

① Le module de Tate d'une courbe elliptique

Soit E une courbe elliptique définie sur un corps parfait K . Soit $m \geq 2$ un entier premier à $p = \text{car}(K)$ si la caractéristique de K est positive. Alors

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

le groupe de Galois $\text{Gal}(\bar{K}/K)$ agit sur les points de torsion $E[m]$. En effet, si $P \in E(\bar{K})$ satisfait à $[m]P = 0$, alors

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

↑
[m] défini sur K

On a donc une représentation

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

↑
choix d'une base

Il est en général plus simple de considérer des représentations à valeurs dans un corps de caractéristique zéro.

Définition. Soit l un nombre premier. Les entiers l -adiques $\mathbb{Z}_l$ sont la limite projective

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

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 $l^{n+1} \mathbb{Z} \subset l^n \mathbb{Z}$.

Un élément de $\mathbb{Z}_l$ est donc une suite

$$x = (x_1, x_2, \dots) \text{ avec } x_n \in \mathbb{Z}/l^n \mathbb{Z}$$

$$\pi_n(x_n) = x_{n-1}$$

Pour la courbe elliptique E , on peut considérer le système projectif

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

si $P \in E[l^n]$, alors
 $[l^{n-1}]([l]P) = [l^n]P = 0$,
 donc $[l]P \in E[l^{n-1}]$

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

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

Un élément de $T_l E$ est une suite $(P_n)_n$ de points de torsion $P_n \in E[l^n]$ tels que

$$[l]P_n = P_{n-1}$$

le module de Tate $T_l E$ est un $\mathbb{Z}_l$ -module libre de rang 2, muni d'une représentation

$$\text{Gal}(\bar{K}/K) \rightarrow \text{Aut}(T_l E) \subset GL_2(\mathbb{Q}_l)$$

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

La construction de $T_l E$ 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

$$\varphi_\ell: T_\ell E_1 \longrightarrow T_\ell E_2$$

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

$$\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}(T_\ell E_1, T_\ell E_2)$$

$$\varphi \longmapsto \varphi_\ell$$

est injective.

Démonstration.

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

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

on affirme que M^{div} est encore finiment engendré. Sur $\mathrm{Hom}(E_1, E_2)$ on a l'application degré

$$\deg: \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{N}$$

qui est une forme quadratique définie positive, c'est-à-dire satisfait à

$$\deg(\varphi) \geq 0 \quad \text{et} \quad \deg(\varphi) = 0 \iff \varphi = 0.$$

(3)

La bilinéarité de l'application

$$\deg(\varphi + \psi) = \deg(\varphi) + \deg(\psi)$$

se démontre en utilisant l'isomorphisme

$$\begin{aligned} \mathbb{Z} &\hookrightarrow \text{End}(E_1) \\ n &\longmapsto [n] \end{aligned}$$

pour calculer :

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

qui est bien $\mathbb{Z}$ -bilinéaire en (φ, ψ) .

on étend l'application degré à

$$\deg: M \otimes \mathbb{R} \longrightarrow \mathbb{R}$$

et on regarde le noyau ouvert de

$0 \in M \otimes \mathbb{R}$ donné par

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

Comme $\text{Hom}(E_1, E_2)$ n'a pas de torsion,

M^{dir} s'injecte dans $M \otimes \mathbb{R}$ et satisfait

$$M^{\text{dir}} \cap \mathcal{U} = \{0\}$$

car une isogène a degré ≥ 1 . Cela veut dire que M^{dir} est discret dans l'espace vectoriel de dimension finie $M \otimes \mathbb{R}$, donc finiment engendré.

- Étape 2: Soit $\varphi = \sum_{i=1}^n \alpha_i \varphi_i$ un élément de $\text{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell$. Soit M le sous-groupe engendré par $\varphi_1, \dots, \varphi_n$. Alors M^{dir} admet une base $\psi_1, \dots, \psi_s$ dans laquelle φ s'écrit

$$\varphi = \beta_1 \psi_1 + \dots + \beta_s \psi_s \quad \beta_i \in \mathbb{Z}_\ell$$

Supposons que $\boxed{\varphi_1 = 0}$. À n fixé, choisissons des entiers $b_1, \dots, b_n$ tels que

$$b_i \equiv \beta_i \pmod{\ell^n}$$

Soit $\psi = b_1 \psi_1 + \dots + b_n \psi_n \in M^{\text{dir}}$.

Alors ψ induit l'application nulle

sur les points de torsion $E_1[l^n]$.

lemme. Soient $\varphi: E_1 \rightarrow E_2$ et $\psi: E_1 \rightarrow E_3$ des isogénies avec φ séparable. Si

$$\text{Ker } \varphi \subset \text{Ker } \psi$$

alors il existe une isogénie $\lambda: E_2 \rightarrow E_3$ telle que $\psi = \lambda \circ \varphi$.

