Elliptic Curves

LEI Bichang

2024 Spring - Summer

1 Algebraic Curves

Let K be a perfect field, $\bar{K}$ a fixed algebraic closure of K, and $G_K := \mathrm{Gal}(\bar{K}/K)$ the absolute Galois group. I think there are two main additional features of algebraic curves compared to Riemann surfaces:

- the Galois group G_K acts on a variety (and many objects relevant to it) over K, and
- there are inseparable extensions in the positive characteristics.

1.1 Affine and Projective Vartieties over $\bar{K}$

Let $\bar{K}[\boldsymbol{X}] := \bar{K}[X_1, \dots, X_n]$ or $\bar{K}[X_0, X_1, \dots, X_n]$, $\mathbb{A}^n := \mathbb{A}^n(\bar{K})$, and $\mathbb{P}^n := \mathbb{P}^n(\bar{K})$.

1.1.1 Vartieties and Local Rings

An affine variety V is defined as an irreducible algebraic set in $\mathbb{A}^n$; that is, $I(V) \subset \bar{K}[\boldsymbol{X}]$ is a prime ideal. The affine coordinate ring and the function field of V is

$$\bar{K}[V] := \bar{K}[\boldsymbol{X}]/I(V) \quad \text{and} \quad \bar{K}(V) := \mathrm{Frac}\,\bar{K}[V].$$

For a point $P \in V$, we define the maximal ideal $\mathfrak{m}_P$ at P to be the ideal of regular functions vanishing at P, i.e.,

$$\mathfrak{m}_P := \{f \in \bar{K}[V] : f(P) = 0\};$$

and the local ring $\bar{K}[V]_P$ at P to be the localisation of $\bar{K}[V]$ at $\mathfrak{m}_P$. So we have a chain of function sets

$$\mathfrak{m}_P \subset \bar{K}[V] \subset \bar{K}[V]_P \subset \bar{K}(V),$$

and elements in $\bar{K}[V]_P$ are called regular functions at P.

The dimension of V is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$. Let $P \in V$ and $I(V) = (f_1, \dots, f_m)$. The variety V is said to be nonsingular or smooth at P, if the Jacobian matrix

$$J_V(P) := \left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

has rank $n - \dim V$, which is equivalent to

$$\dim_{\bar{K}} \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim V.$$

For examples,

- $\dim \mathbb{A}^n = n$, and
- $\dim V = n - 1 \iff I(V) = (f)$ for some $f \in \bar{K}[\boldsymbol{X}]$, and V is singular iff

$$\frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0.$$

Now we turn to projective varieties. A projective variety V is a projective algebraic set $V \subset \mathbb{P}^n$ s.t. the homogeneous ideal

$$I_+(V) = (f \in K[\boldsymbol{X}] : f \text{ is homogeneous and } f(V) = \{0\}) \subset K[X_0, \dots, X_n]$$

is prime. The field of rational functions is

$$\bar{K}(V) := \left\{ \frac{f}{g} : f, g \in \bar{K}[\boldsymbol{X}]/I_+(V) \text{ are homogeneous of the same degree}, g \neq 0 \right\}$$

Let us fix an immersion $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$, say $\mathbb{A}^n = \{X_0 \neq 0\} \subset \mathbb{P}^n$. We have two opposite processes.

- For a projective $V \subset \mathbb{P}^n$, $V \cap \mathbb{A}^n$ is an affine variety with ideal

$$I(V \cap \mathbb{A}^n) = \big(f(1, X_1, \dots, X_n) : f(X_0, X_1, \dots, X_n) \in I_+(V)\big)$$

- For an affine $V \subset \mathbb{A}^n$, the projective closure $\bar{V}$ has ideal $I_+(\bar{V})$ generated by the homogenisation of $I(V)$ w.r.t. X_0.

Proposition 1.1. Let $V \subset \mathbb{P}^n$ be a projective variety.

1. The affine variety $V \cap \mathbb{A}^n$ is either empty or projective closure equal to V. In the latter case, $\bar{K}(V \cap \mathbb{A}^n) \simeq \bar{K}(V)$.
2. For different choices of $\mathbb{A}^n \hookrightarrow \mathbb{P}^n$ containing $P \in V$, $\bar{K}[V \cap \mathbb{A}^n]_P$'s are canonically isomorphic as local rings.

Therefore, for $P \in V \subset \mathbb{P}^n$, we define $\mathfrak{m}_P$ and $\bar{K}[V]_P$ to be the corresponding local objects of $V \cap \mathbb{A}^n$, and the functions in $\bar{K}[V]_P$ are regualr functions at P.

1.1.2 Rational Maps

1.2 Affine and Projective Vartieties over K

1.3 Connection with Schemes

1.4 Curves over char p and Frobenius

In this subsection, assume that $\operatorname{char} K = p > 0$.