

# Elliptic Curves

Lectured by Prof Tom Fisher  
Typed by David Kurniadi Angdinata

Michaelmas 2020

**Syllabus**

# Contents

<b>1</b>	<b>Fermat's method of infinite descent</b>	<b>3</b>
1.1	Primitive triangles . . . . .	3
1.2	A variant for polynomials . . . . .	4
<b>2</b>	<b>Some remarks on algebraic curves</b>	<b>5</b>
2.1	Rational curves . . . . .	5
2.2	Order of vanishing . . . . .	5
2.3	Riemann Roch spaces . . . . .	6
2.4	The degree of a morphism . . . . .	7
<b>3</b>	<b>Weierstrass equations</b>	<b>8</b>
3.1	The Weierstrass form . . . . .	8
3.2	Discriminant and $j$ -invariant . . . . .	9
<b>4</b>	<b>Group law</b>	<b>10</b>
4.1	The Picard group law . . . . .	10
4.2	Explicit formulae for the group law . . . . .	11
4.3	Maps on an elliptic curve . . . . .	12
4.4	Elliptic curves over $\mathbb{C}$ . . . . .	12
4.5	Group structure over other fields . . . . .	13
<b>5</b>	<b>Isogenies</b>	<b>14</b>
5.1	Isogenies . . . . .	14
5.2	The degree quadratic form . . . . .	15
<b>6</b>	<b>The invariant differential</b>	<b>18</b>
6.1	Differentials . . . . .	18
6.2	Regular differentials . . . . .	18
6.3	The invariant differential . . . . .	19
6.4	Separability criterion . . . . .	20
<b>7</b>	<b>Elliptic curves over finite fields</b>	<b>21</b>
7.1	Hasse's theorem . . . . .	21
7.2	Zeta functions . . . . .	21
<b>8</b>	<b>Formal groups</b>	<b>23</b>
8.1	Complete rings . . . . .	23
8.2	Expansion near the identity . . . . .	23

# 1 Fermat's method of infinite descent

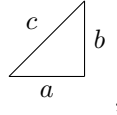
Lecture 1  
Friday  
09/10/20

The following are the books.

- J H Silverman, The arithmetic of elliptic curves, 1986
- J W S Cassels, Lectures on elliptic curves, 1991
- J H Silverman and J Tate, Rational points on elliptic curves, 1992
- J S Milne, Elliptic curves, 2006

## 1.1 Primitive triangles

**Definition.** Let  $\Delta = \Delta(a, b, c)$  be a right triangle



so  $a^2 + b^2 = c^2$  and the area of  $\Delta$  is  $\frac{1}{2}ab$ . Then  $\Delta$  is **rational** if  $a, b, c \in \mathbb{Q}$ , and  $\Delta$  is **primitive** if  $a, b, c \in \mathbb{Z}$  are coprime.

**Lemma 1.1.** Every primitive triangle is of the form  $\Delta(u^2 - v^2, 2uv, u^2 + v^2)$  for some  $u, v \in \mathbb{Z}$  such that  $u > v > 0$ .

*Proof.* Without loss of generality  $a$  is odd,  $b$  is even, and  $c$  is odd, so  $(b/2)^2 = ((c+a)/2)((c-a)/2)$  is a product of coprime positive integers. By unique prime factorisation in  $\mathbb{Z}$ ,

$$\frac{c+a}{2} = u^2, \quad \frac{c-a}{2} = v^2, \quad u, v \in \mathbb{Z},$$

so  $a = u^2 - v^2$ ,  $b = 2uv$ , and  $c = u^2 + v^2$ . □

**Definition.**  $D \in \mathbb{Q}_{>0}$  is a **congruent number** if there exists a rational triangle  $\Delta$  with area  $D$ .

Note that it suffices to consider  $D \in \mathbb{Z}_{>0}$  squarefree.

**Example.**  $D = 5, 6$  are congruent numbers.

**Lemma 1.2.**  $D \in \mathbb{Q}_{>0}$  is congruent if and only if  $Dy^2 = x^3 - x$  for some  $x, y \in \mathbb{Q}$  such that  $y \neq 0$ .

*Proof.* Lemma 1.1 shows  $D$  is congruent if and only if  $Dw^2 = uv(u^2 - v^2)$  for some  $u, v, w \in \mathbb{Q}$  such that  $w \neq 0$ . Put  $x = u/v$  and  $y = w/v^2$ . □

Fermat showed that 1 is not a congruent number.

**Theorem 1.3.** There is no solution to

$$w^2 = uv(u+v)(u-v), \quad u, v, w \in \mathbb{Z}, \quad w \neq 0. \quad (1)$$

*Proof.* Without loss of generality  $u$  and  $v$  are coprime, and  $u > 0$  and  $w > 0$ . If  $v < 0$  then replace  $(u, v, w)$  by  $(-v, u, w)$ . If  $u \equiv v \pmod{2}$  then replace  $(u, v, w)$  by  $((u+v)/2, (u-v)/2, w/2)$ . Then  $u, v, u+v, u-v$  are pairwise coprime positive integers whose product is a square. By unique factorisation in  $\mathbb{Z}$ ,

$$u = a^2, \quad v = b^2, \quad u+v = c^2, \quad u-v = d^2, \quad a, b, c, d \in \mathbb{Z}_{>0}.$$

Since  $u \not\equiv v \pmod{2}$  both  $c$  and  $d$  are odd. Then  $((c+d)/2)^2 + ((c-d)/2)^2 = (c^2 + d^2)/2 = u = a^2$ , so  $\Delta((c+d)/2, (c-d)/2, a)$  is a primitive triangle. Its area is  $(c^2 - d^2)/8 = v/4 = (b/2)^2$ . Let  $w_1 = b/2$ . By Lemma 1.1,  $w_1^2 = u_1v_1(u_1^2 - v_1^2)$  for some  $u_1, v_1 \in \mathbb{Z}$ , that is we have a new solution to (1). But  $4w_1^2 = b^2 = v \mid w^2$ , so  $w_1 \leq w/2$ . So by Fermat's method of infinite descent, there is no solution to (1). □

## 1.2 A variant for polynomials

In this section,  $K$  is a field with  $\text{ch } K \neq 2$ , with algebraic closure  $\overline{K}$ .

**Lemma 1.4.** *Let  $u, v \in K[t]$  be coprime. If  $\alpha u + \beta v$  is a square for four distinct  $(\alpha : \beta) \in \mathbb{P}^1$  then  $u, v \in K$ .*

*Proof.* Without loss of generality  $K = \overline{K}$ . Changing coordinates on  $\mathbb{P}^1$  we may assume the ratios  $(\alpha : \beta)$  are  $(1 : 0), (0 : 1), (1 : -1), (1 : -\lambda)$  for some  $\lambda \in K \setminus \{0, 1\}$ . Then  $u = a^2$  and  $v = b^2$  for some  $a, b \in K[t]$ , so  $u - v = (a + b)(a - b)$  and  $u - \lambda v = (a + \mu b)(a - \mu b)$  for  $\mu = \sqrt{\lambda}$ . By unique factorisation in  $K[t]$ ,  $a + b, a - b, a + \mu b, a - \mu b$  are squares. But  $\max(\deg a, \deg b) \leq \frac{1}{2} \max(\deg u, \deg v)$ . So by Fermat's method of infinite descent  $u, v \in K$ .  $\square$

**Definition 1.5.**

- An **elliptic curve**  $E/K$  is the projective closure of the plane affine curve  $y^2 = f(x)$  where  $f \in K[x]$  is a monic cubic polynomial with distinct roots in  $\overline{K}$ .
- For  $L/K$  any field extension

$$E(L) = \{(x, y) \in L^2 \mid y^2 = f(x)\} \cup \{\mathcal{O}\},$$

where  $\mathcal{O}$  is the **point at infinity**.

**Fact.**  $E(L)$  is naturally an abelian group.

In this course we study  $E(L)$  for  $L$  a finite field, a local field  $[L : \mathbb{Q}_p] < \infty$ , or a number field  $[L : \mathbb{Q}] < \infty$ . By Lemma 1.2 and Theorem 1.3, if  $E$  is  $y^2 = x^3 - x$  then  $E(\mathbb{Q}) = \{\mathcal{O}, (0, 0), (\pm 1, 0)\}$ .

**Corollary 1.6.** *Let  $E/K$  be an elliptic curve. Then  $E(K(t)) = E(K)$ .*

*Proof.* Without loss of generality  $K = \overline{K}$ . By a change of coordinates we may assume  $E$  is

$$y^2 = x(x - 1)(x - \lambda), \quad \lambda \in K \setminus \{0, 1\}.$$

Suppose  $(x, y) \in E(K(t))$ . Write  $x = u/v$  for  $u, v \in K[t]$  coprime. Then  $w^2 = uv(u - v)(u - \lambda v)$  for some  $w \in K[t]$ . By unique factorisation in  $K[t]$ ,  $u, v, u - v, u - \lambda v$  are all squares. By Lemma 1.4,  $u, v \in K$ , so  $x, y \in K$ .  $\square$

## 2 Some remarks on algebraic curves

Work over  $K = \overline{K}$ .

