Le morphisme de Frobenius

parfait !

Soit p un nombre premier et k un corps de caractéristique p. Soit q une puissance de p. Pour $f \in k[X_0, \dots, X_n]$, on note

$$f^{(q)} = \sum a_I^q X^I \in k[X_0, \dots, X_n]$$

obtenu en prenant les puissances q-ièmes de chaque coefficient.

C/k courbe $\quad I(C)$ son idéal homogène

$$= \{ f \in \bar{k}[X_0, \dots X_n] \mid f \text{ homogène } f(P) = 0 \text{ pour tout } P \in C \}$$

Définition : $C^{(q)}$ est la courbe sur k d'idéal homogène

$$I(C^{(q)}) = \text{l'idéal engendré par } f^{(q)} \text{ pour } f \in I(C)$$

Il y a un morphisme de Frobenius

$$\varphi_q : C \longrightarrow C^{(q)}$$
$$[X_0 : \dots : X_n] \longmapsto [X_0^q : \dots : X_n^q]$$

En effet, pour tout $P = [X_0 : \dots : X_n] \in C$ et tout $f \in I(C)$, on a

$$f^{(q)}(\varphi_q(P)) = f^{(q)}([X_0^q : \dots : X_n^q])$$

$$= f(X_0, \dots, X_n)^q$$

car $K = p$

$$= 0$$

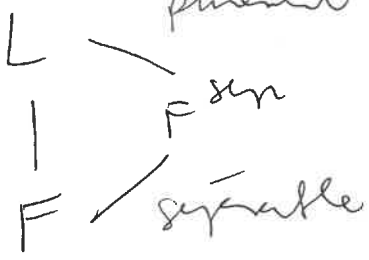
Proposition :

(a) $\varphi_q^* K(C^{(q)}) = K(C)^q$ $\quad \{f^q \mid f \in K(C)\}$

(b) φ_q est purement inséparable

(c) $\deg \varphi_q = q$

Rappel : si L/F est une extension finie de corps, il existe une unique sous-extension



c'est-à-dire pour tout $\alpha \in L$ il existe n tel que $\alpha^{p^n} \in F^{sep}$.

Preuve : (a) Rappelons que $K(C)$ est l'ensemble des $\frac{f}{g}$ où $f, g \in K[X_0, \dots X_n]$

sont homogènes du même degré, $g \notin I(C)$ et $\frac{f}{g} = \frac{f'}{g'} \Rightarrow fg' - f'g \in I(C)$. On a donc :

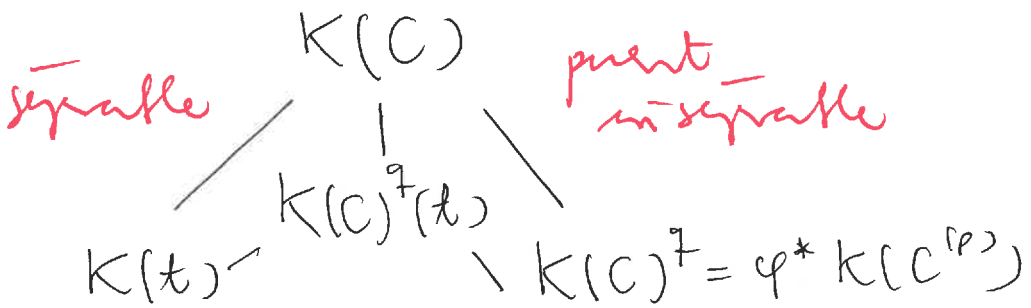
$$\varphi_q^* K(C^{(q)}) = \left\{ \frac{f^{(q)}(X_0^q, \dots X_n^q)}{g^{(q)}(X_0^q, \dots X_n^q)} \mid f, g \in K[C] \right\}$$

$$= \left\{ \frac{f(X_0, \dots X_n)^q}{g(X_0, \dots X_n)^q} \right\}$$

$$= K(C)^q$$

(b) Par définition, si $f \in K(C)$, alors $f^q \in \varphi_q^* K(C^{(q)})$, donc l'extension $K(C) / \varphi_q^* K(C^{(q)})$ est purement inséparable.

(c) Soit P un point lisse de C et t une uniformisante en P. On a :



$$\Rightarrow \boxed{K(C) = K(C)^q(t)}$$

$$\deg \varphi_q = [K(C)^q(t) : K(C)^q]$$

Comme $t^q \in K(C)^q$, $\deg \varphi_q \mid q$ = puissance de p

Montrons que $t^{q/p} \notin K(C)^q$. En effet, si $t^{q/p} = f^q$ pour un $f \in K(C)$, alors

$$q/p = \mathrm{ord}_p(t^{q/p}) = q \cdot \mathrm{ord}_p(f),$$

absurde. Donc $\deg \varphi_q = q$ □

Corollaire : Tout morphisme $\Psi : C_1 \to C_2$ entre courbes lisses sur un corps de caractéristique $p > 0$ se factorise

$$C_1 \xrightarrow{\varphi_q} C_1^{(q)} \xrightarrow{\lambda} C_2$$

$$C_1 \xrightarrow{\Psi} C_2$$

où $q = \deg_i(\Psi)$ et λ est séparable.

