Elliptic Curves

LEI Bichang

2024 Spring-Summer, Fall-Winter

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

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

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

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

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 ϕ is regular or defined at P if $\phi(P)$ does make sense. So ϕ 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 $f \in \bar{K}[\boldsymbol{X}]$,

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

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

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

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

It holds that

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

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 ϕ is defined over K if ϕ is fixed by G. This is equivalent to that there exists a constant $\lambda \in \bar{K}^\times$ sending every coordinate of ϕ 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 ord_P to be the valuation
$$\operatorname{ord}_P : \bar{K}[C]_P \to \mathbb{Z}_{\geq 0} \cup \{\infty\}.$$
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 ϕ to be the corresponding "degrees" of the field extension $K(C_1)/K(C_2)$ induced by ϕ.
- Let $P \in C_1$ whose image is a smooth point. The **ramification index** of ϕ at P is

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

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

[6] The set of morphism defined over K.

Differentials

Constructively, we define the space Ω_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:

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

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 Ω_C, and thus every $\omega \in \Omega_C$ can be written as $\omega = g\,\mathrm{d}t$ 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.

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

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

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

2. If $\omega \neq 0$, then $\mathrm{ord}_P(\omega) = 0$ 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 $\mathrm{ord}_P(\omega)$ is well-defined.

1. Direct calculation.
2. Let dx be a basis of Ω_C and $\omega = f\,\mathrm{d}x$. 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
$$1 = \mathrm{ord}_P(x - x(P)) = \mathrm{ord}_P(x^*(a \mapsto a - x(P))) = e_P(x). \qquad \square$$

1.6 Divisors and Riemann-Roch Theorem

The **divisor group** $\mathrm{Div}(C)$ 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 $\omega = f\,\mathrm{d}t$ with $\mathrm{ord}_P(dt) = 1, \forall P \in C$ 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

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

giving a homomorphism $\div : \bar{K}(C)^\times \to \mathrm{Div}^0(C) \hookrightarrow \mathrm{Div}(C)$ 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

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

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 ω is

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

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

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

This is $\bar{K}$-vector space, and we write $\ell(D) := \dim_{\bar{K}} L(D)$. If $D = D' + \div(f)$, 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 ∞ is the only point at infinity. For a chart at ∞, 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 ∞ 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 $e_i := [e_i : 0 : 1]$, $s = x/y$ is a uniformiser at ∞. For all other points $[a : b : 1] \neq e_i$, both $x - a$ and $y - b$ are uniformisers.
- *Functions.* $\div(x - e_i) = 2 \cdot e_i - 2 \cdot \infty$, $\div(y) = e_1 + e_2 + e_3 - 3 \cdot \infty$.
- *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
$$\div(dx) = e_1 + e_2 + e_3 - 3 \cdot \infty,$$
and thus
$$\div\left(\frac{dx}{y}\right) = 0.$$

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 $K(t)$. □

2 Elliptic Curves

2.1 The Tate Module

3 Elliptic Curves over Finite Fields

3.1 Weil Conjecture for Elliptic Curves

4 Elliptic Curves over Local Fields

In this section, let K be a perfect local field with valuation v and value group $\mathbb{Z}$. Let $R = \mathcal{O}_K$, π a uniformizer, and $k = R/\pi$ the residue field. Denote the quotient map $\mathcal{O}_K \to k$ by $t \mapsto \tilde{t}$.

4.1 Minimal Weierstrass Equation

Definition 3. Let A be a ring,
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in A$$
an Weierstrass equation over A. We define many quantities in $\mathbb{Z}[a_1, a_2, a_4, a_3, a_4, a_6]$:
$$b_2,\ b_4,\ b_6,\ b_8,\ \Delta,\ c_4,\ c_6.$$
Among them, Δ is the most important one, called **discriminant**.

Remark.

