# 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 $\bar{K}[\boldsymbol{X}] := \bar{K}[X_1, \ldots, X_n]$ or $\bar{K}[X_0, X_1, \ldots, X_n]$, $\mathbb{A}^n := \mathbb{A}^n(\bar{K})$, 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 $I(V) = (f_1, \ldots, f_m)$. 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

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

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

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

- 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 has 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 $P \in V$, the local rings $\bar{K}[V \cap \mathbb{A}^n]_P$ 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 regular functions at $P$.

### 1.1.2 Rational Maps

Let $V \subset \mathbb{P}^m$ and $W \subset \mathbb{P}^n$ be projective varieties. A **rational map** $\phi : V \to W$ is a $(n+1)$-tuple

$$\phi = [f_0 : \cdots : f_n],$$

where $f_i \in \bar{K}(V_1)$ are not all identically zero[1], and

$$\phi(P) := [f_0(P) : \cdots : f_n(P)] \in W$$

when the left-hand-side makes sense. We say $\phi$ is regular or defined at $P$ if $\phi(P)$ does make sense. So $\phi$ being regular is equivalent to that $\exists g \in \bar{K}(V)$ s.t. every $gf_i$ is regular at $P$ (i.e., $gf_i \in \bar{K}[V]_P$) and not all $gf_i$'s are zero. An everywhere regular rational function is called a **morphism**[2]. An **isomorphism** is a bijective morphism whose inverse is also a morphism.

[1] Slightly informally, $f_i = F_i/G_i$ with $F_i, G_i \in \bar{K}[\boldsymbol{X}]$ homogeneous of the same degree, $G_i \notin I_+(V)$, and $\exists i$, $F_i \notin I_+(V)$.
[2] So a morphism is a rational map that is actually a map.

## 1.2 Affine and Projective Vartieties over $K$

An affine/projective variety over $K$ is a variety $V$ defined by polynomials with coefficients in $K$; i.e., its ideal $I = I(V)$ or $I_+(V)$ is generated by

$$I(V_{/K}) \text{ or } I_+(V_{/K}) := \{f \in I : f \in K[\boldsymbol{X}]\}.$$

The set of $K$-rational points are

$$V(K) := V \cap \mathbb{A}^n(K) \text{ or } V \cap \mathbb{P}^n(K).$$

*Remark.* $I(V_{/K})$ being prime does not implies that $I(V)$ is prime.

Let $V_{/K}$ be an affine or projective variety. Since for $P \in \mathbb{A}^n$ or $\mathbb{P}^n$ and $f \in \bar{K}[\boldsymbol{X}]$,

$$P \in \mathbb{A}^n(K) \text{ or } \mathbb{P}^n(K) \iff P^\sigma = P\text{[3]},$$

$$f \in K[\boldsymbol{X}] \iff f^\sigma = f,$$

and

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

for all $\sigma \in G_K$, we see that $G_K$ also acts on $V$, and

$$V(K) = V^{G_K}.$$

The Galois group also acts on $\bar{K}[V]$ and $\bar{K}(V)$. We define the coordinate ring and function field over $K$ by

$$K[V] := \bar{K}[V]^{G_K} \quad \text{and} \quad K(V) := \bar{K}(V)^{G_{/K}}.$$

It holds that

$$K[V] = K[\boldsymbol{X}]/I(V_{/K}) \quad \text{and} \quad K(V) = \operatorname{Frac} K[V].$$

*Remark.* What about $\mathfrak{m}_P \cap K[V]$ ?

Consider $V_{1/K}$ and $V_{2/K}$. The Galois group also acts on the rational functions $\phi : V_1 \to V_2$ coordinate-wisely, and

$$\phi(P)^\sigma = \phi^\sigma(P^\sigma),\ \forall \sigma \in G_K.$$

We say $\phi$ is defined over $K$ if $\phi$ is fixed by $G$. This is equivalent to that there exists a constant $\lambda \in \bar{K}^\times$ sending every coordinate of $\phi$ in $\bar{K}(V_1)$ to $K(V_1)$.

## 1.3 Products

We begin by realising the set-theoretic product $\mathbb{P}^n \times \mathbb{P}^m$ as a projective variety. Define the **Segre embedding**

$$S : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^N,\ ([x_0 : \cdots : x_n], [y_0 : \cdots : y_m]) \mapsto [x_0y_0 : x_0y_1 : \cdots : x_ny_m],$$

where

$$N = (n+1)(m+1) - 1 = n + m + nm.$$

This is a well-defined injection.

**Proposition 1.2.** Denote the coordinates on $\mathbb{P}^n$, $\mathbb{P}^m$ and $\mathbb{P}^N$ by $X_i$'s, $Y_j$'s and $T_{ij}$'s, repectively.

[3]The Galois group acts on $\mathbb{A}^n$ or $\mathbb{P}^n$ coordinate-wisely.

