Elliptic Curves

Lectured by Prof Tom Fisher
Typed by David Kurniadi Angdinata

Michaelmas 2020

Syllabus

Contents

1 Fermat's method of infinite descent

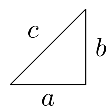
Lecture 1
Friday
09/10/20

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 Δ is $\frac{1}{2}ab$. Then Δ is **rational** if $a, b, c \in \mathbb{Q}$, and Δ is **primitive** if $a, b, c \in \mathbb{Z}$ are coprime.

Lemma 1.1. *Every primitive triangle is of the form* $\Delta\left(u^2 - v^2, 2uv, u^2 + v^2\right)$ *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 $\mathbb{Z}$,

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

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

Definition. $D \in \mathbb{Q}_{>0}$ is a **congruent number** if there exists a rational triangle Δ 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 $Dw^2 = uv\left(u^2 - v^2\right)$ for some $u, v, w \in \mathbb{Q}$ such that $w \neq 0$. Put $x = u/v$ and $y = w/v^2$. $\square$

Fermat showed that 1 is not a congruent number.

Theorem 1.3. *There is no solution to*

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

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 $u \equiv v \mod 2$ 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 $\mathbb{Z}$,

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

Since $u \not\equiv v \mod 2$ both c and d are odd. Then $((c+d)/2)^2 + ((c-d)/2)^2 = \left(c^2 + d^2\right)/2 = u = a^2$, so $\Delta((c+d)/2, (c-d)/2, a)$ is a primitive triangle. Its area is $\left(c^2 - d^2\right)/8 = v/4 = (b/2)^2$. Let $w_1 = b/2$. By Lemma 1.1, $w_1^2 = u_1 v_1\left(u_1^2 - v_1^2\right)$ 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). $\square$

1.2 A variant for polynomials

In this section, K is a field with $\operatorname{ch} K \neq 2$, 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

$$E(L) = \left\{(x, y) \in L^2 \;\middle|\; y^2 = f(x)\right\} \cup \{\mathcal{O}\},$$

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

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

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

Lecture 2 Monday 12/10/20

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

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

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 $(x+1)\left(x - 1 + t^2(x+1)\right) = 0$. Thus $x = -1$ or $x = \left(1-t^2\right)/\left(1+t^2\right)$. 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
$$(x,y) = \left(t^2, t^3\right).$$
- Corollary 1.6 shows that elliptic curves are not rational.

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

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

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

1. *C is rational as in Definition 2.1 if and only if $\mathrm{g}(C) = 0$.*
2. *C is an elliptic curve as in Definition 1.5 if and only if $\mathrm{g}(C) = 1$.*

Proof.

1. Omitted.
2. 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 $\mathrm{ord}_P\, f$ for the order of vanishing of $f \in K(C)$ at P, which is negative if f has a pole.

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

$$\mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P\, f_1 + \mathrm{ord}_P\, f_2, \qquad \mathrm{ord}_P(f_1 + f_2) = \min(\mathrm{ord}_P\, f_1, \mathrm{ord}_P\, f_2).$$

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

Example 2.5. Let $C = \{g = 0\} \subset \mathbb{A}^2$ for $g \in K[x, y]$ irreducible, so $K(C) = \operatorname{Frac}(K[x, y] / \langle g \rangle)$ 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 α and β are not both zero. Let $\gamma, \delta \in K$. A fact is that

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

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

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

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

$$w = t(t - w)(t - \lambda w). \tag{2}$$

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

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

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

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

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

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

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

$$\mathcal{L}(D) = \left\{f \in K(C)^* \;\middle|\; \operatorname{div} f + D \geq 0\right\} \cup \{0\},$$

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 $\left\{y^2 = x(x-1)(x-\lambda)\right\} \subset \mathbb{A}^2$. Then $\operatorname{ord}_P x = -2$ and $\operatorname{ord}_P y = -3$. We deduce

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

This motivates the proof of Theorem 3.1.

Assume $K = \overline{K}$ and $\operatorname{ch} K \neq 2$. Lecture 3 Wednesday 14/10/20

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*

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

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

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

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

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 $Y^2Z = Z^3f\left(X/Z\right)$ for f a monic cubic polynomial. Since C is smooth, f has distinct roots, without loss of generality $0, 1, \lambda$. Thus C is

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

the **Legendre form**. $\square$

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 3×3 matrix.

2.4 The degree of a morphism

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

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

- The **degree** of ϕ is
$$\deg \phi = \left[K\left(C_1\right) : \phi^*K\left(C_2\right)\right].$$
- ϕ is **separable** if $K\left(C_1\right)/\phi^*K\left(C_2\right)$ is a separable field extension, which is automatic if $\operatorname{ch} K = 0$.
- Suppose $P \in C_1$ and $Q \in C_2$ such that $\phi : P \mapsto Q$. Let $t \in K\left(C_2\right)$ be a uniformiser at Q. The **ramification index** of ϕ at P is
$$\mathrm{e}_\phi\left(P\right) = \operatorname{ord}_P \phi^*t,$$
which is always at least one, and independent of t.

