



# Elliptic Curves, n° 2

Lei Bichang

October 11, 2024

We prepare some lemmas here.

**Lemma 1.** If  $C_1, C_2$  are smooth curves,  $\phi : C_1 \rightarrow C_2$  is a surjective morphism,  $f \in \bar{K}(C_1)^\times$  and  $D \in \text{Div}(C_2)$ , then

$$f(\phi^* D) = (\phi_* f)(D)$$

if both sides are well-defined.

*Proof.* (\*) Assume that both sides of the desired equation are well-defined. For simplicity of notations, assume that  $K = \bar{K}$ .

By Lemma 2 and the fact that  $\phi^* : \text{Div}(C_2) \rightarrow \text{Div}(C_1)$  is additive, it suffices to prove in the case of  $D = (P)$ , where  $P \in C_2$  is a point. In this case,

$$f(\phi^*(P)) = f\left(\sum_{Q \in \phi^{-1}(P)} e_\phi(Q) \cdot (Q)\right) = \prod_{Q \in \phi^{-1}(P)} f(Q)^{e_\phi(Q)},$$

$$(\phi_* f)((P)) = (\phi_* f)(P) = (N_{K(C_1)/K(C_2)} f)(P),$$

where we identify  $K(C_2)$  with  $\phi^* K(C_2) \subset K(C_1)$ .

Since  $f(\phi^* D)$  is well-defined and the support of  $\phi^*(D)$  is  $\phi^{-1}(P)$ , every points  $Q \in \phi^{-1}(P)$  is not a zero or pole for  $f$ , so  $f \in K(C_1)_Q^\times$ , where  $K(C_1)_Q$  is the local ring of  $C_1$  at  $Q$ .

Similarly,  $\phi_* f \in K(C_2)_P^\times$  because  $(\phi_* f)(D)$  is well-defined, and  $(\phi_* f)(P)$  is the image of  $\phi_* f$  in the residue field  $k_P := K(C_2)_P / \mathfrak{m}_P$ .

Let  $B$  be the integral closure of  $K(C_2)_P$  in  $K(C_1)$ . Then  $f \in B$  and  $N_{B/K(C_1)_P} f = \phi_* f$ . By the commutative diagram

$$\begin{array}{ccc} B & \longrightarrow & B/\mathfrak{m}_P B \\ \downarrow & & \downarrow \\ K(C_1)_P & \longrightarrow & k_P \end{array}$$

where the vertical arrows are the corresponding norm maps, we have  $(\phi_* f)(P) = \det(u)$ , where  $u : B/\mathfrak{m}_P B \rightarrow B/\mathfrak{m}_P B$  is the  $k_P$ -linear map given by multiplication-by- $\bar{f} \in B/\mathfrak{m}_P B$ .

The ideal  $\mathfrak{m}_P B$  decomposes in  $B$  as

$$\mathfrak{m}_P B = \prod_{Q \in \phi^{-1}(P)} \mathfrak{m}_Q^{e_\phi(Q)},$$

where  $\mathfrak{m}_Q$  is the intersection of the maximal ideal of  $K(C_2)_Q$  with  $B$ . This gives an isomorphism of  $k_P$ -modules

$$B/\mathfrak{m}_P B \simeq \prod_{Q \in \phi^{-1}(P)} B/\mathfrak{m}_Q^{e_\phi(Q)}.$$

For  $Q \in \phi^{-1}(P)$ , let  $\pi_Q \in \mathfrak{m}_Q$  be a uniformiser, then  $1, \bar{\pi}_Q, \dots, \bar{\pi}_Q^{e_\phi(Q)-1}$  form a  $k_P$ -basis for  $B/\mathfrak{m}_Q^{e_\phi(Q)}$ . Write  $\phi^{-1}(P) = \{Q_1, \dots, Q_r\}$ , then

$$1, \bar{\pi}_{Q_1}, \dots, \bar{\pi}_{Q_1}^{e_\phi(Q_1)-1}, \dots, 1, \bar{\pi}_{Q_r}, \dots, \bar{\pi}_{Q_r}^{e_\phi(Q_r)-1}$$



