Mastermath Elliptic Curves, Homework 6
Due: 27th October 2015, 10:15

Students are expected to (try to) solve all problems below. The ones marked as "Homework" are to be handed in and count towards your grade according to the rules on the web page.

All problems and their solutions are part of the course, and could play a role in the exam. More importantly, they help you digest the material of the previous lecture and help you prepare for the next lecture.

Problem 37 (Homework)**.** Let $\mathbb{F}_q$ be a finite field with q elements and let $\phi\colon \mathbb{P}^n \to \mathbb{P}^n$ denote the *Frobenius morphism*, given by

$$\phi(x_0\colon \cdots \colon x_n) = (x_0^q\colon \cdots \colon x_n^q).$$

(a) Show that ϕ is indeed a morphism.

(b) Show that ϕ gives a bijection $\mathbb{P}^n(\bar{\mathbb{F}}_q) \to \mathbb{P}^n(\bar{\mathbb{F}}_q)$.

(c) Show that ϕ is not an isomorphism.

(d) Show that ϕ is inseparable.

Problem 38 (Homework)**.** Let C be a smooth projective curve of genus 0 over a field k, and assume that $C(k)$ contains a point P.

(a) Show that there exists a rational function $f \in k(C)$ having a pole of order 1 at P.

(b) Prove that C is isomorphic to $\mathbb{P}^1$.

Problem 39. Let $C, C' \subset \mathbb{P}^2$ be two smooth, irreducible plane curves over an algebraically closed field k and let $\phi\colon C \to C'$ be a morphism. In this exercise we will prove that ϕ is either constant or surjective.

(a) Suppose that $P \in C'(k)$ does not lie in the image of ϕ. Show that there is a non-constant rational function $f \in k(C')$ having no poles except at P, and deduce that the image of ϕ is contained in a strict algebraic subset of C'. [Hint: a rational function on C with no poles must be constant.]

(b) A strict algebraic subset of C' is a finite set of points (use Fulton, Section 1.6, Corollary 2).

(c) Show that the image of ϕ cannot consist of $n > 1$ distinct points of C', and deduce that ϕ is either constant or surjective. [Hint: use the irreducibility of C.]

Problem 40 (Homework)**.** Let k be an algebraically closed field, and let $C \subset \mathbb{P}^2$ be the smooth projective plane curve having affine Weierstrass equation

$$y^2 = f(x),$$

where f is a polynomial of degree 3 with distinct roots. Consider the differential $\omega = dx/y \in \Omega_{k(C)/k}$. Show that $\operatorname{div}(\omega) = 0$, and deduce that C has genus 1.

Problem 41. Let k be a field, and let C be a smooth projective curve over k of genus 0. Prove that $\operatorname{Pic}^0(C)$ is trivial.

Problem 42 (Homework)**.** Let k be a field, and let $E \subset \mathbb{P}^2$ be an elliptic curve defined by a Weierstrass equation. Let $O \in E(k)$ be the point at infinity.

(a) Let P, Q be two distinct points of $E(k)$. Let L be the straight line passing through P and Q, defined by a linear equation $f = 0$. If R is the third point of intersection of L with E, let the vertical line through R be defined by the linear equation $g = 0$. Show that

$$\operatorname{div}(f/g) = P + Q - (P \boxplus Q) - O,$$

where $\boxplus$ denotes the chord-tangent group operation on $E(k)$.

(b) Formulate and prove an appropriate version of (a) for the case $P = Q$.

(c) Deduce that the bijection $E(k) \to \operatorname{Pic}^0(E)$ given by $P \mapsto [P - O]$ identifies $\boxplus$ with the natural group operation on $\operatorname{Pic}^0(E)$, and in particular that $\boxplus$ is associative.