MAT 562 - Exercices du chapitre 5

Dans tous les exercices, la lettre p désigne un nombre premier différent de 2 et la lettre q une puissance de p.

Exercice 1. On suppose k algébriquement clos de caractéristique différente de 2 et 3.

a) Soit E une courbe elliptique sur k donnée par l'équation $Y^2 = X^3 + AX + B$. Montrer que $(x, y) \to (x, -y)$ est un endomorphisme de E.

b) Soit E une courbe elliptique sur k donnée par l'équation $Y^2 = X^3 + B$. Montrer que $(x, y) \to (\zeta x, -y)$, où $\zeta^3 = 1$ une racine primitive de l'unité, est un endomorphisme de E.

c) Soit E une courbe elliptique sur k donnée par l'équation $Y^2 = X^3 + AX$. Montrer que $(x, y) \to (-x, iy)$ est un endomorphisme de E dans lui-même.

Exercice 2. On suppose k algébriquement clos de caractéristique différente de 2 et de 3. Soit E une courbe elliptique donnée par une équation $Y^2 = X^3 + AX + B$. On définit le j-invariant de E par la formule

$$j = j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

a) Soient E_1 et E_2 deux courbes elliptiques données par des équations $y^2 = x^3 + A_i x + B_i$. Montrer que si $j(E_1) = j(E_2)$, alors il existe $\mu \in k^\times$ tel que $A_2 = \mu^4 A_1$ et $B_2 = \mu^6 B_1$.

b) En déduire que l'application $(x, y) \mapsto (\mu^2 x, \mu^3 y)$ induit un isomorphisme de groupes de E_1 sur E_2.

Exercice 3. Soit E la courbe elliptique définie sur $\mathbb{F}_q$. Vérifier que $\phi_q - 1$ est séparable.

Exercice 4. Soit E la courbe elliptique $Y^2 = X^3 + X + 1$ sur $\mathbb{F}_5$.

a) Montrer que $|E(\mathbb{F}_5)| = 9$.

b) Montrer que $[3](0, 1) = (2, 1)$ sur E.

c) Montrer que $(0, 1)$ engendre le groupe $E(\mathbb{F}_5)$.

Exercice 5. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Montrer que le groupe $E(\mathbb{F}_q)$ est isomorphe au groupe $\mathbb{Z}/n_1 \oplus \mathbb{Z}/n_2$ pour certains $n_1 \geqslant 1$ et $n_2 \geqslant 1$ tels que $n_1 \mid n_2$.

Exercice 6. Soit k un corps algébriquement clos et E une courbe elliptique définie sur k. Soit $\alpha \in \operatorname{End} E$ un endomorphisme séparable et $f \in k(E)$.

a) Soit $P \in E \smallsetminus E[2]$. Montrer que la fonction rationnelle $X - x_P$ est une uniformisante de E en P.

b) Montrer que si $P \in E \smallsetminus \alpha^{-1}(E[2])$, en déduire que $\operatorname{ord}_{f(P)}(f \circ \alpha) = \operatorname{ord}_P(f)$.

c) En déduire que pour tout $P \in E$, on a $\operatorname{ord}_{f(P)}(f \circ \alpha) = \operatorname{ord}_P(f)$.

Exercice 7. Soit k un corps algébriquement clos ainsi que E et E' deux courbes elliptiques définie sur k. Soit $\alpha \in \mathrm{Hom}(E, E')$.

a) Si E est la courbe elliptique d'équation $y^2 - (x^3 + ax + b) = 0$ et $n \geqslant 1$, on note $E^{(p^n)}$ la courbe elliptique d'équation $y^2 - (x^3 + a'x + b') = 0$ avec $(a')^{p^n} = a$ et $(b')^{p^n} = b$. Montrer qu'il existe $n \geqslant 0$ et $\beta \in \mathrm{Hom}(E^{(p^n)}, E')$ séparable tels que $\alpha = \beta \circ \phi_p^n$.

b) En déduire que si $P \in E$, et $f \in k(E')$, alors $\mathrm{ord}_P(f \circ \alpha) = p^n \,\mathrm{ord}_{f(P)}(f)$.

Exercice 8. Soit k un corps algébriquement et soit E une courbe elliptique définie sur k. Soit $N \in \mathbb{N}_{\geqslant 1}$ premier à la caractéristique de k.

a) Soit $T \in E[N]$ et soit $T' \in E$ tel que $[N](T') = T$. Montrer qu'il existe deux fonctions $f_T, g_T \in k(E)$ telles que

$$\mathrm{div}(f_T) = \sum_{P \in E[N]} (N[T] - N[0]), \quad \mathrm{div}(g_T) = \sum_{P \in E[N]} ([T' + P] - [P]).$$

b) Montrer qu'il existe $\lambda \in k^\times \smallsetminus \{0\}$ tel que $g_T^N = \lambda(f_T \circ [N])$.

c) En déduire que pour tout $S \in E[N]$, il existe un unique $e_N(S, T) \in \mu_N$ tel que

$$g_T(X + S) = e_N(S, T) g_T(X).$$

d) Montrer que l'application e_N est linéaire à gauche.

e) Si T_1 et T_2 sont deux points de $E[N]$, notons $h \in k(E)$ telle que $\mathrm{div}(h) = (T_1 + T_2) - (T_1) - (T_2) + (0)$. Montrer alors qu'il existe des éléments non nuls c et c' de k tels que

$$f_{T_1+T_2} = c f_{T_1} f_{T_2} h^N, \quad g_{T_1+T_2} = c' g_{T_1} g_{T_2} (h \circ [N]).$$

En déduire que e_N est linéaire à droite.

f) En considérant son diviseur, montrer que la fonction rationnelle $\prod_{i=0}^{N-1} f(X + [i]T)$ est constante. En déduire qu'il en est de même de la fonction $\prod_{i=0}^{N-1} g(X + [i]T')$.

g) Montrer que pour tout $T \in E[N]$, on a $e_N(T, T) = 1$.

h) Soient $\alpha \in \mathrm{End}\, E$ de degré premier à N, $T \in E[N]$ et $[N]T = T'$. Si g' vérifie

$$\mathrm{Div}(g') = \sum_{P \in E[N]} [\alpha(T') + P] - [P],$$

montrer que $g' \circ \alpha = g^{\deg \alpha}$.

i) En déduire que $e_N(\alpha(S), \alpha(T)) = e_N(S, T)^{\deg \alpha}$.