MAT 562 - Introduction to algebraic geometry and elliptic curves

Exam - 18 March 2024 - 3 hours

Allowed documents : *course notes, handwritten notes, printed dictionnary. You can write in French or in English.*

The exam is composed of 3 independent exercises that cover different parts of the course :

Exercise	Topic
Exercise 1	Affine and projective varieties
Exercise 2	Elliptic curves over $\mathbb{C}$
Exercise 3	Elliptic curves over finite fields and over $\mathbb{Q}$

Exercice 1 Let k be an algebraically closed field of characteristic 0. Let $d > n \geqslant 2$ be integers and $P \in k[X]$ a polynomial of degree d. Consider the affine variety :

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

1) What is the dimension of the variety V ? Is it equidimensional ?
2) Give a necessary and sufficient condition on the polynomial P for V to be irreducible and smooth.
3) Can the variety V be isomorphic to $\mathbb{A}^1_k$?

We now embed $\mathbb{A}^2_k$ into $\mathbb{P}^2_k$ by the map $(x, y) \mapsto [x : y : 1]$.

4) What is the closure $\overline{V}$ of V in $\mathbb{P}^2_k$? What is the dimension of the projective variety $\overline{V}$?
5) Give a necessary and sufficient condition on the integers n and d and on the polynomial P for $\overline{V}$ to be irreducible and smooth.

In the sequel of the exercise, we assume that these conditions are satisfied.

6) Prove that, for every point $Q \in \overline{V}$, we have $m_Q(\overline{V}, T_Q(\overline{V})) \leqslant d$.
7) Exhibit a point of $\overline{V}$ for which the previous inequality is an equality.
8) Find all polynomials P such that the variety $\overline{V}$ contains at least two points for which the inequality of question 6) is an equality.
9) When $d = 3$, the variety $\overline{V}$ is an elliptic curve. Provide an interpretation of the previous question in terms of the group law on $\overline{V}$.

Exercice 2 Let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ be a lattice of $\mathbb{C}$. Denote by M the fundamental parallelogram associated to (ω_1, ω_2) and introduce the group of divisors :

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

An element of Div_Λ is then a formal sum $D = \sum_{z \in M} n_z[z]$ with $(n_z)_{z \in M}$ a family of integers such that $n_z = 0$ for almost all z. We say that $D \geqslant 0$ (resp. $D > 0$, $D \leqslant 0$, $D < 0$) if $n_z \geqslant 0$ (resp. $n_z > 0$, $n_z \leqslant 0$, $n_z < 0$) for all $z \in M$. We say that D has a zero at a point $z_0 \in M$ if $n_{z_0} > 0$. The degree of D is defined by :

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

To each non-zero Λ-elliptic function f one can associate a divisor :

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

In the whole exercise, we fix a divisor $D \in \mathrm{Div}_\Lambda$ and we aim at understanding the following set of Λ-elliptic functions :

$$L(D) := \{0\} \cup \{f \text{ a non-zero } \Lambda\text{-elliptic function} : \mathrm{div}(f) + D \geqslant 0\}.$$

1) Check that $L(D)$ is a $\mathbb{C}$-vector space. In the sequel of the exercise, we denote by $\ell(D)$ its dimension.
2) Assume that $\deg D < 0$. Prove that $\ell(D) = 0$.
3) Assume that $\deg D = 0$. Prove that $\ell(D) \leqslant 1$.
4) In this question, we assume that $\deg D > 0$.
   a) i) Let $n \in \mathbb{N}_{>0}$. By using the $\wp$ function associated to the lattice Λ, give a basis of $L(n[0])$. Deduce that $\ell(n[0]) = n$.
      ii) Thanks to the previous question, prove that, if 0 is the only zero of D, then $\ell(D) \geqslant \deg D$.
      iii) Without assuming anymore that 0 is the only zero of D, deduce that $\ell(D) \geqslant \deg D$.
   b) i) Prove that there exists a divisor E of degree 0 such that $D - E \geqslant 0$ and $\ell(E) = 0$.
      ii) Deduce that $\ell(D) \leqslant \deg D$.

   Thus $\ell(D) = \deg(D)$ whenever $\deg D > 0$.

Exercice 3

1) *(Preliminary question)* Let $\mathbb{F}$ be a finite field with q elements and with q perfect square. Let E be an elliptic curve over $\mathbb{F}$ such that $|E(\mathbb{F})| = q + 1 + 2\sqrt{q}$. Let $\phi_q : (x, y) \mapsto (x^q, y^q)$ be the Frobenius morphism on E.
   a) Prove that $\phi_q + \sqrt{q} = 0$.
   b) Deduce that
   $$E(\overline{\mathbb{F}})[\sqrt{q} + 1] \subset E(\mathbb{F}).$$
   c) Conclude that : $E(\mathbb{F}) \cong \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}+1)\mathbb{Z}$.

Let now p be a prime number and E the projective curve defined over $\mathbb{F}_p$ by :

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

2) a) What are the values of p for which E is an elliptic curve ?
   b) For the smallest value of p such that E is an elliptic curve :
      i) Determine the order and the structure of the group $E(\mathbb{F}_p)$.
      ii) Determine the order and the structure of the group $E(\mathbb{F}_{p^2})$.
3) Consider now the case where $p = 41$ and choose the point $P = (30, 16)$. The following table provides some multiples of 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) Determine the order of P. Deduce the order and the structure of the group $E(\mathbb{F}_{41})$.

Senator Palpatine [1] sends messages to Darth Vader[1] via the ElGamal cryptosystem described in class, applied to the elliptic curve E and to the point P. Messages are represented by multiples of P in the elliptic curve E according the the following dictionnary :

Point	Message
(40,6)	The Death Star[2] is being attacked
(29,3)	The rebels[1] are hidden on Satellite Yavin 4
(21,22)	The jedi[1] conspire on Planet Coruscant
(15,21)	Everything is happening as planned at the Senate, do not intervene

On his side, Master Yoda[1] has managed to access their communication channel. He sees that Palpatine has sent to Darth Vader the message composed of the following points : $M_1 = (22, 25)$ and $M_2 = (8, 8)$. Moreover, he knows that at that moment, a session in the Senate is ongoing and evolving just as Palpatine wants.

b) Help Master Yoda to compose an encoded message to be sent to Darth Vader in order to decoy him into Satellite Yavin 4. For that purpose, help him choose the message he should send among the following possibilities :
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) In this question, we consider the elliptic curve $\tilde{E}$ defined over $\mathbb{Q}$ by :

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

a) Find integers a and b such that $\tilde{E}$ is isomorphic to the elliptic curve defined by the equation $y^2z = x^3 + axz^2 + bz^3$.
b) Compute $\tilde{E}(\mathbb{Q})_{\text{tors}}$.
c) Show that the rank r of $\tilde{E}$ satisfies $1 \leqslant r \leqslant 7$.

1. Characters from Star Wars. Master Yoda collaborates with the rebels and with the jedi, and works against Senator Palpatine and Darth Vader 2. Combat station used by Palpatine and Darth Vader