- The image of $S$ is
$$Z_+(\{T_{ij}T_{kl} - T_{il}T_{kj} : i, j = 0, \dots, n; k, l = 0, \dots, m\}).$$
- The ideal generated by $T_{ij}T_{kl} - T_{il}T_{kj}$'s is irreducible, so $\mathbb{P}^n \times \mathbb{P}^m$ is bijective with a projective variety in $\mathbb{P}^N$.

*Proof.* Let $I$ be the ideal generated by all $T_{ij}T_{kl} - T_{il}T_{kj}$'s. For the image, it suffices to show that on the affine charts,
$$S(U_i \times U_j) = Z_+(I) \cap U_{ij}{}^{4},$$
which is obvious.

The second statement follows by showing that $I$ is the kernel of the homomorphism
$$\psi : A[\boldsymbol{T}] \to A[\boldsymbol{X}, \boldsymbol{Y}],\ T_{ij} \mapsto X_i Y_j \tag{1}$$
for any ring $A$[5]. But proving $\operatorname{im} S = Z_+(\ker\psi)$ to show irreducibility is easier. First, $I \subset \ker\psi$ and $Z_+(\ker\psi) \subset Z_+(I)$. For the other direction, if $t \in Z_+(I) = \operatorname{im} S$, any $f \in \ker\psi$ must kill $t = [x_0y_0 : \cdots : x_ny_m]$ by definition.

□

So we use the Segre embedding to define algebraic sets and varieties in $\mathbb{P}^n \times \mathbb{P}^m$. One sees that a subset $V \subset \mathbb{P}^n \times \mathbb{P}^m$ is algebraic, if and only if
$$V = \{(x, y) : F_\alpha(x, y) = 0\}$$
for some bi-homogeneous polynomials $F_\alpha(X, Y) \in \bar{K}[\boldsymbol{X}, \boldsymbol{Y}]$. In particular, the Zariski topology on $\mathbb{P}^n \times \mathbb{P}^m$ is finer than its product topology.

Let $V \subset \mathbb{P}^n$ and $W \subset \mathbb{P}^m$ be two varieties. Their set-theoretic product $V \times W$ is an algebraic set, and, in fact, a variety.

## 1.4 Connection with Schemes

## 1.5 Curves and Function Fields

A **curve** over $K$ is a projective variety $C$ of dimension 1 over $K$. Let $C_{/K}$ be a curve.

The first important property of curves is that their local rings $\bar{K}[C]_P$ at smooth points are DVR, because in this case the cotangent space $\mathfrak{m}_P/\mathfrak{m}_P^2$ have $\bar{K}$-dimension 1. So for a smooth point $P \in C$, we can define the order function $\operatorname{ord}_P$ to be the valuation
$$\operatorname{ord}_P : \bar{K}[C]_P \to \mathbb{N} \cup \{\infty\}.$$
In addition, there exist uniformisers in $K[C]$.

**Proposition 1.3.** If $C$ is a smooth curve and $f$ is a nonzero rational function on $C$, then $f$ has only finitely many poles and zeros. Moreover, a rational function without poles must be constant.

Another important property is that rational maps from curves are regular at every smooth point. In particular, rational maps from smooth curves are all morphisms. This can be deduced using the DVR structures.

[4] $U_i = \{X_i \neq 0\}$, and so on.
[5] See the first answer of this post.

**Example 1.** Let $C$ be a smooth curve, then there is a bijection between $K(C) \cup \infty$ with $\{C \to_{/K} \mathbb{P}^1\}$[6] in the obvious way.

Now we consider morphisms between curves. Let $C_1, C_2$ be curves over $K$, $\phi : C_1 \to_{/K} C_2$ a nonconstant morphism.

**Theorem 1.** Morphisms from a smooth curve to another curve are either constant or surjective.

So $\phi : C_1 \twoheadrightarrow C_2$ induces a field extension

$$\phi^* : K(C_2) \hookrightarrow K(C_1), \ f \mapsto \phi^* f = f \circ \phi.$$

**Theorem 2.** For a nonconstant morphism $\phi : C_1 \twoheadrightarrow C_2$, the extension $K(C_1)/K(C_2)$ given by $\phi^* : K(C_2) \hookrightarrow K(C_1)$ is finite.

Conversely, if $\iota : K(C_2) \hookrightarrow K(C_1)$ is a $K$-field extension, there is a unique $K$-morphism $\phi : K(C_1) \to K(C_2)$ s.t. $\phi^* = \iota$.

**Theorem 3.** Let $C$ be a smooth curve over $K$. If $L$ is a subfield in $K(C)$ of finite index containing $K$, then there exists a unique curve $C'_{/K}$, up to $K$-isomorphism,together with a surjection $C \twoheadrightarrow_{/K} C'$ inducing an isomorphism $K(C') \simeq L$.

