Elliptic curves exercise sheet 2

David Holmes

Abstract

This is due in on 16/2/2015 before the start of the lecture (13:45), either by email to ellipticcurvesleiden@gmail.com (with subject line EC2) or a physical copy in Giulio Orecchia's mailbox. Please include your student number on your answer sheet.

Attempt all questions unless otherwise noted. You may work together on the problems, but please write up your answers separately.

The grade for this work is out of 25. Of this, 20 points are for the content, and 5 points are for clarity and style. This is about mathematical style, not handwriting (though the latter must be legible - if you have terrible handwriting, it may help to use `LATEX`). It is likely that only a subset of the questions (to be chosen later) will be graded, but please attempt all questions.

0. Read up to page 11 of the online lecture notes (this is approximately what was covered in the lecture, but contains some extra details). This will not be graded.

1. Let
$$I = (x^2 + y^2 - 3) \lhd \mathbb{Q}[x, y].$$
Compute $V_I^A(\mathbb{Q})$.

2. (a) Let $(E, 0)$ be an elliptic curve. Show that the equation for E is unique if we require that the coefficient of y^2z is 1.

   (b) Let $C \subset \mathbb{P}^2_k$ be a plane curve. Let f be an equation for C. We say C is *irreducible* if the polynomial f is irreducible in $k[x_0, \cdots, x_n]$. Check this does not depend on the choice of equation for C. Show that every elliptic curve is irreducible.

3. This question is about checking when varieties are smooth.

   (a) Let k be a field, and fix $n > 0$. Let $f \in k[x_1, \cdots, x_n]$ be an irreducible non-zero polynomial with no terms of degree 0 or 1. Show that $V^A_{(f)}$ is not smooth. Give a counterexample if we do not assume f is irreducible.

   (b) Let k be a field, and let a, $b \in k$. Define a projective variety E/k by the equation $y^2z = x^3 + axz^2 + bz^3$. Define $\Delta = 2(4a^3 + 27b^2)$. Show that E is smooth if and only if $\Delta \neq 0$. This is a special case of the discriminant of an elliptic curve.

4. Fix a field k and an integer $n \geq 0$. Let $\varphi \colon k^{n+1} \to k^{n+1}$ be a linear automorphism.

(a) Show that φ induces an automorphism $\mathbb{P}_\varphi$ of the functor $\mathbb{P}^n_k$. We call such a map a *linear automorphism of* $\mathbb{P}^n$;

(b) Let $V \subset \mathbb{P}^n_k$ be a projective variety. We define the image of V under $\mathbb{P}_\varphi$ in the obvious way as the functor

$$\begin{aligned} \underline{\mathrm{Fld}}_k &\to \underline{\mathrm{Set}} \\ K &\mapsto \{\mathbb{P}_\varphi(K)(V(K))\}, \end{aligned}$$

which the obvious action on morphisms (check this makes sense).

Show that the image of V under $\mathbb{P}_\varphi$ is also a variety.

(c) Assume now that the characteristic of k is not 3. Let $(E, 0)$ be an elliptic curve over k. Find a linear automorphism of $\mathbb{P}^2$ which fixes $[(0, 1, 0)]$ puts the equation for E in the form

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

for some A, $B \in k$.

5. Fix a field k and an integer n. Let $I \lhd k[x_0, \cdots, x_n]$ be a homogeneous ideal. Show that the projective variety V_P^I is empty if and only if the radical ideal $\sqrt{I}$ contains the ideal $(x_0, \cdots, x_n)$.

[Recall that $\sqrt{I} = \{f \in k[x_0, \cdots, x_n] : f^r \in I \text{ for some r} > 0\}$.]

Remark: the ideal $(x_0, \cdots, x_n)$ is often called the 'irrelevant ideal'.

6. *This is a difficult optional exercise, which assumes quite a lot more algebraic geometry. The idea is to understand the functor of points of a projective variety over a ring which is *not* a field.

(a) Let R be a ring and $I = (f_1, \ldots, f_m) \subset R[T_0, \ldots, T_n]$ a homogeneous ideal, where each f_i is a homogeneous polynomial of degree d_i. Show that the following two functors are isomorphic:

$$\begin{aligned} F_1 : R\text{-Alg} &\to \text{Sets} \\ A &\mapsto \mathrm{Hom}_{\mathrm{Sch}_R}\left(\operatorname{Spec} A, \operatorname{Proj} \frac{R[T_0, \ldots, T_n]}{I}\right) \end{aligned}$$

and

$$F_2 : R\text{-Alg} \to \text{Sets}$$

$$A \mapsto \left\{ (L; t_0, \ldots, t_n) : \begin{array}{l} L \text{ a locally free } A\text{-module of rank 1} \\ (t_0, \ldots, t_n) \in L^{n+1} \\ t_0A + \cdots + t_nA = L \\ \forall j \in \{1, \ldots m\}, f_j(\underline{t}) = 0 \text{ in } L^{\otimes d_j} \end{array} \right\} / \sim$$

In particular, you should give a precise definition of the symbol '$\sim$' in the definition of F_2.

(b) Give an example of a $\mathbb{Z}[\sqrt{-5}]$-valued point of $\mathbb{P}^1_{\mathbb{Z}}$ which cannot be written in the form $(a_0 : a_1)$ with a_0 and a_1 in $\mathbb{Z}[\sqrt{-5}]$.