

# Elliptic Curves

Lei Bichang

Sep 19

## Exercise 1

1. A point  $(x, y) \in C_P$  is singular iff

$$\begin{cases} y^2 = P(x), \\ 2y = P'(x) = 0. \end{cases} \quad (1)$$

If  $\text{char } k \neq 2$ , then the condition is equivalent to  $y = 0$  and  $x$  being a multiple root of  $P$ . Hence  $C_P$  is smooth iff  $P$  has no multiple roots in  $k$ .

If  $\text{char } k = 2$ , then since  $k$  is algebraically closed, ?? can be satisfied whenever  $P'$  has a root in  $k$ . So  $C_P$  is smooth iff  $P'$  is a nonzero constant, which means that  $P(X)$  has degree 1.

2. The projective closure  $\bar{C}_P$  of  $C_P$  in  $\mathbb{P}^2(k)$  is defined by

$$\frac{Y^2}{Z^2} = P\left(\frac{X}{Z}\right).$$

If  $\text{char } k = 2$  and  $\bar{C}_P$  is smooth, then  $P(X) = aX + b$  with  $a \in k^\times$  and  $b \in k$ , so  $\bar{C}_P$  is defined by

$$Y^2 = aXZ + bZ^2.$$

Let  $F := aXZ + bZ^2 - Y^2$ . and  $A = [x : y : 0] \in \bar{C}_P$ . If  $x = 0$ , then  $y^2 = 0$ , which implies  $y = 0$ . Therefore  $x \neq 0$ , and thus

$$\frac{\partial F}{\partial Z}(A) = ax \neq 0.$$

Hence  $\bar{C}_P$  is smooth.

Now suppose  $\text{char } k \neq 2$  and  $P$  has no multiple roots. Then  $\bar{C}_P$  is smooth iff all the points of  $\bar{C}_P$  on the chart  $X \neq 0$  are smooth.

Wrong answer:

Let  $C'$  be the intersection of  $\bar{C}_P$  with the chart  $X \neq 0$ ,  $m := \deg P$  and  $2n \geq m$  be an even integer. Let  $z := Z/X$  and  $w := Z^{n-1}Y/X^n$ , then  $z^{2n}P(1/z) \in k[z]$ , and  $C'$  is the affine plane curve

$$w^2 = z^{2n}P\left(\frac{1}{z}\right).$$

This is not  $C'$ . It cannot even embed into  $\mathbb{P}^2$ . By assumption, write

$$P(X) = \prod_{i=1}^m (X - a_i)$$

with  $a_i \in k$  distinct, then

$$z^{2n}P\left(\frac{1}{z}\right) = z^{2n-m} \prod_{i=1}^m (1 - a_i z).$$

Therefore, the polynomial  $z^{2n}P\left(\frac{1}{z}\right)$  would have no multiple roots, if we choose  $n$  s.t.  $2n$  is the smallest integer greater than or equal to  $m$ . Such  $n$  always exists, and taking such  $n$  tells us that  $C'$  is smooth. Hence,  $\bar{C}_P$  is smooth.

In conclusion, the projective closure  $\bar{C}_P$  is smooth iff  $P$  is smooth.

3. If  $\text{char } k \mid d$ , then  $C_P$  is smooth iff  $P$  has degree 1, and  $\bar{C}_P$  is smooth in this case.

If  $\text{char } k \nmid d$ ,  $C_P$  is smooth iff  $P$  has no multiple roots. The projective closure  $\bar{C}_P$  is now defined by

$$\frac{Y^d}{Z^d} = P\left(\frac{X}{Z}\right).$$

Look at the affine curve  $C' := C \cap \{[X : Y] \in \mathbb{P}^1 \mid X \neq 0\}$  again, and let  $n$  be the smallest integer s.t.  $dn \geq \deg P$ ,  $z := Z/X$ ,  $w := Z^{n-1}Y/X$ , then  $C'$  is the affine plane curve defined by

$$w^d = z^{dn}P\left(\frac{1}{z}\right).$$

This curve is smooth iff  $dn = \deg P$  or  $dn = \deg P + 1$ . Therefore,  $\bar{C}_P$  is smooth iff  $P$  has no multiple roots, and  $d$  divides  $\deg P$  or  $\deg P + 1$ .