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

$$\sum_{P \in \phi^{-1}(Q)} \mathrm{e}_\phi\left(P\right) = \deg \phi, \qquad Q \in C_2.$$

Moreover if ϕ is separable then $\mathrm{e}_\phi\left(P\right) = 1$ for all but finitely many $P \in C_1$. In particular

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

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

$$\begin{array}{cccc} \phi & : & C & \dashrightarrow & \mathbb{P}^n \\ & & P & \longmapsto & \left(f_0\left(P\right) : \dots : f_n\left(P\right)\right) \end{array},$$

where $f_0, \dots, f_n \in K\left(C\right)$ not all zero. A fact is if C is smooth then ϕ 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. $\left\{X^3 + pY^3 + p^2Z^3 = 0\right\} \subset \mathbb{P}^2$ 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 $D \in \operatorname{Div} E$ is defined over K, that is fixed by $\operatorname{Gal}\left(\overline{K}/K\right)$, 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 $\operatorname{ord}_{\mathcal{O}_E} x = -2$ and $\operatorname{ord}_{\mathcal{O}_E} y = -3$. 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

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

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

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

Then

$$[K(E) : K(x)] = \deg\left(x : E \to \mathbb{P}^1\right) = \operatorname{ord}_{\mathcal{O}_E} \frac{1}{x} = 2, \qquad [K(E) : K(y)] = \deg\left(y : E \to \mathbb{P}^1\right) = \operatorname{ord}_{\mathcal{O}_E} \frac{1}{y} = 3,$$

so

$$\begin{tikzcd} & K(E) \arrow[dl, dash, "2"'] \arrow[d, dash] \arrow[dr, dash, "3"] & \\ K(x) \arrow[r, dash] & K(x,y) \arrow[r, dash] & K(y) \end{tikzcd}.$$

By the tower law, $[K(E) : K(x,y)] = 1$, so $\deg(\phi : E \to E') = 1$, so ϕ 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 ϕ^{-1} to see that ϕ^{-1} is a morphism, so ϕ is an isomorphism. $\square$

Lecture 4
Friday
16/10/20

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*

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

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

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

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

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 $\operatorname{ch} K \neq 2, 3$ then we can reduce to the case E is

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

with **discriminant**

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

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

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

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

Proof.

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

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

4 Group law

Let $E = E\left(\overline{K}\right) \subset \mathbb{P}^2$ 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 $\mathrm{T}_P E$ instead, etc. This is the **chord and tangent process**.

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

Associativity is hard.

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

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

Let

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

The **Picard group** is

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

If

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

is the degree zero divisors on E, let

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

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

Proposition 4.2. *Let*

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

Then

1. *$\psi(P \oplus Q) = \psi(P) + \psi(Q)$, and*
2. *ψ 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

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

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 $\operatorname{div} f = P - Q$, and $\deg\left(f : E \to \mathbb{P}^1\right) = \operatorname{ord}_P f = 1$, so $E \cong \mathbb{P}^1$, a contradiction. For surjectivity, let $[D] \in \operatorname{Pic}^0 E$. 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 $\operatorname{div} f + D + (\mathcal{O}_E) \geq 0$. Since $\operatorname{div} f + D + (\mathcal{O}_E)$ has degree one, $\operatorname{div} f + D + (\mathcal{O}_E) = (P)$ 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 $\mathrm{T}_{\mathcal{O}_E} E$ 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,

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

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

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

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

$\square$

4.2 Explicit formulae for the group law

Lecture 5 Monday 19/10/20

We consider E in Weierstrass form

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \tag{3}$$

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 $P_2 = (x_3, y_3)$, 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

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

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

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

It remains to find formulae for λ and ν.

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

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

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

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

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

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

- 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,*

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

are morphisms of algebraic varieties.

Proof. The above formulae show $[-1]$ and $+$ are rational maps. By Remark 2.9, $[-1] : E \to E$ 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

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

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

$$\begin{array}{rcccc} [n] & : & E & \longrightarrow & E \\ & & P & \longmapsto & \underbrace{P + \dots + P}_{n} \end{array},$$

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

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

Lemma 4.5. *Assume* $\operatorname{ch} K \neq 2$. *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 ω_1 and ω_2 a basis for $\mathbb{C}$ as an $\mathbb{R}$-vector space. Then

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

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 Λ. 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

$$y^2 = 4x^3 - g_2 x - g_3.$$

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 $\operatorname{ch} K \nmid n$.