Démonstration. Si φ est séparable, alors l'extension $\bar{K}(E_1)/\varphi^*\bar{K}(E_2)$ est galoisienne. On a:

$$\text{Ker } \varphi = \text{Gal}(\bar{K}(E_1)/\varphi^*\bar{K}(E_2))$$

$$\text{Ker } \psi = \text{Aut}(\bar{K}(E_1)/\psi^*\bar{K}(E_3))$$

L'inclusion $\text{Ker } \varphi \subset \text{Ker } \psi$ implique
alors $\psi^*\bar{K}(E_3) \subset \varphi^*\bar{K}(E_2) \subset \bar{K}(E_1)$,
d'où une factorisation

$$\begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_3 \\ & \searrow \varphi & \nearrow \lambda \\ & E_2 & \end{array}$$

De plus, $\lambda(0) = \lambda(\varphi(0)) = \psi(0) = 0$ et donc λ est une isogénie □

Appliqué à $\ker([l^n]) \subset \ker \Psi$, le lemme implique l'existence de $\lambda \in \text{Hom}(E_1, E_2)$ tel que $\Psi = [l^n] \circ \lambda$, c'est-à-dire $\lambda \in M^{\text{div}}$ on écrit

$$\lambda = c_1 \Psi_1 + \dots + c_s \Psi_s$$

et on trouve par comparaison avec

$$\Psi = b_1 \Psi_1 + \dots + b_s \Psi_s$$

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

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

Remarque: si K est un corps fini ou un corps de nombres, cette application est surjective aussi. C'est la conjecture de Tate démontrée par Tate pour les corps finis et par Faltings pour les corps de nombres.

② L'accouplement de Weil

E courbe elliptique définie sur K

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

Supposons qu'on sache déjà que la multiplication $[n]_E$ est une isogénie séparable de degré n^2 .

But: construire un accouplement

$$E[n] \times E[n] \longrightarrow \mu_n = \mu_n(K)$$

↑
racines n -ièmes
de l'unité

Rappel: $D = \sum n_p [P] \in \text{Div}(E)$ est le diviseur d'une fonction $f \in K(E)^\times$

$$\Leftrightarrow \begin{cases} \sum n_p = 0 & (\text{addition dans } \mathbb{Z}) \\ \sum [n_p](P) = 0 & (\text{addition dans } E(K)) \end{cases}$$

(En effet, l'application $E(K) \xrightarrow{\sim} \text{Pic}^0(E)$
 $P \longmapsto [P] - [O]$

est un isomorphisme de groupes.)

Soit $T \in E[m]$. Appliqué au diviseur $D = m[T] - m[0]$, l'opération montre l'existence de $f_T \in \bar{k}(E)^{\times}$ telle que

$$\operatorname{div}(f_T) = m[T] - m[0].$$

Soit $T' \in E(\bar{k})$ avec $[m]T' = T$. Alors

$$[m]^*([T] - [0]) = \sum_{R \in E[m]} ([T' + R] - [R])$$

$$\xrightarrow{\text{dans } \operatorname{Pic}^0(E)} = \sum_{R \in E[m]} ([T'] - [0])$$

$$\xrightarrow{|E[m]| = m^2} = m^2([T'] - [0])$$

$$\xrightarrow{[m^2]T' = [m]T = 0} = 0$$

Il existe donc $g_T \in \bar{k}(E)^{\times}$ telle que

$$\operatorname{div}(g_T) = [m]^*([T] - [0]).$$

Les fonctions f_T et g_T sont uniques à multiplication par un élément de $\bar{k}^{\times}$ près. On a :

$$\begin{aligned}
\operatorname{div}(g_T^m) &= m \operatorname{div}(g_T) \\
&= m [m]^* ([T] - [0]) \\
&= [m]^* (\underbrace{m [T] - m [0]}_{\operatorname{div} f_T}) \\
&= \operatorname{div}(f_T \circ [m])
\end{aligned}$$

Quitte à multiplier f_T par un scalaire, on peut donc supposer

$$g_T^m = f_T \circ [m]$$

Soit $S \in E[m]$. Pour tout $X \in E(K)$,

$$\begin{aligned}
g_T(X+S)^m &= f_T([m]X + [m]S) \\
&= f_T([m]X) \\
&= g_T(X)^m
\end{aligned}$$

et ces deux fonctions diffèrent donc par multiplication par une racine m -ième de l'unité.

Définition. Soit $e_m(S, T) \in \mu_m(\bar{\mathbb{K}})$
la seule racine m-ème de l'unité
telle que

$$e_m(S, T) = \frac{g_T(X+S)}{g_T(X)}$$

pour tout $X \in E(\bar{\mathbb{K}})$ tel que $g_T(X+S)$
et $g_T(X)$ sont définis et non nuls.
Cette racine ne dépend du choix de g_T .