Preuve : $K(C_1)$ / $\deg \Psi$ | / $\Psi^* K(C_2)$; F = la plus grande sous-extension séparable

Alors $K(C_1)/F$ est purement inséparable de

degré q, d'où $K(C_1)^q \subset F$. Mais :

$$K(C_1)^q = \varphi_q^* K(C_1^{(q)}) \quad \Rightarrow F = \varphi_q^* K(C_1)$$

$$[K(C_1) : K(C_1)^q] = q$$

d'où une tour d'extensions

$$\begin{array}{c} K(C_1) \\ | \\ \varphi_q^* K(C_1^{(q)}) \\ | \\ \psi^* K(C_2) \end{array}$$

$$C_1 \xrightarrow{\varphi_q} C_1^{(q)} \xrightarrow{\lambda} C_2, \qquad \psi = \lambda \circ \varphi_q$$

avec λ séparable car l'extension

$$\varphi_q^* K(C_1^{(q)}) / \psi^* K(C_2) \quad \text{l'est} \qquad \square$$

Isogénies duales

E, E' des courbes elliptiques sur un corps k. Rappelons qu'une isogénie est un morphisme de courbes algébriques $\varphi : E \to E'$ non constant tel que $\varphi(O_E) = O_{E'}$.

D'un côté, on a l'application d'Abel-Jacobi
$$E(\bar{k}) \xrightarrow{\sim} \mathrm{Pic}^0(E)$$
$$P \longmapsto \text{classe de } [P] - [O]$$

D'un autre côté, φ induit via le tiré en arrière des diviseurs un morphisme de groupes
$$\varphi^* : \mathrm{Pic}^0(E') \to \mathrm{Pic}^0(E)$$
$$[Q] \longmapsto \left[\sum_{\varphi(P)=Q} e_\varphi(P)\,[P] \right]$$

(Un lemme dit que $\varphi^*(\mathrm{div}\, f) = \mathrm{div}(f \circ \varphi)$)

On peut donc considérer la composition
$$\hat{\varphi} : E'(\bar{k}) \xrightarrow{\sim} \mathrm{Pic}^0(E') \xrightarrow{\varphi^*} \mathrm{Pic}^0(E) \xrightarrow{\sim} E(\bar{k})$$
qui envoie un point $Q \in E'(\bar{k})$ vers le point $\hat{\varphi}(Q)$ caractérisé par :
$$[\hat{\varphi}(Q)] - [O_E] = \varphi^*\left([Q] - [O_{E'}]\right).$$

But : montrer que $\hat{\varphi}$ est une isogénie

Soit P un point de $E(\bar{K})$ avec $\varphi(P) = Q$.
Alors la préimage de Q est l'ensemble

$$\{ P + R \mid R \in \ker \varphi \}$$

où $\ker \varphi = \varphi^{-1}(O_{E'})$ est un sous-groupe de $E(\bar{K})$, d'ordre $\deg_s(\varphi)$ le degré séparable de φ. On a donc :

$$\varphi^*([Q] - [O_{E'}]) = \sum_{\varphi(T) = Q} e_\varphi(T)\,[T] - \sum_{\varphi(R) = O_{E'}} e_\varphi(R) \cdot [R]$$

$$= \sum_{R \in \ker(\varphi)} \deg_i(\varphi)\,([P+R] - [R])$$

↑ degré inséparable

Comme par ailleurs $[P+R] - [R] \sim [P] - [O_E]$ dans $\mathrm{Pic}^0(E)$,

$$\varphi^*([Q] - [O_{E'}]) = \deg_i(\varphi) \sum_{R \in \ker(\varphi)} ([P] - [O_E])$$

$|\ker \varphi| = \deg_s(\varphi)$

$$= \underbrace{\deg_i(\varphi)\deg_s(\varphi)}_{\deg(\varphi)}([P] - [O_E])$$

* φ séparable : on a alors $|\ker(\varphi)| = m$,

d'où $\ker\varphi \subset \ker[m]$.

