

EXERCICES SUR LA LOI DE GROUPE D'UNE COURBE ELLIPTIQUE

Dans toute cette feuille k désigne un corps algébriquement clos.

1. POINTS D'INFLEXION

Soit $f \in k[x_0, x_1, x_2]$ un polynôme homogène de degré d et soit $X \subset \mathbb{P}^2(k)$ la courbe algébrique associée.

Exercice 1.1 (Formule d'Euler). Montrer l'égalité suivante :

$$\deg(f)f = \sum_{i=0}^2 x_i \frac{\partial^2 f}{\partial x_i^2}.$$

Définition 1.2. Un point lisse x de X est appelé *point d'inflexion* si la multiplicité d'intersection de X avec la droite tangente à x est > 2 . Si la droite tangente à x n'est pas une composante de X , on dira que x est un point d'inflexion *propre*.

Définition 1.3. L'*hessienne* de f est le polynôme homogène de degré $3(d-2)$ suivant :

$$\text{Hess}(f) = \det \left(\frac{\partial^2 f}{\partial x_i \partial x_j} : i, j = 0, 1, 2 \right).$$

Exercice 1.4. Montrer la relation suivante :

$$\text{Hess}(f) = \det \begin{pmatrix} d(d-1)f & (d-1)f_{x_1} & (d-1)f_{x_2} \\ (d-1)f_{x_1} & f_{x_1 x_1} & f_{x_1 x_2} \\ (d-1)f_{x_2} & f_{x_1 x_2} & f_{x_2 x_2} \end{pmatrix},$$

où, pour un polynôme $g \in k[x_0, x_1, x_2]$, on pose $g_{x_i} = \frac{\partial g}{\partial x_i}$. En particulier, $\text{Hess}(f) = 0$ si la caractéristique de k divise $d-1$.

Exercice 1.5. On suppose $d \geq 3$ et que la caractéristique du corps k est $> d$. Montrer les faits suivants :

- (1) $\text{Hess}(f)$ est un multiple de f si et seulement si X est une union de droites.
- (2) Soit $p \in X$ un point lisse et L la droite tangente à X en p . Alors $\text{Hess}(f)$ s'annule en p si et seulement si la multiplicité d'intersection de L avec X en x est > 2 . (Indication : on choisira des coordonnées telles que $p = [1 : 0 : 0]$ et L est d'équation $x_2 = 0$.)
- (3) Si $\text{Hess}(f)$ n'est pas un multiple de f , l'intersection de f et $\text{Hess}(f)$ consiste des points singuliers de X et des points d'inflexion de X .
- (4) Soit $p \in X$ un point tel que la tangente de L en p ne soit pas une composante irréductible de X . Alors,

$$i_p(X, L) = i_p(\text{Hess}(f), f) + 2.$$

- (5) On suppose k de caractéristique 3. Montrer que tous les points lisses de la courbe d'équation $x_2^2 x_0 = x_1^3$ sont des points d'inflexion.

Exercice 1.6. Soit $E \subset \mathbb{P}^2(k)$ une courbe elliptique ayant comme élément neutre un point d'inflexion. Montrer les faits suivants :

- (1) un point $p \in E$ est de 3-torsion (*i.e.* $3p = 0$ dans E) si et seulement si p est un point d'inflexion ;
- (2) si k est caractéristique différente 2, 3 il y a exactement 9 points de 3-torsion.

2. FORMULES EXPLICITES POUR LA LOI DE GROUPE ET DÉGÉNÉRESCENCE

Exercice 2.1. 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*,

$$y^2 + a_1xy + a_2y = x^3 + b_1x^2 + b_2x + b_3.$$

(Indication : utiliser le théorème de Riemann-Roch). Si $\text{car}(k) \neq 2, 3$ 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 2.2. 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 $E \subset \mathbb{P}^2(k)$ 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 $X \setminus \{[1 : 0 : 0]\}$ est isomorphe à la droite affine $\mathbb{A}^1(k)$.
 (5) Vérifier que la loi de groupe à la question 3 induit sur $X \setminus \{[1 : 0 : 0]\}$ la loi de groupe additive.

Exercice 2.3. 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 :

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

- (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 $x_1 \neq x_2$,

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

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

- (2) Montrer que $Y \setminus \{[1 : 0 : 0]\}$ 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 $\mathbb{P}^2 \setminus T_1$.
- (5) Montrer que la loi de groupe induite sur $Y \setminus \{[1 : 0 : 0]\}$ est celle du groupe multiplicatif $\mathbb{G}_m(k) = k^*$.

3. INTÉGRALES ELLIPTIQUES

Soient $a > b > 0$ des nombres réels strictement positifs. On se propose de calculer la longueur ℓ d'un arc de l'ellipse

$$\left(\frac{u}{a}\right)^2 - \left(\frac{v}{b}\right)^2 = 1.$$

Autrement dit, avec les coordonnées $u = a \cos \theta$, $v = b \sin \theta$, on veut calculer l'intégrale

$$\ell = \int_0^{\theta_1} \sqrt{a^2(\sin \theta)^2 + b^2(\cos \theta)^2} d\theta,$$

pour $0 \leq \theta_1 \leq \frac{\pi}{2}$.

Exercice 3.1. Avec les notations précédentes,

- (1) Montrer l'égalité

$$\ell = a \int_0^{x_1} \frac{1 - k^2 x^2}{\sqrt{(1 - x^2)(1 - k^2 x^2)}} dx$$

où $k = \sqrt{\frac{b^2}{a^2} - 1}$ est l'*excentricité* de l'ellipse et $x_1 = \cos \theta_1$.

On considère la courbe projective plane complexe X donnée par l'équation affine

$$y^2 = (1 - x^2)(1 - k^2 x^2).$$

- (2) Déterminer les points singuliers de X .
- (3) Trouver un changement de coordonnées rationnelles (x', y') tel que X , dans ces nouvelles coordonnées est donnée par l'équation

$$(y')^2 = x'(x' - 1)(x' - \lambda),$$

pour un nombre complexe λ à déterminer.

- (4) Comment se traduit-elle la loi de groupe au niveau des intégrales ?