Elliptic curves

Problem sheet 2

November 12, 2009

1 (easy) Assume that $\mathrm{char}(k) \neq 2$. For any polynomial $f(x)$ find the singular points

(a) of the affine curve C given by $y^2 = f(x)$,

(b) of the projective closure of C.

(c) Now let $\mathrm{char}(k) = 2$. When is the affine curve $y^2 + y = f(x)$ singular?

2 (a) (easy) Prove that no irreducible plane curve of degree 4 has three collinear singular points.

(b) (harder) Can you construct an irreducible curve of degree 4 with two singular points?

3 Find the dimension of the space of cubics that are singular at a given point P.

4 (easy) For the following elliptic curves

$y^2 + xy = x^3 - 2x^2 + x$, $y^2 + xy = x^3 + x^2 + x$, $y^2 + y = x^3$, $y^2 + 3xy = x^3 + x$

(a) find the short Weierstrass form, (b) hence find the disriminant, and (c) find $\mathbf{Q}$-points of order 2.

5 (easy) In lectures we did a linear change of coordinates over $\mathbf{Q}$ to reduce the Fermat cubic $x^3 + y^3 = z^3$ to the Weierstrass form $y^2 = x^3 - 27/4$. Let E be the elliptic curve in this Weierstrass form with the point at infinity as the neutral element of the group law, us usual. Find the points of E that correspond to the three obvious $\mathbf{Q}$-points on the Fermat cubic under this isomorphism. Use addition and duplication formulas to determine the subgroup of $E(\mathbf{Q})$ generated by them.

6 Write addition and duplication formulas for the curve $y^2 + y = x^3 - x$ (warning: it is not a short Weierstarss form, so you can't apply the formulas from lectures as they are). Using these formulas find nP, where $P = (0, 0)$ and $n = 1, 2, 3, 4, 5, 6$.

7 (a) (easy) Let $G = \mathbf{Z}/2$. Let M be the trivial G-module $\mathbf{Z}$, $\mathbf{Z}/2$, $\mathbf{Z}/3$, $\mathbf{Z}/4$. Working with the definition from lectures compute $H^1(G, M)$.

(b) (harder) Let $G = \mathbf{Z}/2$ be the Galois group of $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$. Compute $H^1(G, \mathbf{Q}(\sqrt{d}))$.