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

Courbes elliptiques

Corrigé de l'examen du 21 Décembre 2018.

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 $\Delta(\lambda)$.* On trouve

$$\Delta(\lambda) = 16 \cdot \mathrm{disc}(x(x-1)(x-\lambda)) = 16 \cdot \lambda^2(\lambda-1)^2.$$

Lorsque $\Delta(\lambda) \neq 0$, calculer l'invariant $j(\lambda)$ de C_λ.

Si $\mathrm{car}(k) \neq 3$, un changement de variable $x' = x - \frac{1}{3}(\lambda+1)$ met l'équation sous forme de Weierstraß simple et on applique la formule du cours. En caractéristique 3, l'équation est déjà simplifiée si $\lambda + 1 = 0$, sinon on simplifie le terme en x par un changement de variable $x' = x - \frac{\lambda}{2(\lambda+1)}$. À partir des formules données pour les formes simplifiées en cours, on trouve

$$j(\lambda) = 2^8 \frac{(\lambda^2-\lambda+1)^2}{\lambda^2(\lambda-1)^2}.$$

Lorsque $\Delta(\lambda) = 0$, trouver le point singulier et indiquer la nature du lieu singulier de C_λ (groupe additif ou multiplicatif).

On sait que le seul point singulier a pour ordonnée $y = 0$ et abscisse une racine double de $x(x-1)(x-\lambda)$. On a donc deux cas. Si $\lambda = 0$, l'équation est $y^2 = x^3 - x^2$, le point singulier est $(0,0)$ et le lieu lisse est multiplicatif (non déployé si -1 n'est pas un carré dans k). Si $\lambda = 1$, l'équation est $y^2 = x(x-1)^2$, le point singulier est $(1,0)$ et le lieu lisse est multiplicatif (toujours déployé).

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

Un point (x,y) est d'ordre 2 si et seulement si sa tangente à la courbe passe par O. Or une droite $aX + bY + cZ = 0$ passe par O si et seulement si $b = 0$. Donc P est d'ordre 2 si et seulement si $\frac{\partial}{\partial y}(y^2 - x(x-1)(x-\lambda))(P) = 0$ donc si et seulement si $y = 0$. Les points de 2 torsion sont donc O, $(0,0)$, $(1,0)$ et $(\lambda,0)$.

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

TSVP

(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 $\Phi(\{P_0, P_1, P_\lambda\}) = \{P_0, P_1, P_{\lambda'}\}$.*

On sait d'après le cours que tout isomorphime entre deux cubiques de Weierstraß est induit par un automorphisme linéaire Φ de $\mathbb{P}^2$ tel que $\Phi(O) = O$ et $\Phi(\{Z = 0\}) = \{Z = 0\}$. Un tel isomorphisme préserve la loi de groupe et donc envoie les éléments d'ordre 2 sur les éléments d'ordre 2.

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

Puisque $\Phi(\{Y = 0\}) = \{Y = 0\}$, la matrice de Φ est de la forme $\begin{pmatrix} u^2 & 0 & r \\ 0 & u^3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ On voit que $\{0, 1, \lambda'\} = \{r, u^2 + r, \lambda u^2 + r\}$. S'en suit une discussion élémentaire...

Exercice 2. *Le but de l'exercice est 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.*

Pour la description de $E[2]$, voir question ii. de l'exercice 1. Le reste est clair. Pour se ramener à $\mathbb{Z}[X]$ on remarque qu'un changement de variable $x' = u^2x$, $y' = u^3x$ transforme $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ en $y^2 = (x-u^2\alpha)(x-u^2\beta)(x-u^2\gamma)$.

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 $x(P_1)x(P_2)x(P_3) \in (\mathbb{Q}^\times)^2$.*

Notons (x_i, y_i) les coordonnées de P_i. Les points $-P_3 = (x_3, -y_3)$, P_1 et P_2 sont alignés.

Supposons $P_1 \neq P_2$. Puisque $P_3 \neq O$, on a $x_1 \neq x_2$ et la droite (P_1P_2) a une équation de la forme $y = \lambda x + \mu$ avec $\mu \neq 0$. Le polynôme cubique unitaire $f(x) - (\lambda x + \mu)^2$ a pour racines x_1, x_2 et x_3 et pour terme constant $-\mu^2$. Donc $x_1x_2x_3 = \mu^2$.

