Tate modules of hyperelliptic curves

Edwina Aylward

November 21st, 2025

Tate Module

Let C/K be a hyperelliptic curve of genus g over a field K and let $J = \mathrm{Jac}\, C$.

Definition

For a prime ℓ, the ℓ-adic Tate module $T_\ell J$ is given by

$$T_\ell J = \varprojlim_n J(K^{\mathrm{sep}})[\ell^n]$$

with respect to the multiplication by ℓ maps.

The *rational ℓ-adic Tate module* is $V_\ell J := T_\ell J \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

Elements of $T_\ell J$ look like sequences $\{P_n\}_n$ with $P_n \in J(K^{\mathsf{sep}})[\ell^n]$ and $\ell P_n = P_{n-1}$.

Lemma

When char $K \neq \ell$, $T_\ell J \simeq \mathbb{Z}_\ell^{2g}$ as a topological group.

The absolute Galois group $G_K = \mathrm{Gal}(K^{\mathsf{sep}}/K)$ acts on $T_\ell A$, yielding the representation

$$\rho_{J,\ell} \colon G_K \to \mathrm{GL}(T_\ell J) \simeq \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

For $\sigma \in G_K$, $\rho_{J,\ell}(\sigma) \mod \ell^n$ describes how σ acts on $J(K^{\mathrm{sep}})[\ell^n]$. This is a continuous ℓ-adic representation.

Néron–Ogg–Shafarevich Criterion

Let K be a local field with ring of integers $\mathcal{O}_K$ and residue field k, and let $\ell \neq \operatorname{char} k$.

Theorem (Néron–Ogg–Shafarevich)

Let C/K be a hyperelliptic curve and let $J = \operatorname{Jac} C$. Then J/K has good reduction if and only if $T_\ell J$ is unramified, i.e. $T_\ell J^{I_K} = T_\ell J$.

Good reduction of Jacobian: The abelian variety J/K admits a *Néron model* $\mathcal{J}/\mathcal{O}_K$. Let $\mathcal{J}_k^0$ be the identity component of the special fibre. Then J has *good reduction* if $\mathcal{J}_k^0$ is an abelian variety over k.

In this case, the reduction map induces isomorphisms

$$J[\ell^n] \simeq \mathcal{J}_k^0[\ell^n], \qquad T_\ell J \simeq T_\ell \mathcal{J}_k^0$$

as $\operatorname{Gal}(K^{\mathrm{nr}}/K) \simeq \operatorname{Gal}(\overline{k}/k)$-modules.

Remark: $T_\ell J^{I_K} \simeq T_\ell \mathcal{J}_k^0$ holds generally.

Curves with good reduction

Let K be a local field as before, with residue field k of size q and $2, \ell \nmid q$.

Suppose C/K is a hyperelliptic curve of genus g given by an affine equation

$$C : y^2 = f(x), \qquad f(x) \in \mathcal{O}_K[x].$$

Let

$$\Delta_{C,f} = (\text{leading coefficient})^{4g+2} \cdot \text{disc}(f).$$

Then C/K has good reduction $\Leftrightarrow$ there is some hyperelliptic model for C/K as above with $v_\pi(\Delta_{C,f}) = 0$. In this case, reducing coefficients mod π defines a hyperelliptic curve over k with affine equation

$$\overline{C} : y^2 = \overline{f}(x).$$

Fact: $\mathcal{J}_k^0 = \mathrm{Jac}\,\overline{C}$. Thus J/K also has good reduction, $T_\ell \,\mathrm{Jac}\, C$ is unramified, and

$$(T_\ell \,\mathrm{Jac}\, C)^{I_K} = T_\ell \,\mathrm{Jac}\, C \simeq T_\ell \,\mathrm{Jac}\,\overline{C}$$

as $G_K/I_K \simeq \mathrm{Gal}(\overline{k}/k)$-modules.

Consider the zeta function $Z(\overline{C}/k, T)$. As a consequence of the Weil Conjectures,

$$Z(\overline{C}/k, T) := \exp\left(\sum_{n\geq 1} \frac{\#\overline{C}(\mathbb{F}_{q^n})}{n} T^n\right) = \frac{P(T)}{(1-T)(1-qT)},$$

where $P(T) = \det(1 - T \cdot \mathrm{Frob}^{-1} | (V_\ell \,\mathrm{Jac}\,\overline{C})^*)$.

Curves with good reduction

Equating coefficients,

$$\#C(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n, \qquad \text{where } P(T) = \prod_{i=1}^{2g} (1 - \alpha_i T).$$

Thus the α_i (and hence the eigenvalues of Frob acting on $V_\ell \operatorname{Jac} C$) can be retrieved by counting $C(\mathbb{F}_{q^n})$ for finitely many n.

