The Tate Module

Intro-SO Final Presentation

Javier López-Contreras

Supervised by Daniel Macías

INSTITUTO DE CIENCIAS MATEMÁTICAS

Objective

This will be an overview talk: mainly story, no hard proofs.

Definition (Tate Module)

Let E/K be an elliptic curve over a field K and $l \in \mathbb{Z}$ a prime. The l-adic Tate Module is

$$T_l(E) = \varprojlim_n E[l^n]$$

Motivating example:

Proposition

Let E_1, E_2 be elliptic curves over K. Then $\mathrm{Hom}(E_1, E_2)$ *has rank at most* 4 *as a $\mathbb{Z}$-module.*

Structure of the talk

1. Elliptic curves
2. Isogenies, $\mathrm{Hom}(E_1, E_2)$
3. The torsion subgroup, $E_{\text{tors}} = \cup_n E[n]$
4. The Tate Module

All the propositions in the presentation are taken verbatim from Silverman's *The Arithmetic of Elliptic Curves* chapters 1, 2 and 3.

Part 1

Curves, Riemann-Roch and Weierstrass Form

What is an Elliptic Curve?

A priori, it is not $y^2 = x^3 + ax + b$. Having a Weierstrass form is a consequence of Riemann-Roch Theorem.

Definition (Elliptic Curve)

An elliptic curve E over a base field K is a ***connected***, ***non-singular projective algebraic variety*** *on $\overline{K}$ of* ***dimension 1*** *and* ***genus 1*** *together with a base point $O \in E(K)$.*

Recall

1. *Algebraic variety.* Zero-set of a polynomial ideal in $\mathbb{P}^n_K$ or $\mathbb{A}^n_K$
2. *Dimension.* Transcendence degree $K(V)/K$
3. *Non-singular.* At all points $\dim_{\overline{K}} M_P/M_P^2 = \dim V$
4. *Genus.* From R-R, $g := l(K_C)$, $K_C \in \text{Div}(E)$ the canonical divisor.

Reminder of Riemann-Roch I

Let C/K be an algebraic curve.

Definition (Divisors)

Let $\text{Div}(C) = \{\sum_{P \in C} n_P(P) | P \in E, n_P \in \mathbb{Z}\}$ *be the abelian group of formal sums of points in* C*.*

- *It is partially ordered by* $D_1 \geq D_2 \iff n_P(D_1) \geq n_P(D_2) \; \forall P \in C$*.*
- *Define* $\deg(d) = \sum n_P \in \mathbb{Z}$ *and let* $\text{Div}^0(C)$ *be the subgroup of divisors of degree 0.*

Definition (Principal Divisor)

For $f \in K(E)^*$*, define* $\text{div}(f) \in \text{Div}(C)$ *as* $\text{div}(f) = \sum_{P \in C} \text{ord}_P(f)(P)$

Claim. All principal divisors have degree 0. (Analogous to the product formula of all norms on $\mathbb{Q}$).

Reminder of Riemann-Roch II

Definition (Picard Group)

$\text{Pic}^0(C) = \text{Div}^0(C)/\sim$, *with* $d_1 \sim d_2$ *if* $d_1 - d_2$ *is a principal divisor.*

There is a well defined $K_C \in \text{Pic}^0(C)$ called the canonical divisor that is $\text{div}(w)$ for any w differential form.

Definition (Vector space of a divisor)

Let $\mathcal{L}(D) = \left\{ f \in \overline{K}(C)^* : \text{div}(f) \geq -D \right\} \cup \{0\}$. *It is a vector space over* $\overline{K}$, *let* $l(D)$ *be its dimension.*

Claim One can prove the $\mathcal{L}(D)$ are finite dimensional.

Reminder of Riemann-Roch III

Theorem (Hirzebruch-Riemann-Roch)

Let C be a smooth curve of and let K_C be a canonical divisor on C. There is a unique integer $g \geq 0$, called the genus of C, such that for every $D \in \text{Div}(C)$,

$$l(D) - l(K_C - D) = \deg D - g + 1$$

Usecase.

1. R-R is used to prove the existence or non-existence of $f \in K(C)^*$ with certain poles and zeroes of certain orders.
2. We will use it to prove that all elliptic curves have a Weierstrass Form.

Weierstrass Form

Let E be an elliptic curve defined over K

Theorem (Existance of Weierstass Form)

There exist functions $x, y \in K(E)$ such that the map

$$\phi : E \to \mathbb{P}^2$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

$$C : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

with $a_i \in K$ and $\phi(O) = [0, 1, 0]$.

