Elliptic Curves

Group 18

June 14, 2022

Contents

0 Basic Constructions

The main reference of this note is Silverman's *Arithmetic in Elliptic Curves*, and sometimes with examples from *Rational Points on Elliptic Curves* by Silverman & Tate.

In order to study the rational solutions of a certain type of equations, it is important to base all geometric constructions on some algebraically closed extension of the field we are interested in. Say k is a perfect field and K an algebraic closure of k, we denote by $\mathrm{Gal}(K/k)$ the Galois group of K/k (the fixed field of this group is k as K is an algebraic, separable and normal extension of k). We can define a natural group action of $\mathrm{Gal}(K/k)$ on the affine space $\mathbb{A}^n$ over K (we will always reserve the notation with subscripts for the affine schemes) by $(x_1, \ldots, x_n)^\sigma = (x_1^\sigma, \ldots, x_n^\sigma)$ for any σ in the Galois group.

To focus on the