- Under the change of variable
$$y = \frac{1}{2}(y' - a_1 x - a_3),$$
the long Weierstrass equation is converted to[10]
$$y'^2 = 4x^3 + b_2 x + 2b_4 x + b_6.$$
- Under the change of variable
$$(u; r, s, t) := \begin{cases} x = u^2 x' + r, \\ y = u^3 y' + u^2 s x' + t, \end{cases}$$
the discriminant is converted to
$$\Delta' = u^{-12}\Delta.$$
- For a short Weierstrass equation
$$y^2 = x^3 + ax + b,$$
we have
$$\begin{aligned} \Delta &= -16(4a^3 + 27b^2), \\ c_4 &= -48a, \\ c_6 &= -864b. \end{aligned}$$

Proposition 4.1. If E is defined over a field, then E is nonsingular $\iff \Delta \neq 0$.

Back to our setting that $K =$ local field. We need some particular integral equation that modulo π gives something nontrvial.

Definition 4. A Weierstrass equation E over K is called **minimal**, if it is integral (i.e, all coefficients $a_i \in \mathcal{O}_K$), and the valuation of the discriminant $v(\Delta)$ is minimized.

Lemma 4.1. Every elliptic curve E/K admits some minimal Weierstrass equation.

Moreover, an integral Weierstrass equation with $v(\Delta) < 12$ is minimal.

Proof. First, we need to find Weierstrass over $\mathcal{O}_K$. Starting from any equation over K, the change of variable $(u; 0, 0, 0)$ sends a_i to
$$a_i' = u^i a_i.$$
Hence for $v(u) \gg 0$, it will give an integral equation.

For integral Weierstrass equations, $\Delta \in \mathbb{Z}[\{a_i\}_i] \subset \mathcal{O}_K$, so it can be minimized.

Since $v(\Delta) \equiv v(\Delta') \bmod 12$ for any $(u; r, s, t)$, an integral equation with $v(\Delta) < 12$ must be minimal. □

Remark.

- Minimal Weierstrass equations are not unique.
- For a similar reason,
$$v(c_4) < 4 \text{ or } v(c_6) < 6$$
are also sufficient for being minimal.
- If $\operatorname{char} K \neq 2, 3$, then
$$\text{minimal} \iff v(\Delta) < 12 \text{ or } v(c_4) < 4.$$

[10] Careful!! I am not very clear about the notion of "change of variable".

4.2 Reduction and Reduction Type

Let

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathcal{O}_K$$

be a Weierstrass equation for an elliptic curve over K. Then it reduces modulo π to a projective curve $\tilde{E}$, defined also by Weierstrass equation, over k.

- The discriminant of $\tilde{E}$ is $\tilde{\Delta} = \Delta \mod \pi$. In particular,

$$\tilde{E} \text{ is smooth } \iff \Delta \in \mathcal{O}_K^\times.$$

Proposition 4.2. Let E be an elliptic curve over K. Then the reductions $\tilde{E}/k$ are isomorphic for all change of variable between minimal Weierstrass equations.

Proof. Suppose that $(u; r, s, t)$ changes a minimal equation to another, then $u \in \mathcal{O}_K^\times$, so it is an isomorphism over K. It is left (and necessary!) to prove that we can take $r, s, t \in \mathcal{O}_K$. □

Then we classify different kind of reductions. We say that E has **good reduction** if $\tilde{E}$ is an elliptic curve, namely $\tilde{E}$ is smooth or $\Delta \in \mathcal{O}_K^\times$; other wise it has **bad reduction**.

Assume that E has bad reduction. Then $\tilde{E}$ has a *unique* singular point. (T.B.C.)

4.3 Reduction of Rational Poitns

Let E be an elliptic curve over K. For all $P \in E(K)$, we can write $P = [x : y : z]$ with

- $x, y, z \in \mathcal{O}_K$, and
- at least one of the coordinates is in $\mathcal{O}_K^\times$.

