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 $\mathbb{P}^2_{\mathbb{C}}$.
On peut supposer C est donnée par l'équation $XY - Z^2 = 0$. Soit L : $aX + bY + cZ = 0$ une droite tangente à C. La droite $z = 0$ n'est pas tangente à C. On a donc soit $a \neq 0$, soit $b \neq 0$. Si $a \neq 0$, la droite L est tangente à C si et seulement si le discriminant de $-\frac{b}{a}Y^2 - \frac{c}{a}YZ - Z^2$ est nul, i.e. $c^2 - 4ab = 0$. On obtient la même équation pour $b \neq 0$ et on déduit que l'ensemble des droites tangentes à C forme une conique $c^2 - 4ab = 0$ dans l'espace projectif des droites de $\mathbb{P}^2_{\mathbb{C}}$ avec les coordonnées homogènes $[a : b : c]$. (on peut faire le meme argument sans écrire l'équation de C sous la forme $XY - Z^2 = 0$)

   (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' ?
Soit D (resp. D') une conique dans l'espace projectif des droites de $\mathbb{P}^2_{\mathbb{C}}$, correspondante aux droites tangentes à C (resp. à C'.) Les droites tangentes et à C, et à C' correspondent aux points d'intersection de ces deux coniques, d'après le théorème de Bézout, il y a 4 tels points, comptés avec mutiplicités. On ne peut donc pas 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 $\#E(\mathbb{F}_{71})$.
$\#E(\mathbb{F}_{71}) = 72$ d'après un résultat de cours (section 3.2.2), car $71 \equiv 3$ (mod 4).

   (b) Montrer que $E(\bar{\mathbb{F}}_{71})[3] \not\subseteq E(\mathbb{F}_{71})$.
En utilisant l'accouplement de Weil, si $E(\bar{\mathbb{F}}_{71})[3] \subseteq E(\mathbb{F}_{71})$, on a $\mu_3 \subset \mathbb{F}_{71}$ ce qui n'est pas le cas car $71 \equiv 2$ mod 3.

   (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).
$E(\mathbb{F}_{71}) = \mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/9$ car c'est le seul groupe d'ordre 72 qui ne contient pas $(\mathbb{Z}/3)^2$ (ce que l'on doit avoir d'après la question précédente car $E(\bar{\mathbb{F}}_{71})[3] \simeq (\mathbb{Z}/3)^2$) et dont le groupe de 2-torsion est au plus $(\mathbb{Z}/2)^2$.

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 $E(\mathbb{F}_{p^n}) = (p^{\frac{n}{2}} - (-1)^{\frac{n}{2}})^2$.

Comme E est une courbe elliptique supersingulière sur $\mathbb{F}_p$, on a $\#E(\mathbb{F}_p) = p + 1$, donc $a_E = 0$ et les racines α, β du polynôme caractéristique $x^2 - q$ de E sont $\pm\sqrt{q}$. On en déduit a formule en utilisant $E(\mathbb{F}_{p^n}) = p^n + 1 - \alpha^n - \beta^n$.

(b) Supposons ℓ 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.

Comme $E(\mathbb{F}_p)$ contient un point d'ordre ℓ, on a $\ell | p + 1$. Or $\#E(\mathbb{F}_{p^2}) = (p+1)^2$ d'après la question précédente, on obtient $\ell^2 \,|\, \#E(\mathbb{F}_{p^2})$. Si $E(\mathbb{F}_{p^2})$ ne contient un point d'ordre ℓ^2 et $E[\ell] \nsubseteq E(\mathbb{F}_{p^2})$, on a que $\#E(\mathbb{F}_{p^2}) = \mathbb{Z}/\ell \times A$ où A n'a pas de ℓ-torsion, contradiction avec $\ell^2 \,|\, \#E(\mathbb{F}_{p^2})$.

4. Soit $f \in \mathbb{Q}(t)$ une fraction rationnelle non constante : on lécrit $f = P/Q$, 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 $x \in \mathbb{Q}$ avec $h(x) \to \infty$.

Soit $\Phi : \mathbb{P}^1 \to \mathbb{P}^1, [1 : x] \mapsto [Q(x) : P(x)]$, cette application est bien définie. Comme P, Q n'ont pas de racines communes, d'après un résultat de cours $h(f(x)) = h(\Phi(x)) = dh(x) + O(1)$, d'où le résultat en divisant par $h(x)$ et en passant à la limite.

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.

On a $3P = 0 \Leftrightarrow 2P = -P \Leftrightarrow 3x^4 + 6ax^2 + 12bx - a^2 = 0$, après les simplifications, en appliquant la formule pour $2P$. Ainsi les x-coordonnées des points d'ordre exact 3 sont des racines du polynôme $3x^4 + 6ax^2 + 12bx - a^2$.

(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 $E(\mathbb{Q})[3]$.

Par la question précédente, on obtient $x = 0, y^2 = n$ ou $x^3 = -4n, y^2 = -3n$. Dans le deuxième cas on n'a pas de solutions entières. Dans le premier cas $n = m^2$ et on trove $E(\mathbb{Q})[3] = \{O_E, (0, m), (0, -m)\}$.

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 $\mathcal{O}^*_{K,S}/\mathcal{O}^{*2}_{K,S}$.
$S = \{q$ premier $, q|4p^6\}$, d'où $\mathcal{O}^*_{K,S}/\mathcal{O}^{*2}_{K,S} = \{\pm 1, \pm 2, \pm p, \pm 2p\}$.

