

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

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

Autrement dit, φ et $\hat{\varphi}$ sont adjoints par rapport à l'accouplement de Weil.

Démonstration. Par définition,

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

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

Rappelons aussi que si

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

alors $\hat{\varphi}(T) = \sum [n_p](P)$. Il existe donc une fonction $h \in \bar{k}(E_1)^*$ telle que

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

Elle satisfait à

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

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

et donc par définition de l'assemblant

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

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

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

comme on voulait le démontrer □

Soit l un nombre premier différent de la caractéristique de k . Pour chaque entier $n \geq 1$, on a un diagramme

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

lemme. Si $S \in E[m, m']$ et $T \in E[m] \subset E[m, m']$,
 alors $e_{mm'}(S, T) = e_m([m']S, T)$.

Démonstration. Les fonctions f_T et g_T satis-
 font à $\text{div}(f_T^{m'}) = mm'[T] - mm'[0]$
 $(g_T \circ [m'])^{mm'} = (f_T \circ [mm'])^{m'}$,

d'où en reportant les définitions

$$\begin{aligned} e_{mm'}(S, T) &= \frac{(g_T \circ [m'])(X+S)}{(g_T \circ [m'])(X)} \\ &= \frac{g_T(Y + [m']S)}{g_T(Y)} \\ &\quad \text{avec } Y = [m']X \quad \nearrow \\ &= e_m([m']S, T) \quad \square \end{aligned}$$

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

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

et on voit aussi que les $(\ell_{\ell^n})_n$ induisent un accouplement

$$\ell: T_\ell E \times T_\ell E \longrightarrow T_\ell \mu = \varprojlim_n \mu_{\ell^n}$$

↑
applications de
transition
 $\dots \rightarrow \mu_{\ell^{n+1}} \xrightarrow{\ell} \mu_{\ell^n} \rightarrow \dots$

Théorème: L'accouplement ℓ est bilinéaire, alterné, non dégénéré, équivariant pour l'action de $\text{Gal}(\bar{k}/k)$ et φ et $\hat{\varphi}$ sont adjoint l'un pour l'autre par rapport à cet accouplement.

Théorème. Soient $\varphi, \psi: E_1 \rightarrow E_2$ des isogénies. Alors $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.

Démonstration. Si $\text{car } k \neq 2$, on sait déjà que le degré de $[2^n]_{E_1}$ est $(2^n)^2$ pour tout n et on dispose donc de

l'accomplissement de Weil

$$e_{2^n} : E_1[2^n] \times E_1[2^n] \rightarrow \mu_{2^n}$$

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

$$\begin{aligned} & e_{2^n}(S, \widehat{(\varphi + \psi)}(T)) = \widehat{\varphi}(T) - \widehat{\psi}(T) \\ &= e_{2^n}(S, \widehat{(\varphi + \psi)}(T)) e_{2^n}(S, \widehat{\varphi}(T))^{-1} e_{2^n}(S, \widehat{\psi}(T))^{-1} \\ &= e_{2^n}((\varphi + \psi)(S), T) e_{2^n}(\varphi(S), T)^{-1} e_{2^n}(\psi(S), T)^{-1} \\ &= e_{2^n}(\underbrace{(\varphi + \psi)(S) - \varphi(S) - \psi(S)}_0, T) \\ &= 1 \end{aligned}$$

et comme l'accomplissement est un dégréé,
on en déduit

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

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

pour tout T par densité de Zariski

Remarque: En cas $k=2$, on démontre d'abord
que $[3]$ est de degré 9. □

③ les conjectures de Weil pour les courbes elliptiques sur les corps finis

p nombre premier

q puissance de p

K corps fini à q éléments

E courbe elliptique sur K

But: compter le nombre de K -points de E

$$= 1 + \text{nombre de } (x, y) \in K^2$$

point à l'infini ↗
solution de l'équation de Weierstrass

La borne triviale est $\leq 2q + 1$ (pour chaque valeur de x , au plus deux solutions de l'équation de Weierstrass).

Mais la probabilité qu'une équation quadratique ait une solution dans K est $1/2$, donc l'ordre de grandeur attendu est plutôt $q + 1$.

