Elliptic Curves

Group 18

June 15, 2022

Contents

0 Introduction

Blahblahblah hoaidhfaiudsf.

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. Other references: Hartshorne, Vakil, Fulton.

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.

Since we are working with low dimensional cases, it is convenient to define the function field of a projective variety using an affine chart.

Definition 1.1.4. Given a projective variety V/k, choose some $U_i = \{x_i \neq 0\} \subseteq \mathbb{P}^n$. Define the *function field of* V to be the quotient field of

$$k(V) = \frac{k[V \cap U_i]}{\mathbb{I}(V \cap U_i) \cap k[V \cap U_i]}$$

and the *larger function field of* V to be the quotient field of $K[V \cap U_i]$.

Remark 1.1.2. The choice of the chart does not matter — the resulting fields are isomorphic. The elements in $K(V)$ are of the form f/g where f, g are homogeneous polynomials of the same degree in $n+1$ variables, $g \notin \mathbb{I}(V)$.

For some projective variety V, we can define a group action of $\mathrm{Gal}(K/k)$ on $K[V]$ sending $f = \sum a_I x^I$ to $f^\sigma = \sum \sigma(a_I)x^I$, that is, acting on the coefficients of f. We can further extend this group action to $K(V)$ by defining $(f/g)^\sigma = f^\sigma/g^\sigma$. It is easy to check that the invariant sets in $K[V]$ and $K(V)$ are $k[V]$ and $k(V)$ respectively.

Remark 1.1.3. Since $\mathrm{Gal}(K/k)$ consists of field endomorphisms, we have $(f(P))^\sigma = f^\sigma(P^\sigma)$ for all f and points P.

Suppose V_1, V_2 are two projective varieties. For any rational map $\varphi = [f_0 : \cdots : f_n] : V_1 \to V_2$ where $f_i \in K(V_1)$, we define a group action $\varphi^\sigma = [f_0^\sigma : \cdots : f_n^\sigma]$. And by Remark 1.1.3, we get $(\varphi(P))^\sigma = \varphi^\sigma(P^\sigma)$.

Definition 1.1.5. A rational map $\varphi = [f_0 : \cdots : f_n]$ on V is *defined over* k if there exists some nonzero $\lambda \in K$ such that $\lambda f_i \in k(V)$ for all i. Equivalently, $\varphi^\sigma = \varphi$ for all $\sigma \in \mathrm{Gal}(K/k)$.

Definition 1.1.6. For any projective variety V and a smooth point $P \in V$, the maximal ideal at P is $\mathfrak{m}_P = \{f \in K[V] : f(P) = 0\}$. The *local ring of* V *at* P, denoted by $K[V]_P$ is the localization $K[V]_{\mathfrak{m}_P}$ which is simply the local ring

$$K[V]_P = \{f/g : f, g \in K[V] \text{ and } g(P) \neq 0\}$$

A rational function $f \in K(V)$ is said to be regular at P if $f \in K[V]_P$.

These definitions are equivalent to the mostly seen ones, but it would require some nontrivial arguments to prove the equivalence. See Hartshorne: insert reference here for instance. They also allow us to do most of our explicit computations on affine coordinate rings, while using the projective varieties to make certain huge theorems work.

Remark 1.1.4. Since for a projective variety V the closure of $V \cap \mathbb{A}^n$ in ¶^{n} is simply V, we will always use the affine variety to represent V and other objects on V.

1.2 Weil divisors and principal divisors

We reproduce Definition 1.1.1 below.

Definition 1.2.1. A *curve* is a projective variety of dimension 1.

In our report, the term curve refers to **smooth** curves, which are curves with all points smooth. Standard algebraic geometry results show that if P is a smooth point of a projective variety V, then the dimension (over K) of $\mathfrak{m}_P/\mathfrak{m}_P^2$ (insert reference here; can be Hartshorne) equals the dimension of V. Thus, given any curve C, we have $\dim_K \mathfrak{m}_P/\mathfrak{m}_P^2 = 1$, which gives us the following commutative algebra result:

Lemma 1.2.1. *For all points P in the curve C, the local ring $K[C]_P$ is a discrete valuation ring with a valuation defined by*

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

which is a map $K[C]_P \to \mathbb{N} \cup \{\infty\}$. Furthermore, each valuation ord_P can be extended to $K(C)$ as $\operatorname{ord}_P(f/g) = \operatorname{ord}_P(f/1) - \operatorname{ord}_P(g/1)$. This map is called the order of f/g at P*.*

Proof. Insert reference here. Possible choice: A-M Prop. 9.2. □

Remark 1.2.1. The fraction field of a localization of some ring is isomorphic to the fraction field of the original ring. Therefore, $K(C)$ is the fraction field of $K[C]_P$ for any P.

Definition 1.2.2. The *uniformizer for C at P* is some element $t \in K(C)$ such that $\operatorname{ord}_P(t) = 1$.

Remark 1.2.2. There certainly exists a uniformizer: since every discrete valuation ring is a principal ideal domain, $\mathfrak{m}_P = (t)$ for some t, which must be of order one as suggested by commutative algebra results.

If $t \in K(C)$ is of order one, then for any $g \in \mathfrak{m}_P$ (meaning $\operatorname{ord}_P(g) \geqslant 1$), we have

$$\operatorname{ord}_P(g/t) = \operatorname{ord}_P(g) - 1 \geqslant 0$$

so $g/t \in K[C]_P$, meaning there exists some $h \in K[C]_P$ such that $g = th$ and thus $\mathfrak{m}_P = (t)$.

To assist further understandings of this valuation, we present the following example.

Example 1.2.1. Consider the curve $y^2 = x^3 + 2x$ over a field K with characteristic not equal to 2, which is smooth. Let $P = (0,0)$ then $\mathfrak{m}_P = (x,y)$ and $\mathfrak{m}_P^2 = (x^2, xy, y^2)$. Since $x = \frac{1}{2}(y^2 - x^3) \in \mathfrak{m}_P^2$ (this also tells us $\operatorname{ord}_P(x) \geqslant 2$), $\mathfrak{m}_P = (x,y) = (y)$ (in the local ring at P). Thus, $\operatorname{ord}_P(y) = 1$. Now $y^2 = (x^2+2)x$ where $x^2 + 2 \neq 0$ at P which means it's a unit in the local ring, $x = (x^2+2)^{-1}y^2$ and thus

$$\operatorname{ord}_P(x) = \operatorname{ord}_P(\text{some unit}) + 2\operatorname{ord}_P(y) = 2$$

where the order of unit must be zero by definition (otherwise $\mathfrak{m}_P$ wouldn't be maximal). Finally for $2y^2 - 3x = 2x^3 + x = (2x^2+1)x$, we have

$$\operatorname{ord}_P(2y^2 - 3x) = \operatorname{ord}_P(\text{some unit}) + \operatorname{ord}_P(x) = 2$$

where the equality holds since $2x^2 + 1 \neq 0$ at $P = (0,0)$, i.e., $2x^2 + 1$ is a unit.

The order ord_P at any point P satisfies a very important property, which is an essential part of our algebraic geometry machine.

Theorem 1.2.1. *Let C be a curve and $f \in K(C)$. Then the set $\{P \in C : \operatorname{ord}_P(f) \neq 0\}$ is finite.*

Proof. The proof of this theorem by elementary variety theory is rather long and complicated. A short proof using schemes is available in Hartshorne, II.6.1 (insert reference here). □