MAT 562 - Introduction à la géométrie algébrique et aux courbes elliptiques

Examen - 13 mars 2023 - 3 heures

Documents autorisés : *polycopié, notes de cours et de PC, dictionnaire papier.*
Vous pouvez écrire en anglais ou en français.

Le sujet est composé de 4 exercices indépendants portant sur des parties différentes du cours :

Exercice 1	Variétés affines et projectives
Exercice 2	Courbes elliptiques sur $\mathbb{C}$
Exercice 3	Courbes elliptiques sur les corps finis
Exercice 4	Courbes elliptiques sur $\mathbb{Q}$

Les exercices ne sont pas classés par ordre de difficulté : n'hésitez donc pas à les traiter dans l'ordre de votre choix.

Exercice 1 Soit k un corps algébriquement clos de caractéristique 0.

1) Soit $n \geqslant 1$ un entier. Soient $F, G \in k[X_0, \ldots, X_n]$ deux polynômes homogènes non constants. Montrer que, si F et G sont premiers entre eux, alors l'ensemble $V_p(F) \smallsetminus V_p(G)$ est dense dans $V_p(F)$.

Soit maintenant Z l'ensemble des points

$$A = [x_0 : x_1 : x_2 : x_3 : x_4 : x_5] \in \mathbb{P}^5_k$$

tels que le polynôme $\pi_A(S,T) := x_0S^2 + x_1T^2 + x_2ST + x_3S + x_4T + x_5$ n'est ni constant ni irréductible dans $k[S,T]$.

2) a) Construire une application rationnelle $f : \mathbb{P}^5_k \to \mathbb{P}^5_k$ et un ouvert U de $\mathbb{P}^5_k$ tels que f soit définie sur U et $f(U) = Z$.

   b) En déduire que Z est irréductible.

3) a) Vérifier que Z n'est pas fermé dans $\mathbb{P}^5_k$.

   b) i) Trouver un polynôme homogène $F \in k[X_2, X_3, X_4, X_5]$ de degré 2 tel que :

$$Z \cap V_p(X_0, X_1) = V_p(X_0, X_1, F) \smallsetminus V_p(X_2).$$

   ii) Soit $A = [x_0 : x_1 : x_2 : x_3 : x_4 : x_5] \in Z \smallsetminus V_p(X_0(X_2^2 - 4X_0X_1))$. Montrer qu'il existe un point $B \in Z \cap V_p(X_0, X_1)$ tel que les variétés affines $V(\pi_A)$ et $V(\pi_B)$ sont isomorphes. Exprimer les coordonnées de B en fonction de celles de A.

   iii) En déduire que l'adhérence de Z dans $\mathbb{P}^5_k$ est :

$$\overline{Z} = V_p(X_5(X_2^2 - 4X_0X_1) + X_4^2X_0 - X_2X_3X_4 + X_1X_3^2).$$

   c) Calculer la dimension de $\overline{Z}$ et montrer que le lieu singulier de $\overline{Z}$ est l'ensemble des points $A \in \mathbb{P}^5_k$ tels que le polynôme π_A est un carré dans $k[S,T]$.

Exercice 2

1) Soit k un corps algébriquement clos. Dans $\mathbb{P}^2_k$, on considère une courbe elliptique E donnée par une équation de Weierstrass :

$$y^2z = x^3 + Axz^2 + Bz^3,$$

et on la munit de l'élément neutre $O := [0 : 1 : 0]$. On plonge $\mathbb{A}^2_k$ dans $\mathbb{P}^2_k$ via $(x,y) \mapsto [x : y : 1]$, et on se donne quatre points P_1, P_2, P_1', P_2' de $E \smallsetminus \{O\} = E \cap \mathbb{A}^2_k$ tels que :

$$P_1 + P_2 = P_1' + P_2' \neq O.$$

Dans $\mathbb{A}^2_k$, on introduit les droites suivantes :

$$\Delta := \begin{cases} \text{droite passant par } P_1 \text{ et } P_2 \text{ si } P_1 \neq P_2 \\ \text{droite tangente à } P_1 \text{ si } P_1 = P_2, \end{cases}$$

$$\Delta' := \begin{cases} \text{droite passant par } P'_1 \text{ et } P'_2 \text{ si } P'_1 \neq P'_2 \\ \text{droite tangente à } P'_1 \text{ si } P'_1 = P'_2. \end{cases}$$

Montrer que Δ et Δ' sont parallèles si, et seulement si, $\{P_1, P_2\} = \{P'_1, P'_2\}$. Soit maintenant $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ un réseau de $\mathbb{C}$. On note $\wp$ la fonction de Weierstraß associée.

