MAT 562 - Exercices du chapitre 3

Exercice 1. Soit E une courbe elliptique sur un corps algébriquement clos k. Soient O et A deux points de E. Montrer que, pour tous $P, Q \in E$, on a $P +_A Q = P +_O Q -_O A$. En déduire que $(E, +_O)$ et $(E, +_A)$ sont isomorphes.

Exercice 2. Soit C une courbe projective plane irréductible et lisse sur un corps algébriquement clos k.

a) Soit $f \in k(C)^\times$. Le diviseur de f est défini par :

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) \cdot (P).$$

Montrer que ce diviseur est bien défini, et que $\deg \mathrm{div}(f) = 0$. *Pour ce dernier point, on pourra utiliser la version suivante du théorème de Bezout, plus générale que celle du cours : si C et C' sont deux courbes projectives planes irréductibles distinctes et si C est lisse, alors $C \cap C'$ est fini et :*

$$\sum_{P \in C \cap C'} m_P(C, C') = (\deg C)(\deg C').$$

b) Soit E une courbe elliptique sur k. On se donne des entiers n_P pour $P \in C$ tels que $\sum_P n_P = 0$ et $\sum_P n_P P = 0$. Montrer qu'il existe $f \in k(C)^\times$ tel que $\mathrm{div}(f) = \sum_P n_P \cdot (P)$.

c) Dans la question précédente, expliquer pourquoi f est unique à multiplication par un élément de $k^\times$ près.

Remarque : si O est l'élément neutre de E et si $Div^0(E)$ est le groupe des diviseurs sur E de degré 0, on peut en fait montrer que l'application $E \to Div^0(E)/\mathrm{div}(k(E)^\times)$ envoyant P sur $(P) - (O)$ est un isomorphisme de groupes.

Exercice 3. Soit k un corps algébriquement clos de caractéristique différente de 2. Soit E une courbe elliptique définie sur k d'équation de Weierstrass $Y^2Z = X^3 + aXZ^2 + bZ^3$, d'élément neutre $0 = (0 : 1 : 0)$. Montrer que l'ensemble

$$\{P \in E,\ [2]P = 0\}$$

est de cardinal 4. En déduire qu'il s'agit d'un sous-groupe de E isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 4. Soit k un corps algébriquement clos de caractéristique différente de 2. Soit E une courbe elliptique définie sur k d'équation de Weierstrass $Y^2Z = X^3 + aXZ^2 + bZ^3$, d'élément neutre $0 = (0 : 1 : 0)$. Soit $P = (x, y) \in E \setminus \{0\}$.

a) Calculer les coordonnées du point $[2]P$.

b) En déduire que l'application $P \mapsto [2]P$ de E dans E est surjective.

c) En déduire le cardinal de $E[4]$ et sa classe d'isomorphisme.

Exercice 5. Soit k un corps algébriquement clos de caractéristique différente de 2 et 3. Soit E une courbe elliptique définie sur k d'équation de Weierstrass $Y^2Z = X^3 + aXZ^2 + bZ^3$, d'élément neutre $0 = (0 : 1 : 0)$.

a) Soit $P = (x, y) \in E \smallsetminus \{0\}$. Montrer que $P \in E[3]$ si et seulement si x est racine de l'équation

$$3x^4 + 6ax^2 + 12bx - a^2 = 0. \tag{1}$$

b) Montrer que l'équation (**??**) n'a que des racines simples et en déduire le cardinal ainsi que la structure du groupe $E[3]$.

c) Déterminer le sous-groupe de 3-torsion de la courbe elliptique E définie par l'équation $Y^2 = X^3 + 1$ et déterminer $E(\mathbb{Q})[3]$.

Exercice 6. Soit k un corps algébriquement clos de caractéristique différente de 3. Montrer que la courbe projective d'équation $X^3 + Y^3 = Z^3$ est lisse. Expliciter la loi de groupe en choisissant pour élément neutre le point $(1 : 0 : 1)$.

Exercice 7. Soit $a \in \mathbb{Z}$ un entier qui n'est divisible par aucune puissance quatrième (sauf 1) et soit E une courbe elliptique $Y^2 = X^3 + aX$. On se propose de trouver tous les points d'ordre 2^n de $E(\mathbb{Q})$.

a) Déterminer tous les points d'ordre 2.

b) Soient $(x, y), (u, v) \in E$ avec $(x, y) = [2](u, v)$. Montrer que $x = (u^2 - a)^2/4v^2$.

c) Soit $P \in E(\mathbb{Q})$ un point d'ordre 2. Montrer que $P = [2]Q$ implique $a = 4$. Trouver les points d'ordre 4.

d) Conclure.