1 Elliptic Curves

By Proposition **??**, the cotangent bundle of an abelian variety over K is trivial. Thus an abelian variety of dimension 1 has genus 1, i.e. is an elliptic curve. In this section, we prove the converse, i.e. elliptic curve has a group structure and is an abelian variety.

Definition 1.1

An ***elliptic curve*** over K is a geometrically irreducible smooth projective curve E of genus $g(E) = 1$, equipped with a rational point $P_0 \in E(K)$.

Note geometrically irreducible is the same as irreducible for us, since we have at least one K-rational point. Let E be elliptic curve over K and D be a divisor on $E_{\overline{K}}$ of degree $\deg(D) > 0$. The space of global sections $\Gamma(E_{\overline{K}}, \mathscr{O}(D))$ may be realized as the subspace

$$\overline{\mathscr{L}}(D) := \{f \in \overline{K}(E_{\overline{K}})^{\times} : \operatorname{div}(f) \geq -D\} \cup \{0\}$$

in $\overline{K}(E_{\overline{K}})$, using the homomorphism $s \mapsto s/s_D$. By Riemann-Roch, we see

$$\dim_{\overline{K}} \overline{\mathscr{L}}(D) = \deg(D) \tag{Eq. 1.1}$$

hence the corresponding linear system $|D_{\overline{K}}|$ has dimension $\deg(D) - 1$. It follows that two distinct points (viewed as Weil divisors) on E are rationally equivalent over $\overline{K}$.

Let us fix a base point $P_0 \in E(K)$. For two point $P_1, P_2 \in E(\overline{K})$, let $D := [P_1] + [P_2] - [P_0]$. Thus $\deg(D) = 1$ and $\overline{\mathscr{L}}(D)$ is one-dimensional, generated by a function f, unique up to multiplication by a scalar. By construction, if $P_0 \notin \{P_1, P_2\}$, then f has pole divisor $[P_1] + [P_2]$ and vanishes at P_0 and at exactly one other point P_3 (this one extra point is because $\dim(\overline{\mathscr{L}}(D)) = 1$), which is the unique point rationally equivalent to $[P_1] + [P_2] - [P_0]$. This make sense even if P_1 or P_2 equals P_0. Thus we get a well-defined composition law on E by $(P_1, P_2) \mapsto P_1 + P_2 := P_3$.

We should distinguish carefully between addition of points P_1, P_2 on E and of the corresponding divisors $[P_1]$, $[P_2]$. Remembering that $\operatorname{Pic}^0(E_{\overline{K}})$ is the group of rational equivalence classes of divisors of degree 0, we get an additive map

$$E \to \operatorname{Pic}^0(E_{\overline{K}}), \quad P \mapsto [P] - [P_0]$$

By Eq. 1.1 this map is bijective. We will later give more geometric interpretation of the addition rule.

Proposition 1.2

If the group structure on an elliptic curve E over K with base point P_0 is given by bijective map

$$E \to \operatorname{Pic}^0(E_{\overline{K}}), \quad P \mapsto [P] - [P_0]$$

then E is an abelian variety defined over K.

We will prove this result throughout the section, as we gain more understanding of elliptic curves.

Now let us first give a classical argument showing E has a model given by a smooth cubic curve. Let us realize $\Gamma(E, \mathscr{O}(D))$ via

$$\mathscr{L}(D) = \{f \in K(E)^\times : \mathrm{div}(f) \geq -D\} \cup \{0\}$$

for any divisor D on E. If $\deg(D) > 0$, then by Riemann-Rock, $\mathscr{L}(D)$ has dimension $\deg(D)$. We have an ascending chain of K-vector spaces

$$\mathscr{L}([P_0]) \subseteq \mathscr{L}(2[P_0]) \subseteq \ldots \subseteq \mathscr{L}(6[P_0])$$

and the jth member has dimension j.