(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 :

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

Determiner l'image par ϕ des points de 2-torsion.
$\phi(O_E) = (1,1,1)$, $\phi(P_1) = (-1,-p,p)$, $\phi(P_2) = (p,2,2p)$, $\phi(P_3) = (-p,-2p,2)$.

(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. $d_i = \pm 1, \pm 2$).
Si $\phi(Q) = (p^{r_1}d_1, p^{r_2}d_2, p^{r_1+r_2}d_3)$ où ou chaque d_i divise 2 et $r_i = 0$ ou 1 et on voit $r_1 + r_2$ modulo 2, alors $P = (r_2 P_1 + r_1 P_2)$ convient.

(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.

D'après la question précedente il suffit de montrer que pour tout (d_1, d_2, d_3) ou chaque d_i divise 2 et $d_3 = d_1 d_2$ modulo les carrés, le système déquations
(1) $d_1 u^2 - pv^2 = d_2 t^2$
(2) $d_1 u^2 + pv^2 = d_3 w^2$
n'a pas de solutions entières u, v, t, w avec u, v premiers entre eux. De la première équation $d_1 < 0 \Rightarrow d_2 < 0$, et de la deuxième $d_1 > 0 \Rightarrow d_3 > 0$. On a donc les cas suivants pour (d_1, d_2, d_3) à considérer :

$$(1,1,1), (1,2,2), (2,2,1), (2,1,2), (-1,-2,2), (-1,-1,-1), (-2,-1,2), (-2,-2,1).$$

Puisque l'image de ϕ est une puissance de 2, il suffit de montrer qu'au plus 3 de ces cas sont possibles.

i. $(-1,-1,1)$ n'est pas possible : $(2) \Rightarrow 3v^2 = u^2 + t^2$ mod 8. Si 2 ne divise pas v on a 3 est une somme de carrés ($1, 0$ ou 4) mod 8, ce qui n'est pas possible. Si $2|v$, $u^2 = 1$ mod 8 et $3v^2 = 0$ ou 4 donc $3v^2 = u^2 + t^2$ n'est pas possible.

ii. Montrons que $d_1 = \pm 1$ et $2|d_2$ n'est pas possible :
- *si $2|v$, on a $(1) \Rightarrow 2|u$ contradiction.*
- *si 2 ne divise pas v, on a mod 8 : $d_1u^2 - pv^2, d_1u^2 + pv^2 = (4, 2)$ ou $(-2, 4)$, en examinant les possibilités pour un carré mod 8 ($1, 0$ ou 4). Mais 4 n'est pas ± 2 fois un carré, contradiction.*

Cela élimine $(1, 2, 2), (1, -2, -2), (-1, -2, 2)$.

On a donc éliminé 4 élèments. Comme $Im\,\phi$ est un sous-groupe et $(2, 2, 1) \cdot (-2, -2, 1) = (-1, -1, 1)$, au plus un des éléments $(2, 2, 1)$ et $(-2, -2, 1)$ peut être dans l'image de ϕ. On en déduit que $\#Im\phi \leq 3$, donc E est de rang 0.

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.

Puisque L est un sous-module du module Λ_2 libre de rang 2, on a que L est lui-même est libre de rang au plus 2. Comme L contient Λ_1, on a que L est de rang 2. Écrivons $\Lambda_1 = \mathbb{Z}w_1 + \mathbb{Z}w_2$ et $L = \mathbb{Z}f_1 + \mathbb{Z}f_2$. Il reste à montrer que $f_1/f_2 \notin \mathbb{R}$. Puisque $\Lambda_1 \subseteq L$, ils existent $a, b, c, d \in \mathbb{Z}$ tels que $w_1 = af_1 + bf_2$ et $w_2 = cf_1 + df_2$. On a donc

$$\frac{w_1}{w_2} = \frac{a\frac{f_1}{f_2} + b}{c\frac{f_1}{f_2} + d}.$$

Si $\frac{f_1}{f_2} \in \mathbb{R}$, on déduit $\frac{w_1}{w_2} \in \mathbb{R}$, contradiction. On a donc que 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.

On peut écrire $C = L/\Lambda_1$ où $L \subset \mathbb{C}$ est un sous-groupe contenant $\mathbb{C}$. Soit N l'ordre de C. On a donc $NL \subset \Lambda_1$, i.e. $\Lambda_1 \subset L \subset \frac{1}{N}\Lambda_1$. D'après l'exercice précédent, L est un réseau et $\Lambda_3 = L$ convient.

(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 fonctions rationnelles $r(x)$ et $t(x)$ telles que

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

Comme $\alpha\Lambda_1 \subseteq \Lambda_2$, la fonction $\rho_2(\alpha z)$ est Λ_1-périodique : si $z \in \mathbb{C}$ et $w \in \Lambda_1$, on a $\alpha w \in \Lambda_2$ et donc $\rho_2(\alpha(z + w)) = \rho_2(\alpha z + \alpha w) = \rho_2(\alpha z)$.

Puisque ρ_2 est une fonction paire, $z \mapsto \rho_2(\alpha z)$ est Λ_1-périodique, d'après un résultat du cours, c'est une fonction rationnelle en ρ_1 : il existe une fonction rationnelle $r(x)$ telle que $\rho_2(\alpha z) = r_1(\rho_1(z))$. En dérivant, on obtient la deuxième formule.