

TD2 - Torsion, isogénie et courbes elliptiques sur les corps finis

Exercice 1. Montrer que la composition d'endomorphismes inséparables est inséparable.

Exercice 2. On pose $E: y^2 = x^3 + 1$ sur $\mathbb{F}_5$.

1. Vérifier qu'il s'agit bien d'une courbe elliptique.
2. Calculer ψ_3 , le polynôme de 3-division de E .
3. Quels sont les points de 3-torsion de $E(\mathbb{F}_5)$?
4. Déterminer des générateurs de la 3-torsion de E . Quelle est la plus petite extension K de $\mathbb{F}_5$ telle que $E[3] \subseteq E(K)$?

Exercice 3. On pose $\mathbb{F}_9 = \mathbb{F}_3[i] = \mathbb{F}_3[X]/\langle X^2 + 1 \rangle$ (i est la classe de X dans $\mathbb{F}_3[X]/\langle X^2 + 1 \rangle$, i.e. $i^2 = -1$). On pose $E: y^2 = x^3 + x + i$ sur $\mathbb{F}_9$.

1. Montrer que les carrés de $\mathbb{F}_9$ sont $\{0, 1, 2, i, 2i\}$.
2. Montrer que pour tout $x = a + ib \in \mathbb{F}_9$, $x^3 + x + i = 2a + i$.
3. En vous servant de la question précédente montrer que $\#E(\mathbb{F}_9) = 7$. On admettra que $\#E(\mathbb{F}_{81}) = 91$.
4. On admettra que le polynôme de 4-division de E est

$$\psi_4 = 2X^9 + X + 2i = 2(X^3 + X + i)(X^3 + X + i + 1)(X^3 + X + i + 2).$$

- (a) Pourquoi peut-on affirmer que les trois polynômes de la factorisation de ψ_4 sont-ils irréductibles ?
- (b) Pourquoi peut-on affirmer que la 4-torsion de E est dans $E(\mathbb{F}_{9^3})$?

Exercice 4. Soit k un corps de caractéristique p et $f \in k[X]$ un polynôme.

1. Montrer que $f' = 0$ si, et seulement si $f(X) = g(X^p)$ pour un certain $g \in k[X]$.
2. On pose $\phi: E_1 \rightarrow E_2$ une isogénie telle que $\phi(x, y) = \left(\frac{U_1(x)}{V_1(x)}, y \frac{U_2(x)}{V_2(x)}\right)$ avec U_1 et V_1 premiers entre eux.
 - (a) Montrer que si ϕ est inséparable si et seulement si $U_1' = V_1' = 0$, i.e. $\frac{U_1(x)}{V_1(x)} = r(x^p)$ pour un certain $r \in k(X)$.
 - (b) En déduire que si ϕ est inséparable alors $p \mid \deg \phi$.
 - (c) En déduire que si m et p sont premiers entre eux alors $[m]_{E_1}$ est toujours séparable.
3. On admet qu'une isogénie inséparable ϕ peut toujours s'écrire

$$\phi(x, y) = (r(x^p), y^p s(x^p))$$

pour certains $r, s \in k(X)$.

- (a) En déduire qu'on peut écrire $\phi = \psi \circ \phi_p$ avec $\phi_p(x, y) = (x^p, y^p)$ et ψ une isogénie que l'on précisera (attention aux domaines!).
- (b) En déduire que la somme d'isogénies inséparable reste inséparable.

Exercice 5. On considère deux isogénies $\phi = \left(\frac{U}{V}, y \frac{U_2}{V_2}\right)$ et $\psi = \left(\frac{u}{v}, y \frac{u_2}{v_2}\right)$ entre courbes elliptiques telles que $\phi \circ \psi$ ait un sens. On note $N = \deg U, M = \deg V, n = \deg u$ et $m = \deg v$. On pose $U = X^N + \sum_{i=0}^{N-1} a_i X^i$ et $V = X^M + \sum_{j=0}^{M-1} b_j X^j$. On souhaite montrer que $\deg(\phi \circ \psi) = \deg(\phi) \deg(\psi)$.

1. Montrer que $\frac{U\left(\frac{u}{v}\right)}{V\left(\frac{u}{v}\right)} = \frac{u^N + a_{N-1}u^{N-1}v + \dots + a_0v^N}{u^M v^{N-M} + b_{M-1}u^{M-1}v^{N-M+1} + \dots + b_0v^N}$.
2. On suppose que $N > M$. Montrer que $\deg(a_k u^{N-k} v^k) \leq (N-k)n + km$ et $\deg(b_k u^{M-k} v^{N-M+k}) \leq (M-k)n + (N-M+k)m$.
3. En déduire le résultat lorsque $n \neq m$.
4. Traiter le cas manquant $n = m$.