Si $P_1 = P_2$, on a $y_1 = y_2 \neq 0$ car $P_3 \neq O$, donc la tangente en P_1 a une équation de la forme $y = \lambda x + \mu$ et, comme ci-dessus, on a $x_1x_2x_3 = x_1^2x_3 = \mu^2$.

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

On procède comme ci-dessus, sauf qu'on a maintenant $\mu = 0$. Mais le terme en x de $f(x) - \lambda^2x^2$ est $a_4 = f'(0)$, et par les formules de Newton est égal à la somme $x_1x_2 + x_1x_3 + x_2x_3 = x_1x_2$.

TSVP

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

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

Supposons $P_1 + P_2 = P_3$. Si l'un des P_i est égal à O, l'égalité $\theta(P_1)\theta(P_2) = \theta(P_3)$ est claire. Supposons donc que $P_i \neq O$ pour tout i.

Si $P_i \neq P_0$ pour tout i, alors le (a) nous dit que $\theta(P_1)\theta(P_2)\theta(P_3) = 1$ et donc $\theta(P_1)\theta(P_2) = \theta(P_3)$ puisque $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ est d'exposant 2.

Si l'un des P_i est égal à P_0 alors les deux autres ne le sont pas (car sinon l'un des points serait O). On peut supposer par symétrie (et parce que $\theta(-P) = \theta(P) = \theta(P)^{-1}$) que c'est P_3, et le (b) ci-dessus assure l'égalité $\theta(P_1)\theta(P_2) = \theta(P_3)$ voulue.

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 :*

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

Un changement de variable $x' = x - \alpha$ nous ramène à la question précédente.

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

Montrons d'abord que $v_p(x) \geqslant 0$. En effet, sinon on aurait $v_p(x-\alpha_i) = v_p(x) < 0$ pour tout i, donc en particulier $v_p(x)$ impaire et $v_p(y^2) = 3v_p(x)$ impaire, ce qui est aburde.

On a donc $v_p(x-\alpha_i) \geqslant 0$ pour tout i, et la somme $\sum_i v_p(x-\alpha_i)$ doit être paire. Il y a donc deux indices $i = i_1, i_2$ avec $v_p(x-\alpha_i)$ impaire et, en particulier, $v_p(x-\alpha_i) > 0$. Par différence, on obtient $v_p(\alpha_{i_1} - \alpha_{i_2}) > 0$, donc $v_p(\Delta) > 0$.

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

Pour $P = (x, y) \neq P_{\alpha_i}$, on a

$$\theta_{\alpha_i}(P) = \left(\prod_p p^{v_p(x-\alpha_i)}\right)(\mathbb{Q}^\times)^2 = \left(\prod_{v_p(x-\alpha_i)\ \text{impaire}} p\right)(\mathbb{Q}^\times)^2,$$

TSVP

donc d'après la question précédente, $\theta_{\alpha_i}(P)$ est dans l'image de $\mathbb{Z}[\frac{1}{\Delta}]^\times$ dans $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Cette image est bien $\mathbb{Z}[\frac{1}{\Delta}]^\times/(\mathbb{Z}[\frac{1}{\Delta}]^\times)^2$ car $\mathbb{Z}[\frac{1}{\Delta}]^\times \cap (\mathbb{Q}^\times)^2 = (\mathbb{Z}[\frac{1}{\Delta}]^\times)^2$. Par ailleurs, puisque $f'(\alpha_i)|\Delta$, on a aussi $\theta_{\alpha_i}(P_{\alpha_i}) \in \mathbb{Z}[\frac{1}{\Delta}]^\times/(\theta_{\alpha_i}(P_{\alpha_i}))^2$.

