Elliptic Curves

Lectured by Prof Tom Fisher
Typed by David Kurniadi Angdinata

Michaelmas 2020

Syllabus

Contents

1 Fermat's method of infinite descent

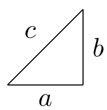
Lecture 1
Friday
09/10/20

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.

$\square$

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

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

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 $K(C) = \mathrm{Frac}(K[x, y] / \langle g \rangle)$ 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

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

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 $\mathrm{ord}_P\, x$ and $\mathrm{ord}_P\, y$. 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 $\mathrm{ord}_P\, t = \mathrm{ord}_P(t - w) = \mathrm{ord}_P(t - \lambda w) = 1$. By (2), $\mathrm{ord}_P\, w = 3$, so

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

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

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

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

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

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 $\mathrm{ord}_P\, x = -2$ and $\mathrm{ord}_P\, y = -3$. 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*

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

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

Proof. We change coordinates such that $P = (0:1:0)$ and $\mathrm{T}_P C = \{Z = 0\}$. Let $C = \{F(X,Y,Z) = 0\}$. 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

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

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 $Y^2Z = Z^3f(X/Z)$ 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**. $\square$

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

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

- The **degree** of ϕ is
$$\deg \phi = [K(C_1) : \phi^* K(C_2)].$$
- ϕ is **separable** if $K(C_1)/\phi^*K(C_2)$ 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 $t \in K(C_2)$ be a uniformiser at Q. The **ramification index** of ϕ at P is
$$\mathrm{e}_\phi(P) = \operatorname{ord}_P \phi^* t,$$
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*

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

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

- *ϕ is surjective, noting that $K = \overline{K}$, and*
- *$\#\phi^{-1}(Q) \leq \deg \phi$, 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

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

where $f_0, \dots, f_n \in K(C)$ not all zero. A fact is if C is smooth then 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. $\left\{X^3 + pY^3 + p^2 Z^3 = 0\right\} \subset \mathbb{P}^2$ 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

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \qquad a_i \in K.$$

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

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

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

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

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. ☐

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*

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

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 $s = \sigma/u^2$. ☐

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 $\Delta\left(a_1, \dots, a_6\right) \neq 0$ where $\Delta \in \mathbb{Z}\left[a_1, \dots, a_6\right]$ 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

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

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

Proof.

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

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

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

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 $P \ne Q$. 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 $\operatorname{div} f + D + (\mathcal{O}_E) \ge 0$. 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 $\psi(P) = [D]$.

$\square$

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.

□

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.

□

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

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

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

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 $0 \ne n \in \mathbb{Z}$ then $[n] : E \to E$ is an isogeny.*

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

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

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

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 Isogenies

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

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "P \mapsto {[(P) - (\mathcal{O}_{E_1})]}"', "\sim"] & E_2 \arrow[d, "\sim"', "Q \mapsto {[(Q) - (\mathcal{O}_{E_2})]}"] \\ \mathrm{Pic}^0 E_1 \arrow[r, "\phi_*"'] & \mathrm{Pic}^0 E_2 \end{tikzcd}$$

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

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

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

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

□

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, $\deg[2] = \max(4, 3) = 4$. □

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.

$\Longrightarrow$ 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,

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

$\Longleftarrow$ On example sheet 2.

□

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

Note that $\deg 0 = 0$. For the proof we assume $\mathrm{ch}\, K \neq 2, 3$. 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,

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

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 λ and ν 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 $(1 : x_3 + x_4 : x_3x_4) = (w_0 : w_1 : w_2)$. ☐

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

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

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

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 ϕ and ψ 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. ☐

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

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

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

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 $b \ne 0$. By Lemma 5.3, $\deg \phi = 2$. We say ϕ is a **2-isogeny**.

6 The invariant differential

Lecture 8 Monday 26/10/20

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

6.1 Differentials

Definition. The space of **differentials** Ω_C is the $K(C)$-vector space generated by $\mathrm{d}f$ for $f \in K(C)$ subject to the relations

- $\mathrm{d}(f+g) = \mathrm{d}f + \mathrm{d}g$,
- $\mathrm{d}(fg) = f\mathrm{d}g + g\mathrm{d}f$, and
- $\mathrm{d}a$ for all $a \in K$.

Fact. Ω_C is a one-dimensional $K(C)$-vector space.

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

$$\mathrm{ord}_P\,\omega = \mathrm{ord}_P\,f.$$

This is independent of the choice of t.

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

$$\mathrm{ord}_P(\mathrm{d}f) = n - 1.$$

We now assume C is a smooth projective curve.

Definition. Let

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

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

6.2 Regular differentials

Definition. The **genus** is

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

the space of **regular differentials**.

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

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

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

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

$$\mathrm{div}\,y = [T_1] + [T_2] + [T_3] - 3[\mathcal{O}]. \tag{4}$$

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

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

Then

$$\mathrm{div}(\mathrm{d}x) = [T_1] + [T_2] + [T_3] - 3[\mathcal{O}]. \tag{5}$$

By (4) and (5), $\mathrm{div}(\mathrm{d}x/y) = 0$. $\square$

6.3 The invariant differential

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

$$\begin{array}{cccccc} \phi^* & : & \Omega_{C_2} & \longrightarrow & \Omega_{C_1} \\ & & f\mathrm{d}g & \longmapsto & \phi^* f \mathrm{d}\left(\phi^* g\right) \end{array}.$$

Lemma 6.2. *Let $P \in E$, let $\omega = \mathrm{d}x/y$ as above, and let*

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

*Then $\tau_P^* \omega = \omega$, so ω 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

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

is a morphism of smooth projective curves but not surjective, since it misses zero and ∞, 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 $\lambda = 1$. ☐

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

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

so $\mathrm{d}x/y = \wp'\left(z\right) \mathrm{d}z / \wp'\left(z\right) = \mathrm{d}z$, which is invariant under $z \mapsto z + c$.