Théorème (Borne de Hasse)

$$\left| |E(k)| - q - 1 \right| \leq 2\sqrt{q}$$

Démonstration: Considérons l'endomorphisme

de Frobenius $\varphi_q : E \rightarrow E$

$$(x, y) \mapsto (x^q, y^q)$$

Comme $\text{Gal}(\bar{k}/k) \cong \hat{\mathbb{Z}}$ avec générateur topologique l'endomorphisme $x \mapsto x^q$ sur k , un point $P \in E(\bar{k})$ appartient à $E(k)$ si et seulement si $\varphi_q(P) = P$, d'où

$$E(k) = \text{Ker}(\text{Id}_E - \varphi_q)$$

le morphisme $\text{Id}_E - \varphi_q : E \rightarrow E$
 $P \mapsto P - \varphi_q(P)$

est une isogénie car il envoie 0 sur 0 et qu'il est non constant. C'est une isogénie séparable car

$$\Omega_E \rightarrow \Omega_E$$

$$\omega \mapsto (\text{Id}_E - \varphi_q)^* \omega = \omega$$

n'est pas le morphisme nul. On a donc

$$|E(K)| = \deg(\text{Id}_E - \varphi_f).$$

Lemme: Soient A un groupe abélien et $d: A \rightarrow \mathbb{Z}$ une forme quadratique définie positive. Alors

$$|d(x+y) - d(x) - d(y)| \leq 2\sqrt{d(x)d(y)}$$

pour tous $x, y \in A$.

Démonstration: Posons

$$L(x, y) = d(x+y) - d(x) - d(y)$$

Comme d est définie positive,

$$0 \leq d(mx - ny) = m^2 d(x) + mn L(x, y) + n^2 d(y)$$

pour tous $m, n \in \mathbb{Z}$. En prenant

$$m = -L(x, y) \quad n = 2d(x)$$

on trouve

$$0 \leq d(x) (4d(x)d(y) - L(x, y)^2),$$

d'où le résultat □

Pour conclure la démonstration de la
 borne de Hasse, on applique le lemme
 à $\deg: \text{End}(E) \rightarrow \mathbb{Z}$ pour trouver:

$$\left| \underbrace{\deg(\text{Id} - \varphi_f)}_{|E(k)|} - \underbrace{\deg(\varphi_f)}_f - \underbrace{\deg(\text{Id})}_1 \right| \leq 2 \sqrt{\underbrace{\deg(\varphi_f) \deg(\text{Id})}_{\sqrt{f}}}$$

□

Soit k un corps fini, soit $\bar{k}$ une clôture
 algébrique de k . Pour chaque $n \geq 1$,

$$k \subset k_n \subset \bar{k}$$

k_n est l'unique sous-extension de degré n .

Définition. Soit X une variété projective
 lisse définie sur k . La fonction zêta de
 X est la série formelle

$$Z(X/k, T) = \exp \left(\sum_{n=1}^{\infty} |X(k_n)| \frac{T^n}{n} \right)$$

Exemple : Si $X = \mathbb{P}^N$ est l'espace projectif, alors

$$X(k_n) = \{ [x_0 : \dots : x_N] \mid x_i \in k_n \}$$

est de cardinal $\frac{q^{nN} - 1}{q^n - 1} = \sum_{i=0}^N q^{ni}$, d'où

$$Z(\mathbb{P}^N/k, T) = \exp \left(\sum_{n=1}^{\infty} \left(\sum_{i=0}^N q^{ni} \right) \frac{T^n}{n} \right)$$

$$= \exp \left(\sum_{i=0}^N \sum_{n=1}^{\infty} \underbrace{\left(q^i T \right)^n}_{- \log(1 - q^i T)} \right)$$

$$= \frac{1}{(1-T)(1-qT)\dots(1-q^NT)}$$

Théorème (Conjectures de Weil pour les courbes elliptiques sur les corps finis)

Soient k un corps fini à q éléments et E une courbe elliptique sur k .

Il existe $a \in \mathbb{Z}$ tel que

$$Z(E/k, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

De plus, le polynôme $1 - \alpha T + q T^2$ est égal à

$$(1 - \alpha T)(1 - \beta T) \text{ avec } |\alpha| = |\beta| = \sqrt{q}$$

et on a la relation

$$Z(E/k, T) = Z(E/k, \frac{1}{qT}).$$

La démonstration repose sur les propriétés du module de Tate

$$T_\ell E = \varprojlim_n E[\ell^n] \simeq \mathbb{T}_\ell \times \mathbb{T}_\ell$$

pour un nombre premier ℓ différent de $\text{car}(k)$.

On a une injection

$$\begin{aligned} \text{End}(E) &\hookrightarrow \text{End}(T_\ell E) \\ \varphi &\longmapsto \varphi_\ell \end{aligned}$$

Proposition. Soit $\varphi \in \text{End}(E)$ une isogénie.

$$\text{Alors } \det(\varphi_\ell) = \deg(\varphi)$$

$$\text{tr}(\varphi_\ell) = 1 + \deg(\varphi) - \deg(\text{Id} - \varphi)$$

En particulier, les éléments

$$\det(\varphi_\ell), \text{tr}(\varphi_\ell) \in \mathbb{T}_\ell$$

sont dans $\mathbb{Z}$ et indépendants de ℓ .