### 2.1 Rational curves

**Definition 2.1.** A plane algebraic curve  $C = \{f(x, y) = 0\} \subset \mathbb{A}^2$  for an irreducible polynomial  $f$  is **rational** if it has a rational parameterisation, that is there exists  $\phi, \psi \in K(t)$  such that

$$\begin{aligned} \mathbb{A}^1 &\longrightarrow \mathbb{A}^2 \\ t &\longmapsto (\phi(t), \psi(t)) \end{aligned}$$

is injective on  $\mathbb{A}^1$  minus a finite set, and  $f(\phi(t), \psi(t)) = 0$ .

**Example 2.2.**

- Any nonsingular plane conic is rational. For example, let  $x^2 + y^2 = 1$ . The line of slope  $t$  at  $(-1, 0)$  is  $y = t(x + 1)$ . Their intersection is  $x^2 + t^2(x + 1)^2 = 1$ , so  $(x + 1)(x - 1 + t^2(x + 1)) = 0$ . Thus  $x = -1$  or  $x = (1 - t^2) / (1 + t^2)$ . The rational parameterisation is

$$(x, y) = \left( \frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

- Any singular plane cubic is rational. For example, let  $y^2 = x^3$ . The line of slope  $t$  at  $(0, 0)$  is  $y = tx$ . The rational parameterisation is

$$(x, y) = (t^2, t^3).$$

- Corollary 1.6 shows that elliptic curves are not rational.

**Remark 2.3.** The genus  $g(C) \in \mathbb{Z}_{\geq 0}$  is an invariant of a smooth projective curve  $C$ .

- If  $K = \mathbb{C}$  then  $g(C)$  is the genus of a Riemann surface.
- A smooth plane curve  $C \subset \mathbb{P}^2$  of degree  $d$  has genus  $g(C) = (d - 1)(d - 2) / 2$ .

**Proposition 2.4.** *Still assuming  $K = \overline{K}$ , let  $C$  be a smooth projective curve.*

- $C$  is rational as in Definition 2.1 if and only if  $g(C) = 0$ .
- $C$  is an elliptic curve as in Definition 1.5 if and only if  $g(C) = 1$ .

*Proof.*

- Omitted.
- For  $\implies$ , use Remark 2.3. For  $\impliedby$ , see later Theorem 3.1.

□

### 2.2 Order of vanishing

Let  $C$  be an algebraic curve, with function field  $K(C)$ . Let  $P \in C$  be a smooth point. Write  $\text{ord}_P f$  for the order of vanishing of  $f \in K(C)$  at  $P$ , which is negative if  $f$  has a pole.

**Fact.**  $\text{ord}_P : K(C)^* \rightarrow \mathbb{Z}$  is a discrete valuation, that is

$$\text{ord}_P(f_1 f_2) = \text{ord}_P f_1 + \text{ord}_P f_2, \quad \text{ord}_P(f_1 + f_2) = \min(\text{ord}_P f_1, \text{ord}_P f_2).$$

**Definition.**  $t \in K(C)^*$  is a **uniformiser** at the point  $P$  if  $\text{ord}_P t = 1$ .

**Example 2.5.** Let  $C = \{g = 0\} \subset \mathbb{A}^2$  for  $g \in K[x, y]$  irreducible, so  $K(C) = \text{Frac}(K[x, y] / \langle g \rangle)$  for  $g = g_0 + g_1(x, y) + \dots$  where  $g_i$  is homogeneous of degree  $i$ . Suppose  $P = (0, 0) \in C$  is a smooth point, that is  $g_0 = 0$  and  $g_1(x, y) = \alpha x + \beta y$  such that  $\alpha$  and  $\beta$  are not both zero. Let  $\gamma, \delta \in K$ . A fact is that

$$\gamma x + \delta y \in K(C) \text{ is a uniformiser at } p \iff \alpha\delta - \beta\gamma \neq 0.$$

**Example 2.6.** The projective closure of  $\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2$  for  $\lambda \neq 0, 1$  is

$$\{Y^2 Z = X(X-Z)(X-\lambda Z)\} \subset \mathbb{P}^2,$$

where  $x = X/Z$  and  $y = Y/Z$ . Let  $P = (0 : 1 : 0)$ . We compute  $\text{ord}_P x$  and  $\text{ord}_P y$ . Put  $t = X/Y$  and  $w = Z/Y$ . Then

$$w = t(t-w)(t-\lambda w). \quad (2)$$

Now  $P$  is the point  $(t, w) = (0, 0)$ . This is a smooth point and  $\text{ord}_P t = \text{ord}_P(t-w) = \text{ord}_P(t-\lambda w) = 1$ . By (2),  $\text{ord}_P w = 3$ , so

$$\text{ord}_P x = \text{ord}_P \frac{X}{Z} = \text{ord}_P \frac{t}{w} = 1 - 3 = -2, \quad \text{ord}_P y = \text{ord}_P \frac{Y}{Z} = \text{ord}_P \frac{1}{w} = -3.$$

Remark that the line  $\{w = 0\}$  meets  $E$  with multiplicity three at  $P$ , so  $P$  is a point of inflection.

### 2.3 Riemann Roch spaces

**Definition.** Let  $C$  be a smooth projective curve. A **divisor** is a formal sum of points on  $C$ , say

$$D = \sum_{P \in C} n_P(P), \quad n_P \in \mathbb{Z},$$

with  $n_P = 0$  for all but finitely many  $P \in C$ . The **degree** of  $D$  is

$$\deg D = \sum_{P \in C} n_P.$$

Then  $D$  is **effective**, written  $D \geq 0$ , if  $n_P \geq 0$  for all  $P \in C$ . If  $f \in K(C)^*$  then the **divisor of  $f$**  is

$$\text{div } f = \sum_{P \in C} (\text{ord}_P f)(P).$$

The **Riemann Roch space** of  $D \in \text{Div } C$  is

$$\mathcal{L}(D) = \{f \in K(C)^* \mid \text{div } f + D \geq 0\} \cup \{0\},$$

that is the  $K$ -vector space of rational functions on  $C$  with poles no worse than specified by  $D$ .

**Riemann Roch for genus one** states that

$$\dim \mathcal{L}(D) = \begin{cases} 0 & \deg D < 0 \\ 0 \text{ or } 1 & \deg D = 0 \\ \deg D & \deg D > 0 \end{cases}.$$

**Example.** Revisiting Example 2.6, let  $P$  be the point at infinity of  $\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2$ . Then  $\text{ord}_P x = -2$  and  $\text{ord}_P y = -3$ . We deduce

$$\mathcal{L}(2(P)) = \langle 1, x \rangle, \quad \mathcal{L}(3(P)) = \langle 1, x, y \rangle.$$

This motivates the proof of Theorem 3.1.

Assume  $K = \overline{K}$  and  $\text{ch } K \neq 2$ .

**Proposition 2.7.** *Let  $C \subset \mathbb{P}^2$  be a smooth plane cubic and  $P \in C$  a point of inflection. Then we may change coordinates such that  $C$  is*

$$Y^2 = X(X - Z)(X - \lambda Z), \quad \lambda \neq 0, 1,$$

and  $P = (0 : 1 : 0)$ .

*Proof.* We change coordinates such that  $P = (0 : 1 : 0)$  and  $T_P C = \{Z = 0\}$ . Let  $C = \{F(X, Y, Z) = 0\}$ . Since  $P \in C$  is a point of inflection,  $F(t, 1, 0)$  is a constant times  $t^3$ , that is no terms  $X^2Y, XY^2, Y^3$ , so

$$F \in \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \rangle.$$

The coefficient of  $Y^2Z$  is nonzero otherwise  $P \in C$  is singular. The coefficient of  $X^3$  is nonzero otherwise  $\{Z = 0\} \subset C$ . We are free to rescale  $X, Y, Z, F$ . Without loss of generality  $C$  is defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

the **Weierstrass form**. Substituting  $Y$  by  $Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$  we may assume  $a_1 = a_3 = 0$ . Now  $C$  is  $Y^2Z = Z^3f(X/Z)$  for  $f$  a monic cubic polynomial. Since  $C$  is smooth,  $f$  has distinct roots, without loss of generality  $0, 1, \lambda$ . Thus  $C$  is

$$Y^2 = X(X - Z)(X - \lambda Z),$$

the **Legendre form**. □

**Remark.** It may be shown that the points of inflection on  $C = \{F = 0\} \subset \mathbb{P}^2$  in coordinates  $(X_1 : X_2 : X_3)$  are given by  $F = \det H = 0$ , where  $H = \left( \frac{\partial^2 F}{\partial X_i \partial X_j} \right)$  is a  $3 \times 3$  matrix.

## 2.4 The degree of a morphism

**Definition.** Let  $\phi : C_1 \rightarrow C_2$  be a nonconstant morphism of smooth projective curves. Let

$$\begin{array}{ccc} \phi^* & : & K(C_2) \longrightarrow K(C_1) \\ f & \longmapsto & f \circ \phi \end{array}.$$

- The **degree** of  $\phi$  is

$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$

- $\phi$  is **separable** if  $K(C_1) / \phi^* K(C_2)$  is a separable field extension, which is automatic if  $\text{ch } K = 0$ .
- Suppose  $P \in C_1$  and  $Q \in C_2$  such that  $\phi : P \mapsto Q$ . Let  $t \in K(C_2)$  be a uniformiser at  $Q$ . The **ramification index** of  $\phi$  at  $P$  is

$$e_\phi(P) = \text{ord}_P \phi^* t,$$

which is always at least one, and independent of  $t$ .