## Exercise 2

1. A point  $[x, y, z] \in C$  is singular iff

$$\begin{cases} x^3 + y^3 + z^3 + dxyz = 0, \\ 3x^2 = -dyz, \\ 3y^2 = -dxz, \\ 3z^2 = -dxy. \end{cases} \quad (2)$$

Note that if one of  $x, y, z$  is zero, the other two are also zero. Hence  $xyz \neq 0$ . Multiply the last three equations and divide the result by  $(xyz)^2$ , we get  $d^3 = -27$ .

Conversely, suppose  $d^3 = -27$ , then  $d = -3\omega$  with  $\omega \in \mu_3 \subset \bar{k}$ . Note that  $[1 : \omega : \omega]$  is a singular point on  $C$ , so  $C$  is not smooth.

2. Since  $O = [1 : -1 : 0] \in C(k)$ , we can deduce that  $C$  is an elliptic curve once we know that the genus of  $C$  is  $g_C = 1$ .

Let

$$\pi : C \rightarrow \mathbb{P}^1, \quad [x : y : z] \mapsto [x : y].$$

This rational map is nonconstant and have degree 3.

Consider  $P = [x : 1 : z] \in C$  in the chart  $Y \neq 0$ . The corresponding affine curve  $C_0$  is

$$z^3 + dxz + x^3 + 1 = 0 \quad (3)$$

and the map is

$$\pi(x, z) = x$$

If  $\pi$  ramifies at  $P$ , then the equation, regarded as a polynomial in  $z$ , would have discriminant

$$-(4 \cdot (dx)^3 + 27 \cdot (x^3 + 1)^2) = 0. \quad (4)$$

So  $x^3$  is a solution to a quadratic equation with no multiple roots, and thus gives us 6 values of  $x$  s.t.  $P$  could possibly be a ramification point.

- If  $d \neq 0$ , then clearly  $e_\pi(P) \neq 3$ . Therefore,  $\pi$  has six ramification points of index 2 in  $C_0$ .

- If  $d = 0$ , then the solution to ?? are  $x = -\omega$  with  $\omega^3 = 1$ , and ?? becomes

$$z^3 = 1.$$

Hence,  $\pi$  has three ramification points  $[-\omega : 1 : 0]$  of degree 3.

On  $C \setminus C_0$ ,  $X^3 + Z^3 = 0$ , so

$$C \setminus C_0 = \{[1 : 0 : -1], [1 : 0 : -\omega], [1 : 0 : -\omega^2]\},$$

where  $\omega \in \mu_3$  and  $\omega \neq 1$ . Working on the chart  $X \neq 0$ , the corresponding affine curve is

$$z^3 + dyz + y^3 + 1$$

and the map is

$$\pi(y, z) = y.$$

So  $\pi$  does not ramify at the points in  $C \setminus C_0$ .

By Riemann-Hurwitz formula,

$$2g_C - 2 = 3 \cdot (-2) + 6 \cdot 1$$

when  $d \neq 0$ , or

$$2g_C - 2 = 3 \cdot (-2) + 3 \cdot 2$$

when  $d = 0$ . Therefore,  $g_C = 1$ .

### Exercise 3

The curve  $E$  is given by a Weierstrass equation with  $4 \cdot 1^3 + 27 \cdot 0 = 4 \neq 0$ , so  $E$  together with  $O := [0 : 1 : 0] \in E(\mathbb{F}_5)$  defines an elliptic curve over  $\mathbb{F}_5$ .

Suppose that  $[x : y : 1] \in E(\mathbb{F}_5)$ . Then  $x(x^2 + 1) = x^3 + x = y^2$  is a square in  $\mathbb{F}_5$ , which is 0, 1 or 4 = -1. Direct computation shows that

$$E(\mathbb{F}_5) = \{[0 : 0 : 1], [2 : 0 : 1], [-2 : 0 : 1], [0 : 1 : 0]\}.$$

### Exercise 4

1. A point  $(x, y) \in C_0$  is singular iff

$$\begin{cases} (1+x)^2(1+y)^2 = xy, \\ 2(1+x)(1+y)^2 = y, \\ 2(1+x)^2(1+y) = x. \end{cases} \quad (5)$$

If  $y = 0$ , then ?? has no solution.

If  $y \neq 0$ , then  $\text{char } k \neq 2$ , and divide the 1st equation by the 2nd tells us that  $x = 1$ . By symmetry or a similar argument, we know that if  $x \neq 0$  then  $y = 1$ . So singularity could only appear at  $(1, 1)$ , which indeed satisfies ?? only when  $\text{char } k = 3$  or  $\text{char } k = 5$ . Therefore,  $C_0$  is smooth iff  $\text{char } k \neq 3$  or 5.