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.*

Soit $P = (x_0, y_0)$ dans le noyau de $\theta_{\alpha_1} \times \theta_{\alpha_2}$. Supposons d'abord que $y_0 \neq 0$. Alors $(x_0 - \alpha_1)$ et $(x_0 - \alpha_2)$ sont des carrés non nuls, et puisque $y_0^2 \neq 0$, il en est de même de $(x_0 - \alpha_3)$. Écrivons $x_0 - \alpha_i = \beta_i^2$ en choisissant les β_i de sorte que $y_0 = -\beta_1\beta_2\beta_3$. Un changement de variable $x' = x - x_0$ envoie P sur le point $P' = (0, y_0)$ de la courbe E' de l'énoncé. Il s'agit de montrer que P' est divisible par 2 dans $E'(\mathbb{Q})$. La droite fournie par l'énoncé passe par $-P'$ et est tangente à E' en son autre point d'intersection Q', de sorte que $[2](Q') = P'$. Or, Q' est l'unique point d'intersection de multiplicité 2 d'une droite définie sur $\mathbb{Q}$ et d'une courbe définie sur $\mathbb{Q}$. Il est donc fixe par $G_\mathbb{Q}$.

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.

On a $\mathbb{Z}[\frac{1}{\Delta}]^\times = \{\pm 1\} \times \prod_{p|\Delta} p^\mathbb{Z}$, donc $\mathbb{Z}[\frac{1}{\Delta}]^\times/(\mathbb{Z}[\frac{1}{\Delta}]^\times)^2 = \{\pm 1\} \times (\mathbb{Z}/2\mathbb{Z})^{\{p|\Delta\}}$. Or, d'après les questions v. et iv., $E(\mathbb{Q})/[2]E(\mathbb{Q})$ s'injecte dans $(\mathbb{Z}[\frac{1}{\Delta}]^\times/(\mathbb{Z}[\frac{1}{\Delta}]^\times)^2)^2$.

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.*

Puisque $j(E)$, toute équation de Weierstraß simplifiée pour E est de la forme $y^2 = x^3 + a_6$, avec $a_6 \in \mathbb{Q}$. Un changement $x' = u^2x$, $y' = u^3x'$ fournit l'équation $y'^2 = x'^3 + u^6a_6$. Il suffit donc de prendre $u = \prod_p p^{m_p}$ avec m_p le reste de la division euclidienne de $v_p(a_6)$ par 6.

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 $|E(\mathbb{F}_p)| = p+1$.*

Pour $p > 3$, le polynôme $X^3 + d$ est séparable dans $\mathbb{F}_p[X]$ si et seulement si $d \neq 0$ dans $\mathbb{F}_p$. Donc la courbe E a bonne réduction dès que p ne divise pas $6d$. Si de plus $p \equiv 2[3]$, alors 3 ne divise pas $p-1$ donc le terme en X^{p-1} dans le polynôme $(X^3+d)^{\frac{p-1}{2}}$ est nul et on sait que la courbe est supersingulière modulo p. On sait aussi que dans ce cas on a $|E(\mathbb{F}_p)| \equiv 1[p]$ et que, par ailleurs, $|E(\mathbb{F}_p)| = 1+p-a_p$ avec $|a_p| \leqslant 2\sqrt{p}$. Puique $p \geqslant 5$, on a $2\sqrt{p} < p$ donc $1 < |E(\mathbb{F}_p)| < 1+2p$, et finalement $|E(\mathbb{F}_p)| = 1+p$.

iii. *Prenons $d = 3$.*

TSVP

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

Pour le calcul de $|E(\mathbb{F}_7)|$, on utilise la formule $|E(\mathbb{F}_7)| = 8 + \sum_{x\in\mathbb{F}_7} \chi(x^3+3)$, sachant que le caractère quadratique χ est donnée par $\chi(y) = 1$ pour $y = 1, 2, 4$ et $\chi(y) = -1$ pour $y = 3, 5, 6$.

Maintenant, le cours nous dit que pour tout m premier à 7, la réduction modulo 7 donne une injection de $E(\mathbb{Q})[m]$ dans $E(\mathbb{F}_7)$. Le groupe $E(\mathbb{Q})_{tors,7'}$ de torsion "première à 7" est donc d'ordre divisant 13. Mais d'après le ii), on a $|E(\mathbb{F}_5)| = 6$, donc pour la même raison, l'ordre de $E(\mathbb{Q})_{tors,5'}$ divise 6. Ces deux contraintes impliquent que $E(\mathbb{Q})_{tors}$ est trivial.