form a basis of  $B/\mathfrak{m}_B$  over  $k_P$ . Note that

$$f \cdot \pi_Q^i \in f(P)\pi_Q^i + \mathfrak{m}_Q^{i+1}$$

for every  $Q \in \phi^{-1}(P)$ , so each subspace  $\langle 1, \pi_Q, \dots, \pi_Q^{e_\phi(Q)-1} \rangle \subset B/\mathfrak{m}_P B$  is  $u$ -stable, and the matrix of  $u$  under the chosen basis is block-wise diagonal of the form

$$u = \begin{pmatrix} u_1 & & \\ & \ddots & \\ & & u_r \end{pmatrix}$$

where

$$u_i = \begin{pmatrix} f(Q_i) & * & * \\ & \ddots & * \\ & & f(Q_i) \end{pmatrix}$$

is upper-triangular. Therefore,

$$(\phi_* f)(P) = \det(u) = \prod_{Q \in \phi^{-1}(P)} f(Q)^{e_\phi(Q)}.$$

□

**Lemma 2.** If  $D, E \in \text{Div}(C)$  and  $f, g \in \bar{K}(E)^\times$ , then

$$f(D + E) = f(D)f(E),$$

$$(fg)(D) = f(D)g(D)$$

if both sides are well-defined.

*Proof.* Write  $D = \sum_{P \in C} a_P(P)$ ,  $E = \sum_{P \in C} b_P(P)$ , then

$$f(D + E) = \prod_{P \in C} f(P)^{a_P + b_P} = \prod_{P \in C} f(P)^{a_P} f(P)^{b_P} = f(D)f(E),$$

$$(fg)(D) = \prod_{P \in C} f(P)^{a_P} g(P)^{a_P} = f(D)g(D).$$

□

## Exercise 1

(a) Write

$$\text{div}(f) = \sum_{i \in I} n_i(A_i), \quad \text{div}(g) = \sum_{j \in J} m_j(B_j),$$

where  $\{n_i\}_{i \in I}$  and  $\{m_j\}_{j \in J}$  are finite sets of nonzero integers and  $A_i, B_j$  are distinct points on  $C = \mathbb{P}^1$ . Let  $[X : Y]$  be a homogeneous coordinate on  $\mathbb{P}^1$  s.t. all of the  $A_i$ 's and  $B_j$ 's are in the chart  $Y \neq 0$ , then we can write

$$A_i = [a_i : 1], \quad B_j = [b_j : 1]$$

with  $a_i, b_j \in \bar{K}$ , and thus

$$f = a \prod_{i \in I} (X - a_i Y), \quad g = b \prod_{j \in J} (X - b_j Y)$$



with  $a, b \in \bar{K}^\times$ . Hence

$$\begin{aligned} f(\text{div } g) &= \prod_j f(B_j)^{m_j} = \prod_{i,j} a^{n_j} (b_j - a_i)^{n_i m_j} = (-1)^{\sum_{i,j} n_i m_j} a^{\deg \text{div } g} b^{\deg \text{div } f} \prod_{i,j} (a_i - b_j)^{n_i m_j} \\ &= (-1)^{\sum_{i,j} n_i m_j} \prod_i g(A_i)^{n_i} = (-1)^{\sum_{i,j} n_i m_j} g(\text{div } f) = g(\text{div } f), \end{aligned}$$

because  $\deg \text{div } f = \deg \text{div } g = 0$  and  $\sum_{i,j} n_i m_j = (\sum_i n_i)(\sum_j n_j) = (\deg \text{div } f)(\deg \text{div } g) = 0$ .

- (b) Let  $[X : Y]$  be a homogeneous coordinate on  $\mathbb{P}^1$  and  $x := X/Y \in \bar{K}(\mathbb{P}^1)$ . Then  $\operatorname{div} g = g^*(\operatorname{div} x)$ . Write  $\operatorname{div}(f) = \sum_{i \in I} n_i(A_i)$  with  $n_i \neq 0$  for all  $i \in I$ . Then  $g(A_i) \in \bar{K}^\times$ , and the corresponding point in  $\mathbb{P}^1$  is  $[g(A_i) : 1]$ . Thus we see that

$$\begin{aligned} f(\operatorname{div} g) &= f(g^*(\operatorname{div} x)) \stackrel{(!)}{=} (g_* f)(\operatorname{div} x) \\ &= x(\operatorname{div}(g_* f)) = x(g_* \operatorname{div} f) \\ &= x \left( \sum_{i \in I} n_i([g(A_i) : 1]) \right) \\ &= \prod_{i \in I} g(A_i)^{n_i} = g(\operatorname{div} f), \end{aligned}$$

where (!) is deduced from Lemma 1.