2) a) Montrer qu'il existe une fonction méromorphe impaire ζ sur $\mathbb{C}$ telle que :

$$\forall z \in \mathbb{C} \smallsetminus \Lambda, \quad \zeta'(z) = -\wp(z)$$

Écrire la fonction ζ sous forme de série. S'agit-il d'une fonction Λ-elliptique ?

b) On fixe $y_0 \in \mathbb{C} \smallsetminus \frac{1}{2}\Lambda$, et on introduit les fonctions méromorphes :

$$\varphi(z) = \frac{1}{2} \cdot \frac{\wp'(z) - \wp'(y_0)}{\wp(z) - \wp(y_0)} \quad \text{et} \quad \psi(z) = \zeta(z + y_0) - \zeta(z) - \zeta(y_0).$$

Montrer qu'elles sont Λ-elliptiques.

c) Montrer que la fonction $\rho := \varphi - \psi$ est holomorphe sur tout le plan complexe.

d) En déduire que :

$$\frac{1}{2} \cdot \frac{\wp'(z) - \wp'(y)}{\wp(z) - \wp(y)} = \zeta(z + y) - \zeta(z) - \zeta(y)$$

pour tous $y, z \in \mathbb{C} \smallsetminus \Lambda$ tels que $z \pm y \in \mathbb{C} \smallsetminus \Lambda$.

3) Soit $(z_1, z_2, z'_1, z'_2) \in (\mathbb{C} \smallsetminus \Lambda)^4$ vérifiant :

$$\begin{cases} z_1 + z_2 = z'_1 + z'_2 \notin \Lambda \\ \zeta(z_1) + \zeta(z_2) = \zeta(z'_1) + \zeta(z'_2). \end{cases}$$

A l'aide des questions 1) et 2), montrer que $\{z_1, z_2\} = \{z'_1, z'_2\}$. On pourra commencer par supposer que $z_1 - z_2 \notin \Lambda$ et $z_3 - z_4 \notin \Lambda$.

Exercice 3 Soient k un corps parfait et E la courbe projective définie sur k par :

$$y^2 z = x^3 + 3z^3.$$

1) A quelle condition sur k la courbe E est-elle une courbe elliptique ?

Dans les questions qui suivent, on supposera toujours cette condition satisfaite.

2) a) Calculer les coordonnées des points de 2-torsion de $E(\overline{k})$.
   b) Calculer les coordonnées des points de 3-torsion de $E(\overline{k})$.
3) En prenant $k = \mathbb{F}_5$, calculer la structure des groupes $E(\mathbb{F}_5)$, $E(\mathbb{F}_{25})$ et $E(\mathbb{F}_{125})$.
4) On prend maintenant $k = \mathbb{F}_{31}$. On choisit le point $P = (1, 2) \in E(\mathbb{F}_{31})$. Le tableau qui suit fournit les coordonnées de certains multiples de P :

n	1	2	3	4	5	6	7	8
nP	(1,2)	(16,10)	(22,24)	(24,30)	(26,8)	(5,2)	(25,29)	(30,8)
n	9	10	11	12	13	14	15	16
nP	(9,22)	(4,6)	(14,22)	(18,10)	(6,23)	(28,21)	(11,30)	(7,6)
n	17	18	19	20	21	22	23	24
nP	(20,6)	(17,24)	(27,1)	(8,9)	(23,7)	(23,24)	(8,22)	(27,30)

   a) i) Quel est l'ordre r de P dans $E(\mathbb{F}_{31})$?
      ii) En déduire que P engendre $E(\mathbb{F}_{31})$.