2. The curve  $\bar{C}_0$  is defined by

$$(Z + X)^2(Z + Y)^2 = XYZ^2.$$

The point  $O := [1 : 0 : 0] \in \bar{C}_0$  is singular, because  $O$  lies in  $X = 1$ , while both  $\frac{\partial f}{\partial y}$  and  $\frac{\partial f}{\partial z}$  vanish at  $O$ , where  $y = Y/X$ ,  $z = Z/X$ , and  $f = (z + 1)^2(z + y)^2 + yz^2$ .

3. The curve  $C$  is defined by

$$(Z + X)^2(Z' + Y)^2 = XYZZ'. \quad (6)$$

The set  $C \setminus C_0$  consists of the points on  $C$  with  $Z = 0$  or  $Z' = 0$ .

Let  $Z = 0$  in ??, we get

$$X^2(Z' + Y)^2 = 0,$$

so  $X = 0$  or  $Z' + Y = 0$ . But  $(X : Z)$  is a homogeneous coordinate of  $\mathbb{P}^1$ , so  $X$  and  $Z$  cannot be zero simultaneously. Hence we have  $Z' + Y = 0$ , giving one point  $([1 : 0], [1 : -1])$ . The case of  $Z' = 0$  is similar, and the result is

$$C \setminus C_0 = \{O, O'\},$$

where

$$O := ([1 : 0], [1 : -1]), \quad O' := ([1, -1], [1, 0]).$$

4. Let  $C_0$  be smooth. It suffices to check that  $O$  and  $O'$  are smooth. These points lie in the chart  $X = Y = 1$ . Let  $z = Z/X$ ,  $z' = Z'/Y$ , then the defining equation becomes

$$(z + 1)^2(z' + 1)^2 = zz'. \quad (7)$$

The affine curve defined by this equation is isomorphic to  $C_0$ , so it is smooth. Therefore  $O$  and  $O'$  are smooth, and thus  $C$  is smooth.

5. Both  $O$  and  $O'$  are  $k$ -rational, so we just need to calculate the genus  $g_C$  of  $C$ . I assume  $\text{char } k \neq 2$  from now on, because I don't know how to deal with  $\text{char } k = 2$ ...

Let  $f : E \rightarrow \mathbb{P}^1$  be the composition of the embedding  $E \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1$  and the projection  $\mathbb{P}^1 \times \mathbb{P}^1 \rightarrow \mathbb{P}^1$  to the first factor; i.e.,

$$f([X : Z], [Y, Z']) = [X : Z].$$

This map is nonconstant of degree 2. A point  $(x, y) \in C_0$  is a ramification point for  $f$  iff  $y$  is a double root of the polynomial

$$(1 + x)^2(1 + Y)^2 - xY$$

in  $Y$ , i.e., the discriminant

$$(2(1 + x)^2 - x)^2 - 4(1 + x)^4 = -x(4x^2 + 7x + 4) = 0.$$

So  $f$  ramifies at three points in  $C_0$ . In particular,  $f$  ramifies at  $(x, y) = (0, -1)$  and does not ramify at  $(x, y) = (-1, 0)$ . Then by looking at ??, we deduce immediately that  $f$  ramifies at  $O$  and does not ramify at  $O'$ .

Now we can apply the Riemann-Hurwitz formula to  $f$ , and obtain

$$2g_C - 2 = 2 \cdot (2 \cdot 0 - 2) + 4 \cdot (2 - 1),$$

given  $\text{char } k \neq 2$ . Hence  $g_C = 1$ .

*Weierstrass equation.* The equation of  $C_0$  is

$$(1 + x)^2 y^2 + (2(1 + x)^2 - x)y + (1 + x)^2 = (1 + x)^2 y^2 + (2x^2 + 3x + 2)y + (1 + x)^2.$$

Under the birational transformation

$$\mathbb{A}^2 \dashrightarrow \mathbb{A}^2, \quad (x, y) \mapsto (x, 2(1 + x)^2 y + 2x^2 + 3x + 2),$$

the equation becomes

$$y^2 - (2x^2 + 3x + 2)^2 + 4(1 + x)^4 = 0,$$

which reduces to

$$y^2 = -4x^3 - 7x^2 - 4x.$$