Démonstration. Soit $\{v_1, v_2\}$ une $\mathbb{Z}_\ell$ -base de $T_\ell E$. La matrice de φ_ℓ dans cette base est $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. on utilise l'accomplissement de Weil

$$e: T_\ell E \times T_\ell E \longrightarrow T_\ell \mu$$

pour calculer

$$\begin{aligned} e(v_1, v_2)^{\deg \varphi} &= e([\deg \varphi]v_1, v_2) \\ &= e(\hat{\varphi}_\ell \varphi_\ell v_1, v_2) \\ &= e(\varphi_\ell v_1, \varphi_\ell v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^a \\ &= e(v_1, v_2)^{\det(\varphi_\ell)}, \end{aligned}$$

d'où $\deg \varphi = \det(\varphi_\ell)$ puisque e est non dégénéré.

La deuxième égalité résulte alors de

$$\begin{aligned} \text{tr } A &= 1 + \det A - \det(\text{Id} - A) \\ &= 1 + ad - bc - (1 - a)(1 - d) + bc \\ &= a + d \end{aligned}$$

□

Soit $\varphi = \varphi_f : E \rightarrow E$ le morphisme de Frobenius. On a

$$|E(K_n)| = \deg(1 - \varphi^n) \text{ pour } n \geq 1$$

D'après le lemme,

$$\begin{aligned} \det(T - \varphi_e) &= T^2 - \text{tr}(\varphi_e)T + \det(\varphi_e) \\ &= (T - \alpha)(T - \beta) \in \mathbb{Z}[T] \end{aligned}$$

pour des nombres complexes $\alpha, \beta \in \mathbb{C}$.

Par ailleurs,

$$\begin{aligned} \det\left(\frac{m}{n} \text{Id} - \varphi_e\right) &= \frac{\det(m \text{Id} - n \varphi_e)}{n^2} \\ &= \frac{\deg(m \text{Id} - n \varphi_e)}{n^2} \geq 0 \end{aligned}$$

pour tout $\frac{m}{n} \in \mathbb{Q}$, ce qui veut dire que les racines de $\det(T - \varphi_e)$ sont soit complexes conjuguées soit une racine double. On a donc $|\alpha| = |\beta|$. Comme

$$\alpha\beta = \det(\varphi_e) = \deg(\varphi_e) = f,$$

on trouve $\boxed{|\alpha| = |\beta| = \sqrt{f}}$.

le polynôme caractéristique de q_ℓ^n est

$$\det(T - q_\ell^n) = (T - \alpha^n)(T - \beta^n),$$

d'où la formule pour le nombre de points

$$\begin{aligned} |E(k_n)| &= \deg(1 - q^n) \\ &= \det(\text{Id} - q_\ell^n) \\ &= (1 - \alpha^n)(1 - \beta^n) \\ &= 1 - \alpha^n - \beta^n + \gamma^n \end{aligned}$$

Démonstration du théorème : Calculons

$$\begin{aligned} \log Z(E/k, T) &= \sum_{n=1}^{\infty} |E(k_n)| \frac{T^n}{n} \\ &= \sum_{n=1}^{\infty} (1 - \alpha^n - \beta^n + \gamma^n) \frac{T^n}{n}, \end{aligned}$$

d'où

$$Z(E/k, T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - \gamma T)}$$

L'entier a dans l'exposant est

$$\alpha = \alpha + \beta = \text{tr}(\varphi_e) = 1 + q - \deg(\text{Id} - \varphi)$$

Enfin, pour l'équation fonctionnelle :

$$\begin{aligned} Z(E/k, \frac{1}{qT}) &= \frac{(1 - \frac{\alpha}{qT})(1 - \frac{\beta}{qT})}{(1 - \frac{1}{qT})(1 - \frac{q}{qT})} \\ &= \frac{(qT - \alpha)(qT - \beta)}{(qT - 1)(qT - q)} \\ &= \frac{q(qT^2 - (\alpha + \beta)T + 1)}{q(1 - T)(1 - qT)} \\ &= Z(E/k, T) \quad \square \end{aligned}$$

Remarque : avec le changement de variable

$T = q^{-s}$ la fonction zêta prend la forme

$$Z_{E/k}(s) = \frac{1 - \alpha q^{-s} + q^{1-2s}}{(1 - q^{-s})(1 - q^{1-s})},$$

l'équation fonctionnelle

$$Z_{E/k}(s) = Z_{E/k}(1-s)$$

et si $Z_{E/k}(s) = 0$, alors $|q^s| = \sqrt{q}$,

c'est-à-dire $\operatorname{Re}(s) = \frac{1}{2}$. c'est l'analyse
de l'hypothèse de Riemann.