MAT 562 - Introduction to algebraic geometry and elliptic curves

Exam - 13th March 2023 - 3 hours

Allowed documents : *course notes, notes from the classes and tutorials, printed dictionnary. You can write in English or in French.*

The exam consists in 4 independent exercises that concern different parts of the course :

Exercise 1	Affine and projective varieties
Exercise 2	Elliptic curves over $\mathbb{C}$
Exercise 3	Elliptic curves over finite fields
Exercise 4	Elliptic curves over $\mathbb{Q}$

The exercises are not ordered by difficulty : do not hesitate to treat them in the order of your choice.

Exercise 1 Let k be a field of characteristic 0.

1) *(Preliminary question)* Let $n \geqslant 1$ be an integer. Let $F, G \in k[X_0, \ldots, X_n]$ be two non-constant homogeneous polynomials. Prove that, if F and G are coprime, then the set $V_p(F) \smallsetminus V_p(G)$ is dense in $V_p(F)$.

Let now Z be the set of points

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

such that the polynomial $\pi_A(S,T) := x_0 S^2 + x_1 T^2 + x_2 ST + x_3 S + x_4 T + x_5$ is neither constant nor irreducible in $k[S,T]$.

2) In this question, we study the irreducibility of Z.
   a) Construct a rational map $f : \mathbb{P}^5_k \to \mathbb{P}^5_k$ and an open subset U of $\mathbb{P}^5_k$ such that f is defined on U and $f(U) = Z$.
   b) Deduce that Z is irreducible.
3) In this question, we study the closure of Z in $\mathbb{P}^5_k$.
   a) Check that Z is not closed in $\mathbb{P}^5_k$.
   b) i) Find a homogeneous polynomial $F \in k[X_2, X_3, X_4, X_5]$ of degree 2 such that :

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

      ii) Let $A = [x_0 : x_1 : x_2 : x_3 : x_4 : x_5] \in Z \smallsetminus V_p(X_0(X_2^2 - 4X_0X_1))$. Prove that there exists a point $B \in Z \cap V_p(X_0, X_1)$ such that the affine varieties $V(\pi_A)$ and $V(\pi_B)$ are isomorphic. Write down the coordinates of B in terms of the coordinates of A.

      iii) Deduce that the closure of Z in $\mathbb{P}^5_k$ is :

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

   c) Compute the dimension of $\overline{Z}$ and prove that the singular locus of $\overline{Z}$ is the set of points $A \in \mathbb{P}^5_k$ such that the polynomial π_A is a square in $k[S,T]$.

Exercise 2

1) Let k be an algebraically closed field. In $\mathbb{P}^2_k$, consider an elliptic curve E given by a Weierstraß equation :

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

and endow it with the neutral element $O := [0:1:0]$. Embed $\mathbb{A}_k^2$ into $\mathbb{P}_k^2$ via $(x,y) \mapsto [x:y:1]$, and consider four points P_1, P_2, P_1', P_2' of $E \setminus \{O\} = E \cap \mathbb{A}_k^2$ such that :

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

In $\mathbb{A}_k^2$, introduce the following lines :

$$\Delta := \begin{cases} \text{line passing through } P_1 \text{ and } P_2 \text{ if } P_1 \neq P_2 \\ \text{line tangent to } P_1 \text{ if } P_1 = P_2, \end{cases}$$

$$\Delta' := \begin{cases} \text{line passing through } P_1' \text{ and } P_2' \text{ if } P_1' \neq P_2' \\ \text{line tangent to } P_1' \text{ if } P_1' = P_2', \end{cases}$$

Prove that Δ and Δ' are parallel if, and only if, $\{P_1, P_2\} = \{P_1', P_2'\}$.

Let now $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ be a lattice in $\mathbb{C}$. Denote by $\wp$ the Weierstraß associated function.

2) a) Prove that there exists an odd meromorphic function ζ on $\mathbb{C}$ such that :

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

Write the ζ function as a convergent series. Is it a Λ-elliptic function ?

b) Fix $y_0 \in \mathbb{C} \setminus \frac{1}{2}\Lambda$, and introduce the meromorphic functions :

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

Prove that they are Λ-elliptic.

c) Prove that the function $\rho := \varphi - \psi$ is holomorphic on the whole complex plane.

d) Deduce that :

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

for all $y, z \in \mathbb{C} \setminus \Lambda$ such that $z \pm y \in \mathbb{C} \setminus \Lambda$.

3) Let $(z_1, z_2, z_1', z_2') \in (\mathbb{C} \setminus \Lambda)^4$ be such that :

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

By using questions 1) and 2), prove that $\{z_1, z_2\} = \{z_1', z_2'\}$. You may start by assuming that $z_1 - z_2 \notin \Lambda$ and $z_1' - z_2' \notin \Lambda$.