**Theorem 2.8.** *Let  $\phi : C_1 \rightarrow C_2$  be a nonconstant morphism of smooth projective curves. Then*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi, \quad Q \in C_2.$$

Moreover if  $\phi$  is separable then  $e_\phi(P) = 1$  for all but finitely many  $P \in C_1$ . In particular

- $\phi$  is **surjective**, noting that  $K = \overline{K}$ , and
- $\#\phi^{-1}(Q) \leq \deg \phi$ , with equality for all but finitely many  $Q$ , assuming  $\phi$  is separable.

**Remark 2.9.** Let  $C$  be an algebraic curve. A rational map is given by

$$\begin{array}{ccc} \phi & : & C \dashrightarrow \mathbb{P}^n \\ P & \longmapsto & (f_0(P) : \cdots : f_n(P)) \end{array},$$

where  $f_0, \dots, f_n \in K(C)$  not all zero. A fact is if  $C$  is smooth then  $\phi$  is a morphism.

### 3 Weierstrass equations

In this section  $K$  is a perfect field, with algebraic closure  $\overline{K}$ .

**Definition.** An **elliptic curve**  $E$  over  $K$  is a smooth projective curve of genus one defined over  $K$  with a specified  $K$ -rational point  $\mathcal{O}_E$ .

**Example.**  $\{X^3 + pY^3 + p^2Z^3 = 0\} \subset \mathbb{P}^2$  for  $p$  prime is not an elliptic curve over  $\mathbb{Q}$ , since it has no  $\mathbb{Q}$ -points.

#### 3.1 The Weierstrass form

**Theorem 3.1.** Every elliptic curve  $E$  is isomorphic over  $K$  to a curve in Weierstrass form, via an isomorphism taking  $\mathcal{O}_E$  to  $(0 : 1 : 0)$ .

**Remark.** Proposition 2.7 treated the special case where  $E$  is a smooth plane cubic and  $\mathcal{O}_E$  is a point of inflection.

**Fact.** If  $D \in \text{Div } E$  is defined over  $K$ , that is fixed by  $\text{Gal}(\overline{K}/K)$ , then  $\mathcal{L}(D)$  has a basis in  $K(E)$ , not just in  $\overline{K}(E)$ .

*Proof.* Pick bases  $\langle 1, x \rangle = \mathcal{L}(2(\mathcal{O}_E)) \subset \mathcal{L}(3(\mathcal{O}_E)) = \langle 1, x, y \rangle$ . Then  $\text{ord}_{\mathcal{O}_E} x = -2$  and  $\text{ord}_{\mathcal{O}_E} y = -3$ . The seven elements  $1, x, y, x^2, xy, x^3, y^2$  in the six-dimensional vector space  $\mathcal{L}(6(\mathcal{O}_E))$  must satisfy a dependence relation. Leaving out  $x^3$  or  $y^2$  gives a basis for  $\mathcal{L}(6(\mathcal{O}_E))$  since each term has a different order pole at  $\mathcal{O}_E$ , so the coefficients of  $x^3$  and  $y^2$  are nonzero. Rescaling  $x$  and  $y$  we get

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K.$$

Let  $E'$  be the curve defined by this equation, or rather its projective closure. There is a morphism

$$\begin{aligned} \phi : E &\longrightarrow E' \subset \mathbb{P}^2 \\ P &\longmapsto (x(P) : y(P) : 1) = \left( \frac{x}{y}(P) : 1 : \frac{1}{y}(P) \right) \\ \mathcal{O}_E &\longmapsto (0 : 1 : 0) \end{aligned}$$

Then

$$[K(E) : K(x)] = \deg(x : E \rightarrow \mathbb{P}^1) = \text{ord}_{\mathcal{O}_E} \frac{1}{x} = 2, \quad [K(E) : K(y)] = \deg(y : E \rightarrow \mathbb{P}^1) = \text{ord}_{\mathcal{O}_E} \frac{1}{y} = 3,$$

so

$$\begin{array}{ccc} & K(E) & \\ & | & \\ 2 & K(x, y) & 3 \\ & | & \\ K(x) & & K(y) \end{array} .$$

By the tower law,  $[K(E) : K(x, y)] = 1$ , so  $\deg(\phi : E \rightarrow E') = 1$ , so  $\phi$  is birational. If  $E'$  is singular then  $E$  and  $E'$  are rational, a contradiction. So  $E'$  is smooth and we may apply Remark 2.9 to  $\phi^{-1}$  to see that  $\phi^{-1}$  is a morphism, so  $\phi$  is an isomorphism.  $\square$

**Proposition 3.2.** Let  $E$  and  $E'$  be elliptic curves over  $K$  in Weierstrass form. Then  $E \cong E'$  over  $K$  if and only if the Weierstrass equations are related by a change of variables

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t, \quad u, r, s, t \in K, \quad u \neq 0.$$

*Proof.* Let  $\langle 1, x \rangle = \mathcal{L}(2(\mathcal{O}_E)) = \langle 1, x' \rangle$  and  $\langle 1, x, y \rangle = \mathcal{L}(3(\mathcal{O}_E)) = \langle 1, x', y' \rangle$ . Then

$$x = \lambda x' + r, \quad y = \mu y' + \sigma x' + t, \quad \lambda, r, \mu, \sigma, t \in K, \quad \lambda, \mu \neq 0.$$

Looking at coefficients of  $x^3$  and  $y^2$ ,  $\lambda^3 = \mu^2$ , so  $(\lambda, \mu) = (u^2, u^3)$  for some  $u \in K^*$ . Put  $s = \sigma/u^2$ .  $\square$

Lecture 4  
Friday  
16/10/20



### 3.2 Discriminant and j-invariant

A Weierstrass equation defines an elliptic curve if and only if it defines a smooth curve, if and only if  $\Delta(a_1, \dots, a_6) \neq 0$  where  $\Delta \in \mathbb{Z}[a_1, \dots, a_6]$  is a certain polynomial. If  $\text{ch } K \neq 2, 3$  then we can reduce to the case  $E$  is

$$y^2 = x^3 + ax + b,$$

with **discriminant**

$$\Delta = -16(4a^3 + 27b^2).$$

**Corollary 3.3.** *Assume  $\text{ch } K \neq 2, 3$ . Elliptic curves  $E = \{y^2 = x^3 + ax + b\}$  and  $E' = \{y^2 = x^3 + a'x + b'\}$  are isomorphic over  $K$  if and only if  $a' = u^4a$  and  $b' = u^6b$  for some  $u \in K^*$ .*

*Proof.*  $E$  and  $E'$  are related as in Proposition 3.2 with  $r = s = t = 0$ . □

**Definition.** The **j-invariant** is

$$j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

**Corollary 3.4.** *If  $E \cong E'$ , then  $j(E) = j(E')$ , and the converse holds if  $K = \overline{K}$ .*

*Proof.*

$$E \cong E' \iff \exists u \in K^*, \begin{cases} a' = u^4a \\ b' = u^6b \end{cases} \implies (a^3 : b^2) = (a'^3 : b'^2) \iff j(E) = j(E'),$$

and the converse holds if  $K = \overline{K}$ . □

## 4 Group law

Let  $E = E(\overline{K}) \subset \mathbb{P}^2$  be a smooth plane cubic, and let  $\mathcal{O}_E \in E(K)$ . Then  $E$  meets each line in three points counted with multiplicity.

### 4.1 The Picard group law

Let  $P, Q \in E$ , let  $S$  be the third point of intersection of  $PQ$  and  $E$ , and let  $R$  be the third point of intersection of  $\mathcal{O}_E S$  and  $E$ . We define

$$P \oplus Q = R.$$

If  $P = Q$  then take  $T_P E$  instead, etc. This is the **chord and tangent process**.

**Theorem 4.1.**  $(E, \oplus)$  is an abelian group.

Associativity is hard.

**Definition.**  $D_1, D_2 \in \text{Div } E$  are **linearly equivalent**, written  $D_1 \sim D_2$ , if there exists  $f \in \overline{K}(E)^*$  such that

$$\text{div } f = D_1 - D_2.$$

Let

$$[D] = \{D' \mid D' \sim D\}.$$

The **Picard group** is

$$\text{Pic } E = \text{Div } E / \sim.$$

If

$$\text{Div}^0 E = \ker(\deg : \text{Div } E \rightarrow \mathbb{Z})$$

is the degree zero divisors on  $E$ , let

$$\text{Pic}^0 E = \text{Div}^0 E / \sim.$$

Note that  $\text{div } fg = \text{div } f + \text{div } g$ .

**Proposition 4.2.** Let

$$\begin{aligned} \psi &: E \longrightarrow \text{Pic}^0 E \\ P &\longmapsto [(P) - (\mathcal{O}_E)] \end{aligned}$$

Then

1.  $\psi(P \oplus Q) = \psi(P) + \psi(Q)$ , and
2.  $\psi$  is a bijection.

