

L'accouplement de Weil

E/K courbe elliptique

$n \geq 2$ entier premier à $p = \text{car}(K)$ si celle-ci est > 0

Supposons que l'on sache déjà que $[m]_E$ est une isogénie (séparable) de degré m^2

But: construire un accouplement

$$E[m] \times E[m] \longrightarrow \mu_m = \mu_m(\bar{K})$$

racines m -èmes
de l'unité

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

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

↑ addition dans
la courbe elliptique $E(\bar{K})$

(En effet, l'application $E(\bar{K}) \xrightarrow{\sim} \text{Pic}^0(E)$
 $P \mapsto [P] - [O]$
est un isomorphisme de groupes)

Soit $T \in E[m]$. Il existe $f_T \in \bar{K}(E)^*$ telle que

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

Soit $T' \in E(\bar{K})$ tel que $[m]T' = T$. Alors:

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

$$\sim \sum_{R \in E[m]} ([T'] - [0])$$

$$|E[m]| = m^2 \rightarrow \sim m^2 ([T'] - [0])$$

$$\sim 0 \quad \text{car } [m^2]T' = 0$$

donc il existe $g_T \in \bar{K}(E)^*$ telle que

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

(les fonctions f_T et g_T sont linéaires à multiplication par un élément de $\bar{K}^*$ près)

Composons:

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

Qu'il s'agit de multiplier f par un scalaire on peut donc supposer $\boxed{g_T^m = f_T \circ [m]}$

Soit $S \in E[m]$. Pour tout $X \in E(\bar{k})$,

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

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

Définition: Soit $e_m(S, T) \in \mu_m(\bar{k})$ la seule racine m -ième de l'unité telle que

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

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

Proposition: L'accomplissement de Weil

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

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

Démonstration: 1) Bilinéarité $e_m(S_1 + S_2, T)$
 $= e_m(S_1, T) e_m(S_2, T)$

$$e_m(S, T_1 + T_2) = e_m(S, T_1) e_m(S, T_2)$$

Dans la première variable:

$$e_m(S_1 + S_2, T) = \frac{g_T(X + S_1 + S_2)}{g_T(X)} \frac{g_T(X + S_1)}{g_T(X + S_1)}$$

$$= e_m(S_1, T) \cdot e_m(S_2, T)$$

Dans la deuxième variable:

$$\operatorname{div} \left(g_{T_1}^{-1} g_{T_2}^{-1} g_{T_1 + T_2} \right) = [m]^* \left([T_1] [T_2] \right. \\ \left. + [T_1 + T_2] + [0] \right)$$

$$= [m]^* \operatorname{div}(h)$$

$$= \operatorname{div}(h \circ [m])$$

pour un certain $h \in \bar{K}(E)^*$ car $-[T_1] [T_2] + [T_1 + T_2] + [0]$ est nul dans $\operatorname{Pic}^0(E)$.

Autre à vérifier h par un multiple, on peut donc prendre $g_{T_1 + T_2} = g_{T_1} g_{T_2} (h \circ [m])$

$$e_m(S, T_1 + T_2) = \frac{g_{T_1 + T_2}(X + S)}{g_{T_1 + T_2}(X)}$$

$$= \frac{g_{T_1}(X+S) g_{T_2}(X+S) h(\cancel{[m]X} + [m]S)}{g_{T_1}(X) g_{T_2}(X) h(\cancel{[m]X})} \quad (3)$$

$$= e_m(S, T_1) e_m(S, T_2)$$

2) Alterné: $e_m(T, T) = 1$

Soit $z_p: E \rightarrow E$ l'application de translation par p .
 $X \mapsto X + p$

Alors

$$\begin{aligned} \operatorname{div}(g_T \circ z_p) &= z_p^* [m]^* ([T] - [0]) \\ &= ([m] \circ z_p)^* ([T] - [0]) \\ &= (z_{mp} \circ [m])^* ([T] - [0]) \\ &= [m]^* z_{mp}^* ([T] - [0]) \\ &= [m]^* ([T - mp] - [mp]) \end{aligned}$$

