough idea behind extending deg from M to $M \otimes \mathbb{R}$ is similar to the following ideas:
(i)To prove that the ring of integers in a number field is finitely generated we embed them in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where r_1 and $2r_2$ are the number of real and imaginary embeddings, respectively.
(ii). To prove that the units in a number field are finitely generated we embed them in $\mathbb{R}^{r_1 + r_2}$.
Then we show that our groups sits as a discrete subgroup and hence it is finitely generated. And, if one simply has a group and a positive definite quadratic form, as is the case for $\mathrm{End}(E)$ and the degree map deg, then it is quite natural to tensor with $\mathbb{R}$ and extend the quadratic form to put a Euclidean structure on the resulting vector space.

Theorem 1.5. *(Isogeny Theorem) Let $\ell \neq \mathrm{char}(K)$ be a prime. Then the natural map*

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

is an isomorphism if:
(a) K is a finite field.
(b) K is a number field.

Remark 1.2. *(A rough idea of the proof of Theorem 1.3) Note that $\phi \in \mathrm{Hom}_K(T_\ell(E_1), T_\ell(E_2))$ induces $\phi_n : E_1[\ell^n] \to E_2[\ell^n]$ for each n. We want to show, given such an $\phi \neq 0$, there exist one or more homomorphism $E_1 \to E_2$ whose induced actions on the Tate module, in some $\mathbb{Z}_\ell$-linear combination, give ϕ.*

It's important to note that given just a single $\phi_n : E_1[\ell^n] \to E_2[\ell^n]$, we cannot reach the desired conclusion. In fact, there can be such an ϕ_n for n very large but no nonconstant maps $E_1 \to E_2$ at all.

So we have to take advantage of the fact that ϕ_n exists for infinitely many n.

We will do this by contrasting this infinitude against something else we know to be finite. For K finite, this finiteness is going to ultimately boil down to the finiteness of K. For K a number field, it's going to be subtler, but ultimately boil down to the fact that there are finitely many elements of bounded size (at each infinite place) in the ring of integers of K.

For each n, we can make an abelian surface that remembers the data of ϕ_n, by writing $\Phi_n = E_1 \times E_2/\{(x, y) \in E_1[\ell^n] \times E_2[\ell^n] \mid y = \phi_n(x)\}$.

A priori, this appears to be infinitely many different abelian surfaces. The key claim to prove is that there are actually only finitely many different surfaces Φ_n up to isomorphism.

Once we prove this, we will immediately get a bunch of isomorphisms $\Phi_n \to \Phi_m$ which combined with the natural maps $E_1 \to \Phi_n$ and $\Phi_m \to E_2$ will give us a lot of maps $E_1 \to E_2$. We have to do some algebra to show that we can combine these maps to recover a.

But the main arithmetic step is proving the finiteness of isomorphism classes.

For K finite, we can first think about how we would solve the problem if the Φ_i were elliptic curves. Then they would each have a j-invariant in the field K. There are infinitely many curves and only finitely many different j-invariants, and it's not so hard to see there can be finitely many (in fact, at most 6) curves over a finite field with a given j-invariant, up to isomorphism.

*For K a number field, to get finitely many j-invariants, we have to show the numerator and denominator of the j-invariant are bounded. An equivalent statement is that the **height** of the j-invariant is bounded. This height was given by Faltings.*

Theorem 1.6. *(Serre) Let K be a number field and let E/K be an elliptic curve without complex multiplication.*
(a) $\rho_\ell\left(G_{\bar{K}/K}\right)$ is of finite index in $\mathrm{Aut}(T_\ell(E))$ $\quad \forall \ell \neq \mathrm{char}(K)$.
(b) $\rho_\ell\left(G_{\bar{K}/K}\right) = \mathrm{Aut}(T_\ell(E))$ for all but finitely many primes ℓ.

§2 The Weil Pairing

Let E/K be an elliptic curve and fix $m \geq 2$ such that $(m, p) = 1$, where $p = \text{char}(K)$ if $p > 0$. Now, $E[m]$ is a free $\mathbb{Z}/m\mathbb{Z}$- module of rank two. Every free module comes equipped with a natural nondegenerate alternating multilinear map, the determinant. Choosing a basis $\{T_1, T_2\}$ for $E[m]$, the determinant pairing on $E[m]$ is given by

$$\det : E[m] \times E[m] \to \mathbb{Z}/m\mathbb{Z}, \quad (aT_1 + bT_2, cT_1 + dT_2) \mapsto ad - bc.$$

However, the determinant pairing on $E[m]$ is not Galois invariant. We can achieve Galois invariance by using instead a modified pairing of the form $\zeta^{\det(P,Q)}$, where ζ is primitive m-th root of unity. To define this pairing, we will make frequent use of [Si] (III.3.5). Let $T \in E[m]$. Then there is a function $f \in \bar{K}(E)$ satisfying,

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

Next take $T' \in E$ to be a point with $[m]T' = T$. Then there is a function $g \in \bar{K}(E)$ satifying,

$$\text{div}(g) = [m] * (T) - m * [O] = \sum_{R \in E[m]} ((T' + R) - (R)).$$

Then we can observe that this divisor sums to 0 since, $\#E[m] = m^2$ ([Si] III.6.4) and $[m^2]T' = 0$. Also, we observe that the functions $f \circ [m]$ and g^m have the same divisor, so multiplying f by an appropriate constant $\bar{K}^*$, we may assume that $f \circ [m] = g^m$. Now let $S \in E[m]$ also be an m-torsion point, where we allow $S = T$. Then for any point $X \in E$, we have

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

Thus considered as a function of X, the function $\frac{g(X+S)}{g(X)}$ takes on finitely many values, i.e., for every $X \in E$, it is an m-th root of unity. In particular, the morphism

$$E \to \mathbb{P}^1, \quad X \to \frac{g(X + S)}{g(X)}$$

is not surjective, so it is constant. This allows us to define a pairing

$$e_m : E[m] \times E[m] \to \mu_m, \quad (S, T) \mapsto \frac{g(X + S)}{g(X)}$$

μ_m, denotes the group of m-th roots of unity and $X \in E$ such that $g(X + S)$ and $g(X)$ are both defined and nonzero. The pairing that we have just defined is called the Weil e_m-pairing.