Proof of Existence of Weierstrass Form

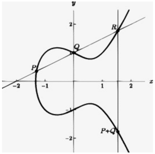
- Study $\mathcal{L}(n(O))$, the space of $f \in K(E)^*$ with at most a single pole at O, at most of order n.
- By R-R it has size $l(n) = l(K_C - n(O)) + n - g + 1 = n \ \forall n \geq 1$.
- We can choose x, y such that $\{1, x\}$ is a base of $\mathcal{L}(2(O))$ and $\{1, x, y\}$ is a base of $\mathcal{L}(3(O))$.
- Now, $L(6(O))$ has dimension 6 but contains all seven $1, x, y, y^2, x^2, x^3, xy$, so there must be a linear relation

$$A_1 + A_2 x + A_3 y + A_4 x^2 + A_5 xy + A_6 y^2 + A_7 x^2 = 0$$

Claim. By algebraic manipulation, we can get to a simpler Weierstrass equation. If char$(K) \neq 2, 3$ we can reduce to $y^2 = x^3 + ax + b$.

Group Law Revisited

Comment. The addition of points in an Elliptic Curve is often justified geometrically. There is also a algebraic interpretation that comes from R-R and $g = 1$.



Proposition

Let $(E/K, O)$ *an elliptic curve*

1. $(P) \sim (Q) \iff P = Q$
2. $\forall d \in \text{Div}^0(E), \exists P \in E$ *such that* $D \sim (P) - (O)$

Hence, there is a bijection of sets $\kappa : E \xrightarrow{\sim} \text{Pic}^0(E)$

Obs. E inherits a group structure from $\text{Pic}^0(E)$.

Part 2

Isogenies of an Elliptic Curve

Isogenies

Let (E_1, O_1) and (E_2, O_2) be elliptic curves over K.

Definition (Isogeny)

An isogeny between E_1 and E_2 is a morphism of curves $\phi : E_1 \to E_2$ that sends $\phi(O_1) = O_2$.

Comment. They are the morphisms in the category of elliptic curves.

Claim. $\phi(P + Q) = \phi(P) + \phi(Q)$, hence the group structure maps correctly.

$$
\begin{array}{ccc}
E_1 & \xrightarrow{\ \phi\ } & E_2 \\
{\scriptstyle \kappa_1^{-1}} \uparrow & & \downarrow {\scriptstyle \kappa_2} \\
\mathrm{Pic}^0(E_1) & \overset{\widehat{\phi}}{\dashrightarrow} & \mathrm{Pic}^0(E_2)
\end{array}
$$

Degree of an Isogeny

Let $\phi : E_1 \to E_2$ be an isogeny.

Obs. As morphism of curves, it defines $\phi^* : \overline{K}(E_2) \to \overline{K}(E_1)$

Definition (Degree)

If ϕ is constant, it has degree 0. Else, the degree of ϕ is the degree of the extension $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$. We note $\deg \phi = [\overline{K}(E_1) : \phi^*(\overline{K}(E_2))]$

Claims.

1. $\deg \phi < \infty$
2. $\deg(\psi \circ \phi) = \deg(\psi) \deg(\phi)$

Multiplication by m

Let (E, O) be an elliptic curve over K.

Definition

Let $m > 0$, multiplication map is

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto \underbrace{P + \cdots + P}_{m} \end{aligned}$$

Extend it to $m \in \mathbb{Z}$ with $[0]P := O$ and $[-m](P) := -[m](P)\ \forall P \in E$.

Obs.

1. $[m]$ is an isogeny. This is a corollary of an important proposition that states that the $+ : E \times E \to E$ and $- : E \to E$ are morphisms of varieties.
2. $[m] + [n] = [m + n]$
3. $[m] \circ [n] = [mn]$

Claim. $[m] = [n] \iff m = n$

Obs. There is an injection $\mathbb{Z} \hookrightarrow \mathrm{Aut}(E) := \mathrm{Hom}(E, E)$

Dual Isogeny I

Let E_1, E_2 be elliptic curves on K and $\phi : E_1 \to E_2$ an non constant isogeny.

