Elliptic Curves

Group 18

June 14, 2022

Contents

0 Introduction

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.

1 Basic Constructions

1.1 Curves and rational points

We require all varieties in this report to be irreducible.

Definition 1.1.1. A *curve* is a projective variety of dimension 1.

Therefore, we are only interested in projective varieties and most of the objects will be constructed in them. In order to study the rational solutions of a certain type of equations (that is, on some curves), 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 projective space $\mathbb{P}^n$ over K by $[x_0 : \cdots : x_n]^\sigma = [x_0^\sigma : \cdots : x_n^\sigma]$ for any σ in the Galois group.

We introduce the following notations/definitions.

Definition 1.1.2. The *set of k-rational points* $\mathbb{P}^n(k)$ is the set $\{[x_0 : \cdots : x_n] : \forall i, x_i \in K\}$. Given a projective variety V, the *k-rational points of V* is the set $V(k) = V \cap \mathbb{P}^n(k)$.

Definition 1.1.3. A projective variety V is said to be *defined over k*, written as V/k, if $\mathbb{I}(V)$ can be generated by homogeneous polynomials with rational coefficients (i.e., in $k[x_0, \ldots, x_n]$).

Remark 1.1.1. We can also use Galois-theoretic languages:

$$\mathbb{P}^n(k) = \{P \in \mathbb{P}^n : P^\sigma = P, \forall \sigma \in \mathrm{Gal}(K/k)\},$$

and

$$V(k) = \{P \in V : P^\sigma = P, \forall \sigma \in \mathrm{Gal}(K/k)\}$$

as the fixed field of the Galois group is k.