

MAS 6396 Elliptic Curves

Quiz #1: Endomorphisms

Let E be an elliptic curve given by a Weierstrass equation

$$y^2 = x^3 + Ax + B \quad ,$$

and let

$$\alpha(x, y) = \left(\frac{p(x)}{q(x)}, y \cdot \frac{s(x)}{t(x)} \right)$$

be an endomorphism of E . Here $p, q, s, t \in K[x]$ are polynomials over the field K with p, q having no root in common and s, t having no root in common.

Problem 1 Show that

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}$$

for some $u(x) \in K[x]$ such that q and u have no common root.

Hint: You may like to use that a common root of u and q is root of p .

Problem 2 Let $(x_0, y_0) \in E(\overline{K})$ such that $t(x_0) = 0$. Show that $q(x_0) = 0$.
Conclude that whenever $q(x_0) \neq 0$, then $\alpha(x_0, y_0)$ is defined.

Hint: The polynomial $x^3 + Ax + B$ has no multiple roots.