Proposition. L'accomplissement de Weil

$$\begin{aligned} e_m : E[m] \times E[m] &\longrightarrow \mu_m \\ (S, T) &\longmapsto e_m(S, T) \end{aligned}$$

est bilinéaire, alterné, non dégénéré
et compatible à l'action de $\text{Gal}(\bar{\mathbb{K}}/\mathbb{K})$.

Démonstration:

1) Bilinéarité. Par rapport à la
première variable,

(7)

$$\begin{aligned}
e_m(S_1 + S_2, T) &= \frac{g_T(X + S_1 + S_2)}{g_T(X)} \\
&= \frac{g_T(X + S_1 + S_2)}{g_T(X + S_1)} \cdot \frac{g_T(X + S_1)}{g_T(X)} \\
&= e_m(S_1, T) \cdot e_m(S_2, T)
\end{aligned}$$

Par rapport à la deuxième variable,

$$\begin{aligned}
&\text{div}(g_{T_1}^{-1} g_{T_2}^{-1} g_{T_1+T_2}) \\
&= [m]^* (-[T_1] - [T_2] + [T_1 + T_2] + [0]) \\
&= [m]^* \text{div}(h) \\
&= \text{div}(h \circ [m])
\end{aligned}$$

pour un certain $h \in \bar{k}(E)^x$ par le même raisonnement pour qu'un diviseur de degré 0 soit le diviseur d'une fonction. Autant à remplacer h par un multiple, on peut donc choisir

$$g_{T_1+T_2} = g_{T_1} g_{T_2} (h \circ [m])$$

et dans ce cas

$$\begin{aligned}
 e_m(S, T_1 + T_2) &= \frac{g_{T_1 + T_2}(X + S)}{g_{T_1 + T_2}(X)} \\
 &= \frac{g_{T_1}(X + S) g_{T_2}(X + S) h(\cancel{[m]X} + [m]S)}{g_{T_1}(X) g_{T_2}(X) h(\cancel{[m]X})} \\
 &= e_m(S, T_1) e_m(S, T_2).
 \end{aligned}$$

2) Alterné. Soit $z_p: E \rightarrow E$
 $X \mapsto X + P$

l'application de translation par P . Alors:

$$\begin{aligned}
 \text{div}(g_T \circ z_p) &= [z_p]^* \text{div}(g_T) \\
 &= [z_p]^* [m]^* ([T] - [O]) \\
 &= [m \circ z_p]^* ([T] - [O]) \\
 &= [z_{mP} \circ m]^* ([T] - [O]) \\
 &= [m]^* [z_{mP}]^* ([T] - [O]) \\
 &= [m]^* ([T - mP] - [-mP])
 \end{aligned}$$

Soit $T' \in E(\bar{k})$ avec $[m]T' = T$. Alors:

⑧

$$\operatorname{div} \left(\prod_{i=0}^{m-1} g_T \circ z_{[i]T'} \right) = [m]^* \left(\sum_{i=0}^{m-1} [(1-i)T] - [-iT] \right) = 0,$$

ce qui implique que la fonction

$$\prod_{i=0}^{m-1} g_T \circ z_{[i]T'} \text{ est constante.}$$

En particulier,

$$\prod_{i=0}^{m-1} g_T (X + [i]T') = \prod_{i=0}^{m-1} g_T (X + [i+1]T')$$

évaluation en X évaluation en $X+T'$

$$\Rightarrow g_T(X) = g_T(X + [m]T') = g_T(X+T)$$

$$\text{d'où enfin } e_m(T, T) = \frac{g_T(X+T)}{g_T(X)} = 1$$

3) Non dégénérée Supposons que $e_m(S, T) = 1$

pour tout $S \in E[m]$. Alors

$$g_T(X+S) = g_T(X) \text{ pour tout } S \in E[m]$$

et donc il existe $h \in \mathbb{K}(E)^X$ telle que

$$g_T = h \circ [m]$$

Comme $(h \circ [m])^m = g_T^m = f_T \circ [m]$, on a $h^m = f_T$, d'où

$$m \operatorname{div}(h) = \operatorname{div}(f_T) = m([T] - [O]),$$

c'est-à-dire $\operatorname{div}(h) = [T] - [O]$, mais alors $T = O_E$ par l'isomorphisme entre $E(\bar{k})$ et $\operatorname{Pic}^0(E)$.

4) Invariance à l'action de $\operatorname{Gal}(\bar{k}/k)$

Soient $\sigma \in \operatorname{Gal}(\bar{k}/k)$ et f_T, g_T comme ci-dessus. Alors $\sigma(f_T)$ et $\sigma(g_T)$ sont des fonctions pour $\sigma(T)$ et

$$\begin{aligned} e_m(\sigma(S), \sigma(T)) &= \frac{g_{\sigma(T)}(\sigma(X) + \sigma(S))}{g_{\sigma(T)}(\sigma(X))} \\ &= \sigma \left(\frac{g_T(X + S)}{g_T(X)} \right) \\ &= \sigma(e_m(S, T)) \end{aligned}$$

□