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

Examen - 18 mars 2024 - 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 3 exercices indépendants portant sur des parties différentes du cours :

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

Exercice 1 Soit k un corps algébriquement clos de caractéristique nulle. Soient $d > n \geqslant 2$ des entiers et $P \in k[X]$ un polynôme de degré d. On considère la variété affine :

$$V := V(Y^n - P(X)) \subset \mathbb{A}^2_k.$$

1) Quelle est la dimension de la variété V ? Est-elle équidimensionnelle ?
2) Donner une condition nécessaire et suffisante sur le polynôme P pour que V soit irréductible et lisse.
3) La variété V peut-elle être isomorphe à $\mathbb{A}^1_k$?

On plonge maintenant $\mathbb{A}^2_k$ dans $\mathbb{P}^2_k$ via $(x, y) \mapsto [x : y : 1]$.

4) Quelle est l'adhérence $\overline{V}$ de V dans $\mathbb{P}^2_k$? Quelle est la dimension de la variété projective $\overline{V}$?
5) Donner une condition nécessaire et suffisante sur les entiers n et d et sur le polynôme P pour que $\overline{V}$ soit irréductible et lisse.

Dans la suite de l'exercice, on suppose que ces conditions sont satisfaites.

6) Montrer que, pour tout point $Q \in \overline{V}$, on a $m_Q(\overline{V}, T_Q(\overline{V})) \leqslant d$.
7) Exhiber un point de $\overline{V}$ pour lequel l'inégalité précédente est une égalité.
8) Trouver tous les polynômes P tels que la variété $\overline{V}$ contient au moins deux points pour lequels l'inégalité de la question 6) est une égalité.
9) Dans le cas où $d = 3$, la variété $\overline{V}$ est une courbe elliptique. Interpréter la question précédente en termes de la loi de groupe de $\overline{V}$.

Exercice 2 Soit $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ un réseau de $\mathbb{C}$. On note M le parallélogramme fondamental associé à (ω_1, ω_2) et on introduit le groupe des diviseurs :

$$\mathrm{Div}_\Lambda := \bigoplus_{z \in M} \mathbb{Z} \cdot [z].$$

Un élément de Div_Λ est donc une somme formelle $D = \sum_{z \in M} n_z[z]$ avec $(n_z)_{z \in M}$ une famille presque nulle d'entiers relatifs. On dit que $D \geqslant 0$ (resp. $D > 0$, $D \leqslant 0$, $D < 0$) si $n_z \geqslant 0$ (resp. $n_z > 0$, $n_z \leqslant 0$, $n_z < 0$) pour tout $z \in M$. On dit que D a un zéro en un point $z_0 \in M$ si $n_{z_0} > 0$. Le degré de D est défini par :

$$\deg D = \sum_{z \in M} n_z.$$

A chaque fonction Λ-elliptique non nulle f on peut lui associer un diviseur :

$$\mathrm{div}(f) := \sum_{z \in M} \mathrm{ord}_z(f) \cdot [z] \in \mathrm{Div}_\Lambda.$$

Dans tout l'exercice, on fixe un diviseur $D \in \mathrm{Div}_\Lambda$ et on s'intéresse à l'ensemble de fonctions Λ-elliptiques suivant :

$$L(D) := \{0\} \cup \{f \text{ fonction } \Lambda\text{-elliptique non nulle} : \mathrm{div}(f) + D \geqslant 0\}.$$

1) Vérifier que $L(D)$ est un $\mathbb{C}$-espace vectoriel. Dans la suite de l'exercice, on notera $\ell(D)$ sa dimension.
2) On suppose que $\deg D < 0$. Montrer que $\ell(D) = 0$.
3) On suppose que $\deg D = 0$. Montrer que $\ell(D) \leqslant 1$.
4) Dans toute cette question, on suppose que $\deg D > 0$.
   a) i) Soit $n \in \mathbb{N}_{>0}$. En utilisant la fonction $\wp$ associée au réseau Λ, donner une base de $L(n[0])$. En déduire que $\ell(n[0]) = n$.
      ii) A l'aide de la question précédente, montrer que, si 0 est le seul zéro de D, alors $\ell(D) \geqslant \deg D$.
      iii) En ne supposant plus que 0 est le seul zéro de D, en déduire que $\ell(D) \geqslant \deg D$.
   b) i) Montrer qu'il existe un diviseur E de degré 0 tel que $D - E \geqslant 0$ et $\ell(E) = 0$.
      ii) En déduire que $\ell(D) \leqslant \deg D$.