### Degrees and Ramification

**Definition 1.** Let $\phi : C_1 \to_{/K} C_2$ be nonconstant.

- We define the **degree** deg, **seperable degree** $\deg_s$ and **inseparable degree** $\deg_i$ of $\phi$ to be the corresponding "degrees" of the field extension $K(C_1)/K(C_2)$ induced by $\phi$.
- Let $P \in C_1$ whose image is a smooth point. The **ramification index** of $\phi$ at $P$ is

$$e_\phi(P) := \mathrm{ord}_P(\phi^* t_{\phi P}) \geq 1,$$

where $t_{\phi P}$ is any uniformiser at $\phi(P)$.

One sees immediately that if $C_1 \xrightarrow{\phi} C_2 \xrightarrow{\psi} C_2$, then

$$e_{\psi\circ\phi}(P) = e_\psi(\phi(P)) e_\phi(P).$$

**Proposition 1.4.** Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth curves.

1. For all $Q \in C_2$,
$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi.$$
2. For all but finitely many $Q \in C_2$,
$$\#\phi^{-1}(Q) = \deg_s \phi.$$

As a corollary, $\phi$ is unramified iff $\#\phi^{-1}(Q) = \deg \phi$, $\forall Q \in C_2$. So if $\phi$ is seperable, then $\phi$ ramifies at finitely many points.

[6] The set of morphism defined over $K$.

**Differentials**

Constructively, we define the space $\Omega_C$ of **meromorphic differential forms** on $C$ to be the $\bar{K}(C)$-vector space generated by symbols $dx$ for $x \in \bar{K}(C)$, subject to the conditions:

- $d(x+y) = dx + dy$, $\forall x, y \in \bar{K}(C)$;
- $d(xy) = y\,dx + x\,dy$, $\forall x, y \in \bar{K}(C)$;
- $da = 0$, $\forall a \in \bar{K}$.

**Proposition 1.5.** $\dim_{\bar{K}(C)} \Omega_C = 1$, and $dx$ is a $\bar{K}(C)$-basis iff $\bar{K}(C)/\bar{K}(x)$ is finite seperable.

Let $P \in C$ be a smooth point and $t$ a uniformiser at $P$. Then by Proposition 1.7, $dt$ is a $\bar{K}(C)$-basis of $\Omega_C$, and thus every $\omega \in \Omega_C$ can be written as $\omega = g\,dt$ with a unique function $g \in \bar{K}(C)$. We define $\omega/dt := g$.

**Proposition 1.6.** If $f \in \bar{K}(C)$ is regular at a $P$, then $df/dt$ is regular at $P$ too.

**Proposition-Definition 2.** Let $\omega \in \Omega_C$. If $t$ is a uniformiser at $P \in C$, then $\operatorname{ord}_P(\omega/dt)$ is independent of the choice of the uniformiser $t$, and we define the **order of** $\omega$ **at** $P$ $\operatorname{ord}_P(\omega) := \operatorname{ord}_P(\omega/dt)$.

1. Let $P$ be a smooth point, $x, f \in \bar{K}(C)$ with $x(P) = 0$, $p = \operatorname{char} K$, then

$$\begin{aligned} \operatorname{ord}_P(f\,dx) &= \operatorname{ord}_P(f) + \operatorname{ord}_P(x) - 1, & p \nmid \operatorname{ord}_P(x)^{7}, \\ \operatorname{ord}_P(f\,dx) &\geq \operatorname{ord}_P(f) + \operatorname{ord}_P(x), & p \mid \operatorname{ord}_P(x). \end{aligned}$$

2. If $\omega \neq 0$, then $\operatorname{ord}_P(\omega) = 0$ for almost all $P \in C$[8].

*Proof.* Let $s$ be another uniformiser. By Proposition 1.6, $ds/dt$ is regular, so

$$\frac{\omega}{dt} = \frac{\omega}{ds}\frac{ds}{dt}$$

shows that $\operatorname{ord}_P(\omega)$ is well-defined.

1. Direct calculation.
2. Let $dx$ be a basis of $\Omega_C$ and $\omega = f\,dx$. By a corollary of Proposition 1.4, $x : C \to \mathbb{P}^1$ ramifies at finitely many points, so we may consider only those points $P$ at which $x$ is unramified. Also, we may assume $x(P) \neq \infty$, so
$$1 = \operatorname{ord}_P(x - x(P)) = \operatorname{ord}_P(x^*(a \mapsto a - x(P))) = e_P(x).$$ ☐

## 1.6 Divisors and Riemann-Roch Theorem

The **divisor group** $\operatorname{Div}(C)$ of a curve $C$ is the free abelian group generated by points on $C$. We denote the divisor associates to a point $P \in C$ by $(P)$, so a divisor on $C$ is a formal sum

$$D = \sum_{P \in C} n_P \cdot (P)$$

[8]This is not trivial, because a uniform uniformiser does not exist, so we cannot obtain $\omega = f\,dt$ with $\operatorname{ord}_P(dt) = 1, \forall P \in C$ from the previous formula directly.

with $n_P = 0$ for almost every $P$. The deg of the above divisor is

$$\deg D := \sum_P n_P,$$

giving a homomorphism $\deg : \mathrm{Div}(C) \to \mathbb{Z}$ whose kernel $\mathrm{Div}^0(C) := \ker \deg$ is the subgroup of degree zero divisors.