$\rightsquigarrow \tilde{P} := [\tilde{x}, \tilde{y}, \tilde{z}] \in \tilde{E}(k)$. This is independent to the choice of coordinate, giving a map

$$\pi : E(K) \to \tilde{E}(k).$$

Definition 5. Denote by $\tilde{E}_{\text{ns}}$ the set of non singular points of $\tilde{E}$, and $\tilde{E}_{\text{ns}}(k) = \tilde{E}_{\text{ns}} \cap \tilde{E}(k)$. Let

$$E_0(K) := \{P \in E(K) \mid \pi(P) \in \tilde{E}_{\text{ns}}(k)\},$$
$$E_1(K) := \{P \in E(K) \mid \pi(P) = \tilde{O}\}$$

Proposition 4.3. We have an exact sequence of *groups*:

$$0 \to E_1(K) \to E_0(K) \xrightarrow{\pi} \tilde{E}_{\text{ns}}(k) \to 0.$$

Proof (when E has good reduction). In case $\tilde{E}$ smooth, $\tilde{E}_{\text{ns}} = \tilde{E}$ is an elliptic curve, and $E_0(K) = E(K)$.

- π is a homomorphism := by

  Note that π sends a line to a line. A real proof needs to take care of the tangent lines.

- π is surjective := by

  Hensel's lemma. Choose a minimal (integral) equation $E : F(x, y) = 0$. Let $(\tilde{x}, \tilde{y}) \in \tilde{E}_{\text{ns}}(k)$. Smoothness means

$$\frac{\partial \tilde{F}}{\partial X}(\tilde{x}, \tilde{y}) \neq 0 \text{ or } \frac{\partial \tilde{F}}{\partial Y}(\tilde{x}, \tilde{y}) \neq 0.$$

  Hence, say, $\dfrac{\partial F}{\partial X}(x, y) \in \mathcal{O}_K^\times$. By Hensel's lemma, there is a unique $x' \in \mathcal{O}_K$ s.t. $F(x', y) = 0$. □

Remark. In case $\tilde{E}$ singular, Proposition 4.3 still holds. In particular,

- $\tilde{E}_{\mathrm{ns}}$ is a group, with $\tilde{E}_{\mathrm{ns}}(k)$ being a subgroup.

Proposition 4.4. $E_0(K)$ has finite index in $E(K)$.

4.4 Torsion points

Let E be an elliptic curve over the local field $K/\mathbb{Q}_p < \infty$ defined by a Weierstrass equation.

The first step is to look at the group

$$E_1(K) = \ker\left(E_0(K) \to \tilde{E}_{\mathrm{ns}}(k)\right).$$

A point $P = (x, y) = [x : y : 1] \in E(K)$ reduces to $\tilde{P} = \tilde{O} \in \tilde{E}(k)$, iff

$$v(y) < \min\{0 = v(1), v(x)\}.$$

If $v(x) \geq 0$, then $v(y^2 + a_1xy + a_3y) \geq 0$; hence $v(x) < 0$. Meanwhile,

$$v(x^3 + a_2x^2 + a_4x + a_6) = v(y^2 + a_1xy + a_3y).$$

As $v(x), v(y) < 0$, we have

$$3v(x) = 2v(y).$$

So

$$v(x) = -2n,\ v(y) = -3n, \quad n \geq 1.$$

Conversely, if $(x, y) \in E(K)$ and $v(x) < 0$, the above computation holds. So

$$E_1(K) = \{(x, y) \in E(K) \mid v(x) \leq -2\}.$$

This leads to the following filtration on $E_1(K)$.

Definition 6. For $n \in \mathbb{Z}_{\geq 1}$, set

$$E_n(K) := \{(x, y) \in E(K) \mid v(x) \leq -2n, v(y) \leq -3n\} \cup \{O\}.$$

Lemma 4.2. $E_n(K)$ are subgroups of $E_1(K)$.

