

Feuille de TD N°2
Arithmétique des courbes elliptiques

Exercice 1. *Rappel* : Soit A un anneau ; on dit que $f \in A[t_1, \dots, t_n]$ est *symétrique* si

$$f(t_1, \dots, t_n) = f(t_{\sigma(1)}, \dots, t_{\sigma(n)}) \quad \forall \sigma \in S_n.$$

D'autre part, les *fonctions symétriques élémentaires* sont définies par :

$$\sigma_1 = \sum_i t_i, \quad \sigma_2 = \sum_{i < j} t_i t_j, \quad \sigma_3 = \sum_{i < j < k} t_i t_j t_k, \dots, \quad \sigma_n = \prod_i t_i.$$

On a le résultat suivant :

Théorème. *Tout polynôme symétrique s'écrit (de manière unique) comme un polynôme en les fonctions symétriques élémentaires.*

Ce théorème s'applique en particulier aux *sommes de Newton* définies par $s_0 = n$ et $s_j = \sum_i t_i^j \quad \forall j \geq 1$; les formules reliant les s_j aux σ_i sont appelées «formules de Newton».

- (1) Soit $x^3 + ax + b = \prod_{i=1}^3 (x - \alpha_i)$ et $\Delta = \prod_{i < j} (\alpha_i - \alpha_j)^2$. Expliquer pourquoi il est possible d'écrire Δ comme un polynôme en a et b . Nous allons mener les calculs de manière astucieuse : en remarquant que $\delta = \prod_{i < j} (\alpha_i - \alpha_j)$ est un déterminant de Vandermonde, exprimer Δ en fonction des sommes de Newton (astuce : une matrice et sa transposée ont même déterminant !). Conclure à l'aide des formules de Newton.
- (2) En déduire que le polynôme $f(x) = x^3 + ax + b$ à coefficients dans un corps k possède des racines deux à deux distinctes dans une clôture algébrique de k si et seulement si $4a^3 + 27b^2 \neq 0$.
- (3) On suppose que k est de caractéristique différente de 2 et de 3 et que $\Delta = 0$. Soit α la racine multiple de f ; exprimer a et b en fonction de α . En déduire à quelle condition l'unique point singulier de la cubique projective C définie sur k par l'équation $Y^2Z - X^3 - aXZ^2 - bZ^3 = 0$, avec $4a^3 + 27b^2 = 0$, est un noeud ou une pointe.
- (4) On suppose maintenant que $k = \mathbb{R}$. Donner l'allure de la courbe $y^2 = f(x)$; on distinguera le cas régulier (discuter également sur le nombre de racines réelles), le cas du noeud (discuter sur le signe de la racine double) et de la pointe.

Exercice 2. Pour chacune des cubiques projectives planes C définies par les polynômes homogènes $F \in k[X, Y, Z]$ ci-dessous, étudier la régularité et déterminer (en discutant éventuellement sur le corps k) si l'on peut munir C d'un point rationnel afin d'en faire une courbe elliptique définie sur k .

(i) $X^3 + Y^3 + Z^3$;

(ii) $X^3 + pY^3 + p^2Z^3$, p premier et $k = \mathbb{Q}$ (puis $k = \mathbb{R}$, $k = \mathbb{Q}(p^{\frac{1}{3}}) \subset \mathbb{R}$) ;

- (iii) $Y^2Z - X(X - Z)(X - \lambda Z)$, $\lambda \in k \setminus \{0, 1\}$;
 (iv) $Y^2Z - X^3 - 3XZ^2 + 11Z^3$.

Exercice 3. Points rationnels sur les coniques rationnelles.

- (1) Les coniques suivantes admettent-elles des point rationnels ?

$$(i) X^2 - Y^2 = 6Z^2; \quad (ii) X^2 - 2Y^2 = 6Z^2; \quad (iii) 3X^2 + 5Y^2 = 4;$$

$$(iv) 3X^2 + 6Y^2 = 4; \quad (v) 11X^2 + 13Y^2 = 19Z^2.$$

- (2) Dans le cas (iv), paramétrer l'ensemble des points rationnels.
 (3) Même question dans le cas (i). A l'aide des formules obtenues, établir un isomorphisme de courbes projectives planes définies sur \mathbb{Q} entre la conique et la droite projective $\mathbb{P}^1 : Z = 0$.
 (4) Exhiber dans le cas (v) un point rationnel (on appliquera l'algorithme de Legendre).

Exercice 4. Soit $C : y^2 = x^3 + ax + b$ une cubique projective singulière définie sur \mathbb{Q} . Notant α l'abscisse de l'unique point singulier P , on a vu à l'exercice 1 (3) que $a = -3\alpha^2$ et $b = 2\alpha^3$, de sorte que α est rationnel et l'équation de C se réécrit $y^2 = (x - \alpha)^3 + 3\alpha(x - \alpha)^2$. Donc P est un point rationnel ; si $\alpha = 0$, alors P est une pointe, sinon c'est un noeud.

