Courbes Elliptiques - Définitions et théorèmes majeurs

Johan Manuel

5 mars 2018

1 Définitions

On notera dans cette section E, E_1 et E_2 des courbes elliptiques, et $q = p^r$ avec p premier et $r \in \mathbb{N}$.

Degré d'une application (21): Soit $\phi : E_1 \to E_2$. Si ϕ est constante, on définit $\deg\ \phi = 0$. Sinon, $\deg\ \phi = [K(E_1) : \phi^* K(E_2)]$.

Application séparable (21): L'application $\phi : E_1 \to E_2$ est dite séparable si $K(E_1)/\phi^* K(E_2)$ est séparable en tant qu'extension de corps. On note $\deg_s\ \phi$ et $\deg_i\ \phi$ les degrés séparables et inséparables de l'extension, respectivement.

Forme quadratique (85): Soit G un groupe commutatif. $d : G \to R$ est une forme quadratique si
— $\forall a \in G,\ d(a) = d(-a)$
— $\psi : (a, b) \in G^2 \mapsto d(a + b) - d(a) - d(b)$ est une forme bilinéaire
d est de plus dite *définie positive* si $\forall a \in G,\ d(a) \geq 0$ et $d(a) = 0 \Leftrightarrow a = 0$

Application non ramifiée (24): L'application $\phi : E_1 \to E_2$ est dite non-ramifiée si $\forall Q \in E_2,\ \#\phi^{-1}(\{Q\}) = \deg\ \phi$.

Isogénie (66): Une isogénie est un morphisme ϕ de E_1 dans E_2 tel que $\phi(O) = O$.

Application [m] (69): Soit $m \in \mathbb{N}$. On appelle $[m] : E \to E$ l'application "multiplication par m" et on note $\forall P \in E,\ [m](P) = [m]P$.

Sous groupe de m-torsion (69): On note $E[m]$ l'ensemble des points de E d'ordre m, i.e $E[m] = \{P \in E \mid [m]P = O\} = \text{Ker } [m]$.

Courbe $E^{(q)}$ (25): Notons $a_1,\ ...,\ a_6$ les coefficients de l'équation de Weierstrass de E. Alors on note $E^{(q)}$ la courbe elliptique définie par les coefficients $a_1^q,\ ...,\ a_6^q$.

Morphisme de Frobenius (25, 70): L'application

$$\phi_q : E \to E^{(q)}$$
$$(x, y) \mapsto (x^q, y^q)$$

est appelée morphisme de Frobenius. ϕ_q est inséparable et deg $\phi_q = q$. Si E est définie sur F_q, alors $E = E^{(q)}$ et ϕ_q est un endomorphisme.

Trace de Frobenius: On appelle trace de Frobenius l'entier $a = q + 1 - \#E(F_q)$, puisque a est la trace de $\phi_{q\ell}$, l'application induite par ϕ_q sur le module de Tate de E.

2 Théorèmes et propositions

Proposition: $End(E)$ a une structure d'anneau et forme un domaine intègre.

Proposition: Soit $m \in \mathbb{N}$. L'application $[m]$ est de degré m^2.

Proposition (70): Soit E/F_q. Alors l'ensemble des points fixes de ϕ_q est $E(F_q)$, l'ensemble des points à coordonnées dans F_q, i.e $E(F_q) = \{P \in E \mid \phi_q(P) = P\} = \mathrm{Ker}(\phi_q - Id)$.

Théorème III.4.10: Soit $\phi : E_1 \to E_2$ une isogénie non nulle. Alors

1. $\forall Q \in E_2,\ \#\phi^{-1}(\{Q\}) = \deg_s \phi$,
2. L'application $\psi : T \in \mathrm{Ker}\,\phi \mapsto \tau_T^*$ est un isomorphisme de $\mathrm{Ker}\,\phi$ sur $Aut(\overline{K}(E_1)/\phi^*\overline{K}(E_2))$,
3. Si ϕ est séparable, alors
   (a) ϕ est non ramifiée,
   (b) $\#\,\mathrm{Ker}\,\phi = \deg\phi$,
   (c) $\overline{K}(E_1)$ est une extension de Galois de $\phi^*\overline{K}(E_2)$.