Proof. Consider the change of variable

$$\begin{cases} x = \pi^{-2n}x', \\ y = \pi^{-3n}y' \end{cases}$$

on E. This gives a non-minimal integral equation, which reduces mod π to

$$\tilde{E}_n : y'^2 = x'^3$$

and gives a map

$$\pi_n : E(K) \to \tilde{E}_n(k).$$

One verifies that:

- $(0, 0)$ is the only singular point of $\tilde{E}_n$, and $\tilde{E}_{n,\mathrm{ns}}(k) \simeq k$ as additive groups.
- $E_n(K) = \pi_n^{-1}(\tilde{E}_{n,\mathrm{ns}}(k))$.

- $E_{n+1}(K) = \ker\Big(\pi_n : E(K) \twoheadrightarrow \tilde{E}_{n,\mathrm{ns}}(k) \simeq k\Big)$. □

Proposition 4.5. $E_1(K)[m] = 0$ for $m \in \mathbb{Z}$ prime to p.

Proof. Let $P \in E_1(K)[m]$. Then

$$0 = \pi_1(mP) = m(\pi_1(P)) \in k.$$

As $p \nmid m$, this implies $\pi_1(P) = 0$, i.e, $P \in E_2(P)$. Inductively, we see that $P \in E_n(P)$ for all n, so $P = O$. □

Corollary 4.1. If E/K has good reduction, and $p \nmid m$, then

$$E(K)[m] \hookrightarrow \tilde{E}(k)$$

injectively.

Bounding the denominators of torsion points

Theorem 5. Let $P \in E(K)$ be a torsion point of order $m \geq 2$.

(1) If m is not a power of p, then $x(P), y(P) \in \mathcal{O}_K$.

(2) If $m = p^n$, then

$$\pi^{2r}x(P), \pi^{3r}y(P) \in \mathcal{O}_K, \quad r = \left\lfloor \frac{v(p)}{p^n - p^{n-1}} \right\rfloor \geq 0.$$

Theorem 6. Let

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z},\ \Delta := 4a^3 + 27b^2 \neq 0.$$

If $P = (x, y) \in E(\mathbb{Q})$ is a torsion point, then $x, y \in \mathbb{Z}$, and either $y = 0$ or $y \mid \Delta$[11].

5 Elliptic Curves over Global Fields

5.1 Mordell-Weil Theorem

Theorem 7. Ler K be a number field, E an elliptic curve over K. Then $E(K)$ is of finite type.

Consequently,

$$E(K) = \mathbb{Z}^r \oplus E(K)_{\mathrm{tor}}.$$

We call $r \in \mathbb{Z}_{\geq 0}$ the **rank** of E/K.

Remark. In contrast, if K is a local field (here we mean $K = \mathbb{R}, \mathbb{C}$ or a finite extension of $\mathbb{Q}_p$) or algebraically closed, then $E(K)$ is NOT finitely generated. See DM5.

The proof consists two steps.

1. Weak Mordell-Weil theorem: $E(K)/2E(K)$ is fintie.
2. Descent. Let $\{P_1, \ldots, P_r\}$ represents $E(K)/2E(K)$. Any $P \in E(K)$ is of the form $P = P_i + 2Q$ for some P_i. The idea is that $Q \mapsto P_i + 2Q$ "increases the complexity (height)" of the point Q, and $E(K)$ is generated by P_i's with points of bounded height.

[11] Note that this Δ is the discriminant of a polynomial, rather than discriminant of a elliptic curve.

5.2 Step 1 - A Special Case: $E/\mathbb{Q}$, $E(\mathbb{Q})[2] \neq 0$

Take an elliptic curve $E : y^2 = A(x)$ with some rational 2-torsion point on it, namely $A(x_0) = 0$ for an $x_0 \in \mathbb{Q}$. Translating & scaling if necessary, we assume $A(X) \in \mathbb{Z}[X]$ and $x_0 = 0$, so that $(0,0) \in E(\mathbb{Q})[2]$, and then write

$$E : y^2 = x(x^2 + ax + b), \quad a, b \in \mathbb{Z},\ b \neq 0^{12}, a^2 - 4b \neq 0$$

Determine $E' = E/\langle (0,0) \rangle$

Define

$$t : E \to E \quad P \mapsto P + (0,0).$$

This is an involution over $\mathbb{Q}$ of algebraic curves, thus induces an involution

$$t^* : \mathbb{Q}(E) \to \mathbb{Q}(E).$$

The quotient map $E \to E/\langle (0,0) \rangle$ is induced by t, so $K(E/\langle (0,0) \rangle)$ is isomorphic to the subfield of $K(E)$ fixed by t^*.

