

le module de Tate

E/K courbe elliptique

$m \geq 2$ un entier premier à $p = \text{car}(K)$

si la caractéristique de K est > 0

Rappel: $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$

le groupe de Galois $\text{Gal}(\bar{K}/K)$ agit sur $E[m]$ car si $[m]P = 0$, alors

$$[m]\sigma(P) = \sigma([m]P) = \sigma(0) = 0$$

on a donc une représentation

$$\text{Gal}(\bar{K}/K) \rightarrow \text{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$$

↑
chacun d'une
base

Il est en général plus commode de travailler avec des représentations à coefficients dans un corps de caractéristique zéro.

Définition: Soit l un nombre premier.

Les entiers l -adiques $\mathbb{Z}_l$ sont

$$\mathbb{Z}_l = \varprojlim_n \mathbb{Z}/l^n\mathbb{Z}$$

par les applications de transition

$$\dots \rightarrow \mathbb{Z}/l^{n+1}\mathbb{Z} \xrightarrow{\pi_{n+1}} \mathbb{Z}/l^n\mathbb{Z} \rightarrow \dots$$

associées aux inclusions $\ell^{n+1}\mathbb{Z} \subset \ell^n\mathbb{Z}$.

Les éléments de $\mathbb{T}_\ell$ sont donc des suites

$$X = (X_1, X_2, X_3, \dots) \text{ avec } X_n \in \mathbb{Z}/\ell^n\mathbb{Z}$$

$$\pi_n(X_n) = X_{n-1}$$

Pour la courbe elliptique E , on peut considérer le système

$$\dots \rightarrow E[\ell^n] \xrightarrow{[\ell]} E[\ell^{n-1}] \rightarrow \dots$$

si $P \in E[\ell^n]$, alors

$$[\ell^{n-1}]([\ell]P) = 0,$$

$$\text{donc } [\ell]P \in E[\ell^{n-1}]$$

Définition. Le module de Tate ℓ -adique de E est la limite projective

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

Un élément de $T_\ell(E)$ est une suite $(P_n)_n$

de points de torsion $P_n \in E[\ell^n]$ avec $[\ell]P_n = P_{n-1}$.

C'est un $\mathbb{T}_\ell$ -module

$$T_\ell(E) \simeq \mathbb{T}_\ell \times \mathbb{T}_\ell$$

muni d'une représentation

$$\text{Gal}(\bar{K}/K) \rightarrow \text{Aut}(T_\ell(E)) \subset GL_2(\mathbb{Q}_\ell).$$

Remarque: si $l = p = \text{car}(k)$, alors la même définition donne $T_p(E) \simeq \mathbb{Z}_p$ ou $\{0\}$ en fonction que la courbe soit ordinaire ou supersingulière.

La structure de $T_\ell(E)$ est fonctorielle:

si $\varphi: E_1 \rightarrow E_2$ est une isogénie, alors

$$\varphi \circ [l^n]_{E_1} = [l^n]_{E_2} \circ \varphi$$

et donc φ envoie $E_1[l^n]$ dans $E_2[l^n]$.

Par passage à la limite, on trouve

$$\varphi_\ell: T_\ell(E_1) \rightarrow T_\ell(E_2)$$

Théorème: L'application $\mathbb{Z}_\ell$ -linéaire

$$\begin{aligned} \mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell &\rightarrow \mathrm{Hom}(T_\ell(E_1), T_\ell(E_2)) \\ \varphi &\longmapsto \varphi_\ell \end{aligned}$$

est injective.

