# EXERCICES SUR LES POINTS DE TORSION

Dans toute cette feuille $k$ désigne un corps algébriquement clos.

## 1. Plongements

Soit $E$ une courbe elliptique d'élément neutre $o \in E$. Pour tout $m \geqslant 1$ on considère l'application $\iota_m \colon E \to \mathbb{P}(\mathcal{L}^*_{m[0]})$. Soit $f \in \mathcal{L}_{2[0]}$ non constante et soit $g \in \mathcal{L}_{3[0]}$ telle que $1, f, g$ forment une base de $\mathcal{L}_{3[0]}$.

**Exercice 1.1** ([Silverman, Chapitre III, Ex. 3.10])**.** Montrer les assertions suivantes :

(1) $\iota_4$ est une immersion fermée.

(2) L'application $\iota_4$, pour tout $p \in E \smallsetminus \{0\}$ est donné par
$$\iota_4(p) = [1 : f(p) : g(p) : f(p)^2].$$

(3) L'image de $\iota_4$ est donnée par une intersection de deux quadriques dans $\mathbb{P}^3$.

(4) Étant donné un plan $H \subset \mathbb{P}^3$, l'intersection est formée exactement de 4 points (en comptant la multiplicité).

(5) L'hyperplan d'équation $T_0 = 0$ rencontre $\iota_4(E)$ en le point $\iota_4(o)$ avec multiplicité 4.

(6) Étant donnés $p_1, \ldots, p_4 \in E$, on a $p_1 + \cdots + p_4 = o$ si et seulement si $\iota_4(p_1), \ldots, \iota_4(p_4)$ sont coplanaires.

(7) Un point $p \in E$ est de 4-torsion si et seulement si il existe un hyperplan qui rencontre $\iota_4(E)$ en $p$ avec multiplicité 4.

(8) Si la caractéristique du corps $k$ est différente de 2 il y a exactement 16 points de 4-torsion. (Indication : $p$ est de 4-torsion si et seulement si $p+p+2p = 0$.)

(9) Si $\mathrm{car}(k) \neq 2$, trouver un changement de variables pour lequel $\iota_4(E)$ a équations
$$t_0 t_3 = t_0^2 + t_2^2,$$
$$t_2 t_3 = t_1^2 + \alpha t_2^2,$$
pour un certain $\alpha \in k$. (Indication : que remarque-t-on sur ces deux formes quadratiques ?)

Réciproquement, étant donné des équations comme ci-dessus, pour quelles valeurs de $\alpha$ la courbe associée est non singulière ?

**Exercice 1.2** ([Silverman, Chapitre III, Ex. 3.11])**.** Montrer les assertions suivantes :

(1) Pour $m \geqslant 3$, $\iota_m$ est une immersion fermée.

(2) Les fonctions rationelles $1, f, f^2, \ldots, f^{\lfloor m/2 \rfloor}, g, fg, \ldots, f^{\lfloor (m-3)/2 \rfloor} g$ forment une base du $k$-espace vectoriel $\mathcal{L}_{m[o]}$.

(3) L'image d'un point $p \in E \smallsetminus \{0\}$ par $\iota_m$ est
$$[1 : f(p) : \cdots : f(p)^{\lfloor m/2 \rfloor} : g(p) : f(p)g(p) : \cdots : f(p)^{\lfloor (m-3)/2 \rfloor} g(p)].$$

(4) L'hyperplan d'équation $T_0 = 0$ rencontre $\iota_m(E)$ en le point $\iota_m(o)$ avec multiplicité $m$.

(5) Étant donné un hyperplan $H \subset \mathbb{P}^{m-1}$, l'intersection est formée exactement de $m$ points (en comptant la multiplicité). On dit que $\iota_m(E)$ est une courbe de degré $m$.

(6) Étant donnés $p_1, \ldots, p_m \in E$, on a $p_1 + \cdots + p_m = o$ si et seulement si $\iota_m(p_1), \ldots, \iota_m(p_m)$ sont contenus dans un hyperplan.

(7) Un point $p \in E$ est de $m$-torsion si et seulement s'il existe un hyperplan qui rencontre $\iota_m(E)$ en $p$ avec multiplicité $m$.

(8) $(*)$ Si la caractéristique du corps $k$ est $> m$ ou nulle, montrer qu'il y a exactement $m^2$ points de $m$-torsion.