Let $P = (x, y) \in E$, $P_1 = (x_1, y_1) = t(P)$. What is P_1? The line through P and $(0,0)$ takes the form

$$L : \begin{cases} X = \lambda x, \\ Y = \lambda y, \end{cases} \quad , \quad \lambda \in \bar{\mathbb{Q}},$$

and intersects E also at $-P_1 = (x_1, -y_1)$[13]. Hence

$$-\frac{y_1}{x_1} = \frac{y}{x}, \implies \left(\frac{y_1}{x_1}\right)^2 = \left(\frac{y}{x}\right)^2.$$

One checks that

$$f := \left(\frac{y}{x}\right)^2 \in \mathbb{Q}(E)$$

is invariant under t^*.

(Why do) We need another function invariant under t^*. Observe that

$$g := y + y_1 \in \mathbb{Q}(E)^{t^* = \mathrm{id}},$$

because t has order 2. Now f, g must have algebraic relation. Begin by compute P_1. Subsituting L into E, we get

$$L \cap E : \lambda(x^3\lambda^2 + (ax^2 - y^2)\lambda + bx) = 0.$$

Here $\lambda = 0$ corresponds to $(0,0)$, and $\lambda = 1$ corresponds to P. Denote by $\lambda = \lambda_1$ the parameter of $-P_1$, then

$$1 \cdot \lambda_1 = \frac{b}{x^2}, \quad \implies \begin{cases} x_1 = \dfrac{b}{x}, \\ y_1 = -\dfrac{by}{x^2}, \end{cases}$$

[12] Because $A(X)$ can't have multiple roots.

[13] E is not in short Weierstrass equation. For a long Weierstrass equation,

$$-P = (x, -y - a_1 x - a_3)\,.$$

$$\implies g^2 = \left(y - \frac{by}{x^2}\right)^2 = \frac{y^2}{x^2}\left(x^2 - 2b + \frac{b^2}{x^2}\right).$$

As

$$f = \left(\frac{y}{x}\right)^2 = \frac{x^2+b}{x} + a,$$

we have

$$g^2 = f\left(\left(\frac{x^2+b}{x}\right)^2 - 4b\right) = f\left((f-a)^2 - 4b\right).$$

Therefore, we get a rational map

$$\phi := (f, g) = \left(x + a + \frac{b}{x},\ y - \frac{by}{x^2}\right) : E \to E',$$

where

$$E' : y'^2 = x'(x'^2 + a_1 x' + b_1), \quad \begin{cases} a_1 = -2a \\ b_1 = a^2 - 4b \end{cases} \in \mathbb{Z}.$$

Because $\mathrm{ord}_O(x) = -2$ and $\mathrm{ord}_O(y) = -3$, we have $\mathrm{ord}_O(f) = -2$ and $\mathrm{ord}_O(g) = -3$. So ϕ sends O to

$$\phi(O) = [f(O) : g(O) : 1] = [0 : 1 : 0] = O'.$$

Moreover,

$$\phi(P) = O \implies f(P) = \infty \iff P = O \text{ or } P = (0,0),$$

hence ϕ is a non-constant isogeny. The field $\mathbb{Q}$ has characteristic 0, so ϕ is separable, and $\deg \phi = \#\ker \phi = 2$. Comparing degree shows that

