Notes on Elliptic Curves

Yourong Zang

May 30, 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 Geometry

In order to study the rational solutions of a certain type of equations, it is important to construct our geometric objects in a Galois-theoretic flavor. Say k is a perfect field[1] and K an algebraic closure of k, we denote by $\mathrm{Gal}(K/k)$ the Galois group of K/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.

Introduce the following notations. The *set of k-rational points* $\mathbb{A}^n(k)$ is the invariant set of $\mathrm{Gal}(K/k)$. It is also clear that for any point P and $f \in k[x_1, \ldots, x_n] = k[X]$ we have $f(P^\sigma) = f(P)^\sigma$ for all $\sigma \in \mathrm{Gal}(K/k)$ since by constructions all σ restricts to the identity on k. Denoted by V/k, an algebraic set V *is defined over* k if its ideal $I(V)$ is generated by polynomials with coefficients in k. The set of k-rational points of V is then written as $V(k)$. It is therefore reasonable to define the ideal $I(V/k) = I(V) \cap k[X]$ (for any V), from which one can immediately see that V/k iff $I(V) = (I(V/k))$.

If V/k, then as $I(V)$ is generated by polynomials in $k[X]$, elements of $\mathrm{Gal}(K/k)$ map points in V to V. Therefore, we have $V(K) = V^{\mathrm{Gal}(K/k)}$. We can define the affine coordinate ring of a variety V/k to be

$$k[V] = \frac{k[X]}{I(V/k)}$$

which is an integral domain if we require varieties to be irreducible. Similarly we define the function field $k(V)$ to be the field of fraction of $k[V]$.

The Galois group clearly acts on $K[V]$: for any $\sigma \in \mathrm{Gal}(K/k)$ and $f \in K[V]$, f^σ is defined to be the polynomial function with $\mathrm{Gal}(K/k)$ acting on f's coefficients.

[1] Note: to characterize the rational points with Galois theoretic-languages, we would only need a separable and possibly infinite algebraic closure (then it's algebraic and normal) so that the fixed field of the Galois group is exactly the ground field k; but I don't know how Silverman would use this condition, so I will leave it here.

Therefore, for any $f \in K[V]$ and $P \in V$, we have

$$(f(P))^\sigma = f^\sigma (P^\sigma)$$

The constructions for projective varieties are similar. Since the Galois group consists of field automorphisms, it can act on homogeneous coordinates. For any point $P = [x_0, \ldots, x_n]$ in the n-projective space, We define an extra object called the *minimal field of definition for P over K*, defined by

$$k(P) = k(x_0/x_i, \ldots, x_n/x_i)$$

for any $x_i \neq 0$.

Lemma 1.1.1. *Let H be the subgroup of $\mathrm{Gal}(K/k)$ which fixes P. Then $k(P) = K^H$.*

Proof. **Insert proof here!** □