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

On observe que $(1, 2) \in E(\mathbb{Q})$ est un point rationnel distinct de O. D'après la question précédente il est d'ordre infini.

iv. *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.*

Le théorème de Dirichlet assure l'existence d'une infinité de nombres premiers congrus à 2 modulo $3q$. On peut trouver en particulier un tel p ne divisant $6d$. Mais alors l'application de rédution modulo p induit une injection de $E(\mathbb{Q})[q]$ dans $E(\mathbb{F}_p)$ qui, d'après la question ii, est de cardinal $p + 1$ donc non divisible par q. Donc $E(\mathbb{Q})[q] = \{O\}$.

(b) *Montrer que* 2 *divise* $|E(\mathbb{Q})_{\text{tors}}|$ *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*.*

On a déjà vu que les points de 2-torsion sont sur l'axe $y = 0$. Mais le polynôme $X^3 + d$ possède au plus une racine dans $\mathbb{Q}$, et exactement une racine si et seulement si d est un cube.

(c) *Montrer que* 3 *divise* $|E(\mathbb{Q})_{\text{tors}}|$ *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*.*

Notons $g(X, Y, Z) = X^3 - Y^2Z + dZ^3$ l'équation projective de E. Par construction de la loi de groupe, les points de 3-torsion sont les points d'inflexion, i.e. les points où la tangente a un contact de multiplicité 3 avec la courbe. Puisqu'on est en caractéristique nulle, $E[3]$ est donc l'intersection de E et de sa Hessienne, dont l'équation est $\det(\frac{\partial^2 g}{\partial X_i \partial X_j})$ (avec $X_1 = X$, $X_2 = Y$ et $X_3 = Z$). Un calcul fournit l'équation $-24X(3dZ^2 + Y^2) = 0$ pour la Hessienne. Les points d'ordre 3 (donc distincts de O) sont dans le plan affine $\{Z \neq 0\}$ et sont donc les solutions du système d'équations $\begin{cases} y^2 = x^3 + d \\ x(y^2 + 3d) = 0 \end{cases}$. On remarque d'abord que si $(x, y) \in E(\mathbb{Q})$ est solution de $\begin{cases} y^2 = x^3 + d \\ y^2 + 3d = 0 \end{cases}$, alors on doit avoir $\begin{cases} y^2 = -3d \\ x^3 = -4d \end{cases}$, ce qui implique que $d < 0$ et $\begin{cases} v_3(d) \equiv 1[2] \text{ et } p \neq 3 \Rightarrow v_p(d) \equiv 0[2] \\ v_2(d) \equiv 1[3] \text{ et } p \neq 2 \Rightarrow v_p(d) \equiv 0[3] \end{cases}$, et donc

TSVP

$v_2(d) \equiv 4[6]$, $v_3(d) \equiv 3[6]$ et $p \neq 2,3 \Rightarrow v_p(d) \equiv 0[6]$. Il s'ensuit que $d = -2^4.3^3 = -432$ (modulo $(\mathbb{Q}^\times)^6$) et $(x, y) = (12, \pm 36)$.

Reste à étudier l'intersection de E avec $\{x = 0\}$, dont les points sont $(0, \pm\sqrt{d})$, et sont rationnels si et seulement si d est un carré dans $\mathbb{Q}^\times$.

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

On a finalement montré que (avec la contrainte $0 \leqslant v_p(d) < 6$ pour tout p)

$$E(\mathbb{Q})_{\text{tors}} = \begin{cases} \mathbb{Z}/6\mathbb{Z} \text{ si } d = 1 \\ \mathbb{Z}/3\mathbb{Z} \text{ si } d \in (\mathbb{Q}^\times)^2 \text{ ou } d = -432 \\ \mathbb{Z}/2\mathbb{Z} \text{ si } d \in (\mathbb{Q}^\times)^3 \text{ et } d \neq 1. \end{cases}$$