## Exercise 2

- (a) First, we need to show the existence of  $D_P, D_Q, f_P$  and  $f_Q$  for every  $P, Q \in E[m]$ . Let  $D_P = (P) - (O)$ . For  $D_Q$ , we seek for points  $Q_1, Q_2, Q_3 \in E \setminus \{P, O\}$  s.t.  $Q_2 + Q_3 = Q_1$ , then set

$$D_Q := (Q) + (Q_1) - (Q_2) - (Q_3).$$

For example, let  $n \geq 4$  be an integer that is prime to  $m$  and  $\operatorname{char}(K)$ , then  $E[n] \neq \{O\}$  and we can choose  $Q_2 \in E[n] \setminus \{O\}$ ,  $Q_3 := 2Q_2$ ,  $Q_1 := 3Q_2$ .

Since

$$\sigma(mD_P) = m\sigma(D_P) = mP = 0,$$

$mD_P$  is a principal divisor and thus there exists  $f_P \in \bar{K}(E)^\times$  with  $\operatorname{div} f_P = mD_P$ . The function  $f_Q$  exists for the same reason.

*Independent of choices.* Let  $D'_P, D'_Q, f'_P$  and  $f'_Q$  be another set of choices. We prove in the following steps.

- (1) Suppose  $D'_P = D_P$  and  $D'_Q = D_Q$ . Then  $\operatorname{div} f'_P = \operatorname{div} f_P$ , so  $f'_P = cf_P$  for some  $c \in \bar{K}^\times$ . Hence for any divisor  $D = \sum_{X \in E} n_X(X) \in \operatorname{Div}^0(E)$ ,

$$f'_P(D) = \prod_{X \in E} (cf_P(X))^{n_X} = c^{\deg D} f_P(D) = f_P(D).$$

Similarly,  $f'_Q(D) = f_Q(D)$  for all  $D \in \operatorname{Div}^0(E)$ . Therefore, the choice of  $f_P$  and  $f_Q$  does not affect  $\tilde{e}_m(P, Q)$ .

- (2) Suppose  $D'_P = D_P$  and  $f'_P = f_P$ . Then

$$\sigma(D'_Q - D_Q) = \sigma(D'_Q) - \sigma(D_Q) = O$$

and  $\deg(D'_Q - D_Q) = 0$ . So  $D'_Q - D_Q = \operatorname{div} g$  for some  $g \in \bar{K}(E)^\times$ , and

$$\operatorname{div} \left( \frac{f'_Q}{f_Q} \right) = mD'_Q - mD_Q = m(D'_Q - D_Q) = \operatorname{div}(g^m).$$

Hence there is a  $c \in \bar{K}^\times$  s.t.  $f'_Q = cg^m f_Q$ . Note that  $\operatorname{div} f_P = mD_P$  and  $\operatorname{div} g = D'_Q - D_Q$  have disjoint supports.

Now by Lemma 2 and Exercise 1,

$$\begin{aligned} \frac{f_P(D'_Q)}{f'_Q(D_P)} &= \frac{f_P(D_Q + \operatorname{div} g)}{(cf_Q g^m)(D_P)} = \frac{f_P(D_Q) f_P(\operatorname{div} g)}{(cf_Q)(D_P)(g(D_P)^m)} \\ &= \frac{f_P(D_Q)}{c^{\deg D_P} f_Q(D_P)} \frac{f_P(\operatorname{div} g)}{g(mD_P)} \\ &= \frac{f_P(D_Q)}{f_Q(D_P)} \frac{g(\operatorname{div} f_P)}{g(mD_P)} = \frac{f_P(D_Q)}{f_Q(D_P)}. \end{aligned}$$

Therefore,  $\tilde{e}_m(P, Q)$  is independent of the choice of  $D_P$ .