Properties of $P(T)$:

- $P(T) \in \mathbb{Z}[T]$ and is independent of ℓ for all $\ell \nmid q$.
- The eigenvalues satisfy $|\alpha_i| = q^{\frac{1}{2}}$,
- $P(T) = 1 + b_1 T + \cdots + b_{g-1} T^{g-1} + b_g T^g + q b_{g-1} T^{g+1} + \cdots + q^{g-1} b_1 T^{2g-1} + q^g T^{2g}$.

Example (Genus 2)

Suppose that C/K has genus 2. Define the traces

$$a_q := q + 1 - \#\overline{C}(\mathbb{F}_q), \qquad a_{q^2} := q^2 + 1 - \#\overline{C}(\mathbb{F}_{q^2}).$$

Using Newton identities and the above we obtain

$$P(T) = 1 - a_q T + \frac{1}{2}(a_q^2 - a_{q^2}) T^2 - a_q q T^3 + q^2 T^4.$$

Good reduction example

Example

Consider the genus 2 curve

$$X_1(13) : y^2 = x^6 + 4x^5 + 6x^4 + 2x^3 + x^2 + 2x + 1 \quad \text{over } \mathbb{Q}_7,$$

with discriminant $\Delta = -169$. Since $v_7(\Delta) = 0$, the curve has good reduction at 7. One computes

$$\#\overline{X_1(13)}(\mathbb{F}_7) = 8, \quad \#\overline{X_1(13)}(\mathbb{F}_{49}) = 64.$$

Thus

$$a_7 = 7 + 1 - 8 = 0, \quad a_{49} = 49 + 1 - 64 = -14.$$

It follows that $P(T) = 1 + 7T^2 + 49T^4$.

Note that $P(1) = 57 = 3 \cdot 19$. This is the size of $\mathrm{Jac}\,\overline{X_1(13)}(\mathbb{F}_7)$, and because prime-to-$\ell$ torsion injects we obtain

$$\mathrm{Jac}\,X_1(13)(\mathbb{Q}_7)_{\mathrm{tors}} \simeq \mathbb{Z}/3 \times \mathbb{Z}/19 \times \text{(possibly a finite 7-group)}.$$

Reduction of curve vs. reduction of Jacobian

Recall that $J = \mathrm{Jac}(C) = \mathrm{Pic}^0_{C/K}$. Let $\mathcal{J}_k^0$ be the identity component of the special fibre of the Néron model of J.

Definition

J/K has *semistable reduction* if $\mathcal{J}_k^0$ is the extension of an abelian variety by a torus.

Definition

A *semistable model* of C/K is a proper flat $\mathcal{O}_K$-scheme $\mathcal{C}/\mathcal{O}_K$ whose generic fibre is C and whose special fibre $\mathcal{C}_k$ is

- reduced (all components of multiplicity one),
- has only ordinary double points (nodes) as singularities.

C/K is called *semistable* if it admits such a model.

Theorem

Let C/K be a semistable hyperelliptic curve with model $\mathcal{C}/\mathcal{O}_K$. Then

$$\mathcal{J}_k^0 \simeq \mathrm{Pic}^0_{\mathcal{C}_k/k}.$$

Theorem (Mumford)

J/K semistable $\Leftrightarrow$ C/K semistable.

Curves with almost good reduction

We've seen that if C/K has good reduction then $\mathrm{Jac}\, C/K$ has good reduction, but the converse does not hold when $g \geq 2$.

Suppose a genus 2 curve C/K has a semistable model with special fibre $\mathcal{C}_k$ consisting of two elliptic curves joined by a chain of $\mathbb{P}^1$'s, then

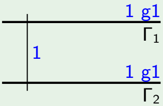
$$\mathcal{J}_k^0 \simeq E_1 \times E_2,$$

so the Jacobian has good reduction even though C does not.

In this case, $V_\ell J \simeq V_\ell \mathcal{J}_k^0 \simeq V_\ell E_1 \oplus V_\ell E_2$.

Example

$C : y^2 = (x^3 + 5^{18})(x^3 + 5^6)/\mathbb{Q}_5$. Special fibre of a semistable model for C is



Decomposition of the unramified part

Let C/K be a hyperelliptic curve with semistable reduction, $J = \mathrm{Jac}\, C$. Fix a semistable model $\mathcal{C}/\mathcal{O}_K$ for C, and let $\mathcal{C}_{\bar{k}}$ be its special fibre base changed to $\overline{k}$. Let $\mathcal{J}$ be the set of irreducible components of $\mathcal{C}_{\bar{k}}$.

Dual graph

The *dual graph* Υ of $\mathcal{C}_{\bar{k}}$ has vertex set $\mathcal{J}$. Two vertices are joined by one edge for each singular point lying on both of the corresponding components.

Normalisation

The normalisation $\widetilde{\mathcal{C}_{\bar{k}}}$ of $\mathcal{C}_{\bar{k}}$ is the disjoint union of the normalisations of the individual components. The morphism $\pi : \widetilde{\mathcal{C}_{\bar{k}}} \to \mathcal{C}_{\bar{k}}$ is an isomorphism away from singular parts.