$$\mathbb{Q}(E') \simeq \mathbb{Q}(f, g) = \mathbb{Q}(E)^{t^*=\mathrm{id}}.$$

Study $E \to E' \to E$

The curve E' takes a much similar form to E, so we can do the same thing, and get an isogeny

$$\psi = \left(x' + a_1 + \frac{b_1}{x'},\ y' - \frac{b_1 y'}{x'^2}\right) : E' \to E''$$

of degree 2 with $\ker \psi = \{O, (0,0)\}$, and

$$E'' : y''^2 = x''(x''^2 + 4ax'' + 16b).$$

This time E'' is isomorphic to E via $\begin{cases} x = x''/4, \\ y = y''/8. \end{cases}$ We can write the map still by ψ, that is

$$\psi = \left(\frac{1}{4}\left(x' + a_1 + \frac{b_1}{x'}\right), \frac{1}{8}\left(y' - \frac{b_1 y'}{x'^2}\right)\right) : E' \to E.$$

So we obtain an endomorphism $E \to E$ given by $\psi \circ \phi$, whose kernel is $\ker(\psi \circ \phi) = E[2]$, because

$$\phi^{-1}((0,0)) = \{(x,y) \in E = E(\bar{\mathbb{Q}}) \mid x^2 + ax + b = 0\} = \text{ the other 2-torsion points on } E.$$

Moreover, $\mathrm{Aut}(E) = \{[\pm 1]\}$; one verifies this by noting that: an automorphism is just a change of variable $(u; r, s, t)$ with u invertible that fixes the equation. Hence $\psi \circ \phi = [\pm 2]$, and $\psi(\phi(E)) = 2E$.

Study $\phi(E) \subset E'$

Lemma 5.1. If $(u, v) \in E'(\mathbb{Q})$, then

$$(u,v) \in \phi(E(\mathbb{Q})) \iff u \in (\mathbb{Q}^\times)^2 \text{ or } \begin{cases} u = 0, \\ a^2 - 4b \in (\mathbb{Q}^\times)^2. \end{cases}$$

This suggests us to consider

$$q : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \quad (u,v) \mapsto \begin{cases} [u], & u \neq 0, \\ [a^2 - 4b], & u = 0 \end{cases}$$
$$O \mapsto [1].$$

Lemma 5.2. q is a group homomorphism.

Proof. We need to prove: if $P_1, P_2, P_3 \in E'(\mathbb{Q})$ and $P_1 + P_2 + P_3 = O$, then

$$q(P_1)q(P_2)q(P_3) \in \left(\mathbb{Q}^\times\right)^2.$$

Not hard. □

So we can write $\phi(E(\mathbb{Q})) = \ker q$.

Lemma 5.3. The image of q is finite.

Proof. Any element in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ can be written *uniquely* as $[r]$, where $r \in \mathbb{Z}$ and r is square-free. We show that:

$$[r] \in \operatorname{im} q \implies r \mid b_1.$$

Assume that $(u, v) \in E'(\mathbb{Q})$, and $q((u, v)) = [r]$, where $r \in \mathbb{Z}$ is square free. No matter $u = 0$ or not,

$$\exists s, t \in \mathbb{Q}, \quad \begin{cases} u = rt^2, \\ u^2 + a_1 u + b_1 = rs^2. \end{cases}$$

Write

$$t = \frac{l}{m}, \quad l, m \in \mathbb{Z},\ (l, m) = 1.$$

Elliminating u in the above equation, we get

$$r^2 l^4 + a_1 r l^2 m^2 + b_1 m^4 = r n^2, \quad \text{where } n := m^2 s. \tag{2}$$

The LHS is in $\mathbb{Z}$ and it is not square-free, yet r is square-free, so $n = m^2 s \in \mathbb{Z}$. Suppose that there is a prime $p \mid r$ but $p \nmid b_1$. From Eq. (2), we have

$$p \mid b_1 m^4 \overset{p \nmid b_1}{\implies} p \mid m \implies p^2 \mid r n^2 \overset{r \text{ square-free}}{\implies} p \mid n \implies p^3 \mid r^2 l^4 \implies p \mid l, \tag{3}$$

contradicting $(l, m) = 1$. □

Therefore, we deduce that:

Theorem 8. $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \simeq \operatorname{im} q$ is finite.

