ARITHMÉTIQUE DES COURBES ELLIPTIQUES
FEUILLE DE TD 4

Exercice 1. Soient $\Lambda \subset \mathbb{C}$ un réseau, $\mathrm{E} = \mathbb{C}/\Lambda$ la courbe elliptique associée et

$$\mathrm{E} : \qquad y^2 = 4x^3 - g_2 x - g_3$$

l'équation de la courbe via son plongement dans $\mathbb{P}^2(\mathbb{C})$ par $(\wp, \wp')$. Montrer les faits suivants :

(1) $\pi^* \mathrm{d}x/y = \mathrm{d}z$ où $\pi\colon \mathbb{C} \to \mathrm{E}$ est l'application quotient.

(2) La forme différentielle $\mathrm{d}x/y$ sur E est invariante par translation.

Exercice 2. Soient E une courbe elliptique sur un corps parfait k, $\mu, p, q\colon \mathrm{E} \times \mathrm{E} \to \mathrm{E}$ la loi de groupe, la première et la deuxième projection respectivement, et ω une forme différentielle sur E. Montrer les faits suivants :

(1) $\mu^*\omega = p^*\omega + q^*\omega$.

(2) $t_x^*\omega = \omega$ où $t_x\colon \mathrm{E} \to \mathrm{E}$ est la translation par un point $x \in \mathrm{E}(k)$.

(3) $[m]^*\omega = m\omega$ pour tout $m \in \mathbb{Z}$.

(4) $(f+g)^*\omega = f^*\omega + g^*\omega$ pour toute isogénie $f, g\colon \mathrm{E} \to \mathrm{E}$.

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

(1) Si $\mathrm{char}(k) = 0$, pour tout $m \in \mathbb{Z}$ l'isogénie $[m]$ a degré m^2 et $\mathrm{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.

(2) Si $\mathrm{char}(k) = p > 0$, $[m]$ est séparable si et seulement si $p \nmid m$.

Dans la suite on suppose que, pour toute isogénie $f, g\colon \mathrm{E} \to \mathrm{E}'$, l'isogénie $\hat{f} + \hat{g}$ est duale à $f + g$.

(3) L'isogénie $[m]$ est auto-duale pour tout $m \in \mathbb{Z} \smallsetminus \{0\}$.

(4) $\deg\,[m] = m^2$.

(5) Si m n'est pas divisible par la caractéristique de k, alors $\mathrm{E}[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.

(6) Si $\mathrm{char}(k) = p > 0$, on a

$$\mathrm{E}[p^n] = \mathbb{Z}/p^n\mathbb{Z} \text{ pour tout } n \geqslant 1 \qquad \text{ou} \qquad \mathrm{E}[p^n] = 0 \text{ pour tout } n \geqslant 1.$$

(7) On suppose de plus $\mathrm{E}[p^n] = \mathbb{Z}/p^n\mathbb{Z}$ pour tout $n \geqslant 1$. Alors $\mathrm{End}\,\mathrm{E}$ est commutatif.

Exercice 4. Soit E une courbe elliptique sur un corps parfait k. Montrer les faits suivants :

(1) L'application qui associe à un endomorphisme f de E l'application linéaire $\omega \mapsto f^*\omega$ sur $\mathrm{H}^0(\mathrm{E}, \Omega^1_{\mathrm{E}})$ est un morphisme d'anneaux

$$\alpha\colon \quad \mathrm{End}\,\mathrm{E} \longrightarrow \mathrm{End}\,\mathrm{H}^0(\mathrm{E}, \Omega^1_{\mathrm{E}}) \;=\; k.$$

(2) L'application linéaire $\omega \mapsto f^*\omega$ est non nulle si et seulement si f est séparable.

(3) Le morphisme α est injectif si et seulement $\mathrm{char}(k) = 0$.

(4) Si k est caractéristique nulle, alors $\mathrm{End}\,\mathrm{E}$ est commutatif.

Exercice 5. Soit E la courbe elliptique sur $\bar{\mathbb{F}}_p$ avec $p \geqslant 5$ d'équation $y^2 = x^3 + 1$. On considère l'endomorphisme f de E donné par $(x, y) \mapsto (ux, y)$ où $u^3 = 1$ et $u \neq 1$. Montrer que

$$f \text{ et } \mathrm{Fr}_p \text{ commutent} \iff p \equiv 1 \pmod 3.$$

Exercice 6. Soit E la courbe elliptique sur $\bar{\mathbb{F}}_p$ avec $p \geqslant 3$ d'équation $y^2 = x^3 + x$. On considère l'endomorphisme f de E donné par $(x, y) \mapsto (-x, uy)$ où $u^2 = -1$. Montrer que

$$f \text{ et } \mathrm{Fr}_p \text{ commutent} \iff p \equiv 1 \pmod 4.$$

Exercice 7. Calculer les points de 2-torsion des courbes elliptiques sur $\bar{\mathbb{F}}_2$ données par les équations suivantes :

$$y^2 + y = x^3, \qquad y^2 + xy = x^3 + 1.$$