*Proof.*

1. Let  $P, Q \in E$ , let  $S$  be the third point of intersection of  $PQ$  and  $E$ , and let  $R$  be the third point of intersection of  $\mathcal{O}_E S$  and  $E$ . Let  $l = 0$  be the line  $PQ$  and let  $m = 0$  be the line  $\mathcal{O}_E S$ . Then

$$\text{div } \frac{l}{m} = (P) + (S) + (Q) - (R) - (S) - (\mathcal{O}_E) = (P) + (Q) - (\mathcal{O}_E) - (P \oplus Q),$$

so  $(P \oplus Q) + (\mathcal{O}_E) \sim (P) + (Q)$ . Thus  $(P \oplus Q) - (\mathcal{O}_E) \sim (P) - (\mathcal{O}_E) + (Q) - (\mathcal{O}_E)$ , so  $\psi(P \oplus Q) = \psi(P) + \psi(Q)$ .

2. For injectivity, suppose  $\psi(P) = \psi(Q)$  for  $P \neq Q$ . Then there exists  $f \in \overline{K}(E)^*$  such that  $\text{div } f = P - Q$ , and  $\deg(f : E \rightarrow \mathbb{P}^1) = \text{ord}_P f = 1$ , so  $E \cong \mathbb{P}^1$ , a contradiction. For surjectivity, let  $[D] \in \text{Pic}^0 E$ . Then  $D + (\mathcal{O}_E)$  has degree one. By Riemann Roch,  $\dim \mathcal{L}(D + (\mathcal{O}_E)) = 1$ , so there exists  $f \in \overline{K}(E)^*$  such that  $\text{div } f + D + (\mathcal{O}_E) \geq 0$ . Since  $\text{div } f + D + (\mathcal{O}_E)$  has degree one,  $\text{div } f + D + (\mathcal{O}_E) = (P)$  for some  $P \in E$ , so  $(P) - (\mathcal{O}_E) \sim D$ . Thus  $\psi(P) = [D]$ .

□

*Proof of Theorem 4.1.*

- $P \oplus Q = Q \oplus P$  is clear.
- $\mathcal{O}_E$  is the identity. Let  $S$  be the third point of intersection of  $\mathcal{O}_E P$  and  $E$ . Then  $P$  is the third point of intersection of  $\mathcal{O}_E S$  and  $E$ , so  $\mathcal{O}_E \oplus P = P$ .
- Inverses. Let  $S$  be the third point of intersection of  $T_{\mathcal{O}_E} E$  and  $E$ , and let  $Q$  be the third point of intersection of  $PS$  and  $E$ . Then  $S$  is the third point of intersection of  $PQ$  and  $E$ , and  $\mathcal{O}_E$  is the third point of intersection of  $\mathcal{O}_E S$  and  $E$ , so  $P \oplus Q = \mathcal{O}_E$ .
- By Proposition 4.2,

$$\psi((P \oplus Q) \oplus R) = \psi(P \oplus Q) + \psi(R) = \psi(P) + \psi(Q) + \psi(R) = \psi(P) + \psi(Q \oplus R) = \psi(P \oplus (Q \oplus R)).$$

Since  $\psi$  is injective,  $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ . We deduce that  $\oplus$  is associative, and

$$\psi : (E, \oplus) \xrightarrow{\sim} (\text{Pic}^0 E, +)$$

is an isomorphism of groups. Note that we did not need  $\psi$  surjective for the proof that  $\oplus$  is associative.  $\square$

## 4.2 Explicit formulae for the group law

We consider  $E$  in Weierstrass form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad (3)$$

and  $\mathcal{O}_E$  is the point at infinity.

**Remark.**  $\mathcal{O}_E$  is a point of inflection. So now  $P_1 \oplus P_2 \oplus P_3 = \mathcal{O}_E$  if and only if  $P_1, P_2, P_3$  are collinear.

Let  $P_1 = (x_1, y_1)$  and  $P_2 = (x_2, y_2)$ , let  $P' = (x', y')$  be the third point of intersection of  $P_1 P_2 = \{y = \lambda x + \nu\}$  and  $E$ , and let  $P_3 = (x_3, y_3)$  be the second point of intersection between  $x = x'$  and  $E$ , so  $P_3 = P_1 \oplus P_2 = \ominus P'$ . Thus

$$\ominus P_1 = (x_1, -(a_1 x_1 + a_3) - y_1).$$

Substituting  $y = \lambda x + \nu$  into (3) and looking at the coefficient of  $x^2$  gives  $\lambda^2 + a_1 \lambda - a_2 = x_1 + x_2 + x'$ , so

$$x_3 = \lambda^2 + a_1 \lambda - a_2 - x_1 - x_2, \quad y_3 = -(a_1 x' + a_3) - y' = -(a_1 x' + a_3) - (\lambda x' + \nu) = -(\lambda + a_1) x_3 - \nu - a_3.$$

It remains to find formulae for  $\lambda$  and  $\nu$ .

Case 1.  $x_1 = x_2$  and  $P_1 \neq P_2$ . Then  $P_1 \oplus P_2 = \mathcal{O}_E$ .

Case 2.  $x_1 \neq x_2$ . Then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = y_1 - \lambda x_1 = \frac{y_1(x_2 - x_1) - (y_2 - y_1)x_1}{x_2 - x_1} = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

Case 3.  $x_1 = x_2$  and  $P_1 = P_2$ . Then

$$\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3}.$$

**Corollary 4.3.**  $E(K)$  is an abelian group.

*Proof.* It is a subgroup of  $E = E(\overline{K})$ .

- Identity is  $\mathcal{O}_E \in E(K)$  by definition.
- Closure and inverses are by the formulae above.
- Associativity and commutativity are inherited.

$\square$

### 4.3 Maps on an elliptic curve

**Theorem 4.4.** *Elliptic curves are group varieties. That is,*

$$\begin{aligned} [-1] : E &\longrightarrow E & + : E \times E &\longrightarrow E \\ P &\longmapsto -P, & (P, Q) &\longmapsto P + Q \end{aligned}$$

are morphisms of algebraic varieties.

*Proof.* The above formulae show  $[-1]$  and  $+$  are rational maps. By Remark 2.9,  $[-1] : E \rightarrow E$  is a morphism. The formulae also show, by case 2, that  $+$  is regular on

$$U = \{(P, Q) \in E \times E \mid P, Q, P + Q, P - Q \neq \mathcal{O}_E\}.$$

For  $P \in E$  let translation by  $P$  be

$$\begin{aligned} \tau_P : E &\longrightarrow E \\ X &\longmapsto P + X, \end{aligned}$$

which is a rational map and therefore a morphism. Let  $A, B \in E$ . We factor  $+$  as

$$E \times E \xrightarrow{\tau_{-A} \times \tau_{-B}} E \times E \xrightarrow{+} E \xrightarrow{\tau_{A+B}} E.$$

Thus  $+$  is regular on  $(\tau_A \times \tau_B)(U)$  for all  $A, B \in E$ , so  $+$  is regular on  $E \times E$ .  $\square$

**Definition.** For  $n \in \mathbb{Z}$  let

$$\begin{aligned} [n] : E &\longrightarrow E \\ P &\longmapsto \underbrace{P + \cdots + P}_n, \end{aligned}$$

and  $[-n] = [-1] \circ [n]$ . The  $n$ -torsion subgroup of  $E$  is

$$E[n] = \ker([n] : E \rightarrow E).$$

**Lemma 4.5.** *Assume  $\text{ch } K \neq 2$ . Let  $E$  be*

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

for  $e_1, e_2, e_3 \in \overline{K}$  distinct. Then

$$E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

*Proof.* Let  $P = (x, y) \in E$ . Then  $[2]P = 0$  if and only if  $P = -P$ , if and only if  $(x, y) = (x, -y)$ , if and only if  $y = 0$ .  $\square$

### 4.4 Elliptic curves over $\mathbb{C}$

Let  $\Lambda = \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}$  for  $\omega_1$  and  $\omega_2$  a basis for  $\mathbb{C}$  as an  $\mathbb{R}$ -vector space. Then

$$\left\{ \begin{array}{c} \text{meromorphic functions on} \\ \text{Riemann surface } \mathbb{C}/\Lambda \end{array} \right\} \rightsquigarrow \left\{ \begin{array}{c} \Lambda\text{-invariant meromorphic} \\ \text{functions on } \mathbb{C} \end{array} \right\}.$$

This field is generated by  $\wp(z)$  and  $\wp'(z)$  where

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

They satisfy

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

for some  $g_2, g_3 \in \mathbb{C}$  depending on  $\Lambda$ . One shows that

$$\mathbb{C}/\Lambda \cong E(\mathbb{C})$$

is an isomorphism as Riemann surfaces and as groups, where  $E$  is the elliptic curve

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

**Theorem 4.6** (Uniformisation theorem). *Every elliptic curve over  $\mathbb{C}$  arises in this way.*

For elliptic curves  $E/\mathbb{C}$  we have

1.  $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ , and
2.  $\deg[n] = n^2$ .

We show 2 holds over any field  $K$  and 1 holds if  $\text{ch } K \nmid n$ .

## 4.5 Group structure over other fields

The following will be a summary of the results.

1. If  $K = \mathbb{C}$ , then

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}.$$

2. If  $K = \mathbb{R}$ , then

$$E(\mathbb{R}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \Delta > 0 \\ \mathbb{R}/\mathbb{Z} & \Delta < 0 \end{cases}.$$

3. If  $K = \mathbb{F}_q$ , then Hasse's theorem states that

$$|\#E(\mathbb{F}_q) - (q + 1)| \leq 2\sqrt{q}.$$

4. If  $[K : \mathbb{Q}_p] < \infty$  with ring of integers  $\mathcal{O}_K$ , then  $E(K)$  has a subgroup of finite index isomorphic to  $(\mathcal{O}_K, +)$ .
5. If  $[K : \mathbb{Q}] < \infty$ , then the Mordell-Weil theorem states that  $E(K)$  is a finitely generated abelian group.