(3) Suppose  $D'_Q = D_Q$  and  $f'_Q = f_Q$ . Then

$$\frac{f_P(D'_Q)}{f'_Q(D_P)} = \left( \frac{f'_Q(D_P)}{f_P(D'_Q)} \right)^{-1} = \tilde{e}_m(Q, P)^{-1} = \left( \frac{f_Q(D_P)}{f_P(D_Q)} \right)^{-1} = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

So  $\tilde{e}_m(P, Q)$  is independent of the choice of  $D_P$ .

In conclusion,  $\tilde{e}_m(P, Q)$  is well-defined and depends only on  $P$  and  $Q$ .

(b) By Lemma 2 and Exercise 1,

$$\tilde{e}_m(P, Q)^m = \frac{f_P(D_Q)^m}{f_Q(D_P)^m} = \frac{f_P(mD_Q)}{f_Q(mD_P)} = \frac{f_P(\operatorname{div} f_Q)}{f_Q(\operatorname{div} f_P)} = 1.$$

(c) The existence of  $g_Q$  and  $g_P$  are similar, so it suffices to prove for  $g_P$ . Write  $D_P = \sum_{X \in E} n_X(X)$ . By the assumption on  $m$ ,  $[m] \in \operatorname{End}(E)$  is separable and thus unramified. Hence

$$\begin{aligned} \operatorname{div}([m]^* f_P) &= [m]^*(\operatorname{div} f_P) = [m]^*(mD_P) \\ &= \sum_{X \in E} mn_X[m]^*(X) = \sum_{X \in E} mn_X \sum_{mY=X} (Y) = \sum_{Y \in E} mn_{mY}(Y). \end{aligned}$$

Let  $D := \sum_{Y \in E} n_{mY}(Y)$ , then  $\operatorname{div}([m]^* f_P) = mD$ . Since  $[m]$  is separable and unramified,

$$\deg D = \sum_{Y \in E} n_{mY} = \sum_{X \in E} \sum_{mY=X} n_X = \sum_{X \in E} m^2 n_X = m^2 \deg D_P = 0.$$

If  $mZ = X \in E$ , then

$$\sum_{mY=X} Y = \sum_{W \in E[m]} (Z + W) = m^2 Z + \sum_{W \in E[m]} W = mX,$$

so

$$\sigma(D) = \sum_{X \in E} n_X \sum_{mY=X} Y = \sum_{X \in E} n_X mX = m\sigma(D_P) = mP = O.$$

Therefore,  $D$  is a principal divisor, so there exists  $h \in \bar{K}(E)^\times$  s.t.  $\operatorname{div} h = D$ . Thus

$$\operatorname{div}(h^m) = mD = \operatorname{div}([m]^* f_P),$$

which means there is a  $c \in \bar{K}^\times$  s.t.  $[m]^* f_P = ch^m$ . Let  $g_P := c^{1/m} h$ , then  $[m]^* f_P = g_P^m$ .

(d) By definition,  $g_P(X)^m = f_P(mX)$  and  $g_Q(X)^m = f_Q(mX)$  for all  $X \in E$ . By Lemma 2,

$$\begin{aligned} \left( \frac{g_P(Q' + R)g_Q(O)}{g_P(R)g_Q(P')} \right)^m &= \frac{f_P(mQ' + mR)f_Q(mO)}{f_P(mR)f_Q(mP')} \\ &= \frac{f_P((Q + mR) - (mR))}{f_Q((P) - (O))}. \end{aligned}$$

The divisor  $(Q + mR) - (mR)$  verifies the conditions for  $D_P$ . If  $(Q + mR) - (mR)$  verifies the conditions for  $D_Q$ , then  $g_P(Q' + R)g_Q(O)/g_P(R)g_Q(P') = \tilde{e}_m(P, Q)$  by setting  $D_P = (P) - (O)$  and  $D_Q = (Q + mR) - (mR)$ .