Definition

Define ϕ^* as the morphism of abelian groups that acts as follows on the generators.

$$\begin{aligned} \phi^* : \mathrm{Pic}^0(E_2) &\to \mathrm{Pic}^0(E_1) \\ (Q) &\mapsto \sum_{R \in \phi^{-1}(Q)} e_R(\phi)(R) \end{aligned}$$

Obs. With ϕ^* we can define a related map $\widehat{\phi} : E_2 \to E_1$.

Claim. This map is an isogeny

$$\begin{array}{ccc} E_2 & \overset{\widehat{\phi}}{\dashrightarrow} & E_1 \\ \downarrow \kappa_2 & & \uparrow \kappa_1^{-1} \\ \mathrm{Pic}^0(E_2) & \xrightarrow{\phi^*} & \mathrm{Pic}^0(E_1) \end{array}$$

Dual Isogeny II

Let E_1, E_2, E_3 be elliptic curves on K and $\phi, \psi : E_1 \to E_2$ and $\theta : E_2 \to E_3$ isogenies.

Proposition (Silverman, III.6.2)

1. $\widehat{\phi} \circ \phi = \phi \circ \widehat{\phi} = [\deg \phi]$
2. $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\phi}$

Corollary

1. *Using 2, inductively on* m, $\widehat{[m]} = [m]$
2. *Using 1,* $[m] \circ \widehat{[m]} = [\deg[m]] = [m^2] \implies \deg[m] = m^2$
3. *By multiplicativity of degrees,* $[m] \circ \phi = [0] \iff \phi = [0]$

Part 3

The Torsion subgroup

Torsion points of order m

Let E/K be an elliptic curve.

Definition (Subgroup of torsion points of order m)

We define $E[m] := \ker[m] = \{P \in E \mid [m]P = O\}$, which is a subgroup of E.

Objective. We will find the cyclic decomposition of $E[m]$ $\forall m \in \mathbb{Z}$. This will enable the explicit computation of the Tate Module.

Recall. This groups were the main component in the definition of the Tate Module

$$T_l(E) = \varprojlim_{n} E[l^n]$$

Torsion points of order m II

Let E/K be an elliptic curve.

Proposition

For any $m \in \mathbb{Z}, m \geq 2$ *such that if* $\text{char} K > 0$, $\text{char} K \not| m$, *we have* $E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

Sketch of proof

1. Prove $|E[m]| = m^2$
2. Prove that an abelian group of order m^2 and such that for every $d|m$ contains a subgroup $E[d] \subseteq E[m]$ of order d^2 implies $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

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

Recall. If C_1, C_2 are curves, $\phi : C_1 \to C_2$ a morphism of curves

- Define $e_P(\phi) = \mathrm{ord}_P(\phi^* t_{\phi(P)})$ the index of ramification of ϕ at P
- Only finitely many P ramify, have $e_P(\phi) \geq 1$
- Proposition. $\sum_{R\phi^{-1}(Q)} e_R(\phi) = \deg \phi$

Then, proof goes as follows

- $[m]$ is not ramified.
- Hence $|E[m]| = |\ker[m]| = |[m]^{-1}(O)| = \deg[m] = m^2$.

Galois Structure on $E[m]$

$E[m]$ has more structure, given by the action of the Galois Group of $\overline{K}/K$.

Proposition (Galois action on $E[m]$)

The absolute Galois group $G_{\overline{K}/K}$ acts on $E[m]$ with

$$G_{\overline{K}/K} \times E[m] \to E[m]$$
$$(\sigma, P) \mapsto P^\sigma$$

This is well defined, $[m](P^\sigma) = ([m](P))^\sigma = O^\sigma = O$, as $O \in \mathbb{P}^2_K$

Obs. $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ is a $\mathbb{Z}/m\mathbb{Z}$-module.

Obs. This gives a representation of char$\rho_m = m > 0$

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

Part 4

The Tate Module

Inverse System

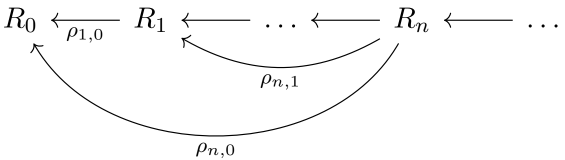
All rings in this talk are commutative and unitary.

Comment. This definition can be given categorically. I restricted to the category of rings for simplicity.

