Elliptic curves

Problem sheet 1

October 20, 2009

Disclaimer: the questions in these sheets will help you understand this course, they are not necessarily the kind of questions that will be in the exam.

Field extensions, algebraic closure

1. (easy, but you need to know something about finite fields) In lectures I sketched the proof that no finite field is algebraically closed. I only considered the case of characteristic different from 2. Fill in the details in my proof, and extend it to characteristic 2.

2. (a) (easy) Prove that $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$.

(b) Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the set of algebraic numbers, i.e. roots of polynomials with rational coefficients. Prove that $\overline{\mathbb{Q}}$ is algebraically closed. Conclude that $\overline{\mathbb{Q}}$ is an algebraic closure of $\overline{\mathbb{Q}}$.

3. (harder) Here is the sketch of a construction of an algebraic closure of a field k. You are asked to fill in the details.

Make the list of all monic irreducible polynomials in $k[x]$, say, $f_1(x)$, $f_2(x)$, and so on. Let x_1, x_2, and so on, be independent variables, one for each polynomial. Consider the ring $R = k[x_1, x_2, \ldots]$, which is a ring of polynomials in infinitely many variables. Let I be the ideal of R generated by all the $f_i(x)$. Prove that $I \neq R$. Any ideal of R is contained in some maximal ideal, say $I \subset M$. Then $k_1 = R/M$ is a field extension of k. Prove that every $f_i(x)$ has a root is k_1. Repeat this operation for k_2, and so get an extension $k_1 \subset k_2$. Let K be the union of all these field extensions. Recall from algebraic number theory that algebraic elements form a subfield (find a proof in a book if you forgot it). Prove that the subfield of K consisting of algebraic elements over k is an algebraic closure of k.

Projective space

Let k be a field with an algebraic closure $\overline{k}$. In lectures I defined $\mathbb{P}^n_k$ as the set of non-zero vectors with $n+1$ coordinates in $\overline{k}$ up to a common multiple in $\overline{k}^*$.

If K is an extension of k contained in $\overline{k}$, then we denote by $\mathbb{P}^n_k(K)$ the set of K-points of $\mathbb{P}^n_k$, that is, the points defined by vectors with coordinates in K. If $C \subset \mathbb{P}^2_k$ is a plane curve, $C(K)$ denotes the set of K-points of C.

4 (a) (easy) Explore $\mathbb{P}^2_{\mathbb{F}_2}(\mathbb{F}_2)$, also called the Fano plane. Make a picture of all the points and lines.

(b) (easy) Let p be a prime, and $\mathbb{F}_{p^s}$ be a finite field with p^s elements, $s \geq 1$. Find the cardinality of the finite set $\mathbb{P}^n_{\mathbb{F}_p}(\mathbb{F}_{p^s})$.

(c) Let $C \subset \mathbb{P}^2_{\mathbb{F}_p}$ be the conic curve given by the homogeneous equation $x^2+yz=0$. Find the cardinality of $C(\mathbb{F}_{p^s})$.

(d) Find the number of $\mathbb{F}_{p^s}$-points of $\mathbb{P}^3_{\mathbb{F}_p}$ that lie on the quadric $xy = zt$.

5 (a) Show that the set of lines in $\mathbb{P}^2_k$ is in a natural bijection with $\mathbb{P}^2_k$. It is called the dual projective plane.

(b) Show that the set of lines through a given point is identified with $\mathbb{P}^1_k$.

(c) (harder) Assume that $\mathrm{char}(k) \neq 2$. Let C be the conic $ax^2 + by^2 + cz^2 = 0$, where $abc \neq 0$. Show that the set of lines that are tangent to C is a curve in the dual plane, and find its equation.

6 (a) Prove that for any four points in $\mathbb{P}^2_k$ such that no three of them are collinear there exists a projective transformation sending the four points to

$$(1:0:0),\ (0:1:0),\ (0:0:1),\ (1:1:1).$$

(b) Find the general equation of a conic through these points.