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** $\phi : E_1 \to E_2$ is a nonconstant morphism with $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$, which is if and only if it is surjective on $\overline{K}$-points, by Theorem 2.8. We say E_1 and E_2 are **isogenous**.
- Let
$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\} \cup \{0\}.$$
This is a group under $(\phi + \psi)(P) = \phi(P) + \psi(P)$. If $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_3$ 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 $[n] : E \to E$ is an isogeny.*

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

$n = 2$. 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 $\mathrm{ch}\, K = 2$ then replace Lemma 4.5 with a lemma computing $E[3]$. ☐

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

5.1 Basic properties

Lemma 5.2. *Let $\phi : E_1 \to E_2$ be an isogeny. Then*
$$\phi(P + Q) = \phi(P) + \phi(Q), \qquad P, Q \in E_1.$$

Proof. ϕ induces a map
$$\begin{array}{cccc} \phi_* : & \mathrm{Div}^0 E_1 & \longrightarrow & \mathrm{Div}^0 E_2 \\ & \sum_{P \in E} n_P (P) & \longmapsto & \sum_{P \in E} n_P (\phi(P)) \end{array}.$$

Recall $\phi^* : K(E_2) \hookrightarrow K(E_1)$. A fact is that
$$\mathrm{div}\left(\mathrm{N}_{K(E_1)/K(E_2)} f\right) = \phi_*(\mathrm{div}\, f), \qquad f \in K(E_1)^*.$$

So ϕ_* takes principal divisors to principal divisors. Since $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ the diagram
$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "P \mapsto \left[(P) - (\mathcal{O}_{E_1})\right]"', "\sim"] & E_2 \arrow[d, "\sim"', "Q \mapsto \left[(Q) - (\mathcal{O}_{E_2})\right]"] \\ \mathrm{Pic}^0 E_1 \arrow[r, "\phi_*"'] & \mathrm{Pic}^0 E_2 \end{tikzcd}$$
commutes. Since ϕ_* is a group homomorphism, ϕ is group homomorphism. ☐

Lemma 5.3. *Let $\phi : E_1 \to E_2$ be an isogeny. Then there exists a morphism ξ making the diagram*
$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "x_1"'] & E_2 \arrow[d, "x_2"] \\ \mathbb{P}^1 \arrow[r, "\xi"'] & \mathbb{P}^1 \end{tikzcd}$$
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 ϕ is a group homomorphism we have $\phi \circ [-1] = [-1] \circ \phi$. If $f \in K(x_2)$ then $[-1]^* f = f$ and $[-1]^*(\phi^* f) = \phi^*\left([-1]^* f\right) = \phi^* f$, so $\phi^* f \in K(x_1)$. Taking $f = x_2$ gives $\phi^* x_2 = \xi(x_1)$ for some rational function ξ, so

$$\begin{tikzcd}
 & K(E_1) \arrow[dl, dash, "2"'] \arrow[dd, dash, "\deg\phi"] \\
K(x_1) \arrow[dd, dash, "\deg\xi"'] & \\
 & K(E_2) \arrow[dl, dash, "2"] \\
K(x_2) &
\end{tikzcd}.$$

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

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

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

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

$\square$

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

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

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

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, $\deg[2] = \max(4, 3) = 4$. $\square$

5.2 The degree quadratic form

Lecture 7
Friday
23/10/20

Definition. Let A be an abelian group. Then $q : A \to \mathbb{Z}$ 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. *$q : A \to \mathbb{Z}$ is a quadratic form if and only if it satisfies the **parallelogram law***

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

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,

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

$\impliedby$ On example sheet 2.

$\square$

Theorem 5.6. $\deg : \mathrm{Hom}\left(E_1, E_2\right) \to \mathbb{Z}$ *is a quadratic form.*

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

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

Proof. By direct calculation,

$$w_0 = \left(x_1 - x_2\right)^2, \qquad w_1 = 2\left(x_1 x_2 + a\right)\left(x_1 + x_2\right) + 4b, \qquad w_2 = x_1^2 x_2^2 - 2a x_1 x_2 - 4b\left(x_1 + x_2\right) + a^2.$$

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

$$x^3 + ax + b - \left(\lambda x + \nu\right)^2 = \left(x - x_1\right)\left(x - x_2\right)\left(x - x_3\right) = x^3 - s_1 x^2 + s_2 x - s_3,$$

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 λ and ν gives

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

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

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

$$\deg\left(\phi + \psi\right) + \deg\left(\phi - \psi\right) \le 2\deg\phi + 2\deg\psi.$$

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

$$\phi : \left(x, y\right) \mapsto \left(\xi_1\left(x\right), \dots\right), \qquad \psi : \left(x, y\right) \mapsto \left(\xi_2\left(x\right), \dots\right),$$

$$\phi + \psi : \left(x, y\right) \mapsto \left(\xi_3\left(x\right), \dots\right), \qquad \phi - \psi : \left(x, y\right) \mapsto \left(\xi_4\left(x\right), \dots\right).$$

By Lemma 5.7,

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

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

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

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

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

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

$$\deg 2\phi + \deg 2\psi \le 2\deg\left(\phi + \psi\right) + 2\deg\left(\phi - \psi\right).$$

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

$$2\deg\phi + 2\deg\psi \le \deg\left(\phi + \psi\right) + \deg\left(\phi - \psi\right).$$

Thus deg satisfies the parallelogram law, so deg is a quadratic form. ☐

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

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

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

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

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

Let

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

Then

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

Let E' be

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

There is an isogeny

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

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