Preuve: Étape 1: Soit $M \subset \mathrm{Hom}(E_1, E_2)$ un sous-groupe finiment engendré. Soit

$$M^{\mathrm{div}} = \left\{ \varphi \in \mathrm{Hom}(E_1, E_2) \mid \exists m \geq 1 \text{ avec } [m] \circ \varphi \in M \right\}$$

Claim: M^{div} est finiment engendré

Preuve: on étend l'application degré à $M \otimes \mathbb{R}$ et on regarde le noyau ouvert de 0 donné par

$$U = \{ \varphi \in M \otimes \mathbb{R} \mid \deg < 1 \}$$

Alors on a à l'intérieur de $M \otimes \mathbb{R}$ (ce qui est possible car $\mathrm{Hom}(E_1, E_2)$ n'a pas de torsion), M^{div} satisfait $M^{\mathrm{div}} \cap U = \{0\}$ car une isogénie a degré ≥ 1 . Cela veut dire que M^{div} est discret dans l'espace vectoriel réel de

division fini $M \otimes \mathbb{K}$, du fini est évident. $\square$

Étape 2: Soit $\varphi = \sum_{i=1}^n \alpha_i \varphi_i \in \text{Hom}(E_1, E_2) \otimes \mathbb{K}_\ell$.

Soit M le sous-groupe engendré par $\varphi_1, \dots, \varphi_n$. Par ce qui précède, M^{div} admet une base $\psi_1, \dots, \psi_s$ et on écrit

$$\varphi = \alpha_1 \psi_1 + \dots + \alpha_s \psi_s \quad \alpha_i \in \mathbb{K}_\ell$$

Supposons que $\varphi_\ell = 0$ et choisissons, pour n fixé, des entiers $a_1, \dots, a_s$ tels que $a_i \equiv \alpha_i \pmod{\ell^n}$.

Soit $\psi = a_1 \psi_1 + \dots + a_s \psi_s \in M^{\text{div}}$. Alors

ψ admet l'application nulle sur $E_1[\ell^n]$.

Lemme. Soient $\varphi: E_1 \rightarrow E_2$ et $\psi: E_1 \rightarrow E_3$ isogènes avec φ séparable. Si $\ker \varphi \subset \ker \psi$, alors il existe une isogénie $\lambda: E_2 \rightarrow E_3$ telle que $\psi = \lambda \circ \varphi$.

Preuve: Si φ est séparable, alors $\bar{\mathbb{K}}(E_1)/\varphi^* \bar{\mathbb{K}}(E_2)$ est Galois et $\ker \varphi \cong \text{Gal}(\bar{\mathbb{K}}(E_1)/\varphi^* \bar{\mathbb{K}}(E_2))$.

$$\ker \psi \cong \text{Aut}(\bar{\mathbb{K}}(E_1)/\psi^* \bar{\mathbb{K}}(E_3))$$

L'inclusion $\ker \varphi \subset \ker \psi$ implique alors

$$\psi^* \bar{\mathbb{K}}(E_3) \subset \varphi^* \bar{\mathbb{K}}(E_2) \subset \bar{\mathbb{K}}(E_1),$$

d'où $\lambda: E_2 \rightarrow E_3$ avec $\psi^* \bar{K}(E_3) = \varphi^* \lambda^* \bar{K}(E_3)$,
 donc $\lambda \circ \varphi = \psi$ par la correspondance entre courbes
 et corps de fonctions. C'est une isogénie car
 $\lambda(0) = \lambda(\varphi(0)) = \psi(0) = 0$ □

Par le lemme, il existe $\lambda \in \text{Hom}(E_1, E_2)$
 telle que $\psi = [\ell^n] \circ \lambda$, c'est-à-dire $\lambda \in M^{\text{div}}$.
 On écrit $\lambda = b_1 \varphi_1 + \dots + b_s \varphi_s$ et on trouve

$$a_i = \ell^n b_i \quad \text{pour } i = 1, \dots, s$$

d'où $a_i \equiv 0 \pmod{\ell^n}$. Comme n est arbitraire,
 tous les a_i sont nuls, c'est-à-dire $\varphi = 0$ □

Remarque: si K est un corps fini ou un
 corps de nombres, cette application est un
 isomorphisme (conjecture de Tate démontrée
 par Tate pour les corps finis et Faltings
 pour les corps de nombres).