Corollary 5.1 (a special case of weak Mordell-Weil)**.** $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Some remarks

This proof offer a way to compute $E(\mathbb{Q})/2E(\mathbb{Q})$ given $E : y^2 = x(x^2 + ax + b)$.

- *Determine* $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$. The coefficients of E' are

  $$a_1 = -2a,\ b_1 = a^2 - 4b.$$

  By the proof of Lemma 5.3, we solve Eq. (2)

  $$r^2l^4 + a_1rl^2m^2 + b_1m^4 = rn^2$$

  in $(l, m, n) \in \mathbb{Z}^3 \smallsetminus \{(0, 0, 0)\}$ for $r \mid b_1$ square-free, then use

  $$(u, v) = \left(\frac{rl^2}{m^2}, \frac{rnl}{m^3}\right)$$

  to find all $(u, v) \in E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \simeq \operatorname{im}\left(E'(\mathbb{Q}) \to \mathbb{Q}^\times/\left(\mathbb{Q}^\times\right)^2\right)$, then compute the points

  $$\psi(u, v) = \left(\frac{1}{4}\left(u + a_1 + \frac{b_1}{u}\right), \frac{1}{8}\left(v - \frac{b_1v}{u^2}\right)\right) \in \psi\left(E'(\mathbb{Q})/\phi(E(\mathbb{Q}))\right).$$

- *Determine* $E(\mathbb{Q})/\psi(E'(\mathbb{Q}))$. Solve [14]

  $$r^2l^4 + arl^2m^2 + bm^4 = rn^2$$

  for $r \mid b$ to get

  $$(u, v) = \left(\frac{rl^2}{m^2}, \frac{rnl}{m^3}\right) \in E(\mathbb{Q})/\psi(E'(\mathbb{Q})).$$

- Determine $E/2E(\mathbb{Q})$. Note that the terms in the exact sequqnce

  $$0 \to \psi\left(E'(\mathbb{Q})/\phi(E)\right) \to E(\mathbb{Q})/\psi(\phi(E(\mathbb{Q}))) \to E(\mathbb{Q})/\psi(E'(\mathbb{Q})) \to 0$$

  of abelian groups are $\mathbb{Z}/2\mathbb{Z}$-modules, so it splits.

There is no algorithm to solve it, so this method is not effective. But we can modulo p to show it has no solution and sometimes we can determine $E(\mathbb{Q})/2E(\mathbb{Q})$.

Example 3. $E : y^2 = x(x^2 - x + 6)$.

- Determine $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$.

  We have $a = -1$, $b = 6$, $a_1 = -2a = 2$, $b_1 = a^2 - 4b = -23$, $\implies r \mid 23$, $\implies r = \pm 1, \pm 23$. The value $r = -23 = b_1 = a^2 - 4b$, by definition of q when $u = 0$, corresponds to $(0, 0)$, so $[-23] \in \operatorname{im} q$. Since $\operatorname{im} q$ is a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, it must be $\operatorname{im} q = \{[1], [-23]\}$ or $\operatorname{im} q = \{[1], [-23], [-1], [23]\}$.

- Determine $E(\mathbb{Q})/\psi(E'(\mathbb{Q}))$.

5.3 Step 1 - General Case

5.4 Step 2 - For $E/\mathbb{Q}$

[14] By definition, we can solve

$$r^2l^4 + 4arl^2m^2 + 16bm^4 = rn^2$$

to get points $\left(\frac{rl^2}{m^2}, \frac{rnl}{m^3}\right) \in E''(\mathbb{Q})$, then get $\left(\frac{rl^2}{4m^2}, \frac{rnl}{8m^3}\right) \in E(\mathbb{Q})$. Composing together gives the computation we use.