ARITHMÉTIQUE DES COURBES ELLIPTIQUES
FEUILLE DE TD 5

Exercice 1. Soit E une courbe elliptique sur un corps parfait k de caractéristique $p > 0$.

(1) Montrer que les conditions suivantes sont équivalentes :
   (a) $\mathrm{E}[p](\bar{k}) = 0$
   (b) $[p]$ est purement inséparable
   (c) l'isogénie duale à Fr_p est inséparable.

   Si l'une de ces conditions est satisfaite on dit que E est *supersingulière*.

(2) On suppose $k = \mathbb{F}_q$ avec $q = p^r$. Montrer que E est supersingulière si et seulement si à $|\mathrm{E}(\mathbb{F}_q)| \equiv 1 \pmod{p}$.

(3) On suppose $p = 2$. Montrer que la courbe $y^2 + y = x^3$ est supersingulière (et c'est l'unique à isomorphisme près sur $\bar{\mathbb{F}}_2$.)

(4) On suppose $p \geqslant 3$ et que E a équation de Weierstrass $y^2 = f(x)$. Alors E est supersingulière si et seulement si le coefficient de x^{p-1} dans $f(x)^{(p-1)/2}$ est nul.

(5) On suppose de plus $f(x) = x(x-1)(x-\lambda)$. Alors E supersingulière si et seulement si

$$\mathrm{H}_p(\lambda) = \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i = 0 \qquad \text{où } m = (p-1)/2.$$

Exercice 2. Soit E une courbe elliptique sur corps algébriquement clos k et $\Gamma \subset \mathrm{E}$ un sous-groupe fini. Montrer les faits suivants :

(1) $k(\mathrm{E})^\Gamma$ est le corps de fonctions d'une courbe elliptique E'.

(2) Le morphisme $\pi\colon \mathrm{E} \to \mathrm{E}'$ donné par l'inclusion $k(\mathrm{E})^\Gamma \subset k(\mathrm{E})$ induit une bijection

$$\mathrm{E}(k)/\Gamma \xrightarrow{\sim} \mathrm{E}'(k).$$

(3) Pour tout ouvert $\mathrm{U} \subset \mathrm{E}'$ on a $\Gamma(\mathrm{U}, \mathcal{O}_{\mathrm{E}'}) = \Gamma(\pi^{-1}(\mathrm{U}), \mathcal{O}_{\mathrm{E}})^\Gamma$.

(4) Si $f\colon \mathrm{E} \to \mathrm{C}$ est un morphisme Γ-invariant entre courbes projectives lisses, il existe un unique morphisme $g\colon \mathrm{E}' \to \mathrm{C}$ tel que $f = g \circ \pi$.

Les propriétés ci-dessus justifient d'appeler E' le *quotient* E/Γ de E par Γ et π la *projection*.

Exercice 3. Soit E une courbe elliptique sur un corps algébriquement clos k. Montrer les faits suivants :

(1) Soit $\varphi\colon \mathrm{E} \to \mathrm{E}'$ une isogénie séparable. Alors E' s'identifie au quotient de E par $\operatorname{Ker}\varphi$ et φ à la projection sur le quotient.

(2) Soit $m \geq 2$ un entier inversible dans k et $f\colon \mathrm{E} \to \mathbb{P}^1$ une fonction rationnelle telle que

$$f(x+t) = f(x) \quad \text{pour tout } x \in \mathrm{E} \text{ et tout } t \in \mathrm{E}[m].$$

   Alors il existe une fonction rationnelle g sur E telle que $f = g \circ [m]$.

(3) Soient $\varphi\colon \mathrm{E} \to \mathrm{E}'$ et $\psi\colon \mathrm{E} \to \mathrm{E}''$ des isogénies. Supposons que φ est séparable et que $\operatorname{Ker}\varphi \subset \operatorname{Ker}\psi$. Alors il existe une isogénie $\lambda\colon \mathrm{E}' \to \mathrm{E}''$ telle que $\psi = \lambda \circ \varphi$.

