Elliptic curves exercise sheet 1

David Holmes

Abstract

This is due in on 9/2/2015 before the start of the lecture (11:15 - note the earlier time), either by email to ellipticcurvesleiden@gmail.com (with subject line EC1) 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.

1. Read up to page 1.6 of the online lecture notes (this is approximately what was covered in the lecture, but contains some extra details). This will not be graded! If you have not seen projective space before, it may help to also read the first section of Appendix A (Projective Geometry) of the book 'Rational points on elliptic curves' by Silverman and Tate. Their definitions are not the same as ours (they work with sets of points rather than functors), but it may aid your intuition.

2. (a) Let k be a field and $n \geq 0$ an integer. Recall that we $\mathbb{P}^n$ for the rule which sends a field L/k to the set $L^{n+1} \setminus \{(0, \cdots, 0)\}/\sim$, where $(x_0, \cdots, x_n) \sim (y_0, \cdots, y_n)$ if and only if there exists $\lambda \in L^\times$ such that

$$(\lambda x_0, \cdots, \lambda x_n) \sim (y_0, \cdots, y_n).$$

Show that this rule can be extended to a functor from $\underline{\text{Fields}_k}$ to $\underline{\text{Set}}$. For this, you need to decide what the functor does on morphisms, and then check that various axioms are satisfied.

(b) Now let $I \lhd k[x_0, \cdots, x_n]$ be a homogeneous ideal. Check that the rule

$$\begin{aligned} V_I^P \colon \underline{\mathrm{Fld}}_k &\to \underline{\mathrm{Set}} \\ K &\mapsto \{[(x_0, \cdots, x_n)] \in \mathbb{P}^n_k(K) : f(x_0, \cdots, x_n) = 0 \text{ for all homogeneous } f \text{ in } I\} \end{aligned}$$

as given in the lecture does actually give a well-defined sub-functor of $\mathbb{P}^n_k$.

3. Let k be a finite field with q elements, and let $n \geq 0$ be a integer.

   (a) What is the cardinality of the set $\mathbb{A}^n(k)$?

   (b) What is the cardinality of the set $\mathbb{P}^n(k)$?

4. In this question, you will show that a projective variety is empty iff its intersection with all the affine coordinate charts is empty. Fix a field k, and an integer $n \geq 0$. Let $I \lhd k[x_0, \cdots, x_n]$ be a homogeneous ideal, generated by homogeneous polynomials $f_1, \cdots, f_r$.

   (a) Show that V_I^P is the same subfunctor of $\mathbb{P}^n_k$ as that given by the rule

$$\begin{aligned} V_I^P \colon \underline{\mathrm{Fld}}_k &\to \underline{\mathrm{Set}} \\ K &\mapsto \{[(x_0, \cdots, x_n)] \in \mathbb{P}^n_k(K) : f_j(x_0, \cdots, x_n) = 0 \text{ for all } 1 \leq j \leq r\} \end{aligned}$$

   (b) For $0 \leq i \leq n$, let $\varphi_i \colon \mathbb{A}^n \to \mathbb{P}^n$ be the 'coordinate chart' natural transformation defined in the lecture: to a field K/k, it associates the map $\varphi_i(K)$ sending $(x_1, \cdots, x_n)$ to the equivalence class $[(x_1, \cdots, x_i, 1, x_{i+1}, \cdots, x_n)]$. Define V_I^i to be the functor

$$\begin{aligned} \underline{\mathrm{Fld}}_k &\to \underline{\mathrm{Set}} \\ K &\mapsto \{(x_1, \cdots, x_n) \in \mathbb{A}^n_k(K) : \varphi_i(K)(x_1, \cdots, x_n) \in V_I^P(K).\} \end{aligned}$$

   Show that V_I^i is an affine variety (this means that it is of the form V_J^A for some suitable ideal J - the challenge is to find a suitable J). It is probably easiest to start with the case $i = 0$ - for the other cases, the notation is not as nice.

   (c) Show that V_I^P is empty if and only if all of the V_I^i are empty.

5. Fix a field k. A *line* in $\mathbb{P}^2_k$ is a projective subvariety which can be written as V_I^P with I a principal homogeneous ideal generated by a non-zero polynomial of degree 1. Show that, if L and M are two lines in $\mathbb{P}^2_k$, then their intersection (i.e. the functor

$$\begin{aligned} \underline{\mathrm{Fld}}_k &\to \underline{\mathrm{Set}} \\ K &\mapsto \{p \in \mathbb{P}^2_k(K) : p \in L(K) \cap M(K)\}) \end{aligned}$$

is non-empty.

6. *This question is optional, and will not be graded. It assumes more background in algebraic geometry.*
This question explains why the 'obvious' definition of a morphism of varieties is not good.

Let k be a field, and let $\underline{\mathrm{SillyVar}}_k$ be the category whose objects are (affine or projective) varieties as defined in the notes, and whose morphisms are just morphisms of functors (forgetting the embeddings into affine or projective space). Write $\underline{\mathrm{Sch}}_k$ for the category of schemes over k (if you don't know what this is, this question is probably not for you - or you could look it up in eg. Liu's wonderful book 'Algebraic geometry and arithmetic curves'). Given an object X of $\underline{\mathrm{SillyVar}}_k$, there is an obvious way to construct a reduced (affine or projective) scheme over k from it.

(a) Set $I = (x, y) \cdot (xy - 1) \triangleleft k[x, y]$, and let $X = V_I^A$, so X is the union of a hyperbola and the origin. Let $\pi \colon X \cup \{0\} \to \mathbb{A}^1$ be the projection to the x-coordinate line. Show that π is an isomorphism in our category $\underline{\mathrm{SillyVar}}_k$.

(b) Can you construct an example of two *integral* varieties X and Y which are isomorphic in $\underline{\mathrm{SillyVar}}_k$ but not as schemes?