MAT562 : Examen de 19 Février 2016, durée 3h

Documents autorisés : polycopié/notes du cours, notes de PC, dictionnaires.

1. (a) Soit $C \subset \mathbb{P}^2_{\mathbb{C}}$ une conique lisse. Montrer que l'ensemble des droites tangentes à C forme une conique dans l'espace projectif des droites de $\mathbb{P}^2_{\mathbb{C}}$.
   (b) Soient C et C' deux coniques distinctes dans $\mathbb{P}^2_{\mathbb{C}}$. Peut-on avoir cinq droites tangentes et à C, et à C' ?

2. Soit E une courbe elliptique $y^2 = x^3 - x$ définie sur un corps fini $\mathbb{F}_{71}$.
   (a) Déterminer le cardinal $\#E(\mathbb{F}_{71})$.
   (b) Montrer que $E(\bar{\mathbb{F}}_{71})[3] \not\subseteq E(\mathbb{F}_{71})$.
   (c) En déduire la structure de groupe de E (c'est-à-dire, exprimer $E(\mathbb{F}_{71})$ comme produit des groupes cycliques à préciser).

3. Soit E une courbe elliptique supersingulière définie sur un corps fini $\mathbb{F}_p$ où p est un nombre premier $p \geq 5$.
   (a) Pour $n \geq 1$ montrer que $\#E(\mathbb{F}_{p^n}) = p^n + 1$ si n est impair et que $\#E(\mathbb{F}_{p^n}) = (p^{\frac{n}{2}} - (-1)^{\frac{n}{2}})^2$ si n est pair.
   (b) Supposons que ℓ est un premier tel que $E(\mathbb{F}_p)$ contient un point d'ordre ℓ. Montrer que $\ell^2 \,|\, \#E(\mathbb{F}_{p^2})$. Déduire qu'on a soit $E[\ell] \subset E(\mathbb{F}_{p^2})$, soit $E(\mathbb{F}_{p^2})$ contient un point d'ordre ℓ^2.

4. Soit $f \in \mathbb{Q}(t)$ une fraction rationnelle non constante : on l'écrit $f = P/Q$, où $P, Q \in \mathbb{Q}[t]$ sont des polynômes premiers entre eux et on pose $d = \max(deg\, P, deg\, Q)$. Monrer que l'on a

$$\lim_{h(x)\to\infty} \frac{h(f(x))}{h(x)} = d,$$

   où la limite est sur $x \in \overline{\mathbb{Q}}$ avec $h(x) \to \infty$.

5. (a) Soit E une courbe elliptique définie sur un corps k par l'équation usuelle $y^2 = x^3 + ax + b$. Déterminer les x-coordonnées des points d'ordre exact 3 de E.
   (b) Soit E_n une courbe elliptique définie sur $\mathbb{Q}$ par l'équation $y^2 = x^3 + n$. Montrer que $E(\mathbb{Q})$ contient un point d'ordre exact 3 si et seulement si n est un carré dans $\mathbb{Z}$ et, dans ce cas, derminer $E(\mathbb{Q})[3]$.

6. Soit E une courbe elliptique définie sur $K = \mathbb{Q}$ par l'équation

$$y^2 = x^3 - p^2 x,$$

où p est un nombre premier. On pose $\alpha_1 = 0, \alpha_2 = p, \alpha_3 = -p$.

(a) Soit S l'ensemble fini de nombres premiers qui divisent Δ_E. Déterminer $\mathcal{O}^*_{K,S}/\mathcal{O}^{*2}_{K,S}$.

(b) Soit $\phi : E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathcal{O}^*_{K,S}/\mathcal{O}^{*2}_{K,S})^3$ le plongement défini comme dans le cours :

$$\phi_i(P) = \begin{cases} x_P - \alpha_i & P \neq P_i = (\alpha_i, 0), 0_E \\ (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}), & P = P_i \\ 1 & P = 0_E, \end{cases}$$

$i = 1, 2, 3$ et $\phi = (\phi_1, \phi_2, \phi_3)$. Determiner l'image par ϕ des points de 2-torsion de E.

(c) Montrer que pour tout $P \in E(\mathbb{Q})$ il existe un point de 2-torsion Q tel que $\phi(P - Q) = (d_1, d_2, d_3)$ ou chaque d_i divise 2 (i.e. $d_i = \pm 1, \pm 2$).

(d) Si $p \equiv 3 \pmod 8$ montrer que le rang de $E(\mathbb{Q})$ est zéro.

i. Montrer que $(-1, -1, 1)$ n'est pas dans $Im\,\phi$.

ii. Montrer que si $d_1 = \pm 1$ et $2|d_2$, alors (d_1, d_2, d_3) n'est pas dans $Im\,\phi$.

iii. Conclure.

7. Soient Λ_1 et Λ_2 deux réseaux dans $\mathbb{C}$. Soient $E_i = \mathbb{C}/\Lambda_i$, $i = 1, 2$ les courbes elliptiques correspondantes.

(a) Montrer que si L est un $\mathbb{Z}$-module tel qu'on a des inclusions $\Lambda_1 \subseteq L \subseteq \Lambda_2$ de $\mathbb{Z}$-modules, alors L est un réseau.

(b) Soit $C \subset E_1$ un sous-groupe fini. Montrer qu'il existe un réseau Λ_3 tel que $\Lambda_1 \subseteq \Lambda_3$ et que le morphisme naturel $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_3$ est de noyau isomorphe à C.

(c) Supposons qu'il existe $\alpha \in \mathbb{C}$ tel que $\alpha\Lambda_1 \subset \Lambda_2$. Soit $\mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$, $z \mapsto \alpha z$. Soit $\rho_i(z)$ la fonction de Weierstrass pour E_i. Montrer qu'ils existent des fractions rationnelles $r(x)$ et $t(x)$ telles que

$$\rho_2(\alpha z) = r_1(\rho_1(z)),\ \rho_2'(\alpha z) = \rho_1'(z) t(\rho_1(z)).$$