Sorbonne Université — Faculté des Sciences et Ingénierie
Master Mathématiques fondamentales — 2018–2019

Courbes elliptiques

Examen du 21 Décembre 2018. Durée 3h00.

Exercice 1. Soit k un corps de caractéristique $\neq 2$. On considère la famille de cubiques de Legendre $C_\lambda \subset \mathbb{P}^2$ d'équation affine $y^2 = x(x-1)(x-\lambda)$, où $\lambda \in \bar{k}$.

i. Calculer le discriminant $\Delta(\lambda)$. Lorsque $\Delta(\lambda) \neq 0$, calculer l'invariant $j(\lambda)$ de C_λ. Lorsque $\Delta(\lambda) = 0$, trouver le point singulier et indiquer la nature du lieu singulier de C_λ (groupe additif ou multiplicatif).

ii. On suppose que C_λ est une courbe elliptique. Trouver tous ses points de 2-torsion.

iii. Soit $\varphi : C_\lambda \xrightarrow{\sim} C_{\lambda'}$ un isomorphisme de courbes elliptiques. On note $P_x = [x : 0 : 1]$ et $O = [0 : 1 : 0]$.

   (a) Montrer que φ est induit par un automorphisme linéaire Φ de $\mathbb{P}^2$ tel que : $\Phi(O) = O$, $\Phi(\{Z = 0\}) = \{Z = 0\}$, et $\Phi(\{P_0, P_1, P_\lambda\}) = \{P_0, P_1, P_{\lambda'}\}$.

   (b) En déduire que $\lambda' \in \{\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}\}$.

Exercice 2. Le but de l'exercice est de fournir une preuve élémentaire de Mordell faible pour une courbe elliptique E sur $\mathbb{Q}$ telle que $E[2] \subset E(\mathbb{Q})$. On suppose E donnée par une équation $y^2 = f(x)$, avec f unitaire de degré 3.

i. Montrer que $E[2] = \{O\} \sqcup \{[\alpha : 0 : 1],\ f(\alpha) = 0\}$ et en déduire que $E[2] \subset E(\mathbb{Q})$ si et seulement si f est scindé dans $\mathbb{Q}[X]$. Montrer qu'après changement de variable éventuel, on peut même supposer que $f \in \mathbb{Z}[X]$ et y est scindé.

ii. Supposons $f(0) = 0$, et notons $P_0 := [0 : 0 : 1] \in E(\mathbb{Q})$. Soient $P_1, P_2, P_3 \in E(\mathbb{Q}) \setminus \{O\}$ trois points tels que $P_3 = P_1 + P_2$.

   (a) Si $P_1, P_2, P_3 \neq P_0$, montrer que $x(P_1)x(P_2)x(P_3) \in (\mathbb{Q}^\times)^2$.

   (b) Si $P_3 = P_0$, montrer que $x(P_1)x(P_2) = a_4 = f'(0)$.

   (c) Montrer que l'application suivante est un morphisme de groupes :

$$\begin{array}{rccl} \theta : & E(\mathbb{Q}) & \to & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ & P & \mapsto & \begin{cases} x(P)\cdot(\mathbb{Q}^\times)^2 & \text{si } P \neq O, P_0 \\ f'(0)\cdot(\mathbb{Q}^\times)^2 & \text{si } P = P_0 \\ (\mathbb{Q}^\times)^2 & \text{si } P = O \end{cases} \end{array}$$

TSVP

iii. Soit $\alpha \in \mathbb{Q}$ tel que $f(\alpha) = 0$, et notons $P_\alpha := [\alpha : 0 : 1] \in E(\mathbb{Q})$. Montrer que l'application suivante est un morphisme de groupes :

$$\begin{array}{rccl} \theta_\alpha : & E(\mathbb{Q}) & \to & \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \\ & P & \mapsto & \begin{cases} (x(P)-\alpha)\cdot(\mathbb{Q}^\times)^2 & \text{si } P \neq O, P_\alpha \\ f'(\alpha)\cdot(\mathbb{Q}^\times)^2 & \text{si } P = P_\alpha \\ (\mathbb{Q}^\times)^2 & \text{si } P = O \end{cases} \end{array}$$

iv. On suppose que $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$ avec $\alpha_i \in \mathbb{Z}$. Pour tout nombre premier p, notons v_p la valuation p-adique sur $\mathbb{Q}^\times$.

(a) Montrer que pour tout $P = [x : y : 1] \in E(\mathbb{Q}) \setminus \{O, P_{\alpha_1}, P_{\alpha_2}, P_{\alpha_3}\}$, si $v_p(x-\alpha_i)$ est impaire pour un $i = 1, 2, 3$, alors $v_p(\Delta) \neq 0$.

(b) Montrer que $\theta_{\alpha_i}(E(\mathbb{Q})) \subset \mathbb{Z}[\frac{1}{\Delta}]^\times/(\mathbb{Z}[\frac{1}{\Delta}]^\times)^2$.

v. Mêmes notations que iv. Montrer que $\mathrm{Ker}(\theta_{\alpha_1}) \cap \mathrm{Ker}(\theta_{\alpha_2}) = [2]E(\mathbb{Q})$. On pourra admettre et utiliser le fait suivant : si E' est une courbe elliptique d'équation $y^2 = (x+\beta_1^2)(x+\beta_2^2)(x+\beta_3^2)$ alors la droite passant par $(0, \beta_1\beta_2\beta_3)$ de pente $\beta_1+\beta_2-\beta_3$ est tangente à E' en son deuxième point d'intersection.

vi. En déduire que $|E(\mathbb{Q})/[2]E(\mathbb{Q})| \leqslant 2^{2(1+\nu(\Delta))}$ où $\nu(\Delta)$ est le nombre de facteurs premiers de Δ.

Exercice 3. Soit E une courbe elliptique sur $\mathbb{Q}$ d'invariant $j(E) = 0$.

i. Montrer qu'il existe un unique entier $d \in \mathbb{Z}$ tel que E soit donnée par l'équation $y^2 = x^3 + d$ et tel que $v_p(d) < 6$ pour tout premier p.

ii. Montrer que pour tout premier $p \equiv 2[3]$ ne divisant pas $2d$, la courbe E a bonne réduction super-singulière modulo p, puis montrer qu'on a $|E(\mathbb{F}_p)| = p+1$.

iii. Prenons $d = 3$.

(a) Montrer que $|E(\mathbb{F}_7)| = 13$ puis que $E(\mathbb{Q})_{\mathrm{tors}} = \{O\}$

(b) Montrer que $E(\mathbb{Q})$ est de rang $\geqslant 1$.

iv. *(Bonus).* Revenons au cas général de i. Soit q un nombre premier.

(a) Montrer que si $q \neq 2, 3$, alors $E(\mathbb{Q})$ n'a pas de point de q-torsion (on pourra utiliser le théorème de Dirichlet sur l'existence de premiers dans certaines progressions arithmétiques.)

(b) Montrer que 2 divise $|E(\mathbb{Q})_{\mathrm{tors}}|$ si et seulement si d est un cube dans $\mathbb{Z}$, et que dans ce cas il y a un unique point rationnel d'ordre 2.

(c) Montrer que 3 divise $|E(\mathbb{Q})_{\mathrm{tors}}|$ si et seulement si d est un carré dans $\mathbb{Z}$ ou $d = -432$, et que dans ce cas il y a deux points rationnels d'ordre 3 (on pourra utiliser le fait que les points de 3 torsion sont les points d'inflexion).

(d) Conclure en décrivant le groupe $E(\mathbb{Q})_{\mathrm{tors}}$ pour tout d comme dans i.