Soit $T' \in E(\bar{K})$ tel que $[m]T' = T$. Alors

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

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

En particulier :

$$\prod_{i=0}^{m-1} g_T(X + [i]T') = \prod_{i=0}^{m-1} g(X + [i+1]T') \quad \begin{matrix} \uparrow & \uparrow \\ \text{évaluation en } X & \text{évaluation en } X+T' \end{matrix}$$

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

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

(NB: en écrivait

$$1 = e_m(S+S, T+T) = e_m(S, S) e_m(S, T) e_m(T, S) e_m(T, T) \quad \begin{matrix} 1 & & 1 \end{matrix}$$

on trouve $e_m(S, T) = e_m(T, S)^{-1}$

3) Non dégénéré : si $e_m(S, T) = 1$ pour tout $S \in E[m]$, alors $T = 0$

si $e_m(S, T) = 1$ pour tout $S \in E[m]$, alors
 $g_T(X+S) = g_T(X)$ pour tout $S \in E[m]$

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

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

$$\text{car } (h \circ [m])^m = g_T^m = f_T \circ [m], \text{ on a}$$

(4)

$$h = f, \text{ d'où } m \operatorname{div}(h) = \operatorname{div}(f) \\ = m([\bar{1}] - [\bar{0}])$$

c'est-à-dire $\operatorname{div}(h) = [\bar{1}] - [\bar{0}]$, mais alors $T = \mathcal{O}_{\bar{E}}$ par l'isomorphisme $E(\bar{K}) \simeq \operatorname{Pic}(E)$.

4) Incompatibilité avec l'action de $\operatorname{Gal}(\bar{K}/K)$

Soit $\sigma \in \operatorname{Gal}(\bar{K}/K)$. Si f_T, g_T sont des fonctions pour T comme ci-dessus, alors $\sigma(f_T)$ et $\sigma(g_T)$ sont des fonctions pour $\sigma(T)$:

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

$$= \sigma\left(\frac{g_T(X+S)}{g_T(X)}\right)$$

$$= \sigma(e_m(S, T)) \quad \square$$

Proposition: Soit $\varphi: E_1 \rightarrow E_2$ une isogénie.

Pour tous $S \in E_1[m]$ et $T \in E_2[m]$, on a l'égalité:

$$e_m(S, \hat{\varphi}(T)) = e_m(\varphi(S), T)$$

c'est-à-dire φ et $\hat{\varphi}$ sont adjoints par rapport à l'accouplement de Weil.

Preuve: par définition,

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

où $f_T \circ [m] = g_T^m$ et $\text{div}(f) = m[T] - m[0]$.

Rappelons aussi que si

$$\varphi^*([T] - [0]) = \sum n_p \cdot p \in \text{Div}(E_1)$$

alors $\hat{\varphi}(T) = \sum [n_p](p)$. Il existe donc une fonction $h \in K(E)^*$ telle que

$$\varphi^*([T] - [0]) = [\hat{\varphi}(T)] - [0_{E_1}] + \text{div}(h)$$

Elle satisfait à

$$\begin{aligned} \text{div}\left(\frac{f_T \circ \varphi}{h^m}\right) &= \varphi^* \text{div}(f_T) - m \text{div}(h) \\ &= m[\hat{\varphi}(T)] - m[0_{E_1}] \end{aligned}$$

$$\left(\frac{g_T \circ \varphi}{h \circ [m]}\right)^m = \frac{f_T \circ [m] \circ \varphi}{(h \circ [m])^m} = \left(\frac{f \circ \varphi}{h^m}\right) \circ [m]$$

et donc par définition de l'accomplissement

$$e_m(S, \hat{\varphi}(T)) = \frac{\left(\frac{g_T \circ \varphi}{h \circ [m]}\right)(X + S)}{\left(\frac{g_T \circ \varphi}{h \circ [m]}\right)(X)}$$