Les questions qui suivent portent sur la cryptographie via des courbes elliptiques. Les données publiques initiales sont à chaque fois la courbe elliptique E et le point P.

   b) Arcanin[1] et Bulbizarre[2] souhaitent d'abord produire une clé secrète commune via le schéma de Diffie-Hellman. Arcanin choisit l'entier 17 comme clé privée et il reçoit le point $P_b = (7, 6)$ de la part de Bulbizarre.
      i) Quelle est la clé privée de Bulbizarre ?
      ii) Quelle est la clé secrète commune produite ?
   c) Arcanin et Bulbizarre échangent maintenant des messages via le cryptosystème ElGamal vu en cours. Pour qu'Arcanin lui adresse un message chiffré, Bulbizarre a commencé par lui envoyer le point $B = (20, 25)$. Il a ensuite reçu les points $M_1 = (6, 23)$ et $M_2 = (27, 30)$ de la part d'Arcanin. Pouvez-vous déchiffrer le message ?
   d) Pour terminer, Arcanin décide de signer ses messages pour Bulbizarre, via l'algorithme de signature électronique décrit en cours. Pour ce faire, il commence par envoyer le point $Q = (25, 29)$ à Bulbizarre. Bulbizarre reçoit ensuite le message $m = 32$, ainsi qu'une signature constituée du point $R = (14, 22)$ et de l'élément $z = 26 \in \mathbb{Z}/r\mathbb{Z}$. Le message a-t'il été envoyé par Arcanin ?

1. Pokémon feu  2. Pokémon plante/poison 

Exercice 4 On considère la courbe projective E définie sur $\mathbb{Q}$ par :

$$y^2z = x^3 - 64xz^2 + 16z^3.$$

On pose $O = [0 : 1 : 0]$.

1) Vérifier que E est une courbe elliptique.
2) Montrer qu'il existe un entier $r \geqslant 1$ tel que $E(\mathbb{Q}) \cong \mathbb{Z}^r$.

Dans la suite de l'exercice, nous allons montrer que $r \geqslant 2$.

3) Montrer qu'il suffit de trouver trois points P_1, P_2, P_3 dans $E(\mathbb{Q}) \smallsetminus 2E(\mathbb{Q})$ tels que $P_1 + P_2 + P_3 = O$.

Dans les deux questions qui suivent, on établit deux conditions suffisantes pour qu'un point $P \in E(\mathbb{Q})$ ne soit pas dans $2E(\mathbb{Q})$.

4) Dans cette question, on étudie l'ensemble $E(\mathbb{R})$. Pour ce faire, on plonge $\mathbb{A}^2_{\mathbb{R}}$ dans $\mathbb{P}^2_{\mathbb{R}}$ via $(x, y) \mapsto [x : y : 1]$, puis on munit $E(\mathbb{R}) \smallsetminus \{O\} = E(\mathbb{R}) \cap \mathbb{A}^2_{\mathbb{R}}$ de la topologie induite par la topologie métrique usuelle de $\mathbb{A}^2_{\mathbb{R}} = \mathbb{R}^2$.
   a) Tracer l'allure de la courbe $E(\mathbb{R}) \cap \mathbb{A}^2_{\mathbb{R}}$. Placer les points de 2-torsion sur le dessin.
   b) Montrer que $E(\mathbb{R}) \smallsetminus E[2]$ possède quatre composantes connexes : deux composantes connexes non bornées C_0^+ et C_0^-, et deux composantes connexes compactes C_1^+ et C_1^-.
   c) Soit C_0 l'adhérence de $C_0^+ \cup C_0^-$ dans $E(\mathbb{R}) \cap \mathbb{A}^2_{\mathbb{R}}$. Montrer que :

$$2E(\mathbb{R}) \subset C_0 \cup \{O\}.$$

5) Soit $P = [x_P : y_P : 1] \in E(\mathbb{Q})$ avec $v_2(x_P) = 3$. Supposons qu'il existe un point $Q = [x_Q : y_Q : 1] \in E(\mathbb{Q})$ tel que $P = 2Q$.
   a) Écrire une équation polynomiale de degré 4 vérifiée par x_Q.
   b) Obtenir une contradiction et en déduire que $P \notin 2E(\mathbb{Q})$.
6) Utiliser les questions 4) et 5) pour trouver des points P_1, P_2, P_3 vérifiant les hypothèses de la question 3).