Exercise 3 Let k be a perfect field and let E be the projective curve defined over k by :

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

1) Under which condition on k is the curve E an elliptic curve ?

In the subsequent questions, we will assume that this condition is always satisfied.

2) a) Compute the coordinates of the 2-torsion points in $E(\overline{k})$.

   b) Compute the coordinates of the 3-torsion points in $E(\overline{k})$.

3) By taking $k = \mathbb{F}_5$, compute the structure of the groups $E(\mathbb{F}_5)$, $E(\mathbb{F}_{25})$ and $E(\mathbb{F}_{125})$.

4) Take now $k = \mathbb{F}_{31}$. Choose the point $P = (1, 2) \in E(\mathbb{F}_{31})$. The following table provides the coordinates of some multiples of 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) What is the order r of P in $E(\mathbb{F}_{31})$?

      ii) Deduce that P generates $E(\mathbb{F}_{31})$.

   The following questions concern elliptic curve cryptography. The intial public data are always the elliptic curve E and the point P.

   b) Arcanine[1] and Bulbasaur[2] would first like to produce a common secret key via the Diffie-Hellman method. Arcanine chooses the integer 17 as private key and he receives the point $P_b = (7, 6)$ from Bulbasaur.

      i) What is the private key of Bulbasaur ?

      ii) What is the produced common private key ?

   c) Arcanine now wants to securely send messages to Bulbasaur thanks to the ElGamal encryption algorithm seen in class. For that purpose, Bulbasaur starts by sending the point $B = (20, 25)$ to Arcanine. He then receives the points $M_1 = (6, 23)$ and $M_2 = (27, 30)$ from Arcanine. Can you decrypt the message ?

1. Fire-type Pokémon  2. Plant/poison-type Pokémon 

d) Finally, Arcanine decides to sign his messages to Bulbasaur, via the electronic signature algorithm described in class. For that purpose, he starts by sending the point $Q = (25, 29)$ to Bulbasaur. Bulbasaur then receives the message $m = 32$, as well as a signature consisting of the point $R = (14, 22)$ and the element $z = 26 \in \mathbb{Z}/r\mathbb{Z}$. Has the message been sent by Arcanine ?

Exercise 4 Consider the projective curve E defined over $\mathbb{Q}$ by :

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

Set $O = [0 : 1 : 0]$.

1) Check that E is an elliptic curve.
2) Prove that there exists an integer $r \geqslant 1$ such that $E(\mathbb{Q}) \cong \mathbb{Z}^r$.

In the rest of the exercise, we aim at proving that $r \geqslant 2$.

3) Prove that it suffices to find three points P_1, P_2, P_3 in $E(\mathbb{Q}) \smallsetminus 2E(\mathbb{Q})$ such that $P_1 + P_2 + P_3 = O$.

In the next two questions, we settle two sufficient conditions for a point $P \in E(\mathbb{Q})$ not to be in $2E(\mathbb{Q})$.

4) In this question, we study the set $E(\mathbb{R})$. For that purpose, we embed $\mathbb{A}^2_{\mathbb{R}}$ in $\mathbb{P}^2_{\mathbb{R}}$ via the map $(x, y) \mapsto [x : y : 1]$, and we endow $E(\mathbb{R}) \smallsetminus \{O\} = E(\mathbb{R}) \cap \mathbb{A}^2_{\mathbb{R}}$ with the topology induced by the usual metric topology on $\mathbb{A}^2_{\mathbb{R}} = \mathbb{R}^2$.
   a) Draw the curve $E(\mathbb{R}) \cap \mathbb{A}^2_{\mathbb{R}}$. Place the 2-torsion points on the picture.
   b) Prove that $E(\mathbb{R}) \smallsetminus E[2]$ has four connected components : two unbounded connected components C_0^+ and C_0^-, and two compact connected components C_1^+ and C_1^-.
   c) Let C_1 be the closure of $C_1^+ \cup C_1^-$ in $E(\mathbb{R}) \cap \mathbb{A}^2_{\mathbb{R}}$. Prove that :

$$C_1 \cap 2E(\mathbb{R}) = \emptyset.$$

5) Let $P = [x_P : y_P : 1] \in E(\mathbb{Q})$ be such that $v_2(x_P) = 3$. Assume that there exists a point $Q = [x_Q : y_Q : 1] \in E(\mathbb{Q})$ such that $P = 2Q$.
   a) Write down a degree 4 polynomial equation satisfied by x_Q.
   b) Get a contradiction and deduce that $P \notin 2E(\mathbb{Q})$.
6) Use questions 4) and 5) to find points P_1, P_2, P_3 satisfying the assumptions of question 3).