$$\begin{array}{c} \bar{K}(E) \\ \text{Galois} \,|\, \\ \varphi^*\bar{K}(E') \end{array} \qquad \ker\varphi \simeq \mathrm{Gal}\left(\bar{K}(E)/\varphi^*\bar{K}(E')\right)$$

d'où les inclusions

$$\bar{K}(E) \supset \varphi^*\bar{K}(E') \supset [m]^*\bar{K}(E)$$

À ces injections entre corps de fonctions correspond une isogénie

$$\bar{K}(E) \xrightarrow{(\varphi^{-1})^*[m]^*} K(E')$$

$$\hat{\varphi} : E' \longrightarrow E$$

tel que $\varphi^*(\hat{\varphi}^*\bar{K}(E)) = [m]^*\bar{K}(E)$,

d'où $\boxed{\hat{\varphi}\circ\varphi = [m]_E}$. Donc

$$\hat{\varphi}(0) = \hat{\varphi}(\varphi(0)) = [m]_E(0) = 0,$$

le morphisme $\hat{\varphi}$ est une isogénie.

* φ est le Frobenius φ_q : si $q = p^e$,

alors $\varphi_q = (\varphi_p)^{\circ e}$ et il suffit donc de déterminer l'isogénie de $\hat{\varphi}_p$. L'application

$[p]_E$ est une isogénie inséparable car

$$[p]^* w = p w = 0$$

pour une différentielle invariante, donc $[p]$ se décompose comme

$$[p] = \Psi \circ \varphi_p^f \quad \text{avec } f \geq 1$$

(Ψ : séparable)

et il suffit alors de poser $\hat{\varphi}_p = \Psi \circ \varphi_p^{f-1}$ □

Définition : Soit $\varphi : E \to E'$ une isogénie. L'isogénie duale est $\hat{\varphi} : E' \to E$.

Théorème : Soient $\varphi, \psi : E \to E'$ des isogénies. Alors

$$\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$$

On admet ce résultat pour l'instant.

Corollaire : Soit $m \geq 1$ un entier.

a) $\deg([m]_E) = m^2$ et $\widehat{[m]} = [m]$.

b) Si $(m, \mathrm{car}\, k) = 1$, alors

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$$

comme groupes abéliens

b) Si $\mathrm{car}(k) = p$, alors soit

$$E[p^n] = 0 \quad \text{pour tout} \quad = 1, \dots$$

soit $E[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z}$ pour tout $n = 1, 2, \dots$

Définition : Si $E[p] = 0$, on dit que E est supersingulière. Sinon, on dit que E est ordinaire.

Preuve du corollaire : (a) La formule $\widehat{[m]} = [m]$ est claire pour $m = 1$, donc

$$\widehat{[m+1]} = \widehat{[m] + [1]} = \widehat{[m]} + \widehat{[1]}$$

$$\uparrow \text{Théorème} \qquad = [m] + [1]$$

$$= [m+1]$$

$$\uparrow \text{récurrence}$$

Soit $d = \deg([m])$. Alors par définition

$$[d] = \widehat{[m]} \circ [m] = [m^2]$$

mais alors $[d - m^2] = 0$ dans $\mathrm{End}(E)$, d'où $d = m^2$ car la multiplication par un entier non nul est une isogénie.

(b) Si $(m, \mathrm{car}(k)) = 1$, alors $[m]$ est une isogénie séparable, donc

$$|E[m]| = |\mathrm{Ker}([m])| = \deg([m]) = m^2$$

De même, pour tout $d \mid m$ on a

$$|E[d]| = d^2$$

Le groupe fini $E[m]$ est abélien, donc produit de groupes cycliques

$$C_1 \times \dots \times C_2$$

où C_i est un groupe d'ordre $p_i^{2k_i}$ pour chaque p_i dans $m = p_1^{k_1} \dots p_2^{k_2}$. Il suffit donc de considérer le cas $m = p^k$.

Si $k = 1$, les possibilités sont

$$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \qquad \mathbb{Z}/p^2\mathbb{Z}$$

mais tout élément non nul de $E[p]$ a ordre p, donc $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Si $E[p^k] = \langle P_1 \rangle \times \dots \times \langle P_2 \rangle$ avec P_i d'ordre p^{e_i}, alors $E[p] = \langle p^{e_1 - 1} P_1 \rangle \times \dots \times \langle p^{e_2 - 1} P_2 \rangle$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$, donc $r = 0$.

Mais alors $E[p^k] \simeq \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^k\mathbb{Z}$ puisque le plus grand ordre d'un élément est p^k.