Definition (Inverse System)

An inverse (or projective) system is a sequence of rings $(R_i)_{i \geq 0}$ *together with a family of morphisms* $\rho_{i,j} : R_i \to R_j \ \ \forall i \geq j$ *such that* $\forall k$ *with* $i < k < j$

$$\rho_{i,j} = \rho_{i,k} \circ \rho_{k,j}$$



Inverse Limit

Definition (Inverse Limit)

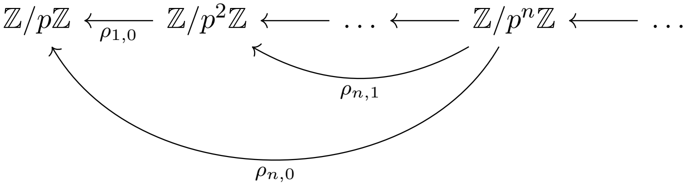
The inverse (or projective) limit of a inverse system is

$$\varprojlim_{n} R_i := \{(x_0, x_1, \dots) \mid x_i \in R_i \text{ and } \forall j < i, \rho_{ij}(x_i) = x_j\}$$

Prop. It is a sub-ring of the product ring, with $\times$ and $+$ working cell-per-cell.

The p-adic integers $\mathbb{Z}_p$

Obs. Let $R_i = \mathbb{Z}/p^i\mathbb{Z}$ and $\rho_{i,j} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ be the usual quotient map. Then, we denote $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ the set of p-adic integer numbers.



Obs. $\mathbb{Z}_p$ can be seen as infinite 'base' expressions at p

$$a_0 + a_1 p + a_2 p^2 + \cdots$$

with $a_i \in \mathbb{Z}/p\mathbb{Z}$.

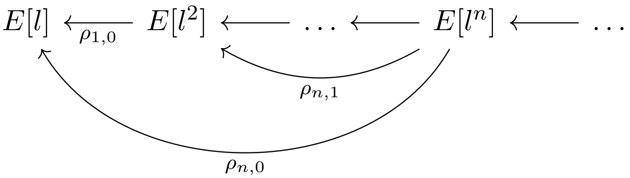
Definition

Definition (Tate Module)

Let E/K be an elliptic curve over a field K and $l \in \mathbb{Z}$ a prime. The l-adic Tate Module is

$$T_l(E) = \varprojlim_n E[l^n]$$

Obs. There is a projective system $(E[l^n])_{n \geq 0}$ with maps $E[l^{n+1}] \xrightarrow{[l]} E[l^n]$ for all $n \geq 1$.



Recall. $T_l(E) = \{(P_1, P_2, \dots) \mid P_i \in E[l^i] \text{ and } [l]P_{i+1} = P_i\}$

Basic Properties

Proposition

1. *$T_l(E)$ is a $\mathbb{Z}_l$-module with a scalar product*

$$\begin{aligned} \cdot : \mathbb{Z}_l \times T_l(E) &\to T_l(E) \\ ((a_i), (P_i)) &\mapsto ([a_i]P_i) \end{aligned}$$

2. *If l is a prime not equal to* char$K$,

$$T_l(E) \simeq \mathbb{Z}_l \times Z_l$$

   is an isomorphism of $\mathbb{Z}_l$-modules.

3. *There is an action*

$$\begin{aligned} G_{\overline{K}/K} \times T_l(E) &\to T_l(E) \\ (\sigma, (P_n)_{n\geq 0}) &\mapsto (P_n^\sigma)_{n\geq 0} \end{aligned}$$

Associated Representation

The action of $G_{\overline{K}/K}$ on $T_l(E)$ gives an l-adic representation.

Definition (Representation associated to the l-Tate Module)

We can define a representation
$\rho : G_{\overline{K}/K} \to \mathrm{Aut}(T_l(E)) \simeq GL_2(\mathbb{Z}_l) \hookrightarrow GL_2(\mathbb{Q}_l)$

Obs.

1. The isomorphism in the definition is not canonical. There is a more canonical way to find a representation.
2. The representation above has characteristic 0, which was one of our aims.

Usecase. Studying Isogenies

Let E_1 and E_2 be elliptic curves on K and $\phi : E_1 \to E_2$ an isogeny.

Obs. ϕ induces a map $\phi_n : E_1[l^n] \to E_2[l^n]$ as $\mathbb{Z}/l^n\mathbb{Z}$-modules. In turn, these induce a map $\phi : T_l(E_1) \to T_l(E_2)$ as $\mathbb{Z}_l$-modules.