   Ainsi, dès que $\deg D > 0$, on a $\ell(D) = \deg(D)$.

Exercice 3

1) *(Question préliminaire)* Soit $\mathbb{F}$ un corps fini à q éléments, avec q carré parfait. Soit E une courbe elliptique sur $\mathbb{F}$ telle que $|E(\mathbb{F})| = q + 1 + 2\sqrt{q}$. Soit $\phi_q : (x, y) \mapsto (x^q, y^q)$ le morphisme de Frobenius sur E.
   a) Montrer que $\phi_q + \sqrt{q} = 0$.
   b) En déduire que
   $$E(\overline{\mathbb{F}})[\sqrt{q} + 1] \subset E(\mathbb{F}).$$
   c) Conclure que : $E(\mathbb{F}) \cong \mathbb{Z}/(\sqrt{q} + 1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q} + 1)\mathbb{Z}$.

Soient maintenant p un nombre premier et E la courbe projective définie sur $\mathbb{F}_p$ par :

$$y^2z = x^3 + 7x^2z - 30xz^2.$$

2) a) Quelles sont les valeurs de p pour lesquelles E est une courbe elliptique ?
   b) Pour la plus petite valeur de p telle que E est une courbe elliptique :
      i) Déterminer l'ordre et la structure du groupe $E(\mathbb{F}_p)$.

ii) Déterminer l'ordre et la structure du groupe $E(\mathbb{F}_{p^2})$.

3) On considère maintenant le cas où $p = 41$ et on choisit le point $P = (30, 16)$. Le tableau qui suit fournit les coordonnées de certains multiples de P :

n	1	2	3	4	5	6	7
nP	(30,16)	(36,35)	(27,14)	(23,16)	(22,25)	(39,30)	(15,21)
n	8	9	10	11	12	13	
nP	(21,22)	(29,38)	(8,33)	(6,40)	(40,35)	(0,0)	

a) Déterminer l'ordre de P. En déduire l'ordre et la structure du groupe $E(\mathbb{F}_{41})$.

Le sénateur Palpatine [1] envoie des messages à Dark Vador[1] via le cryptosystème ElGamal décrit en cours, appliqué à la courbe elliptique E et au point P. Les messages sont réprésentés par des multiples de P dans la courbe elliptique E via le dictionnaire suivant :

Point	Message
(40,6)	L'étoile de la Mort[2] se fait attaquer
(29,3)	Les rebelles[1] se cachent sur le satellite Yavin 4
(21,22)	Les jedi[1] complotent à la planète Coruscant
(15,21)	Tout se passe comme prévu au Sénat, n'interviens pas

De son côté, Maître Yoda[1] a réussi à accéder à leur canal de communication. Il voit que Palpatine a envoyé le message composé des points suivants à Dark Vador : $M_1 = (22, 25)$ et $M_2 = (8, 8)$. De plus, il sait qu'à ce moment-là, une séance au Sénat est en cours et tourne en faveur de Palpatine.

b) Aidez Maître Yoda à composer un message chiffré à destination de Dark Vador afin de l'attirer sur le satellite Yavin 4 pour lui tendre un piège. Pour ce faire, aidez-le à choisir le message qu'il doit envoyer parmi les possibilités suivantes :

A) $M_1' = (39, 30), M_2' = (23, 16)$, B) $M_1' = (6, 40), M_2' = (15, 21)$.
C) $M_1' = (6, 1), M_2' = (21, 19)$, D) $M_1' = (15, 20), M_2' = (8, 33)$.

4) Dans cette question, on considère la courbe elliptique $\tilde{E}$ définie sur $\mathbb{Q}$ par :

$$y^2z = x^3 + 7x^2z - 30xz^2.$$

a) Trouver des entiers a et b tels que $\tilde{E}$ est isomorphe à la courbe elliptique d'équation $y^2z = x^3 + axz^2 + bz^3$.

b) Calculer $\tilde{E}(\mathbb{Q})_{\text{tors}}$.

c) Montrer que le rang r de $\tilde{E}$ vérifie $1 \leqslant r \leqslant 7$.

1. Personnages de Star Wars. Maître Yoda collabore avec les rebelles et les jedi, et s'oppose au sénateur Palpatine et à Dark Vador 2. Station de combat utilisée par Palpatine et Dark Vador