

ARITHMÉTIQUE DES COURBES ELLIPTIQUES

FEUILLE DE TD 4

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

$$E : y^2 = 4x^3 - g_2x - g_3$$

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

- (1) $\pi^*dx/y = dz$ où $\pi: \mathbb{C} \rightarrow E$ est l'application quotient.
- (2) La forme différentielle dx/y sur E est invariante par translation.

Exercice 2. Soient E une courbe elliptique sur un corps parfait k , $\mu, p, q: E \times E \rightarrow E$ 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 $t_x: E \rightarrow E$ est la translation par un point $x \in E(k)$.
- (3) $[m]^*\omega = m\omega$ pour tout $m \in \mathbb{Z}$.
- (4) $(f+g)^*\omega = f^*\omega + g^*\omega$ pour toute isogénie $f, g: E \rightarrow E$.

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

- (1) Si $\text{char}(k) = 0$, pour tout $m \in \mathbb{Z}$ l'isogénie $[m]$ a degré m^2 et $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.
- (2) Si $\text{char}(k) = p > 0$, $[m]$ est séparable si et seulement si $p \nmid m$.

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

- (3) L'isogénie $[m]$ est auto-duale pour tout $m \in \mathbb{Z} \setminus \{0\}$.
- (4) $\deg [m] = m^2$.
- (5) Si m n'est pas divisible par la caractéristique de k , alors $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.
- (6) Si $\text{char}(k) = p > 0$, on a

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

- (7) On suppose de plus $E[p^n] = \mathbb{Z}/p^n\mathbb{Z}$ pour tout $n \geq 1$. Alors $\text{End } E$ 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 $H^0(E, \Omega_E^1)$ est un morphisme d'anneaux

$$\alpha: \text{End } E \longrightarrow \text{End } H^0(E, \Omega_E^1) = k.$$

- (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 si $\text{char}(k) = 0$.
- (4) Si k est caractéristique nulle, alors $\text{End } E$ est commutatif.

Exercice 5. Soit E la courbe elliptique sur $\mathbb{F}_p$ avec $p \geq 5$ 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

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

Exercice 6. Soit E la courbe elliptique sur $\bar{\mathbb{F}}_p$ avec $p \geq 3$ 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

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

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

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