Note that the isomorphisms in 1, 2, and 4 respect the relevant topologies.

## 5 Isogenies

Lecture 6  
Wednesday  
21/10/20

**Definition.** Let  $E_1$  and  $E_2$  be elliptic curves.

- An **isogeny**  $\phi : E_1 \rightarrow E_2$  is a nonconstant morphism with  $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ , which is if and only if it is surjective on  $\bar{K}$ -points, by Theorem 2.8. We say  $E_1$  and  $E_2$  are **isogenous**.

- Let

$$\text{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \rightarrow E_2\} \cup \{0\}.$$

This is a group under  $(\phi + \psi)(P) = \phi(P) + \psi(P)$ . If  $\phi : E_1 \rightarrow E_2$  and  $\psi : E_2 \rightarrow E_3$  are isogenies then  $\psi \circ \phi$  is an isogeny. By the tower law,  $\deg(\psi \circ \phi) = \deg \phi \deg \psi$ .

**Lemma 5.1.** If  $0 \neq n \in \mathbb{Z}$  then  $[n] : E \rightarrow E$  is an isogeny.

*Proof.* By Theorem 4.4,  $[n]$  is a morphism. We must show  $[n] \neq 0$ . Assume  $\text{ch } K \neq 2$ .

$n = 2$ . By Lemma 4.5,  $\#E[2] = 4$ , so  $[2] \neq 0$ .

$n$  odd. By Lemma 4.5, there exists  $0 \neq T \in E[2]$ . Then  $nT = T \neq 0$ , so  $[n] \neq 0$ .

Now use  $[mn] = [m] \circ [n]$ . If  $\text{ch } K = 2$  then replace Lemma 4.5 with a lemma computing  $E[3]$ . □

A corollary is that  $\text{Hom}(E_1, E_2)$  is torsion-free as a  $\mathbb{Z}$ -module.

### 5.1 Isogenies

**Lemma 5.2.** Let  $\phi : E_1 \rightarrow E_2$  be an isogeny. Then

$$\phi(P + Q) = \phi(P) + \phi(Q), \quad P, Q \in E_1.$$

*Proof.*  $\phi$  induces a map

$$\begin{aligned} \phi_* : \quad \text{Div}^0 E_1 &\longrightarrow \text{Div}^0 E_2 \\ \sum_{P \in E} n_P(P) &\longmapsto \sum_{P \in E} n_P(\phi(P)) \end{aligned}$$

Recall  $\phi^* : K(E_2) \hookrightarrow K(E_1)$ . A fact is that

$$\text{div}(\text{N}_{K(E_1)/K(E_2)} f) = \phi_*(\text{div } f), \quad f \in K(E_1)^*.$$

So  $\phi_*$  takes principal divisors to principal divisors. Since  $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$  the diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ P \mapsto [(P) - (\mathcal{O}_{E_1})] \downarrow \sim & & \sim \downarrow Q \mapsto [(Q) - (\mathcal{O}_{E_2})] \\ \text{Pic}^0 E_1 & \xrightarrow[\phi_*]{} & \text{Pic}^0 E_2 \end{array}$$

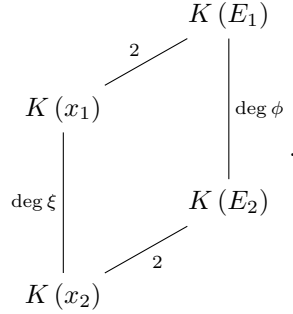
commutes. Since  $\phi_*$  is a group homomorphism,  $\phi$  is group homomorphism. □

**Lemma 5.3.** Let  $\phi : E_1 \rightarrow E_2$  be an isogeny. Then there exists a morphism  $\xi$  making the diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ x_1 \downarrow & & \downarrow x_2 \\ \mathbb{P}^1 & \xrightarrow[\xi]{} & \mathbb{P}^1 \end{array}$$

commute, where  $x_i$  is the  $x$ -coordinate on a Weierstrass equation for  $E_i$ . Moreover if  $\xi(t) = r(t)/s(t)$  for  $r, s \in K[t]$  coprime then  $\deg \phi = \deg \xi = \max(\deg r, \deg s)$ .

*Proof.* For  $i = 1, 2$ ,  $K(E_i)/K(x_i)$  is a degree two Galois extension with Galois group generated by  $[-1]^*$ . Since  $\phi$  is a group homomorphism we have  $\phi \circ [-1] = [-1] \circ \phi$ . If  $f \in K(x_2)$  then  $[-1]^* f = f$  and  $[-1]^* (\phi^* f) = \phi^* ([-1]^* f) = \phi^* f$ , so  $\phi^* f \in K(x_1)$ . Taking  $f = x_2$  gives  $\phi^* x_2 = \xi(x_1)$  for some rational function  $\xi$ , so



By the tower law,  $2 \deg \phi = 2 \deg \xi$ . Now

$$\begin{aligned}
 \phi^* : K(x_2) &\longrightarrow K(x_1) \\
 x_2 &\longmapsto \xi(x_1) = \frac{r(x_1)}{s(x_1)},
 \end{aligned}$$

for  $r, s \in K[t]$  coprime. Claim that the minimal polynomial of  $x_1$  over  $K(x_2)$  is

$$f(t) = r(t) - s(t)x_2 \in K(x_2)[t].$$

Check that  $f(x_1) = 0$  and  $f$  is irreducible in  $K[x_2, t]$ , since  $r$  and  $s$  are coprime. By Gauss' lemma,  $f$  is irreducible in  $K(x_2)[t]$ . Thus

$$\deg \phi = \deg \xi = [K(x_1) : K(x_2)] = \deg f = \max(\deg r, \deg s).$$

□

**Lemma 5.4.**  $\deg[2] = 4$ .

*Proof.* Assuming  $\text{ch } K \neq 2, 3$ , let  $E$  be  $y^2 = f(x) = x^3 + ax + b$ . If  $P = (x, y)$  then

$$x(2P) = \left( \frac{3x^2 + a}{2y} \right)^2 - 2x = \frac{(3x^2 + a)^2 - 8xf(x)}{4f(x)} = \frac{x^4 + \dots}{4f(x)}.$$

The numerator and denominator are coprime. Indeed otherwise there exists  $\theta \in \overline{K}$  with  $f(\theta) = f'(\theta) = 0$ , so  $f$  has a multiple root, a contradiction. By Lemma 5.3,  $\deg[2] = \max(4, 3) = 4$ . □

## 5.2 The degree quadratic form

**Definition.** Let  $A$  be an abelian group. Then  $q : A \rightarrow \mathbb{Z}$  is a **quadratic form** if

1.  $q(nx) = n^2 q(x)$  for all  $n \in \mathbb{Z}$  and all  $x \in A$ , and
2.  $(x, y) \mapsto q(x+y) - q(x) - q(y)$  is  $\mathbb{Z}$ -bilinear.

**Lemma 5.5.**  $q : A \rightarrow \mathbb{Z}$  is a quadratic form if and only if it satisfies the **parallelogram law**

$$q(x+y) + q(x-y) = 2q(x) + 2q(y), \quad x, y \in A.$$

*Proof.*

$\implies$  Let  $\langle x, y \rangle = q(x+y) - q(x) - q(y)$ . Then  $\langle x, x \rangle = q(2x) - 2q(x) = 2q(x)$  by 1 with  $n = 2$ . But by 2,

$$q(x+y) + q(x-y) = \frac{1}{2} \langle x+y, x+y \rangle + \frac{1}{2} \langle x-y, x-y \rangle = \langle x, x \rangle + \langle y, y \rangle = 2q(x) + 2q(y).$$

$\Leftarrow$  On example sheet 2.

□

Lecture 7  
Friday  
23/10/20

**Theorem 5.6.**  $\deg : \text{Hom}(E_1, E_2) \rightarrow \mathbb{Z}$  is a quadratic form.

Note that  $\deg 0 = 0$ . For the proof we assume  $\text{ch } K \neq 2, 3$ . We write  $E_2$  as  $y^2 = x^3 + ax + b$ . Let  $P, Q \in E_2$  with  $P, Q, P + Q, P - Q \neq 0$ . Let  $x_1, \dots, x_4$  be the  $x$ -coordinates of these four points.