(5)

$$= \frac{g_T(\varphi(X) + \varphi(S))}{g_T(\varphi(X))} \frac{h([m]X)}{h([m]X + [m]S)}$$

$$= e_m(\varphi(S), T)$$

comme on voulait montrer. $\square$

Soit l un nombre premier différent de $\text{car}(k)$.
 Pour chaque entier $n \geq 1$, on a l'application

$$\begin{array}{ccc} e_{l^n} : E[l^n] \times E[l^n] & \longrightarrow & \mu_{l^n} \\ \uparrow [l] & & \uparrow [l] \\ e_{l^{n+1}} : E[l^{n+1}] \times E[l^{n+1}] & \longrightarrow & \mu_{l^{n+1}} \end{array}$$

lemme: Si $S \in E[mm']$ et $T \in E[lm] \subset E[mm']$,

$$e_{mm'}(S, T) = e_m([m']S, T)$$

preuve: pour f_T et g_T comme d'habitude

$$\text{div}(f^{m'}) = mm'[T] - mm'[0]$$

$$(g_T \circ [m'])^{mm'} = (f_T \circ [mm'])^{m'},$$

d'où en utilisant les définitions:

$$e_{mm'}(S, T) = \frac{(g_T \circ [m'])(X+S)}{(g_T \circ [m'])(X)} = \frac{g_T(Y+[m']S)}{g_T(Y)}$$

avec $Y = [m']X$.

$$= e_m([m']S, T) \quad \square$$

Lemma: pour tous $S, T \in E[l^{n+1}]$

$$\begin{aligned} e_{l^{n+1}}(S, T) & \stackrel{e}{=} e_{l^{n+1}}(S, \underbrace{[l]T}_{E[l^{n+1}]}) \\ & \quad \uparrow \text{bijectivité} \\ & = e_{l^n}([l]S, [l]T) \end{aligned}$$

et on voit ainsi que les (e_{l^n}) induisent :

$$e: T_l(E) \times T_l(E) \rightarrow T_l(\mu)$$

Théorème: Il existe un accouplement bilinéaire, alterné, non dégénéré et complet équivalent

$$e: T_l(E) \times T_l(E) \rightarrow T_l(\mu)$$

pour lequel φ et $\hat{\varphi}$ sont adjoints l'un de l'autre.

(Ici, $T_l(\mu) = \varprojlim_n \mu_{l^n}$ par rapport aux applications de transition

$$\dots \rightarrow \mu_{l^{n+1}} \xrightarrow{(\cdot)^l} \mu_{l^n} \rightarrow \dots)$$

Preuve de $\widehat{\varphi + \psi} = \widehat{\varphi} + \widehat{\psi}$ $\varphi, \psi: E_1 \rightarrow E_2$

Si $\text{car}(K) \neq 2$, on sait déjà que
le degré de $[2^n]_E$ est $(2^n)^2$ pour tout n et

$E \setminus \{P, -P\}$ on dispose donc de l'ensemble de Weil

$$\times \downarrow \text{IP}^1 \quad e_{2^n}: E[2^n] \times E[2^n] \rightarrow \mathbb{A}_{2^n}^1$$

4 points
de torsion
pour
l'homomorphisme

$$|E[2]| = 4$$

+ séparable

pour tous $T \in E_2[2^n], S \in E_1[2^n]$:

$$e_{2^n}(S, (\widehat{\varphi + \psi})(T)) - \widehat{\varphi}(T) - \widehat{\psi}(T)$$

$$= e_{2^n}(S, \widehat{\varphi + \psi}(T)) e_{2^n}(S, \widehat{\varphi}(T))^{-1} e_{2^n}(S, \widehat{\psi}(T))^{-1}$$

$$= e_{2^n}((\varphi + \psi)(S), T) e_{2^n}(\varphi(S), T)^{-1} e_{2^n}(\psi(S), T)^{-1}$$

$$= e_{2^n}(\underbrace{(\varphi + \psi)(S) - \varphi(S) - \psi(S)}_0, T)$$

$$= 1$$

et comme l'ensemble est non dégénéré,
on en déduit

$$(\widehat{\varphi + \psi})(T) = \widehat{\varphi}(T) + \widehat{\psi}(T)$$

pour tout $T \in \bigcup_n E[2^n] \subset E(\bar{K})$, donc

pour tout $T \in E(\bar{K})$ par densité de Zariski.

En car $(k) = 2$, il faut d'abord montrer
que $[3]_E$ est de degré 9, puis on fait
la même preuve □