Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2020	MATH4151-WE01

Title: Topics in Algebra and Geometry IV

Time (for guidance only):	3 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: There is no restriction on the model of calculator which may be used.

Instructions to Candidates:	Credit will be given for your answers to all questions. All questions carry the same marks. Please start each question on a new page. Please write your CIS username at the top of each page. Show your working and explain your reasoning.

Revision:	

Throughout K denotes an algebraically closed field unless specified differently.

Q1 **1.1** Assume $\mathrm{char}(K) = 0$. Let $g(x) \in K[x]$ of odd degree $d \geq 5$ and let $f(x,y) = y^2 - g(x)$.

(i) Show that $f(x,y)$ is irreducible in $K[x,y]$.

(ii) Derive a criterion for the associated affine curve C_f to be non-singular.

(iii) State when the projective closure of C_f is non-singular.

1.2 Let E be an elliptic curve defined by the equation

$$Y^2Z = X^3 + bXZ^2 + cZ^3, \quad b, c \in K,$$

over a field K with $char(K) = 3$ and neutral point $\mathcal{O} = [0:1:0]$. Find the order of the groups $E[3]$, $E[5]$ and $E[45]$. Justify your answer.

Q2 Let C be a plane projective curve of degree $d \geq 3$ and over any field K given by

$$F(X,Y,Z) = (\alpha Y + Z)X^{d-1} + (-Y^2 + YZ + 2Z^2)X^{d-2} + \sum_{j=3}^{d} G_j(Y,Z)X^{d-j}$$

with $\alpha \in K$ and $G_j(Y,Z)$ homogenous of degree j. Note $P := [1:0:0] \in C$.

2.1 Compute the evaluation of the Hessian $\mathcal{H}_F$ of F at the point P. For which α does the Hessian $\mathcal{H}_F$ at P vanish?

2.2 Let $Q = [a:b:c] \neq P$ be another point in the plane. Write down the equation for the line L through P and Q and compute from the definition the intersection multiplicity $I_P(C,L)$. When do we have $I_P(C,L) = 1$, $I_P(C,L) = 2$, $I_P(C,L) \geq 3$? Interpret your answer.

Q3 Let $P_1, \ldots, P_6$ be six pairwise different points on $\mathbb{P}^2_K$ with no three points collinear. For $j = 1, \ldots, 6$, let L_j be the line through P_j and P_{j+1} (with L_6 determined by P_6 and P_1). Let $Q_1 = L_1 \cap L_4$, $Q_2 = L_2 \cap L_5$, and $Q_3 = L_3 \cap L_6$. Assume that Q_1, Q_2, Q_3 all lie on a line L. Let F_1 be the cubic polynomial underlying $C_1 := L_1 \cup L_3 \cup L_5$ and F_2 the one for $C_2 := L_2 \cup L_4 \cup L_6$.

3.1 Show that all lines L_i are pairwise different. Also show that the points Q_i are also pairwise different and distinct from the points P_i.

3.2 Show that $C_1 \cap C_2 = \{P_1, \ldots, P_6, Q_1, Q_2, Q_3\}$.

3.3 Show that the points P_i do not lie on L.

3.4 Let $Q = [a:b:c] \neq Q_i$ be a fourth point on L, not belonging to either C_1 or C_2. Let $\lambda = F_1(a,b,c)$ and $\mu = F_2(a,b,c)$. Consider

$$G(X,Y,Z) := \mu F_1(X,Y,Z) - \lambda F_2(X,Y,Z).$$

Show that $G \neq 0$. Let C_G be the associated curve. Show that L and C_G must have a common component.

3.5 Use this to show that the points $P_1, \ldots, P_6$ must lie on a conic.

3.6 Give (in words) a geometric interpretation of the result proved in **3.5**.

Q4 **4.1** Let $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2,\ w_1, w_2 \in \mathbb{C}$, be a lattice in $\mathbb{C}$. We write $\wp(z)$ for $\wp(z;\Lambda)$, the Weierstrass $\wp$-function attached to the lattice Λ.

Find the zeros and poles in $\mathbb{C}$, as well as their orders, of the functions:

(i) $f(z) := \wp(4z) - \wp(z)$.

(ii) $g(z) := \wp(5z) - \wp(z)$.

4.2 You are now given that the elliptic curve E defined by $Y^2Z = 4X^3 - 4XZ^2$ over $\mathbb{C}$ corresponds to the lattice $\Lambda = \mathbb{Z}w + \mathbb{Z}\,i\,w$ for some real number w. Does the map $\psi : \mathbb{C} \to \mathbb{C}$, defined as $\psi(z) := i\,z$, induce an endomorphism on $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$? Justify your answer.

Q5 **5.1** Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ where $q = p^r$, with p a prime number, and $r \in \mathbb{N}$. Assume that $E(\mathbb{F}_q)$ is isomorphic to the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for some $m \in \mathbb{N}$.

(i) Show that p does not divide m.

(ii) Show that m divides $q - 1$.

(iii) Let $\{P_1, P_2\}$ be a basis of $E[m]$, and consider the matrix $A_m \in M_2(\mathbb{Z}/m\mathbb{Z})$ associated to the Frobenius endomorphism $\phi_q \in End(E)$, when restricted to $E[m]$, with respect to the selected basis. Show that,

$$\mathrm{Trace}\,(A_m) \equiv 2 \mod m.$$

(iv) Set $a := (q + 1) - \#E(\mathbb{F}_q)$. Does the equation $a = 2 + 3\,m$ hold? Justify your answer.

5.2 Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$, and ℓ be a prime number with $q^2 - q \not\equiv 0 \mod \ell$. Set $N := \#E(\mathbb{F}_q)$ and assume that ℓ divides N. Assume further that there exists a point $P \in E[\ell]$ such that $\phi_q(P) \neq P$, where $\phi_q \in End(E)$ is the Frobenius endomorphism. Show that,

(i) There exists a point $Q \in E(\mathbb{F}_q)[\ell] := E(\mathbb{F}_q) \cap E[\ell]$ such that $\{P, Q\}$ is a basis for $E[\ell]$.

(ii) For any integer $n > 1$ we have,

$$\phi_q^n(P) = P \text{ if and only if } \sum_{i=0}^{n-1} q^i \equiv 0 \mod \ell.$$