Notes on Elliptic Curves

Yourong Zang

June 1, 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 Varieties

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. **Edit**: this condition is used in Lemma 1.2.3

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 $P = [x_0 : \cdots : x_n]$ 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* $\mathrm{Gal}(K/k)$ *that fixes P. Then $k(P) = K^H$.*

Proof. **Insert proof here!** □

Take any rational map $\varphi = [f_0 : \cdots : f_n] : V_1 \to V_2$. The group $\mathrm{Gal}(K/k)$ acts on φ by $\varphi^\sigma = [f_0^\sigma : \cdots : f_n^\sigma]$. Clearly by our previous discussion, $\varphi(P)^\sigma = \varphi^\sigma(P^\sigma)$. A rational map is said to be *defined over k* if there is some nonzero constant λ such that $\lambda f_i \in k(V_1)$ for all i. Two varieties V_1/k and V_2/k are *isomorphic over k* if there exist two morphisms defined over k who compositions are the identity.

1.2 Curves

In this section we construct some necessary tools used to compute or classify elliptic curves. Silverman rarely uses the language of schemes in his book, so all constructions are relatively elementary. This might, however, make theorems and proofs longer. An algebraic curve C is a projective variety of dimension one.

We denote by $\mathfrak{m}_P = \{f \in K[V] : f(P) = 0\}$ the maximal ideal of any point P in some variety V. Denote the local ring at P by $K[V]_P = K[V]_{\mathfrak{m}_P}$. Now we abuse the notations a little and use $\mathfrak{m}_P$ again to denote the unique maximal ideal of the local ring at P. We first prove the following lemma:

Lemma 1.2.1. *Let C be a curve and $P \in C$ nonsingular. Then $K[C]_P$ is a discrete valuation ring.*

Proof. The dimension over $\mathfrak{m}_P$'s residue field of the tangent space $\mathfrak{m}_P/\mathfrak{m}_P^2$ is precisely $\dim C = 1$. Since $K[C]_P$ has Krull dimension one (since $0 < \dim K[C]_P \leqslant \dim K[C] = 1$), every prime ideal in it is maximal but the only maximal ideal is $\mathfrak{m}_P$. Therefore, the radical of any proper ideal, being the intersection of all prime ideals containing that ideal, is simply $\mathfrak{m}_P$. Thus, all ideals are $\mathfrak{m}_P$-primary. Standard

commutative results show that each ideal equals to (x^r) for some unique r where $\mathfrak{m}_P = (x)$. The uniqueness comes from the fact that the ring of interests is non-Artinian. Thus, we can define a discrete valuation $v : a \mapsto k_a$ where $(a) = (x^{k_a})$. We can extend this valuation to the field of fractions of $K[C]_P$ (which is simply $K(C)$) by $v(a/b) = v(a) - v(b)$. Then $K[C]_P$ is the valuation ring of v and thus a DVR. □

The valuation defined above clearly coincides with

$$\mathrm{ord}_P(f) = \sup\{d \in \hat{\mathbb{N}} : f \in \mathfrak{m}_P^d\}$$

which can be extended to $K(C)$ in the same fashion. When a rational function $r \in K(C)$ has order 1 at P, we call it a *uniformizer for C at P*. The valuation above is the *order of f at P*; if the order is positive then f has a zero, and a pole if $\mathrm{ord}_P(f) < 0$. If $\mathrm{ord}_P(f) \geqslant 0$ then f is *regular* at P (which coincides with the definition of rational functions being regular at a point).

Lemma 1.2.2. *If $P \in C(k)$, then there is a uniformizer t at P for C in $k(C)$.*

Proof. **Insert proof here** □

We quote the following result, which admits proofs with or without schemes:

Theorem 1.2.1. *If C is nonsingular and $f \in K(C)$ nonzero. Then the set $\{P \in C : \mathrm{ord}_P(f) \neq 0\}$ is finite. Further, if f is regular on C, then $f \in K$.*

Proof. The first statement is rather hard to prove without schemes, so the proof won't be reproduced here. The second statement follows from the known fact that $\mathscr{O}(C)$, the sheaf of regular functions on the projective variety C, is just K. □

Let k be a field of characteristic $p > 0$.

Lemma 1.2.3. *Given curve C/k and $t \in k(C)$ a uniformizer at a nonsingular $P \in C(k)$. Then $k(C)$ is a finite separable extension of $k(t)$.*

Proof. Since $k(C)$ is a finitely generated k-algebra, Zaraski's lemma ensures it's a finite extension of k. Clearly $k(t)$ has transcendence degree 1 ($t \notin k$ otherwise $\mathrm{ord}_P t = 0$ for all $P \in C$). Now as the transcendence degree of $k(C)/k$ is $\dim C = 1$, $\mathrm{trdeg}\, k(C)/k(t) = 0$, meaning $k(C)$ is an algebraic extension of $k(t)$.

Take any $x \in k(C)$ and we aim to show x is separable over $k(t)$. Since $k(C)$ is algebraic, there is some $\Phi(X, T) \in k[X, T]$ such that $\Phi(x, t) = 0$. Suppose further that Φ has minimal degree over $k(t)$.

If there is some term $a_{ij}T^iX^j$ in Φ where $p \nmid j$, then clearly $\partial\Phi(t,X)/\partial X$ is nonzero, meaning x is separable.

It remains to check when $\Phi(T,X) = \Psi(T,X^P)$ for some polynomial Ψ. Write

$$\Phi = \Psi(T,X^p) = \sum_{k=0}^{p-1}\left(\sum_{i,j} b_{ijk}T^{ip}X^{jp}\right)T^k$$

Since k is perfect of characteristic $p > 0$, every element of k is a pth power. Thus, define $c_{ijk}^p = b_{ijk}$ and thus

$$\sum_{i,j} b_{ijk}T^{ip}X^{jp} = \sum_{i,j}(c_{ijk}X^iT^j)^p = \left(\sum_{i,j} c_{ijk}X^iT^j\right)^p = \varphi_k(T,X)^p$$

Evaluate the order of each summand:

$$\operatorname{ord}_P(\varphi_k(t,x)^p t^k) = p\operatorname{ord}_P(\cdots) + k\operatorname{ord}_P(t) \equiv k \pmod p$$

which means they have different orders, and thus must all vanish as $\Phi(t,x) = 0$. There must exist some k such that φ_k contains X and $\varphi_k(t,x) = 0$. Yet $\Phi(t,X)$ is minimal and $\deg\varphi_k(t,X)^p \leqslant \deg\Phi(t,X)$ so we get a contradiction. $\square$

Due to the existence of uniformizers, every rational map is regular at smooth points.