Clearly 1 is a basis of $\mathscr{L}([P_0])$. Since P_0 is defined over K, there are $x, y \in K(E)$ such that $1, x$ is a basis of $\mathscr{L}(2[P_0])$ and $1, x, y$ is a basis of $\mathscr{L}(3[P_0])$. By looking at the order of pole at P_0, its clear $1, x, y, x^2$ is a basis of $\mathscr{L}(4[P_0])$ and $1, x, y, x^2, xy$ is a basis of $\mathscr{L}(5[P_0])$. Moreover, $x^3, y^2 \in \mathscr{L}(6[P_0])$. This gives 7 elements $1, x, y, x^2, xy, x^3, y^2$ spanning $\mathscr{L}(6[P_0])$, where $\dim \mathscr{L}(6[P_0]) = 6$. Thus there must be $c_i \in K$ so

$$c_0 + c_1 x + c_2 y + c_3 x^2 + c_4 xy + c_5 x^3 + c_6 y^2 = 0$$

By the above, c_5 and c_6 are different from 0, so that we may normalize $c_5 = -1$. If we divide by c_6^3 and replace x by x/c_6 and y by y/c_6^2, we get a relation of the form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad \text{(Eq. 1.2)}$$

with $a_i \in K$. Since $\deg(3[P_0]) = 3 = 2g(E) + 1$, the divisor $3[P_0]$ is very ample. Hence the basis of $\mathscr{L}(3[P_0])$ corresponding to $1, x, y$ induces a closed embedding of E into $\mathbb{P}^2_K$. We know by Eq. 1.2 that the image of E is contained in the projective curve with ***Weierstrass equation***

$$x_0 x_2^2 + a_1 x_0 x_1 x_2 + a_3 x_0^2 x_3 = x_1^3 + a_2 x_0 x_1^2 + a_4 x_0^2 x_1 + a_6 x_0^3$$

in the homogeneous coordinates $(x_0 : x_1 : x_2)$ of $\mathbb{P}^2_K$.

It is easy to prove the curve defined above is geometrically irreducible, hence it gives a projective model of E as a smooth plane cubic curve. Note also that the ratinoal functions $x = x_1/x_0$ and $y = x_2/x_0$ are nothing else than the two functions x, y defined before, hence the affine form Eq. 1.2 of the Weierstrass equation describes the affine curve $E \cap \{x_0 \neq 0\}$. The only point of E outside this part is the point $(0 : 0 : 1) \in \mathbb{P}^2_K$, corresponding to $P_0 \in E$. It is easily seen that, in this model, P_0 is an inflexion point of E.

Remark 1.3

If $\mathrm{char}(K) \neq 2$, then replacing y by $\frac{1}{2}(y - a_1 x - a_3)$ leads to a Weierstrass equation with $a_1 = a_3 = 0$. Then the Jacobi criterion shows a Weierstrass equation describes a smooth curve C in $\mathbb{P}^2_K$ if and only if the discriminant of the cubic polynomial $x^3 + a_2 x^2 + a_4 x + a_6$ is not zero. By the genus formula

$$g(C) = \frac{1}{2}(\deg(C) - 1)(\deg(C) - 2)$$

this is an elliptic curve. If $\mathrm{char}(K) \neq 3$, then a further linear transformation leads to the Weierstrass normal/short form

$$y^2 = 4x^3 - g_2x - g_3$$

Now let us go back to any characteristic. We will describe a more explicit group structure on the abelian group E, beginning by proving the inverse operation is a morphism.

Consider the rational equivalence relation

$$[P_1] + [P_2] + [P_3] \sim 3[P_0] \tag{Eq. 1.3}$$

on $E_{\overline{K}}$. This relation is equivalent to the geometric statement that the points P_1, P_2, P_3 are the three intersection points, counted with multiplicity, of a straight line with E. We verify this as follows. The lines in $\mathbb{P}^2_{\overline{K}}$ are just the divisors of the global sections of $\mathscr{O}_{\mathbb{P}^2_{\overline{K}}}(1)$ and, by construction, the restriction of this line bundle to E is isomorphic to $\mathscr{O}(3[P_0])$. First, we assume $[P_1]+[P_2]+[P_3] \sim 3[P_0]$, then there is $s' \in \Gamma(E_{\overline{K}}, \mathscr{O}(3[P_0]))$ with $\mathrm{div}(s') = [P_1] + [P_2] + [P_3]$. By construction of the embedding $E \hookrightarrow \mathbb{P}^2_{\overline{K}}$, there is $s \in \Gamma(\mathbb{P}^2_{\overline{K}}, \mathscr{O}_{\mathbb{P}^2_{\overline{K}}(1)})$ with $s' = s|_E$. Then the line $\ell = \mathrm{div}(s)$ is the line through the three points P_i. Indeed, by definition of proper intersection product, we have

$$\ell \cdot E = \mathrm{div}(s|_E) = \mathrm{div}(s') = [P_1] + [P_2] + [P_3]$$

The converse is proved the same way by reversing the previous argument.