D'autre part, on rappelle que la loi de groupe sur l'ensemble des points non-singuliers $C_{ns} = C \setminus \{P\}$ est également caractérisée par :

$$P_1 + P_2 + P_3 = O \text{ si et seulement si } P_1, P_2 \text{ et } P_3 \text{ sont alignés,}$$

où O désigne comme toujours le point à l'infini et avec la convention habituelle sur les multiplicités.

- (1) Cas d'une pointe : pourquoi C_{ns} s'identifie-t-elle naturellement à une courbe affine ? Notant $P_i = (x_i : 1 : z_i)$, montrer que les P_i sont alignés si et seulement si $\sum x_i = 0$. En déduire que $C_{ns}(\mathbb{Q})$ est isomorphe au groupe additif \mathbb{Q} .
 (2) Cas d'un noeud à tangentes rationnelles (i.e. $3\alpha = \beta^2$ avec $\beta \in \mathbb{Q}^\times$) : en posant $u = y + \beta(x - \alpha)$ et $v = y - \beta(x - \alpha)$, on se ramène à la cubique d'équation $8\beta^3 uv = (u - v)^3$, munie du point à l'infini $O' = (1 : 1 : 0)$. Justifier que l'on peut munir C'_{ns} d'une loi de groupe, de neutre O' , qui est également caractérisée par :

$$P_1 + P_2 + P_3 = O' \text{ si et seulement si } P_1, P_2 \text{ et } P_3 \text{ sont alignés.}$$

Notant $P_i = (u_i : 1 : w_i)$, montrer que les P_i sont alignés si et seulement si $\prod u_i = 1$. En déduire que $C_{ns}(\mathbb{Q})$ est isomorphe au groupe multiplicatif \mathbb{Q}^\times .

- (3) Le groupe abélien $C_{ns}(\mathbb{Q})$ est-il de type fini dans le cas d'une cubique singulière ?

Exercice 5 (cf. session d'examen de septembre 2004). Soit d un entier relatif supposé sans facteur de puissance quatrième (i.e. si p divise d alors p^4 ne divise pas d) et E_d la courbe elliptique définie sur \mathbb{Q} par l'équation de Weierstrass $y^2 = x^3 + dx$. On se propose de déterminer la partie de torsion $E_d(\mathbb{Q})_{tors}$ du groupe de Mordell-Weil $E_d(\mathbb{Q})$ de E_d .

- (1) (a) Soit p un nombre premier impair ne divisant pas d et \overline{E}_d la réduction de E_d modulo p . Montrer que $\#\overline{E}_d(\mathbb{F}_p) = p + 1$ si $p \equiv 3 \pmod{4}$.
 (b) En déduire que $\#E_d(\mathbb{Q})_{tors}$ divise 4 (on utilisera le théorème de la progression arithmétique de Dirichlet).
 (c) Conclure que $E_d(\mathbb{Q})_{tors}$ est isomorphe à l'un des trois groupes suivants : $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z}$.

- (2) (a) Démontrer que $E_d(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si et seulement si $-d$ est un carré.
 (b) On rappelle la formule suivante de duplication d'un point $P = (x, y)$ sur une courbe elliptique C d'équation $y^2 = x^3 + ax + b$: si P n'est pas d'ordre deux, alors l'abscisse de $2P$ est

$$x_{2P} = \frac{x^4 - 2ax^2 - 8bx + a^2}{(2y)^2}.$$

Montrer que l'équation $2P = (0, 0)$ admet une solution si et seulement si $P = (x, y)$ vérifie $x^2 = d$ et $y^2 = 2x^3$, donc si et seulement si $x = 2$ et $d = 4$ (on rappelle que d est supposé sans facteur de puissance quatrième). En déduire que $E_d(\mathbb{Q})_{tors} \simeq \mathbb{Z}/4\mathbb{Z}$ si et seulement si $d = 4$.

- (c) Conclure que

$$E_d(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{si } d = 4 ; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{si } -d \text{ est un carré ;} \\ \mathbb{Z}/2\mathbb{Z} & \text{sinon.} \end{cases}$$

Exercice 6. Fermat a démontré que l'équation $w^2 = u^4 + v^4$ n'admet pas de solution en entiers non triviale (d'où résulte le théorème de Fermat pour $n = 4$). Nous relierons cette équation à la courbe elliptique $E : y^2 = x^3 - 4x$ et déduisons, à la suite de Fermat, que 2 n'est pas congruent.

- (1) Soit Q_0 la quadrique affine d'équation $p^2 = q^4 + 1$; déterminer $Q_0(\mathbb{Q})$.
- (2) Effectuant le changement de variable $r = q, s = p - q^2$ dans l'équation de Q_0 , on se ramène à une cubique affine C_0 . Vérifier que la cubique projective correspondante C est non-singulière. Quelle est l'équation affine de $C_2 = C \cap \{(r : 1 : t)\}$? En déduire un isomorphisme entre C et la courbe elliptique E .
- (3) Déterminer $E(\mathbb{Q})$ et décrire sa structure de groupe.
- (4) Montrer que 2 n'est pas congruent.