Proposition III.5.5 (79): Soit E/F_q, $q = p^r$, $(m, n) \in \mathbb{Z}^2$. Alors $mId + n\phi_q : E \to E$ est séparable si et seulement si $p \nmid n$. En particulier, $Id - \phi_q$ est séparable.

Lemme V.1.2 (138): Soit A un groupe commutatif, et $d : A \to Z$ une forme quadratique définie positive. Alors $\forall (a, b) \in A^2,\ |d(a - b) - d(a) - d(b)| \leq 2\sqrt{d(a)d(b)}$.
C'est une adaptation de l'inégalité de Cauchy-Schwarz.

Théorème de Hasse (138): Soit E/F_q. Alors $|\#E(F_q) - (q + 1)| \leq 2\sqrt{q}$.

Proposition (89): Soit $\phi : E_1 \to E_2$ une isogénie, ℓ premier. Alors ϕ induit une application Z_ℓ-linéaire $\phi_\ell : T(E_1) \to T(E_2)$. Si $E_1 = E_2$, en choisissant une Z_ℓ-base de $T_\ell(E)$, ϕ_ℓ admet une représentation matricielle dans $GL_2(Z_\ell)$.

Proposition III.8.6 (99, 141): Soit $\psi \in End(E)$. Alors

1. $\det \psi_\ell = \deg \psi$,
2. $\operatorname{tr} \psi_\ell = 1 + \deg \psi - \deg(Id - \psi)$,
3. $\det \psi_\ell,\ \operatorname{tr} \psi_\ell \in \mathbb{Z}^2$.

Théorème V.2.3.1: Soit E/F_q une courbe elliptique, et $a = q + 1 - \#E(F_q)$.

1. Soit $(\alpha,\ \beta) \in \mathbb{C}^2$ les racines de $X^2 - aX + q$. Alors α et β sont complexes conjuguées et vérifient $|\alpha| = |\beta| = \sqrt{q}$, et $\forall n \in \mathbb{N}^*,\ \#E(F_{q^n}) = q^n + 1 - \alpha^n - \beta^n$.
2. ϕ_q vérifie $\phi_q^2 - a\phi_q + qId = 0_{End(E)}$.

3 Démonstrations

Lemme V.1.2: Soit A un groupe commutatif et $d : A \to Z$ une forme quadratique définie positive. Posons $\forall(\psi,\ \phi) \in A,\ L(\psi, \phi) = d(\psi - \phi) - d(\psi) - d(\phi)$. d étant une forme quadratique, L est une forme bilinéaire
Soit $(m,\ n) \in \mathbb{Z}^2$. On a $L(m\psi, n\phi) = d(m\psi - n\phi) - d(m\psi) - d(n\phi)$ d'où $d(m\psi - n\phi) = d(m\psi) + L(n\psi, m\phi) + d(n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi) \geq 0$ par positivité de d. En prenant $m = -L(\psi, \phi)$ et $n = 2d(\psi)$, on obtient

$$0 \leq -d(\psi)L(\psi, \phi)^2 + 4d(\psi)^2 d(\phi) = d(\psi)(4d(\psi)d(\phi) - L(\psi, \phi)^2),$$

d'où

$$|d(\psi - \phi) - d(\psi) - d(\phi)| \leq 2\sqrt{d(\psi)d(\phi)}.$$

Théorème de Hasse: Soit $q = p^n$ avec p premier et $n \in \mathbb{N}^*$, et E/F_q une courbe elliptique.
On a $E(F_q) = \operatorname{Ker}(Id - \phi_q)$ d'après la théorie de Galois (voir en bas de la page 70). Or d'après III.5.5, $Id - \phi_q$ est séparable puisque $p \nmid 1$. Alors par le théorème III.4.10 on a $\#E(F_q) = \deg(Id - \phi_q)$. Comme l'application deg : $End(E) \to Z$ est une forme quadratique et que $End(E)$ forme un groupe commutatif, le lemme V.1.2 donne

$$|\deg(Id - \phi_q) - \deg Id - \deg \phi_q| \leq 2\sqrt{\deg(Id)\deg(\phi_q)},$$

d'où finalement

$$|\#E(F_q) - (q + 1)| \leq 2\sqrt{q}.$$