Exercice 4 (Examen 2024)**.** Étant donnée une courbe elliptique E sur un corps fini k à q éléments, on note $\mathrm{Fr}_q\colon \mathrm{E} \to \mathrm{E}$ l'isogénie de Frobenius définie en coordonnées affines par

$$\mathrm{Fr}_q(x, y) = (x^q, y^q).$$

(1) Est-ce qu'il existe une courbe elliptique E sur $\mathbb{F}_{49}$ telle que $|\mathrm{E}(\mathbb{F}_{49})| = 23$?

(2) Soit E une courbe elliptique définie sur $\mathbb{F}_5$ telle que $\mathrm{E}(\mathbb{F}_5)$ soit de cardinal 9. Quel est le cardinal de $\mathrm{E}(\mathbb{F}_{25})$?

(3) Soient p un nombre premier, k un corps fini à $q = p^2$ éléments et $\bar{k}$ une clôture algébrique de k. Soit E une courbe elliptique sur k telle que $|\mathrm{E}(k)|$ soit aussi grand que la borne de Hasse le permet.

   (a) Démontrer l'égalité $\mathrm{Fr}_q + [p] = 0$ dans $\mathrm{End}(\mathrm{E})$.

   (b) Démontrer que E est supersingulière.

   (c) Démontrer que $\mathrm{E}(\bar{k})[p+1]$ est contenu dans $\mathrm{E}(k)$.

   (d) En déduire que le groupe $\mathrm{E}(k)$ est isomorphe à $\mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}$.

(4) Soient k un corps fini à q éléments et E_1 et E_2 des courbes elliptiques définies sur k. Supposons qu'il existe une isogénie $f\colon \mathrm{E}_1 \to \mathrm{E}_2$ définie sur k.

   Montrer que E_1 et E_2 ont la même fonction zêta :

$$\mathrm{Z}(\mathrm{E}_1/k, \mathrm{T}) = \mathrm{Z}(\mathrm{E}_2/k, \mathrm{T}).$$

   (*Indication : la condition que l'isogénie f est définie sur k signifie $f \circ \mathrm{Fr}_{q,\mathrm{E}_1} = \mathrm{Fr}_{q,\mathrm{E}_2} \circ f$*).

(5) Qu'est-ce qu'il faudrait savoir sur l'application

$$\mathrm{Hom}(\mathrm{E}_1, \mathrm{E}_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}(\mathrm{T}_\ell(\mathrm{E}_1), \mathrm{T}_\ell(\mathrm{E}_2))$$

   pour démontrer la réciproque, c'est-à-dire que si E_1 et E_2 ont la même fonction zêta alors il existe une isogénie $f\colon \mathrm{E}_1 \to \mathrm{E}_2$ définie sur k ?

Exercice 5. Calculer la fonction zêta de la courbe projective $\mathrm{C} \subset \mathbb{P}^2$ sur le corps fini $\mathbb{F}_p$ donnée par l'équation $\mathrm{Y}^2\mathrm{Z} = \mathrm{X}^3$ et comparer le résultat avec la fonction zêta d'une courbe elliptique.

Exercice 6. Soit k un corps algébriquement clos de caractéristique $\neq 2, 3$. Soit E une courbe elliptique d'équation de Weierstrass réduite $y^2 = x^3 + a_4x + a_6$. On pose

$$j(\mathrm{E}) = 1728\frac{4a_4^3}{\Delta}$$

où $\Delta = 4a_4^3 + 27a_6^2$ est le discriminant du polynôme $x^3 + a_4x + a_6$. Montrer les faits suivants :

(1) $j(\mathrm{E})$ ne dépend pas de l'équation de Weierstrass réduite choisie.

(2) $j(\mathrm{E}) = j(\mathrm{E}')$ si et seulement si E et E' sont isomorphes.

(3) Pour $j \neq 0, 1728$ la courbe elliptique d'équation de Weierstrass

$$y^2 = 4x^3 - \frac{27j}{j-1728}x^2 - \frac{27j}{j-1728}$$

   vérifie $j(\mathrm{E}) = j$.

(4) Si k est de caractéristique $p > 0$ on a $j(\mathrm{E}^{(1)}) = j(\mathrm{E})^p$.

(5) Toute courbe supersingulière peut être définie sur $\mathbb{F}_{p^2}$.