**Lemma 5.7.** *There exist  $w_0, w_1, w_2 \in \mathbb{Z}[a, b][x_1, x_2]$  of degree at most two in  $x_1$  and degree at most two in  $x_2$  such that  $(1 : x_3 + x_4 : x_3x_4) = (w_0 : w_1 : w_2)$ .*

*Proof.* By direct calculation,

$$w_0 = (x_1 - x_2)^2, \quad w_1 = 2(x_1x_2 + a)(x_1 + x_2) + 4b, \quad w_2 = x_1^2x_2^2 - 2ax_1x_2 - 4b(x_1 + x_2) + a^2.$$

Alternatively, let  $y = \lambda x + \nu$  be the line through  $P$  and  $Q$ . Then

$$x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) = x^3 - s_1x^2 + s_2x - s_3,$$

where  $s_i$  is the  $i$ -th symmetric polynomial in  $x_1, x_2, x_3$ . Comparing coefficients gives  $\lambda^2 = s_1$ ,  $-2\lambda\nu = s_2 - a$ , and  $\nu^2 = s_3 + b$ . Eliminating  $\lambda$  and  $\nu$  gives

$$F(x_1, x_2, x_3) = (s_2 - a)^2 - 4s_1(s_3 + b) = 0,$$

which has degree at most two in each  $x_i$ . Then  $x_3$  is a root of the quadratic polynomial  $w(t) = F(x_1, x_2, t)$ . Repeating for the line through  $P$  and  $-Q$  shows that  $x_4$  is the other root. Thus  $w_0(t - x_3)(t - x_4) = w(t) = w_0t^2 - w_1t + w_2$ , so  $(1 : x_3 + x_4 : x_3x_4) = (w_0 : w_1 : w_2)$ .  $\square$

*Proof of Theorem 5.6.* We show that if  $\phi, \psi \in \text{Hom}(E_1, E_2)$  then

$$\deg(\phi + \psi) + \deg(\phi - \psi) \leq 2\deg\phi + 2\deg\psi.$$

We may assume  $\phi, \psi, \phi + \psi, \phi - \psi \neq 0$ , otherwise trivial, or use  $\deg[2] = 4$ . Let

$$\begin{aligned} \phi : (x, y) &\mapsto (\xi_1(x), \dots), & \psi : (x, y) &\mapsto (\xi_2(x), \dots), \\ \phi + \psi : (x, y) &\mapsto (\xi_3(x), \dots), & \phi - \psi : (x, y) &\mapsto (\xi_4(x), \dots). \end{aligned}$$

By Lemma 5.7,

$$(1 : \xi_3(x) + \xi_4(x) : \xi_3(x)\xi_4(x)) = (w_0 : w_1 : w_2),$$

where  $w_0, w_1, w_2$  are in terms of  $\xi_1(x)$  and  $\xi_2(x)$ . Put  $\xi_i = r_i/s_i$  for  $r_i/s_i \in K[x]$  coprime. Then

$$(s_3(x)s_4(x) : r_3(x)s_4(x) + r_4(x)s_3(x) : r_3(x)r_4(x)) = (w_0 : w_1 : w_2),$$

where  $w_0, w_1, w_2$  are in terms of  $r_1(x), s_1(x), r_2(x), s_2(x)$ , so

$$\begin{aligned} \deg(\phi + \psi) + \deg(\phi - \psi) &= \max(\deg r_3(x), \deg s_3(x)) + \max(\deg r_4(x), \deg s_4(x)) \\ &= \max(\deg s_3(x)s_4(x), \deg(r_3(x)s_4(x) + r_4(x)s_3(x)), \deg r_3(x)r_4(x)) \\ &\leq 2\max(\deg r_1(x), \deg s_1(x)) + 2\max(\deg r_2(x), \deg s_2(x)) \\ &= 2\deg\phi + 2\deg\psi, \end{aligned}$$

since  $s_3(x)s_4(x), r_3(x)s_4(x) + r_4(x)s_3(x), r_3(x)r_4(x)$  are coprime. Now replace  $\phi$  and  $\psi$  by  $\phi + \psi$  and  $\phi - \psi$  to get

$$\deg 2\phi + \deg 2\psi \leq 2\deg(\phi + \psi) + 2\deg(\phi - \psi).$$

Since  $\deg[2] = 4$  we get

$$2\deg\phi + 2\deg\psi \leq \deg(\phi + \psi) + \deg(\phi - \psi).$$

Thus  $\deg$  satisfies the parallelogram law, so  $\deg$  is a quadratic form.  $\square$

**Corollary 5.8.**  $\deg n\phi = n^2 \deg\phi$  for all  $n \in \mathbb{Z}$  and  $\phi \in \text{Hom}(E_1, E_2)$ . In particular  $\deg[n] = n^2$ .



**Example 5.9.** Let  $E/K$  be an elliptic curve, and let  $0 \neq T \in E(K)[2]$ . Suppose  $\text{ch } K \neq 2$ . Without loss of generality  $E$  is

$$y^2 = x(x^2 + ax + b), \quad a, b \in K, \quad b(a^2 - 4b) \neq 0,$$

and  $T = (0, 0)$ . If  $P = (x, y)$  and  $P' = P + T = (x', y')$ , then

$$x' = \left(\frac{y}{x}\right)^2 - x - a = \frac{x^2 + ax + b}{x} - x - a = \frac{b}{x}, \quad y' = -\left(\frac{y}{x}\right) x' = -\frac{by}{x^2}.$$

Let

$$\xi = x + x' + a = \frac{x^2 + ax + b}{x} = \left(\frac{y}{x}\right)^2, \quad \eta = y + y' = \left(\frac{y}{x}\right) \left(x - \frac{b}{x}\right).$$

Then

$$\eta^2 = \left(\frac{y}{x}\right)^2 \left(\left(x + \frac{b}{x}\right)^2 - 4b\right) = \xi \left((\xi - a)^2 - 4b\right) = \xi (\xi^2 - 2a\xi + a^2 - 4b).$$

Let  $E'$  be

$$y^2 = x(x^2 + a'x + b'), \quad a' = -2a, \quad b' = a^2 - 4b.$$

There is an isogeny

$$\begin{aligned} \phi : E &\longrightarrow E' \\ (x, y) &\longmapsto \left( \left(\frac{y}{x}\right)^2 : \frac{y(x^2 - b)}{x^2} : 1 \right) \\ \mathcal{O}_E &\longmapsto (0 : 1 : 0) \end{aligned}$$

Then  $(y/x)^2 = (x^2 + ax + b)/x$ , which are coprime since  $b \neq 0$ . By Lemma 5.3,  $\deg \phi = 2$ . We say  $\phi$  is a **2-isogeny**.

## 6 The invariant differential

Let  $C$  be an algebraic curve over  $K = \overline{K}$ .

### 6.1 Differentials

**Definition.** The space of **differentials**  $\Omega_C$  is the  $K(C)$ -vector space generated by  $df$  for  $f \in K(C)$  subject to the relations

- $d(f + g) = df + dg$ ,
- $d(fg) = f dg + g df$ , and
- $da$  for all  $a \in K$ .

**Fact.**  $\Omega_C$  is a one-dimensional  $K(C)$ -vector space.

Let  $0 \neq \omega \in \Omega_C$ . Let  $P \in C$  be a smooth point and  $t \in K(C)$  a uniformiser at  $P$ . Then  $\omega = f dt$  for some  $f \in K(C)^*$ . We define

$$\text{ord}_P \omega = \text{ord}_P f.$$

This is independent of the choice of  $t$ .

**Fact.** Suppose  $f \in K(C)^*$  such that  $\text{ord}_P f = n \neq 0$ . If  $\text{ch } k \nmid n$  then

$$\text{ord}_P(df) = n - 1.$$

We now assume  $C$  is a smooth projective curve.

**Definition.** Let

$$\text{div } \omega = \sum_{P \in C} (\text{ord}_P \omega) P \in \text{Div } C,$$

using here the fact that  $\text{ord}_P \omega = 0$  for all but finitely many  $P \in C$ .

### 6.2 Regular differentials

**Definition.** The **genus** is

$$g(C) = \dim_K \{ \omega \in \Omega_C \mid \text{div } \omega \geq 0 \},$$

the space of **regular differentials**.

As a consequence of Riemann Roch we have, if  $0 \neq \omega \in \Omega_C$ , then

$$\deg(\text{div } \omega) = 2g(C) - 2.$$

**Lemma 6.1.** Assume  $\text{ch } K \neq 2$ . Let  $E$  be  $y^2 = (x - e_1)(x - e_2)(x - e_3)$  for  $e_1, e_2, e_3$  distinct. Then  $\omega = dx/y$  is a differential on  $E$  with no zeros or poles, so  $g(E) = 1$ . In particular the  $K$ -vector space of regular differentials on  $E$  is one-dimensional, spanned by  $\omega$ .

*Proof.* Let  $T_i = (e_i, 0)$ , so  $E[2] = \{\mathcal{O}, T_1, T_2, T_3\}$ . Then

$$\text{div } y = [T_1] + [T_2] + [T_3] - 3[\mathcal{O}]. \quad (4)$$

For  $P \in E$ ,  $\text{div}(x - x_P) = [P] + [-P] - 2[\mathcal{O}]$ .

- If  $P \in E \setminus E[2]$  then  $\text{ord}_P(x - x_P) = 1$ , so  $\text{ord}_P(dx) = 0$ .
- If  $P = T_i$  then  $\text{ord}_P(x - x_P) = 2$ , so  $\text{ord}_P(dx) = 1$ .
- If  $P = \mathcal{O}$  then  $\text{ord}_P x = -2$ , so  $\text{ord}_P(dx) = -3$ .

Then

$$\text{div}(dx) = [T_1] + [T_2] + [T_3] - 3[\mathcal{O}]. \quad (5)$$

By (4) and (5),  $\text{div}(dx/y) = 0$ . □

### 6.3 The invariant differential

**Definition.** If  $\phi : C_1 \rightarrow C_2$  is a nonconstant morphism

$$\begin{aligned} \phi^* : \Omega_{C_2} &\longrightarrow \Omega_{C_1} \\ fdg &\longmapsto \phi^*fd(\phi^*g) \end{aligned} .$$

**Lemma 6.2.** Let  $P \in E$ , let  $\omega = dx/y$  as above, and let

$$\begin{aligned} \tau_P : E &\longrightarrow E \\ X &\longmapsto P + X \end{aligned} .$$

Then  $\tau_P^*\omega = \omega$ , so  $\omega$  is called the **invariant differential**.

