Elliptic curves exercise sheet 9

David Holmes

Abstract

Questions 1 and 2 will be graded, the others not. This is maybe more homework than usual, but you have a longer time in which to do it...

This is due in on 20/4/2015 before the start of the lecture (13:45). Please email your solutions to Giulio at ellipticcurvesleiden@gmail.com, or put them in his mailbox. Please include your student number on your answer sheet.

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`).

0. Read up to page ??? of the online lecture notes (this is approximately what was covered in the lecture, but contains some extra details).

1. Let k be a perfect field, $\bar{k}$ an algebraic closure, and $G = \mathrm{Gal}(\bar{k}/k)$. Define an action of G on $\mathbb{P}^n_k(\bar{k})$ by $g(x_0 : \cdots : x_n) = (gx_0 : \cdots : gx_n)$.

   (a) Show this action is well-defined (does not depend on choice of representative).

   (b) Show that the obvious inclusion $\mathbb{P}^n_k(k) \to \mathbb{P}^n_k(\bar{k})^G$ is an isomorphism, where $\mathbb{P}^n_k(\bar{k})^G$ denotes the invariants under the above action [this is the hardest part of the question. It may help to use Hilbert's theorem 90 from the lectures].

   (c) Let $V \subset \mathbb{P}^n_k$ be a variety. Show that the action above restricts to an action of G on $V(\bar{k})$.

   (d) Show $V(\bar{k})^G = V(k)$.

2. (Mordell's part of) the Mordell-Weil Theorem states that for any elliptic curve over $\mathbb{Q}$, $E(\mathbb{Q})$ is a finitely generated abelian group. In other words,

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$$

   for some non-negative integer r, called the *rank* of $E/\mathbb{Q}$. The main aim of this course is to prove this theorem.

   In this question, you may *assume* the Mordell-Weil theorem, and also the finiteness of the Selmer groups (both of which we will eventually prove). There is no known algorithm for computing the rank of a given elliptic curve exactly, but in this question you will use the Selmer groups give bounds on the rank.

(a) For any $n \geq 1$, show that

$$n^r \cdot \#(E[n](\mathbb{Q})) \leq \#(\mathrm{Sel}^n(E/\mathbb{Q})).$$

(b) For any $n \geq 1$, multiplication by n induces a map $E[n^2] \to E[n]$. This map induces a map $\varphi : \mathrm{Sel}^{n2)}(E/\mathbb{Q}) \to \mathrm{Sel}^n(E/\mathbb{Q})$. Show that the image of $E(\mathbb{Q})$ in $\mathrm{Sel}^n(E/\mathbb{Q})$ is contained in $\varphi(\mathrm{Sel}^{n^2}(E/\mathbb{Q}))$. Thus, computing $\varphi(\mathrm{Sel}^{n^2}(E/\mathbb{Q}))$ gives a possibly better bound on rank$E(\mathbb{Q})$. Hint: Look at the definition of the map $E(\mathbb{Q})/nE(\mathbb{Q}) \to \mathrm{Sel}^n(E/\mathbb{Q})$.