Both  $\sigma((Q + mR) - (mR)) = O$  and  $\deg((Q + mR) - (mR)) = 0$  is clear. It is left to show that

$$\{Q + mR, mR\} \cap \{P, O\} = \emptyset. \quad (1)$$

We just need

$$mR \notin \{O, P, -Q, P - Q\},$$

which is equivalent to  $mR \notin \{O, P, -Q\}$  as

$$mR = P - Q \iff mR = 2mR \iff mR = O.$$

This can be satisfied, because there are  $m^2$  possible  $P'$ 's; a fixed choice of  $P'$  gives  $m^2$  choices of  $Q'$  if  $Q \neq \pm P$  and  $m^2 - 2$  choices of  $Q'$  if  $Q = \pm P$ ; every  $Q'$  gives 4 possible  $R$ . So there are  $4m^4 - 8m^2$  choices of  $R$ , but

$$\#\{R \in E | mR \in \{O, P, -Q\}\} \leq 3m^2 < 4m^4 - 8m^2$$

for  $m \geq 2$ .

(e) Keep the choice of  $D_P = (P) - (O)$  and  $D_Q = (Q + mR) - (mR)$ . Then

$$[m]^*(mD_P) = m \left( \sum_{Y \in E[m]} (P' + Y) - (Y) \right),$$

so

$$\operatorname{div}(g_P) = \frac{1}{m} \operatorname{div}(f_P) = \sum_{Y \in E[m]} (P' + Y) - (Y).$$

Similarly,

$$\operatorname{div}(g_Q) = \sum_{Y \in E[m]} (Q' + R + Y) - (R + Y).$$

Therefore,

$$\begin{aligned} & \operatorname{div} \left( \frac{g_P(X + Q' + R)g_Q(X)}{g_P(X + R)g_Q(X + P')} \right) \\ &= \sum_{Y \in E[m]} ((Y + P' - Q' - R) - (Y - Q' - R) + (Y + Q' + R) - (Y + R) \\ & \quad - (Y + P' - R) + (Y - R) - (Y + Q' + R - P') + (Y + R - P')) \\ &= \sum_{Y \in E[m]} ((Y + R) - (Y - Q' - R) + (Y + Q' + R) - (Y + R) \\ & \quad - (Y + P' - R) + (Y - R) - (Y - R) + (Y + R - P')) \\ &= \sum_{Y \in E[m]} (-(Y - Q' - R) + (Y + Q' + R) - (Y + P' - R) + (Y + R - P')). \end{aligned}$$

Since  $(P' - R) - (Q' + R) = O \in E$ , i.e.,  $P' - R = Q' + R$ , we conclude that

$$\operatorname{div} \left( \frac{g_P(X + Q' + R)g_Q(X)}{g_P(X + R)g_Q(X + P')} \right) = 0.$$

Meanwhile,

$$\begin{aligned} \operatorname{div} \left( \prod_{k=0}^{m-1} g_Q(X + kQ') \right) &= \sum_{k=0}^{m-1} \sum_{Y \in E[m]} ((Y + R - (k-1)Q') - (Y + R - kQ')) \\ &= \sum_{Y \in E[m]} (Y + R - (-1)Q') - (Y + R - (m-1)Q') \\ &= \sum_{Y \in E[m]} (Y + R + Q') - (Y + R + Q' - Q) \\ &= [m]^*(mR + Q) - [m]^*(mR + Q - O) = 0. \end{aligned}$$

Therefore, the two functions are both constant.

(f) We have

$$\begin{aligned}
\tilde{e}_m(P, Q) &= \left( \frac{g_P(Q' + R)g_Q(O)}{g_P(R)g_Q(P')} \right)^m \\
&= \prod_{k=0}^{m-1} \frac{g_P((k+1)Q' + R)g_Q(kQ')}{g_P(kQ' + R)g_Q(kQ' + P')} \\
&= \frac{g_P(mQ' + R)}{g_P(R)} \prod_{k=0}^{m-1} \frac{g_Q(kQ')}{g_Q(kQ' + P')} \\
&= \frac{g_P(Q + R)}{g_P(R)}.
\end{aligned}$$

Since  $\text{div}(f_P) = mD_P = m(P) - m(O)$  and  $f_P \circ [m] = g_P^m$ , the value  $\frac{g_P(Q+R)}{g_P(R)} = e_m(P, Q)$ .