**Exercice 1.3.** On considère la courbe $E$ donnée par l'équation

$$y^2 + xy = x^3 + ax + b,$$

avec $a, b \in k$.

(1) Pour quelles valeurs de $a, b \in k$ la courbe $E$ est non singulière ?

(2) Montrer que, pour un point $p = (x, y)$ on a $-p = (x, -x - y)$.

(3) Si la caractéristique de $k$ est 2, calculer les points de 2-torsion de $E$.

## 2. Multiplication par $m$ explicite

Le but de cet exercice ([Silverman, Chapitre III, Ex. 3. 7]) est de donner explicitement les polynômes définissant la multiplication par $m \in \mathbb{N}$ sur une courbe elliptique $E \subset \mathbb{P}^2(k)$ d'équation

$$y^2 = x^3 + ax + b.$$

On suppose que la caractéristique du corps $k$ soit différente de 2, 3 et on considère les « polynômes de division » $\psi_m \in \mathbb{Z}[A, B, x, y]$ définis de manière inductive comme il suit :

$$\begin{aligned}
\psi_1 &= 1, \\
\psi_2 &= 2y, \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3), \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, && (m \geqslant 2), \\
2y\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), && (m \geqslant 3).
\end{aligned}$$

**Exercice 2.1.** Montrer que les $\psi_{2m}$ sont des polynômes.

On définit de plus :

$$\begin{aligned}
\varphi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\
4y\omega_m &= \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2.
\end{aligned}$$

**Exercice 2.2.** Montrer que, pour $m$ impair, les polynômes $\psi_m$, $\varphi_m$, $y^{-1}\omega_m$ ne font intervenir que les variables $A$, $B$, $x$ et $y^2$. Pour $m$ pair prouver que la même conclusion est vraie pour les polynômes $(2y)^{-1}\psi_m$, $\varphi_m$, $\omega_m$.

Dans l'expression des polynômes $\psi_m$, $\varphi_m$, $y^{-1}\omega_m$ ($m$ impair) et $(2y)^{-1}\psi_m$, $\varphi_m$, $\omega_m$ ($m$ pair) le terme $y^2$ par $x^3 + Ax + B$. Autrement dit, on regarde l'image de ces polynômes dans l'anneau

$$\mathbb{Z}[A, B, x, y^2]/(y^2 - (x^3 + Ax + B)).$$

**Exercice 2.3.** Montrer les faits suivants :

(1) En la variable $x$ on a

$$\varphi_m(x) = x^{m^2} + \text{termes de degré plus petit},$$
$$\psi_m(x)^2 = m^2 x^{m^2-1} + \text{termes de degré plus petit}.$$

(2) Si le discriminant $\Delta := -16(4a^3 + 27b^2)$ est non nul dans $k$, les polynômes $\varphi_m(x), \psi_m(x)^2 \in k[x]$ sont premiers entre eux.

(3) Sous l'hypothèse $\Delta \neq 0$, pour un point non nul $p \in E$ on a

$$[m]p = \left( \frac{\varphi_m(p)}{\psi_m(p)^2}, \frac{\omega_m(p)}{\psi_m(p)^3} \right).$$

(4) L'application « multiplication par $m$ » a degré $m^2$.

**Exercice 2.4.** Soit $E$ une courbe elliptique d'élément neutre $o$. Soit $f\colon E \to E$ un morphisme de courbes tel que $f(o) = o$. Montrer les faits suivants :

(1) L'application $f$ est un homomorphisme de groupes.

(2) Si $f$ est séparable, $f$ est non ramifié.

Soit $m \geqslant 1$ un entier. Si la caractéristique $p$ du corps $k$ est positive on suppose que $m$ ne soit pas divisible par $p$. Montrer les faits suivants :

(3) L'application de multiplication par $m$, $[m]\colon E \to E$ est séparable.

(4) Les points de $m$-torsion forment un sous-groupe $E[m]$ isomorphe à $(\mathbb{Z}/m\mathbb{Z})^2$.

(5) Si $k = \bar{\mathbb{F}}_p$, montrer que tout point de $E$ est de torsion.

(6) Si $k$ est non dénombrable, montrer qu'il existe un point d'ordre infini.

(7) Que dire pour $k = \bar{\mathbb{Q}}$ ?