Theorem: We have an exact sequence

$$0 \to H^1(\Upsilon, \mathbb{Z}) \otimes \mathbb{Z}_\ell(1) \to T_\ell \,\mathrm{Pic}^0_{\mathcal{C}_{\bar{k}}/\bar{k}} \to \prod_{\Gamma \in \mathcal{J}} T_\ell \,\mathrm{Jac}\, \widetilde{\Gamma} \to 0.$$

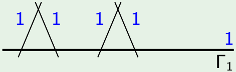
Corollary

We have a short exact sequence of G_k–modules

$$0 \longrightarrow H^1(\Upsilon, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell(1) \longrightarrow T_\ell(J)^{I_K} \longrightarrow \bigoplus_{\Gamma \,\in\, G_k\text{-orbits on } \mathcal{J}} \mathrm{Ind}_{\mathrm{Stab}(\Gamma)}^{G_k} T_\ell\big(\mathrm{Jac}(\widetilde{\Gamma})\big) \longrightarrow 0.$$

Example

Consider $C : y^2 = (x^2 - 7^3)((x-1)^2 - 7^3)(x^2+2)/\mathbb{Q}_7$. This curve has semistable reduction and the special fibre $\mathcal{C}_{\mathbb{F}_7}$ of its minimal regular model looks as follows.



The normalization $\widetilde{\mathcal{C}_{\mathbb{F}_7}}$ has $\mathrm{Pic}^0_{\widetilde{\mathcal{C}_{\mathbb{F}_7}}/\mathbb{F}_7} = 0$, and $H^1(\Upsilon, \mathbb{Z})$ is 2-dimensional, with Frobenius acting on it by $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Decomposition of $V_\ell J^*$

Now look at $V_\ell J^*$ (ok, I mean $H^1_{\text{ét}}(C_{\overline{K}}, \mathbb{Q}_\ell)$) as a G_K-representation. There exists a decomposition into *abelian* and *toric* parts

$$V_\ell J^* = H^1_{\text{ab}} \oplus (H^1_{\text{tor}} \otimes \text{sp}(2)),$$

where sp(2) is the *special representation* with

$$\text{sp}(2)(\sigma) = \begin{pmatrix} 1 & t_\ell(\sigma) \\ 0 & 1 \end{pmatrix} \text{ for } \sigma \in I_K \text{ and } \text{sp}(2)(\mathrm{Frob}) = \begin{pmatrix} 1 & 0 \\ 0 & q^{-1} \end{pmatrix}.$$

The representation H^1_{ab} has finite image of inertia, and $H^1_{\text{tor}} : G_K \to \mathrm{GL}_r(\mathbb{Z})$ for some $0 \le r \le \dim J$.

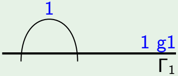
In the case of semistable reduction,

$$\begin{aligned} H^1_{\text{tor}} &= H^1(\Upsilon, \mathbb{Z}), \\ (H^1_{\text{ab}})^* &= \bigoplus_{\Gamma \,\in\, G_K\text{-orbits on } \mathcal{J}} \mathrm{Ind}^{G_k}_{\mathrm{Stab}(\Gamma)} T_\ell(\mathrm{Jac}(\widetilde{\Gamma})). \end{aligned}$$

Abelian and toric parts

Example

Consider $C : y^2 = (x^3+1)((x-1)^2+7^2)/\mathbb{Q}_7$. This curve has semistable reduction and the special fibre $\mathcal{C}_{\mathbb{F}_7}$ of its minimal regular model looks as follows



In this case, $\mathrm{Pic}^0_{\widetilde{\mathcal{C}_{\mathbb{F}_7}}/\mathbb{F}_7}$ is an elliptic curve, and $H^1(\Upsilon, \mathbb{Z})$ is one-dimensional, so $(T_\ell \operatorname{Jac} C)^{I_K}$ is 3-dimensional.

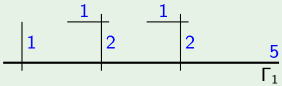
Inertia acts on $V_\ell J^*$ by $\begin{pmatrix} 1 & * & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, and Frobenius acts by $\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -7^{-1} & 0 & 0 \\ 0 & 0 & \alpha & 0 \\ 0 & 0 & 0 & \beta \end{pmatrix}$.

Non-semistable

If C/K has non-semistable reduction, then one can try to compute the Galois representation by finding some extension such that C/F is semistable.

Example

Let $C : y^2 = x^5 + 7^2/\mathbb{Q}_7$. This attains good reduction over the extension $F = \mathbb{Q}_7(\sqrt[5]{7})$. The special fibre of a minimal regular model for $C/\mathbb{Q}_7$ looks like



Thus $T_\ell J^{I_K} = 0$, and $T_\ell J^{I_F} = T_\ell J$, so I_K acts through the $\mathrm{Gal}(F \cdot K^{\mathrm{nr}}/K^{\mathrm{nr}})$-quotient with eigenvalues primitive fifth roots of unity.

The End