

MATH 844: HOMEWORK 4, DUE FEB 23

4. Let E be the elliptic curve $y^2 + y = x^3 - x$, with group law identity $(0 : 1 : 0)$. Let K_m denote the extension of \mathbf{Q} generated by the coordinates of all the points P in $E[m] := \{P \in E(\overline{\mathbf{Q}}) \mid mP = \text{identity}\}$.

(a) Show that K_m is a Galois extension of \mathbf{Q} and that the Galois group of this extension is a subgroup of $GL_2(\mathbf{Z}/m)$.

(b) What is $[K_2 : \mathbf{Q}]$?

(c) Show that K_4 is a nontrivial Galois extension of K_2 with elementary 2-abelian Galois group (meaning abelian of exponent 2).

(d) What is $[K_3 : \mathbf{Q}]$? [Suggestion: note that $GL_2(\mathbf{Z}/3)/\text{scalars} = PGL_2(\mathbf{Z}/3) \cong S_4$. Which subgroups of $GL_2(\mathbf{Z}/3)$ have S_4 as a quotient?]