(c) Posons $p = \mathrm{car}(K)$, et écrivons $[p]_E = \hat{\varphi}_p \circ \varphi_p$ où $\varphi_p : E \to E^{(p)}$ est l'isogénie de Frobenius. Alors :

$$|E[p^n]| = \deg_s([p^n]_E)$$
$$= \deg_s(\hat{\varphi}_p)^n$$

Comme $\deg \hat{\varphi}_p = \deg \varphi_p = p$, il y a deux possibilités :

* si $\hat{\varphi}_p$ est inséparable, alors $\deg_s \hat{\varphi}_p = 1$ et $E[p^n] = \{0\}$ pour tout n

* si $\hat{\varphi}_p$ est séparable, alors $\deg_s \hat{\varphi}_p = p$, d'où $|E[p^n]| = p^n$. Pour $n=1$, on obtient

$$E[p] \simeq \mathbb{Z}/p\mathbb{Z} \simeq \langle P \rangle$$

Comme l'isogénie $[p] : E \to E$ est surjective, il existe $Q \in E(\bar{K})$ avec $pQ = P$. Donc, $E[p^2]$ contient un point d'ordre p^2, et par récurrence $\boxed{E[p^n] \simeq \mathbb{Z}/p^n\mathbb{Z}}$ □

Corollaire : l'application

$$\deg : \mathrm{Hom}(E, E') \longrightarrow \mathbb{N}$$

est une forme quadratique définie positive.

(Rappel : une fonction $d : A \to \mathbb{R}$ sur un groupe abélien A est une forme quadratique si $d(x) = d(-x)$ pour tout $x \in A$ et

$$\begin{aligned} A \times A &\longrightarrow \mathbb{R} \\ x, y &\longmapsto d(x+y) - d(x) - d(y) \end{aligned}$$

est une forme bilinéaire. Elle est définie positive si $d(x) \geq 0$ pour tout $x \in A$ et $d(x) = 0 \iff x = 0$)

Preuve : Il faut montrer que l'application

$$\deg(\varphi + \Psi) - \deg(\varphi) - \deg(\Psi)$$

est bilinéaire. En utilisant l'injection

$$\begin{aligned} [\cdot]\ \mathbb{Z} &\longrightarrow \mathrm{End}(E) \\ m &\longmapsto [m] \text{ isogène} \end{aligned}$$

on a

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

$= \hat{\varphi} \circ \Psi + \hat{\Psi} \circ \varphi$

et cette dernière expression est bien $\mathbb{Z}$-bilinéaire en (φ, Ψ) □

Courbes elliptiques sur les corps finis

p un nombre premier

q puissance de p

K un corps fini à q éléments

E une courbe elliptique sur K

d'équation de Weierstrass

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

But : compter le nombre de K-points de E

$= 1 +$ nombre de $(x, y) \in K^2$ solutions de l'équation de Weierstrass

point à l'infini

* Borne triviale : $\leq 2q + 1$ (pour chaque valeur de x, au plus 2 solutions pour l'équation quadratique)

* Heuristique : probabilité qu'une équation quadratique ait une solution dans $K = 1/2$

un nombre de grandeur $q+1$

Théorème (Hasse) :

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

Démonstration : Considérons l'endomorphisme de Frobenius $\varphi_q : E \longrightarrow E$.

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

Comme $\mathrm{Gal}(\bar{k}/k) \simeq \hat{\mathbb{Z}}$ avec générateur l'automorphisme $t \mapsto t^q$ sur k, on sait que $P \in E(\bar{k})$ appartient à $E(k)$ si et seulement si $\varphi_q(P) = P$. Autrement dit :

$$E(k) = \ker(\mathrm{Id} - \varphi_q).$$

Le morphisme $\mathrm{Id} - \varphi_q : E \longrightarrow E$

$$P \longmapsto P - \varphi_q(P)$$

est une isogénie, car il envoie O sur O et est non constant. C'est une isogénie séparable car l'application

$$\Omega_E \longrightarrow \Omega_E$$
$$w \longmapsto (\mathrm{Id} - \varphi_q)^* w = w$$

n'est pas nulle. (Ici, on a utilisé $\varphi_q^* w = 0$, qui suit par exemple du calcul

$$\varphi_q^*(dx) = d(x^q) = q\, x^{q-1} dx = 0,$$

ou bien du fait que φ_q est inséparable).

loi de groupe dans la courbe elliptique

chaque $n \geq 1$, soit $k \subset k_n \subset \bar{k}$ l'unique sous-extension de degré n.

Soit X une variété projective et lisse définie sur k.

Définition. 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: Soit X l'espace projectif $\mathbb{P}^N$.

Alors $X(k_n) = \{ [X_0 : \dots : X_N] \mid X_i \in k_n \}$ a

$$|X(k_n)| = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}$$

éléments, d'où:

$$\sum_{n=1}^{\infty} |X(k_n)| \frac{T^n}{n} = \sum_{n=1}^{\infty} \left(\sum_{i=0}^{N} q^{ni} \right) \frac{T^n}{n}$$

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

$$\Rightarrow Z(X/k, T) = \frac{1}{(1-T) \cdots (1 - q^N T)}$$

on sait que dans ce cas la fonction zêta est le développement en série entière d'une fonction rationnelle.