Theorem

Let $l \neq \text{char}(K)$ a prime. Then, the natural map of Z_l-modules

$$\text{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \text{Hom}_{\mathbb{Z}_l}(T_l(E_1), T_l(E_2))$$
$$\phi \otimes c \mapsto c \cdot \phi_l$$

is injective.

Motivating Example Solved

Corollary

Let E_1 and E_2 be elliptic curves on K. Then $\text{Hom}(E_1, E_2)$ is a free $\mathbb{Z}$-module or rank at most 4.

Proof.

- $\text{Hom}(E_1, E_2)$ is **torsion-free** over $\mathbb{Z}$ PID $\implies$ $\text{Hom}(E_1, E_2)$ free.
- $\text{rank}_{\mathbb{Z}}(\text{Hom}(E_1, E_2)) = \text{rank}_{\mathbb{Z}_l}(\text{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l) \leq \text{rank}_{\mathbb{Z}_l}(\text{Hom}(T_l(E_1), T_l(E_2)))$
- $\text{Hom}(T_l(E_1), T_l(E_2)) = M_2(\mathbb{Z}_l)$, which has rank 4.

Generalization to Schemes

Important note. My knowledge on Scheme Theory is very limited. This slide is just commentary.

Obs. Some of the objects and theorems we studied have an analogue in the Theory of Number Fields. Here is an approximate correspondance.

Algebraic Varieties/Curves	**Theory of Number Fields**
points	prime ideals
variety	spectrum
$\text{Pic}^0(E)$	Class group $Cl(K)$
Covers and automorphisms of covers	Extensions and Galois groups
Ramification theory	Hilbert Ramification theory

Comment. The theory of schemes seems to unify this two worlds, which will both be examples of schemes.

Comment. Similarly, one can generalize the properties of an Elliptic curve to a class of schemes with a suitable group structure, called Abelian Varieties.

Thank you for your attention

jlopezcontreras10@gmail.com

INSTITUTO DE CIENCIAS MATEMÁTICAS

Extra Slides

Affine Algebraic Varieties

Objective. Define everything intrinsically, without appealing to any topological structure on K. We forget the usual definition of a curve.

Definition (Affine Algebraic Variety)

An affine algebraic variety over a field K is the set of zeros $V \subseteq \mathbb{A}^n_{\overline{K}} \simeq \overline{K}^n$ of a prime ideal $\mathfrak{p} \subseteq \overline{K}[x_1, \ldots, x_n]$, for some $n \geq 1$.

The condition of $\mathfrak{p}$ prime ensures that the set of zeros is 'irreducible'.

Definition (Coordinate Ring)

Is the set of polynomial functions from $V \to K$ quotiented by the equivalent relation of having equal images for all the points on V. Hence $K[V] := K[x_1, \ldots, x_n]/\mathfrak{p}$

Projective Algebraic Varieties

Definition (Projective Algebraic Variety)

An n-th dimensional projective algebraic variety over a field K is the set of zeros $V \subseteq \mathbb{P}^n_{\overline{K}}$ of a homogeneus prime ideal $\mathfrak{p} \subseteq \overline{K}[x_0, x_1, \ldots, x_n]$.

A homogeneus ideal is an ideal generated by homogeneus polynomials. Non-homogeneus polynomials don't define a function $p : \mathbb{P}^n \to \mathbb{P}^n$

Let V be an algebraic projective variety and $V_{\text{aff}} = V \cap \mathbb{A}^n$ any affinization.

Definition (Dimension)

The dimension of V is the transcendence degree $K(V_{\text{aff}}) := \text{Frac}(K[V_{\text{aff}}])$ over K.

Non-singular and Genus

Comment. In an algebraic curve over $K = \mathbb{C}$, there are two notions of the topological/differential added structure that appear naturally.

1. A point $P \in V$ is non-singular if it has a unique tangent.
2. The genus of V is just the topological genus of the curve as a Riemann Surface.

These definitions a priori are not intrinsical, they depend on structure of the base field.

One can give equivalent definitions in a purely algebraic setting.

Comment. This strive of defining properties intrinsically is one of the motivations for the development of the Theory of Schemes, where one can give a general definition of an algebraic variety.

Ramification

Let $\phi : C_1 \to C_2$ a non constant map of curves and $P \in C_1$. Denote t_Q a uniformizer element on Q.

Definition (Ramification index)

Define $e_\phi(P) = \text{ord}_P(\phi^* t_{\phi(P)})$

Theorem

$\sum_{P \in \phi^{-1}} e_\phi(P) = \deg(\phi)$