EXERCICES SUR LA LOI DE GROUPE

Dans toute cette feuille k désigne un corps algébriquement clos.

Exercice 0.1. Soit $f \in k[x, y]$ un polynôme de degré 3 tel que la courbe projective plane correspondante n'a pas de points singuliers. Montrer les faits suivants :

(1) Il existe un changement affine de coordonnées tel que f peut-être mis sous *forme de Weierstrass*,

$$y^2 + ay = x^3 + b_1x^2 + b_2x + b_3.$$

(Indication : utiliser le théorème de Riemann-Roch). Si $\mathrm{char}(k) \neq 2$ donner une preuve basée sur l'existence d'un point d'inflexion.

(2) Si la caractéristique de k est différente de 2, f peut-être mis sous *forme de Legendre*

$$y^2 = x^3 + b_1x^2 + b_2x + b_3.$$

(3) Si la caractéristique de k est différente de 2 et 3, f peut-être mis sous la forme suivante

$$y^2 = 4x^3 - g_2x - g_3,$$

qu'on va appeler *forme de Weierstrass simple*.

Exercice 0.2. On suppose que la caractéristique du corps k est différente de 2 et 3. Soient $p_1 = (x_1, y_1)$, $p_2 = (x_2, y_2)$ deux points distincts de la courbe elliptique $E \subseteq \mathbb{P}^2(k)$ d'équation affine

$$y^2 = 4x^3 - g_2x - g_3.$$

On va déterminer les coordonnées (x_3, y_3) du point $p_3 = -(p_1 + p_2)$ pour la loi de groupe sur E ayant le point à l'infini o comme élément neutre.

(1) Si $x_1 = x_2$ montrer l'égalité $p_3 = o$;

(2) Si $x_1 \neq x_2$ montrer que

$$x_1 + x_2 + x_3 = \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2.$$

En déduire la valeur de y_3.

On considère le changement de carte $u = \frac{x}{y}$ et $v = \frac{1}{y}$ et on pose $u_i = \frac{x_i}{y_i}$, $v_i = \frac{1}{y_i}$ pour $i = 1, 2, 3$.

(3) Montrer que dans la carte $\{[x_0 : x_1 : x_2] \in \mathbb{P}^2(k) : x_0 \neq 0\}$ on a

$$\frac{u_3}{v_3} = \frac{1}{4}\left(\frac{v_1 - v_2}{v_1u_2 - v_2u_1}\right)^2 - \frac{v_1u_2 + v_2u_1}{v_1v_2}.$$

On considère la courbe cuspidale $X \subset \mathbb{P}^2(k)$ d'équation affine $y^2 = 4x^3$.

(4) Montrer que $X \smallsetminus \{[1 : 0 : 0]\}$ est isomorphe à la droite affine $\mathbb{A}^1(k)$.

(5) Vérifier que la loi de groupe à la question 3 induit sur $X \smallsetminus \{[1 : 0 : 0]\}$ la loi de groupe additive.

Exercice 0.3. On considère la courbe elliptique $E \subset \mathbb{P}^2(k)$ d'équation affine

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Soient $p_1 = (x_1, y_1)$, $p_2 = (x_2, y_2)$ deux points distincts de la courbe elliptique. On pose :

$$q = \frac{y_2 - y_1}{x_2 - x_1}, \qquad r = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}.$$

(1) Soient (x_3, y_3) les coordonnées du point $-p_1 - p_2$ pour la loi de groupe sur E ayant le point à l'infini comme élément neutre. Alors, si $x_1 \neq x_2$,

$$x_1 + x_2 + x_3 = q^2 + a_1q - a_2, \qquad y_3 = (q + a_1)x_3 + r + a_3.$$

On considère la courbe nodale Y d'équation affine $y^2 = x^3 - x^2$.

(2) Montrer que $Y \smallsetminus \{[1 : 0 : 0]\}$ est isomorphe, en tant que courbe algébrique, à la droite affine privée de l'origine.

(3) Déterminer les tangentes T_1, T_2 au point singulier $\{[1 : 0 : 0]\}$.

(4) Déterminer la loi de groupe de E dans la carte $\mathbb{P}^2 \smallsetminus T_1$.

(5) Montrer que la loi de groupe induite sur $Y \smallsetminus \{[1 : 0 : 0]\}$ est celle du groupe multiplicatif $\mathbb{G}_m(k) = k^*$.