The zero element of E is $P_0 = (0 : 0 : 1)$. The inverse $P_2 := -P_1$ of a point $P_1 \in E$ is characterized by the rational equivalence $[P_1] + [P_2] \sim 2[P_0]$, which can be rewritten as the special case

$$[P_0] + [P_1] + [P_2] \sim 3[P_0]$$

of Eq. 1.3. It follows P_0, P_1, P_2 are on a straight line and in fact, noting $P_0 = (0 : 0 : 1)$, we see that, if $P_1 \neq P_0$, then P_2 is the residual finite intersection of E with the vertical line in (x, y)-plane going through P_1. If (x_1, y_1) are the affine coordinates of P_1, then, using Eq. 1.2, the affine coordinates (x_2, y_2) of P_2 are given by

$$x_2 = x_1, \quad y_2 = -a_1x_1 - a_3 - y_1$$

Thus the inverse map is an automorphism of the affine part of E defined over K. On the other hand, a rational map of a smooth projective curve is always a morphism. We conclude the above restriction extends to an automorphism of E. This requires 0 map to 0, hence the inverse map is a morphism on E defined over K.

Now we study the addition on the elliptic curve a bit closer. By the above, it is enough to construct

$$P_3 = -(P_1 + P_2)$$

The point P_3 is characterized by the rational equivalence Eq. 1.3. As we have seen above, P_3 is the third intersection point of the line ℓ through P_1 and P_2 with E, taking this line to be the tangent line to E at P_1 if $P_1 = P_2$.

If $P_1 \neq P_0$ and $P_2 \notin \{P_0, -P_1\}$, then the third intersection point of the line through P_1, P_2 with E is contained in the (x, y)-plane. Let $y = ax + b$ be the equation for this line. We eliminate y in Eq. 1.2 obtaining a cubic equation for x, with two known solutions x_1, x_2. This equation has the form

$$x^3 - (a^2 + a_1 a - a_2)x^2 + \text{ lower degree terms} = 0$$

The third solution x_3 is determined by the trace $x_1 + x_2 + x_3 = a^2 + a_1 a - a_2$. Since $P_1 + P_2 = -P_3$, applying the inverse as above, we conclude the following result.

Proposition 1.4: Addition Law

Let E be the elliptic curve in normal form

$$y^2 = a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

Then the origin O of the group E is the unique point at infinity and the group law $+$ is defined as follows. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ be two finite points on E and set

$$a = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2 \\ \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} & \text{otherwise} \end{cases}$$

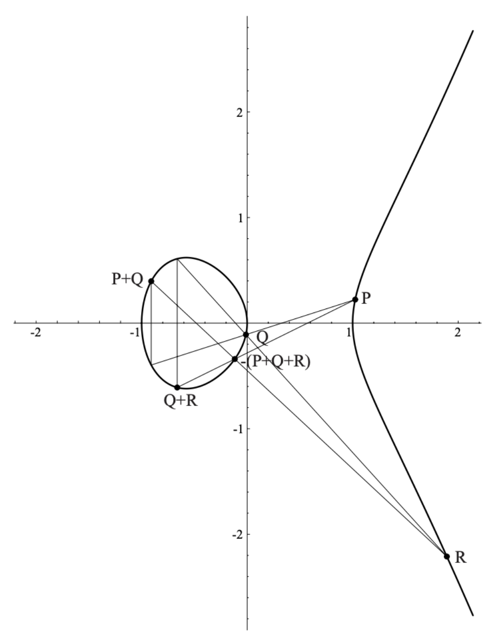
$$b = y_1 - a x_1$$

Then:

1. *The inverse of P_1 is given by $-P_1 = (x_1, -a_1 x_1 - a_3 - y_1)$*
2. *If $x_2 = x_1$ and $y_2 = -a_1 x_1 - a_3 - y_1$, then $P_1 + P_2 = O$*
3. *Otherwise, we have*

$$P_1 + P_2 = (a^2 + a_1 a - a_2 - x_1 - x_2, -(a + a_1)(a^2 + a_1 a - a_2 - x_1 - x_2) - a_3 - b)$$

The addition law can be seen visually as the following:



The addition law shows that addition is a rational map. In order to finish proof of Proposition 1.2, it remains to show $+$ is a morphism. To show rational map extends to a morphism, it suffices to prove that over $\overline{K}$. In a first step, we show translation τ_Q by $Q \in E$ is a morphism. We may assume $Q \neq O$. By the formulae in Proposition 1.4, τ_Q is a rational map which restricts to a morphism $E \backslash \{O, Q, -Q\} \to E \backslash \{Q, O, Q+Q\}$. Since every rational map between projective smooth curves extends to a morphism (valuative criterion), we get a morphism $\tau'_Q : E \to E$ which agrees with τ_Q on $E \backslash \{O, Q, -Q\}$. It remains to prove $\tau_Q = \tau'_Q$. For $R \in E$, we see $\tau'_Q \circ \tau'_R = \tau'_{Q+R}$. In particular, every τ'_Q is an isomorphism with inverse τ'_{-Q}. Thus τ'_Q maps $\{O, Q, -Q\}$ onto $\{Q, Q+Q, O\}$. For any $R \notin \{O, Q, -Q, Q+Q, -Q-Q\}$ we have

$$\tau'_R(\tau'_Q(Q)) = \tau'_{Q+R}(Q) = \tau'_Q(\tau'_R(Q)) = \tau'_Q(Q+R) = Q+Q+R$$

This excludes $\tau'_Q(Q) = Q$ immediately. On the other hand, we know $\tau'_R(O) \in \{O, R, R+R\}$, hence $\tau'_Q(Q) = O$ is only possible if $Q+Q = O$. This proves

$$\tau'_Q(Q) = Q+Q = \tau_Q(Q)$$

The equation

$$\tau'_Q(-Q) = O = \tau_Q(-Q)$$

is proved in a similar fashion. Thus, using that τ'_Q is a bijection, we conclude $\tau'_Q(O) = Q = \tau_Q(O)$. We have handled all exceptions, thereby proving $\tau_Q = \tau'_Q$.

Next we show addition is a morphism. The formulae in Proposition 1.4 show that addition is a rational map m, which is a morphism outside

$$Z := \{(P,P) : P \in E\} \cup \{(P,-P) : P \in E\} \cup (E \times \{O\}) \cup (\{O\} \times E)$$

For $(P,Q) \in Z$, there are $R, S \in E$ such that $(P+R, Q+S) \notin Z$. Since translations are morphisms, we see

$$\tau_{-P-Q} \circ m \circ (\tau_R \times \tau_S)$$

is a morphism in a neighbourhood of (P,Q) and agrees with $+$ everywhere. This proves $+$ is a morphism.

Remark 1.5

Complex analytically, an elliptic curve is biholomorphic to $\mathbb{C}/\Lambda$ where Λ is a lattice in $\mathbb{C}$. In dimension 1 the converse is true, i.e. every one-dimensional complex torus is biholomorphic to an abelian variety. The description of the elliptic curve determined by $\mathbb{C}/\Lambda$ is done quite explicitly by means of Weierstrass $\wp$-function associated to the lattice Λ, namely

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \backslash \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

It is Λ-periodic meromorphic function on $\mathbb{C}$ with double periods at lattice points. In particular it satisfies the first-order differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

where

$$g_2 = 60 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\omega\in\Lambda\setminus\{0\}} \frac{1}{\omega^6}$$

The map $z \mapsto (\wp(z), \wp'(z))$ is biholomorphic from $\mathbb{C}/\Lambda$ onto the elliptic curve with affine Weierstrass equation $y^2 = 4x^3 - g_2 x - g_3$.