*Proof.*  $\tau_P^*\omega$  is a regular differential on  $E$ , so  $\tau_P^*\omega = \lambda_P\omega$  for some  $\lambda_P \in K^*$ . The map

$$\begin{aligned} E &\longrightarrow \mathbb{P}^1 \\ P &\longmapsto \lambda_P \end{aligned}$$

is a morphism of smooth projective curves but not surjective, since it misses zero and  $\infty$ , so it is constant, by Theorem 2.8, that is there exists  $\lambda \in K^*$  such that  $\tau_P^*\omega = \lambda\omega$  for all  $P \in E$ . Taking  $P = \mathcal{O}_E$  shows  $\lambda = 1$ .  $\square$

**Remark.** If  $K = \mathbb{C}$ , there is an isomorphism

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E(\mathbb{C}) \\ z &\longmapsto (\wp(z), \wp'(z)) \end{aligned} ,$$

so  $dx/y = \wp'(z)dz/\wp'(z) = dz$ , which is invariant under  $z \mapsto z + c$ .

**Lemma 6.3.** Let  $\phi, \psi \in \text{Hom}(E_1, E_2)$ , and let  $\omega$  be the invariant differential on  $E_2$ . Then

$$(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega.$$

*Proof.* Write  $E = E_2$ . Let

$$\begin{aligned} \mu : E \times E &\longrightarrow E & \pi_1 : E \times E &\longrightarrow E & \pi_2 : E \times E &\longrightarrow E \\ (P, Q) &\longmapsto P + Q & (P, Q) &\longmapsto P & (P, Q) &\longmapsto Q \end{aligned} .$$

A fact is that  $\Omega_{E \times E}$  is a two-dimensional  $K(E \times E)$ -vector space with basis  $\pi_1^*\omega$  and  $\pi_2^*\omega$ , so

$$\mu^*\omega = f\pi_1^*\omega + g\pi_2^*\omega, \quad f, g \in K(E \times E). \quad (6)$$

For  $Q \in E$  let

$$\begin{aligned} \iota_Q : E &\longrightarrow E \times E \\ P &\longmapsto (P, Q) \end{aligned} .$$

Applying  $\iota_Q^*$  to (6) gives

$$\tau_Q^*\omega = (\mu \circ \iota_Q)^*\omega = \iota_Q^*(\pi_1 \circ \iota_Q)^*\omega + \iota_Q^*(\pi_2 \circ \iota_Q)^*\omega = \iota_Q^*f\omega + 0,$$

which is  $\omega$  by Lemma 6.2. Then  $\iota_Q^*f = 1$  for all  $Q \in E$ , so  $f(P, Q) = 1$  for all  $P, Q \in E$ . Similarly  $g(P, Q) = 1$  for all  $P, Q \in E$ . By (6),  $\mu^*\omega = \pi_1^*\omega + \pi_2^*\omega$ . Now pull back by

$$\begin{aligned} E &\longrightarrow E \times E \\ P &\longmapsto (\phi(P), \psi(P)) \end{aligned} ,$$

to get  $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$ .  $\square$

## 6.4 Separability criterion

**Lemma 6.4.** *Let  $\phi : C_1 \rightarrow C_2$  be a nonconstant morphism. Then  $\phi$  is separable if and only if  $\phi^* : \Omega_{C_1} \rightarrow \Omega_{C_2}$  is nonzero.*

*Proof.* Omitted. □

**Example.** Let  $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} = \mathbb{P}^1 \setminus \{0, \infty\}$  be the **multiplicative group** with group law

$$\begin{aligned} \mathbb{G}_m \times \mathbb{G}_m &\longrightarrow \mathbb{G}_m \\ (x, y) &\longmapsto xy \end{aligned}.$$

Let  $n \geq 1$  be an integer, and let

$$\begin{aligned} \alpha : \mathbb{G}_m &\longrightarrow \mathbb{G}_m \\ x &\longmapsto x^n \end{aligned}.$$

Then  $\alpha^*(dx) = d(x^n) = nx^{n-1}dx$ . So if  $\text{ch } K \nmid n$  then  $\alpha$  is separable. By Theorem 2.8,  $\#\alpha^{-1}(Q) = \deg \alpha$  for all but finitely many  $Q \in \mathbb{G}_m$ . Since  $\alpha$  is a group homomorphism,  $\#\alpha^{-1}(Q) = \#\ker \alpha$  for all  $Q \in \mathbb{G}_m$ . Thus  $\#\ker \alpha = \deg \alpha = n$ , that is  $K = \overline{K}$  contains exactly  $n$  distinct  $n$ -th roots of unity.

**Theorem 6.5.** *If  $\text{ch } K \nmid n$  then  $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ .*

*Proof.* By Lemma 6.3 and induction,  $[n]^*\omega = n\omega$ . So if  $\text{ch } K \nmid n$ ,  $[n]$  is separable. By Theorem 2.8,  $\#[n]^{-1}(Q) = \deg [n]$  for all but finitely many  $Q \in E$ . Since  $[n]$  is a group homomorphism,  $\#[n]^{-1}(Q) = \#E[n]$  for all  $Q \in E$ , so  $\#E[n] = \deg [n] = n^2$ , by Corollary 5.8. By group theory,

$$E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}, \quad d_1 \mid \cdots \mid d_t \mid n,$$

and  $\prod_{i=1}^t d_i = n^2$ . If  $p$  is a prime with  $p \mid d_1$  then  $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$ . But  $\#E[p] = p^2$ , so  $t = 2$ . Then  $d_1 \mid d_2 \mid n$  and  $d_1 d_2 = n^2$ , so  $d_1 = d_2 = n$ . □

**Remark.** Not to be used on example sheet. If  $\text{ch } K = p$  then  $[p]$  is inseparable. It can be shown that either  $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$  for all  $r \geq 1$ , where  $E$  is **ordinary**, or  $E[p] = 0$ , where  $E$  is **supersingular**.

Lecture 9  
Wednesday  
28/10/20

## 7 Elliptic curves over finite fields

### 7.1 Hasse's theorem

Recall  $q(x) = \frac{1}{2} \langle x, x \rangle$ .

**Lemma 7.1.** *Let  $A$  be an abelian group and  $q : A \rightarrow \mathbb{Z}$  a positive definite quadratic form. If  $x, y \in A$  then*

$$|\langle x, y \rangle| = |q(x+y) - q(x) - q(y)| \leq 2\sqrt{q(x)q(y)}.$$

*Proof.* We may assume  $x \neq 0$  otherwise the result is clear. Let  $m, n \in \mathbb{Z}$ . Then

$$\begin{aligned} 0 \leq q(mx + ny) &= \frac{1}{2} \langle mx + ny, mx + ny \rangle = m^2 q(x) + mn \langle x, y \rangle + n^2 q(y) \\ &= q(x) \left( m + \frac{\langle x, y \rangle}{2q(x)} n \right)^2 + n^2 \left( q(y) - \frac{\langle x, y \rangle^2}{4q(x)} \right). \end{aligned}$$

Taking  $m = \langle x, y \rangle$  and  $n = -2q(x)$  we deduce  $\langle x, y \rangle^2 \leq 4q(x)q(y)$ , so  $|\langle x, y \rangle| \leq 2\sqrt{q(x)q(y)}$ .  $\square$

Let  $\mathbb{F}_q$  be the field with  $q$  elements, so  $q = p^m$  and  $\text{ch } \mathbb{F}_q = p$ . Then  $\text{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$  is cyclic of order  $r$  generated by the Frobenius map  $x \mapsto x^q$ .

**Theorem 7.2** (Hasse). *Let  $E/\mathbb{F}_q$  be an elliptic curve. Then*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

*Proof.* Let  $E$  have a Weierstrass equation with coefficients  $a_1, \dots, a_6 \in \mathbb{F}_q$ , so  $a_i^q = a_i$ . Define the Frobenius endomorphism

$$\begin{aligned} \phi : E &\longrightarrow E \\ (x, y) &\longmapsto (x^q, y^q) \end{aligned}$$

an isogeny of degree  $q$ . Then  $E(\mathbb{F}_q) = \{P \in E \mid \phi(P) = P\} = \ker(1 - \phi)$ , and

$$\phi^* \omega = \phi^* \left( \frac{dx}{y} \right) = \frac{d(x^q)}{y^q} = \frac{qx^{q-1}dx}{y^q} = 0,$$

since  $q \equiv 0 \pmod{p}$ . By Lemma 6.3,  $(1 - \phi)^* \omega = \omega - \phi^* \omega \neq 0$ , so  $1 - \phi$  is separable. By Theorem 2.8 and the fact that  $1 - \phi$  is a group homomorphism,  $\# \ker(1 - \phi) = \deg(1 - \phi)$ , so  $\#E(\mathbb{F}_q) = \deg(1 - \phi)$ . By Theorem 5.6,  $\deg : \text{End } E = \text{Hom}(E, E) \rightarrow \mathbb{Z}$  is a positive definite quadratic form. By Lemma 7.1,  $|\deg(1 - \phi) - 1 - \deg \phi| \leq 2\sqrt{\deg \phi}$ , so  $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$ .  $\square$