§3 The Endomorphism Ring

Let E be an elliptic curve. We have learned that
(i) End(E) has characteristic 0, no zero divisors, and rank at most four as $\mathbb{Z}$-module (Corollary 1.4).
(ii) End(E) posseses an anti-involution $\phi \mapsto \hat{\phi}$ ([Si] III.6.2), where $\hat{\phi}$ is the dual isogeny to ϕ.
(iii) For $\phi \in$ End(E), the product $\phi\hat{\phi} = 0$ iff $\phi = 0$ ([Si] III.6.2(a), III.6.3).
Next, we will describe the general classiication of rings satifying $(i) - (iii)$.

Definition 3.1. *Let $\mathcal{K}$ be a (not necessarily commutative) algebra that is finitely generated over $\mathbb{Q}$. An order $\mathcal{R}$ of $\mathcal{K}$ is a subring of $\mathcal{K}$ that is finitely generated as $\mathbb{Z}$-module and satisfies $R \otimes \mathbb{Q} = \mathcal{K}$.*

Definition 3.2. *A quaternion algebra is an algebra of the form*

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

whose multiplication satisfies

$$\alpha^2, \beta^2 \in \mathbb{Q}, \alpha^2, \beta^2 < 0, \text{ and } \beta\alpha = -\alpha\beta.$$

Theorem 3.1. *Let $\mathcal{R}$ be a ring of characteristics 0 having no zero divisors, and assume $\mathcal{R}$ has the following properties:*
(i) $\mathcal{R}$ has rank at most four as $\mathbb{Z}$-module.
(ii) $\mathcal{R}$ has an anti-involution $\alpha \to \hat{\alpha}$ satisfying

$$\widehat{\alpha+\beta} = \hat{\alpha} + \hat{\beta}, \quad \widehat{\alpha\beta} = \hat{\beta}\hat{\alpha}, \quad \hat{\hat{\alpha}} = \alpha, \text{ and } \hat{a} = a \text{ for } a \in \mathbb{Z} \subset \mathcal{R}.$$

(iii) For $\alpha \in \mathcal{R}$, the product $\alpha\hat{\alpha}$ is a nonnegative integer and $\alpha\hat{\alpha} = 0$ iff $\alpha = 0$.
Then $\mathcal{R}$ is one of the following types of rings:
(a) $\mathcal{R} \cong \mathbb{Z}$.
(b) $\mathcal{R}$ is an order in an imaginary quadratic extension over $\mathbb{Q}$.
(c) $\mathcal{R}$ is an order in a quaternion algebra over $\mathbb{Q}$.

Corollary 3.2. *The endomorphism ring of an elliptic curve E/K is either $\mathbb{Z}$, an order in an imaginary quadratic field, or an order in a quaternion algebra. If $\mathrm{char}(K) = 0$, then only the first two are possible.*

Proof. From [Si] III.4.2(b), [Si] III.6.2, and [Si] III.6.3 we have all the facts needed to apply Theorem 3.1 to the ring $\mathrm{End}(E)$. This proves the first part of the corollary. If $\mathrm{char}(K) = 0$, then [Si] III.5.6(c) says that $\mathrm{End}(E)$ is commutative, so in this case $\mathrm{End}(E)$ cannot be an order in a quaternion algebra. □

§4 The Automorphism Group

Theorem. *Let E/K be an elliptic curve. Then its automorphism group $\mathrm{Aut}(E)$ is a finite group of order dividing 24. More precisely, the order of $\mathrm{Aut}(E)$ is given by the following table:*

$\#\mathrm{Aut}(E)$	$j(E)$	$\mathrm{char}(K)$
2	$j(E) \neq 0, 1728$	-
4	$j(E) = 1728$	$\mathrm{char}(K) \neq 2, 3$
6	$j(E) = 0$	$\mathrm{char}(K) \neq 2, 3$
12	$j(E) = 0$, *or* 1728	$\mathrm{char}(K) = 3$
24	$j(E) = 0$, *or* 1728	$\mathrm{char}(K) = 2$

Proof. First we consider the case when $\mathrm{char}(K) \neq 2, 3$. Then E is given by an equation,

$$E : y^2 = x^3 + Ax + B$$

and every automorphism of E has the form $x = u^2x', y = u^3y'$, for some $u \in \bar{K}^*$. Such a substitution gives an automorphism of E iff $u^{-4}A = A$ and $u^{-6}B = B$. If $AB \neq 0$, i.e., if $j(E) \neq 0, 1728$, then the only possibilities are $u = \pm 1$. Similarly, i $B = 0$, then $j(E) = 1728$ and $u^4 = 1$, and if $A = 0$, then $j(E) = 0$ and $u^6 = 1$. Hence $\mathrm{Aut}(E)$ is cyclic of order $2, 4$, or 6, depending on whether $AB \neq 0, B = 0$, or $A = 0$, respectively. For the other cases refer to [Si] A.1.2(c). □

References

[1] [Si] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer Graduate Texts in Mathematics 106, 2nd edition, 2010.

[2] [Neu] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag XIII, 1991.