TD 5. Courbes elliptiques

Exercice 1

1. On considère une courbe elliptique E dont la partie affine a pour équation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ , \tag{1}$$

où les cœfficients a_i appartiennent à un corps K.

a) Écrire le polynôme homogène associé à l'équation ci-dessus et vérifier que la partie à l'infini de E est constituée du seul point de coordonnées homogènes $(0:1:0)$.

b) On suppose que la caractéristique de K est différente de 2. Appliquer le changement de variable $y' = \frac{1}{2}(y - a_1x - a_3)$ à l'équation (1) pour obtenir une équation de la forme :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \ . \tag{2}$$

On donnera l'expression des cœfficients b_i en fonction des a_i.

c) On pose :

$$\begin{array}{rcl} b_8 & = & a_1^2a_6 + 4a_2a_4 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 & = & b_2^2 - 24b_4 \\ c_6 & = & -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta & = & -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j & = & c_4^3/\Delta \end{array}$$

Vérifier que

$$4b_8 = b_2b_6 - b_4^2 \quad \text{et} \quad 1728\Delta = c_4^3 - c_6^2 \ .$$

d) On suppose de plus que la caractéristique de K est différente de 3. En remplaçant (x, y) par $\left(\frac{1}{36}(x - 3b_2), \frac{1}{108}y\right)$, montrer que l'équation (2) devient :

$$y^2 = x^3 - 27c_4x - 54c_6 \ . \tag{3}$$

2. Calculer le discriminant Δ et l'invariant j pour les courbes elliptiques d'équations $y^2 + y = x^3$, $y^2 = x^3 + x$ et

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728} \ ,$$

où j_0 est un nombre réel distinct de 0 et de 1728.

3. On suppose toujours que la caractéristique de K est différente de 2 et 3. On considère une courbe elliptique E d'équation

$$y^2 = x^3 + Ax + B$$

a) Exprimer le discriminant Δ et l'invariant j en fonction de A et B.

b) Soit $u \in K^\times$, on considère le changement de variables $x = u^2x'$, $y = u^3y'$. Déterminer les nombres A' et B' tels que l'équation de E dans les nouvelles variables soit donnée par $y'^2 = x'^3 + A'x' + B'$. Calculer Δ' et j'. Que remarque-t-on ?

c) On suppose maintenant que E a le même invariant j que la courbe elliptique E' d'équation $y^2 = x^3 + A'x + B'$. Montrer que

$$A^3B'^2 = A'^3B^2 \ .$$

En déduire un changement de variables de la forme $x = u^2x'$, $y = u^3y'$, qui envoie E sur E' (on traitera à part les cas $A = 0$ et $B = 0$).

Exercice 2

Soit E la courbe elliptique d'équation $y^2 = x^3 + 17$

a) Vérifier que les points $P_1 = (-2, 3)$, $P_2 = (-1, 4)$, $P_3 = (2, 5)$, $P_4 = (4, 9)$, $P_5 = (8, 23)$, $P_6 = (43, 282)$, $P_7 = (52, 375)$, $P_8 = (5234, 378661)$ appartiennent à E.

b) Pour $P \in E$ et $m \in \mathbb{Z}$, on note $[m]P = P + \cdots + P$ (m termes) si $m \geq 0$, $[m]P = [-m](-P)$ si $m < 0$. À l'aide des formules d'addition, vérifier les relations :

$$P_5 = [-2]P_1 \ , \quad P_4 = P_1 - P_3 \ , \quad [3]P_1 - P_3 = P_7$$

Les 16 points $\pm P_i$, $1 \leq i \leq 8$, sont les seuls points à coordonnées entières de E. Par ailleurs, tous les points à coordonnées rationnelles de E sont de la forme $[m]P_1 + [n]P_3$ avec $m, n \in \mathbb{Z}$.