### 7.2 Zeta functions

For  $K$  a number field

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{(\text{N}\mathfrak{a})^s} = \prod_{\mathfrak{p} \subset \mathcal{O}_K, \mathfrak{p} \text{ prime}} \left( 1 - \frac{1}{(\text{N}\mathfrak{p})^s} \right)^{-1}.$$

For  $K$  a function field, that is  $K = \mathbb{F}_q(C)$  where  $C/\mathbb{F}_q$  is a smooth projective curve,

$$\zeta_K(s) = \prod_{x \in |C|} \left( 1 - \frac{1}{(\text{N}x)^s} \right)^{-1},$$

where  $|C|$  are the **closed points** on  $C$ , the orbits for the action of  $\text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$  on  $C(\overline{\mathbb{F}_q})$ , and  $\text{N}x = q^{\deg x}$  where  $\deg x$  is the size of the orbit. We have  $\zeta_K(s) = F(q^{-s})$  for some  $F \in \mathbb{Q}[[T]]$ , where

$$F(T) = \prod_{x \in |C|} (1 - T^{\deg x})^{-1}.$$

By  $-\log(1-x) = x + \frac{1}{2}x^2 + \dots$ ,

$$\log F(T) = \sum_{x \in C} \sum_{m=1}^{\infty} \frac{1}{m} T^{m \deg x}.$$

Then

$$T \frac{d}{dT} \log F(T) = \sum_{x \in C} \sum_{m=1}^{\infty} (\deg x) T^{m \deg x} = \sum_{n=1}^{\infty} \left( \sum_{x \in C, \deg x | n} \deg x \right) T^n = \sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n}) T^n,$$

so

$$F(T) = \exp \left( \sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n \right).$$

For  $\phi, \psi \in \text{Hom}(E_1, E_2)$  we put

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg \phi - \deg \psi.$$

We define

$$\begin{aligned} \text{tr} &: \text{End } E \longrightarrow \mathbb{Z} \\ \psi &\longmapsto \langle \psi, 1 \rangle. \end{aligned}$$

**Lemma 7.3.** *If  $\psi \in \text{End } E$  then*

$$\psi^2 - [\text{tr } \psi] \psi + [\deg \psi] = 0.$$

*Proof.* See example sheet 2. □

**Definition.** The **zeta function** of a variety  $V/\mathbb{F}_q$  is

$$Z_V(T) = \exp \left( \sum_{n=1}^{\infty} \frac{\#V(\mathbb{F}_{q^n})}{n} T^n \right).$$

**Lemma 7.4.** *Let  $E/\mathbb{F}_q$  be an elliptic curve such that  $\#E(\mathbb{F}_q) = q + 1 - a$ . Then*

$$Z_E(T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}.$$

*Proof.* Let  $\phi: E \rightarrow E$  be the  $q$ -power Frobenius map. By the proof of Hasse's theorem  $\#E(\mathbb{F}_q) = \deg(1 - \phi)$ , so  $\text{tr } \phi = a$  and  $\deg \phi = q$ . By Lemma 7.3,  $\phi^2 - a\phi + q = 0$ , so  $\phi^{n+2} - a\phi^{n+1} + q\phi^n = 0$  for all  $n \geq 0$ , so

$$\text{tr } \phi^{n+2} - a \text{tr } \phi^{n+1} + q \text{tr } \phi^n = 0.$$

This second order difference equation with initial conditions  $\text{tr } 1 = 2$  and  $\text{tr } \phi = a$  has solution  $\text{tr } \phi^n = \alpha^n + \beta^n$  where  $\alpha, \beta \in \mathbb{C}$  are the roots of  $X^2 - aX + q = 0$ , so

$$\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n) = 1 + \deg \phi^n - \text{tr } \phi^n = 1 + q^n - \alpha^n - \beta^n.$$

Thus

$$Z_E(T) = \exp \left( \sum_{n=1}^{\infty} \left( \frac{T^n}{n} + \frac{(qT)^n}{n} - \frac{(\alpha T)^n}{n} - \frac{(\beta T)^n}{n} \right) \right) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)} = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)},$$

using  $-\log(1-x) = \sum_{n=1}^{\infty} x^n/n$ . □

**Remark.** By Hasse's theorem,  $|a| \leq 2\sqrt{q}$ . Then  $\alpha = \bar{\beta}$ , so

$$|\alpha| = |\beta| = \sqrt{q}. \tag{7}$$

Let  $K = \mathbb{F}_q(E)$ . If  $\zeta_K(s) = 0$ , then  $Z_E(q^{-s}) = 0$ , so  $q^s = \alpha$  or  $q^s = \beta$ . Thus  $\Re s = \frac{1}{2}$  by (7).

## 8 Formal groups

### 8.1 Complete rings

**Definition.** Let  $R$  be a ring, and let  $I \subseteq R$  an ideal. The  $I$ -**adic topology** is the topology on  $R$  with basis  $\{r + I^n \mid r \in R, n \geq 1\}$ .

**Definition.** A sequence  $(x_n)$  in  $R$  is **Cauchy** if for all  $k$  there exists  $N$  such that  $x_m - x_n \in I^k$  for all  $m, n \geq N$ .

**Definition.**  $R$  is **complete** if

- $\bigcap_{n \geq 0} I^n = \{0\}$ , and
- every Cauchy sequence converges.

**Remark.** If  $x \in I$  then  $1/(1-x) = 1+x+\dots$ , so  $1-x \in R^\times$ .

**Example.**

- $R = \mathbb{Z}_p$  and  $I = p\mathbb{Z}_p$ .
- $R = \mathbb{Z}[[t]]$  and  $I = \langle t \rangle$ .

**Lemma 8.1** (Hensel's lemma). *Let  $R$  be an integral domain, complete with respect to an ideal  $I$ . Let  $F \in R[X]$  and  $s \geq 1$ . Suppose  $a \in R$  satisfies  $F(a) \equiv 0 \pmod{I^s}$  and  $F'(a) \in R^\times$ . Then there exists a unique  $b \in R$  such that  $F(b) = 0$  and  $b \equiv a \pmod{I^s}$ .*

*Proof.* Let  $u \in R^\times$  with  $F'(a) \equiv u \pmod{I}$ , for example could take  $u = F'(a)$ . Replacing  $F(X)$  by  $F(X+a)/u$  we may assume  $a = 0$  and  $F'(0) \equiv 1 \pmod{I}$ . We put  $x_0 = 0$  and

$$x_{n+1} = x_n - F(x_n). \quad (8)$$

By easy induction,

$$x_n \equiv 0 \pmod{I^s}. \quad (9)$$

Then

$$F(X) - F(Y) = (X - Y)(F'(0) + XG(X, Y) + YH(X, Y)), \quad G, H \in R[X, Y]. \quad (10)$$

Claim that  $x_{n+1} \equiv x_n \pmod{I^{n+s}}$  for all  $n \geq 0$ . By induction on  $n$ .

$n = 0$  Clear.

$n > 0$  Suppose  $x_n \equiv x_{n-1} \pmod{I^{n+s-1}}$ . By (10),  $F(x_n) - F(x_{n-1}) = (x_n - x_{n-1})(1 + c)$  for some  $c \in I$ , so  $F(x_n) - F(x_{n-1}) \equiv x_n - x_{n-1} \pmod{I^{n+s}}$ . Then  $x_n - F(x_n) \equiv x_{n-1} - F(x_{n-1}) \pmod{I^{n+s}}$ , so  $x_{n+1} \equiv x_n \pmod{I^{n+s}}$ .

This proves the claim, so  $(x_n)_{n \geq 0}$  is Cauchy. Since  $R$  is complete,  $x_n \rightarrow b$  as  $n \rightarrow \infty$ , for some  $b \in R$ . Taking the limit as  $n \rightarrow \infty$  in (8),  $b = b - F(b)$ , so  $F(b) = 0$ . Taking the limit as  $n \rightarrow \infty$  in (9),  $b \equiv 0 \pmod{I^s}$ . Uniqueness is proved using (10) and the assumption  $R$  is an integral domain.  $\square$

### 8.2 Expansion near the identity

Let  $E$  be  $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ . In the affine piece  $Y \neq 0$ , let  $t = -X/Y$  and  $w = -Z/Y$ . Then

$$w = f(t, w) = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3.$$

We apply Lemma 8.1 with

$$R = \mathbb{Z}[a_1, \dots, a_6][[t]], \quad I = \langle t \rangle, \quad F(X) = X - f(t, X) \in R[X], \quad s = 3, \quad a = 0.$$

Check that  $F(0) = -f(t, 0) = -t^3 \equiv 0 \pmod{I^3}$  and  $F'(0) = 1 - a_1t - a_2t^2 \in R^\times$ . Thus there exists a unique  $w(t) \in \mathbb{Z}[a_1, \dots, a_6][[t]]$  such that  $w(t) = f(t, w(t))$  and  $w(t) \equiv 0 \pmod{t^3}$ . Following the proof of Lemma 8.1 with  $u = 1$  gives

$$w(t) = \lim_{n \rightarrow \infty} w_n(t), \quad \begin{cases} w_0(t) = 0 \\ w_{n+1}(t) = f(t, w_n(t)) \end{cases}.$$