The divisor of a nonzero rational function $f$ is

$$\mathrm{div}(f) := \sum_P \mathrm{ord}_P(f)(P),$$

giving a homomorphism $\mathrm{div} : \bar{K}(C)^\times \to \mathrm{Div}^0(C) \hookrightarrow \mathrm{Div}(C)$ whose kernel is $\bar{K}^\times$ and its image is denoted by $\mathrm{PDiv}(C)$. These divisors are called **principal** divisors. We call two divisors $D_1, D_2$ to be **linearly equivalent**, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal, and set

$$\mathrm{Pic}(C) := \mathrm{Div}(C)/\,\mathrm{PDiv}(C) \quad \text{and} \quad \mathrm{Pic}^0(C) := \mathrm{Div}^0(C)/\,\mathrm{PDiv}^0(C).$$

The Galois group acts on all these groups, and their $G_K$-invariant part are called the group of those divisors over $K$.

Similarly, the divisor of a nonzero meromorphic differential form $\omega$ is

$$\mathrm{div}(\omega) := \sum_P \mathrm{ord}_P(\omega)(P).$$

These divisors are called **canonical** divisors. Note that all canonical divisors are linearly equivalent.

For a divisor $D \in \mathrm{Div}(C)$, we say $D \geq 0$ if every coefficient of $D$ is nonnegtive. So the space of functions with poles bounded by $D$ from below is

$$L(D) := \{f \in \bar{K}(C) : \mathrm{div}(f) + D \geq 0\}.$$

This is $\bar{K}$-vector space, and we write $\ell(D) := \dim_{\bar{K}} L(D)$. If $D = D' + \mathrm{div}(f)$, then $L(D) \simeq L(D')$ by $g \mapsto fg$.

**Theorem 4.** The dimension $\ell(D)$ is finite, and

$$\ell(D) - \ell(K_C - D) = \deg D + 1 - g,$$

where $K_C$ is a canonical divisor and $g = \ell(K_C)$ is the **genus** of $C$.

## 1.7 Some Examples

**Example 2.** $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$.

- *Points.* Look at the homogenisation

  $$Y^2 Z = (X - e_1 Z)(X - e_2 Z)(X - e_3 Z).$$

  It intersects $Z = 0$ only at $\infty := [0 : 1 : 0]$, so $\infty$ is the only point at infinity. For a chart at $\infty$, use

  $$s := \frac{X}{Y}, \quad t := \frac{Z}{Y}{}^{9},$$

  and the equation is

  $$t = (s - e_1 t)(s - e_2 t)(s - e_3 t).$$

[9] As I am not smart, I DON'T use $z$ and $x$ as notation here, otherwise I would fail to figure out what is $x - e_i$ at $\infty$ and would write things like "$x = \frac{x}{z}$". Replace $Z$ by 1 is also fine, because this is what we do on the chart $Z = 0$.

- *Singularity.* None.
- *Local Rings.* $y = 1/t$ is a uniformiser at $e_i$, $s = x/y$ is a uniformiser at $\infty$.
- *Functions.* $\operatorname{div}(x - e_i) = 2 \cdot e_i - 2 \cdot \infty$, $\operatorname{div}(y) = e_1 + e_2 + e_3 - 3 \cdot \infty$.
- *Differential Forms.* Consider $dx$. Since $dx = d(x - e_i) = -x^2 d(1/x)$ and $\operatorname{ord}_\infty x = \operatorname{ord}_\infty s/t = -2$, we have

  $$\operatorname{div}(dx) = e_1 + e_2 + e_3 - 3 \cdot \infty,$$

  and thus

  $$\operatorname{div}\left(\frac{dx}{y}\right) = 0.$$

**Example 3.** $E : y^2 = x^3 - x$.

## 1.8 Curves over char $p$ and Frobenius

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

**Proposition 1.7.** Let $P \in C(K)$ be a $K$-rational smooth point and $t \in K[C]$ a uniformiser. Then the extension $K(C)/K(t)$ is finite and seperable.

*Proof.* Both $K(C)$ and $K(t)$ has transcendence degree one over $K$, so $K(C)/K(t)$ is algebraic.

Let $x \in K(C)$ and $\Phi(t, X)$ its minimal polynomial over $K(t)$. $\square$