Courbes elliptiques (1)

Exercice 1 Pour toutes les courbes affines C_0, trouver la courbe projective C dont la courbe affine est C_0. Donner ensuite les points à l'infini de la courve projective C.

1. $C_0 : 3x - 7y + 5 = 0$,
2. $C_0 : x^2 + xy - 2y^2 + x - 5y + 7 = 0$,
3. $C_0 : x^3 + x^2y - 3xy^2 - 3y^3 + 2x^2 - x + 5 = 0$.

Exercice 2 Pour toutes les courbes C et les points P, trouver la tangente à C en P ou vérifier que P est un point singulier de C.

1. $C : y^2 = x^3 - x$, $\quad P = (1, 0)$,
2. $C : x^2 + y^2 = z^2$, $\quad P = (3\colon 4\colon 5)$,
3. $C : x^2 + y^4 + 2xy + 2x + 2y + 1 = 0$, $\quad P = (-1, 0)$,
4. $C : x^3 + y^3 + z^3 = xyz$, $\quad P = (1\colon -1\colon 0)$.

Exercice 3 Pour les droites d et les courbes C, trouver les points d'intersection entre la droite d et la courbe C (en incluant les points à l'infini).

1. $d : x - y = 0$, $\quad C : x^2 - y = 0$,
2. $d : x - y - 1 = 0$, $\quad C : x^2 - y^2 + 2 = 0$,
3. $d : x - y - 1 = 0$, $\quad C : x^2 - 2y^2 - 5 = 0$,
4. $d : x - 2 = 0$, $\quad C : y^2 - x^3 + 2x = 0$.

Exercice 4 Pour les droites d et les courbes C, calculer la multiplicité d'intersection de la courbe C avec la droite d au point P.

1. $d : x - y = 0$, $\quad C : x^2 - y = 0$, $\quad P = (0, 0)$,
2. $d : y = 0$, $\quad C : x^2 - y = 0$, $\quad P = (0, 0)$,
3. $d : x - y = 0$, $\quad C : x^3 - y^2 = 0$, $\quad P = (0, 0)$,
4. $d : x + y = 2$, $\quad C : x^2 + y^2 = 2$, $\quad P = (1, 1)$.

Exercice 5 Soit $F \in \mathbb{Q}[x_1, x_2, x_3]$ un polynôme homogène de degré 3 tel que $(0\colon 1\colon 0)$ est un point d'inflexion de $F = 0$ avec pour tangente la droite $x_3 = 0$.

1. Montrer que

$$F = ax_1^3 + bx_1^2x_3 + cx_1x_3^2 + dx_3^3 + ex_2^2x_3 + fx_2x_3^2 + gx_1x_2x_3$$

pour certains $a, \ldots, g \in \mathbb{Q}$ tels que $a \neq 0$ et $e \neq 0$.

2. Trouver un changement de variables linéaire tel que

$$F = a'x_1'^3 + b'x_1'^2x_3' + c'x_1'x_3'^2 + d'x_3'^3 - x_2'^2x_3'$$

pour certains $a', \ldots, e' \in \mathbb{Q}$ (choisir $x_1 = x_1'$, $x_2 = \lambda x_1' + x_2' + \mu x_3'$, $x_3 = \nu x_3'$ pour certains $\lambda, \mu, \nu \in \mathbb{Q}$).

Exercice 6 Soit X l'ensemble des points d'une cubique non-singulière. Montrer que $P \star (P \star Q) = Q$ pour tout $P, Q \in X$, où $P \star Q$ désigne le troisième point sur la droite PQ.

Exercice 7 Soit X l'ensemble des points d'une cubique non-singulière et $O, O' \in X$. On définit deux lois de composition sur X par :

$$P +_O Q = O \star (P \star Q) \qquad\qquad P +_{O'} Q = O' \star (P \star Q)$$

Montrer que $P \mapsto O \star (O' \star P)$ définit un isomorphisme de groupes entre $(X, +_O)$ et $(X, +_{O'})$ (utiliser le fait que $+_O$ est associatif).

Exercice 8 On considère la cubique $u^3 + v^3 = \alpha$, $\alpha \in \mathbb{Q}^\times$, avec le point rationnel $(1\colon -1\colon 0)$ à l'infini. On choisit $O = (1\colon -1\colon 0)$ pour définir une structure de groupe sur les points de la cubique.

1. Trouver une formule pour la somme $(u_1, v_1) + (u_2, v_2)$ pour $(u_1, v_1) \neq (u_2, v_2)$.
2. Trouver une formule pour $2(u_0, v_0)$.

Exercice 9 Soit X l'ensemble des points d'une cubique non-singulière et O un point d'inflexion de X. On définit une structure de groupe sur X à partir de O.

1. Soient $P, Q, R \in X$. Montrer que $P + Q + R = O$ si et seulement s'il existe une droite qui intersecte X aux points P, Q, R comptés avec multiplicités.
2. Pour tout $P \in X$, montrer que P est un point d'inflexion de X si et seulement si $3P = 0$.
3. Soient P, Q des points d'inflexion. Montrer que le 3eme point sur la droite PQ est un point d'inflexion.

Exercice 10 Soit X l'ensemble des points d'une cubique non-singulière et O, P, Q des points d'inflexion non-alignés de X. On définit une structure de groupe sur X à partir de O. Montrer que les points

$$O, Q, 2Q, P, P + Q, P + 2Q, 2P, 2P + Q, 2P + 2Q$$

sont distincts et sont des points d'inflexion de X. Quels points sont colinéaires ?