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

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

Proof. Write $E = E_2$. Let

$$\begin{array}{ccccc} \mu & : & E \times E & \longrightarrow & E \\ & & \left(P, Q\right) & \longmapsto & P + Q \end{array}, \qquad \begin{array}{ccccc} \pi_1 & : & E \times E & \longrightarrow & E \\ & & \left(P, Q\right) & \longmapsto & P \end{array}, \qquad \begin{array}{ccccc} \pi_2 & : & E \times E & \longrightarrow & E \\ & & \left(P, Q\right) & \longmapsto & Q \end{array}.$$

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

$$\mu^* \omega = f \pi_1^* \omega + g \pi_2^* \omega, \qquad f, g \in K\left(E \times E\right). \tag{6}$$

For $Q \in E$ let

$$\begin{array}{ccccc} \iota_Q & : & E & \longrightarrow & E \times E \\ & & P & \longmapsto & \left(P, Q\right) \end{array}.$$

Applying ι_Q^* to (6) gives

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

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

$$\begin{array}{ccc} E & \longrightarrow & E \times E \\ P & \longmapsto & \left(\phi\left(P\right), \psi\left(P\right)\right) \end{array},$$

to get $\left(\phi + \psi\right)^* \omega = \phi^* \omega + \psi^* \omega$. ☐

6.4 Separability criterion

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

Proof. Omitted. $\square$

Lecture 9 Wednesday 28/10/20

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

$$\begin{array}{ccc} \mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}} & \longrightarrow & \mathbb{G}_{\mathrm{m}} \\ (x, y) & \longmapsto & xy \end{array}.$$

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

$$\alpha \quad : \quad \begin{array}{ccc} \mathbb{G}_{\mathrm{m}} & \longrightarrow & \mathbb{G}_{\mathrm{m}} \\ x & \longmapsto & x^n \end{array}.$$

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

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

Proof. By Lemma 6.3 and induction, $[n]^* \omega = n\omega$. So if $\mathrm{ch}\, K \nmid n$, $[n]$ 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,

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

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 $d_1 = d_2 = n$. $\square$

Remark. Not to be used on example sheet. If $\mathrm{ch}\, K = p$ 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**.

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 $q : A \to \mathbb{Z}$ a positive definite quadratic form. If $x, y \in A$ then*

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

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

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

Taking $m = \langle x, y\rangle$ and $n = -2q(x) \ne 0$ we deduce $\langle x, y\rangle^2 \le 4q(x)\,q(y)$, so $|\langle x, y\rangle| \le 2\sqrt{q(x)\,q(y)}$. ☐

Let $\mathbb{F}_q$ be the field with q elements, so $q = p^m$ and $\operatorname{ch}\mathbb{F}_q = p$. Then $\operatorname{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ 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*

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

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

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

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

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

since $q \equiv 0 \mod p$. By Lemma 6.3, $(1-\phi)^*\omega = \omega - \phi^*\omega \ne 0$, 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, $\deg : \operatorname{End}E = \operatorname{Hom}(E, E) \to \mathbb{Z}$ is a positive definite quadratic form. By Lemma 7.1, $|\deg(1-\phi) - 1 - \deg\phi| \le 2\sqrt{\deg\phi}$, so $|\#E(\mathbb{F}_q) - (q+1)| \le 2\sqrt{q}$. ☐

7.2 Zeta functions

For K a number field

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

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

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

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

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

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

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

so

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

Lecture 10 Friday 30/10/20

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

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

We define

$$\begin{array}{cccccc} \operatorname{Tr} & : & \operatorname{End} E & \longrightarrow & \mathbb{Z} \\ & & \psi & \longmapsto & \langle \psi, 1 \rangle \end{array}.$$

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

$$\psi^2 - [\operatorname{Tr} \psi] \psi + [\deg \psi] = 0.$$

Proof. See example sheet 2. ☐

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

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

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

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

Proof. Let $\phi : E \to E$ be the q-power Frobenius map. By the proof of Hasse's theorem $\# E(\mathbb{F}_q) = \deg(1 - \phi)$, so $\operatorname{Tr} \phi = a$ 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

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

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

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

Thus

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

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

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

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

Let $K = \mathbb{F}_q(E)$. If $\zeta_K(s) = 0$, then $\mathrm{Z}_E(q^{-s}) = 0$, 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 $\{r + I^n \mid r \in R,\ n \ge 1\}$.

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 $m, n \ge N$.

Definition. R is **complete** if

- $\bigcap_{n \ge 0} I^n = \{0\}$, 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 $s \ge 1$. Suppose $a \in R$ satisfies $F(a) \equiv 0 \mod I^s$ and $F'(a) \in R^\times$. Then there exists a unique $b \in R$ such that $F(b) = 0$ and $b \equiv a \mod I^s$.*

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

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

By easy induction,

$$x_n \equiv 0 \mod I^s. \tag{9}$$

Then

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

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

$n = 0$ Clear.

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

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

8.2 The main example

Let E be

$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3.$$

In the affine piece $Y \ne 0$, let $t = -X/Y$ and $w = -Z/Y$. Then

$$w = f(t, w) = t^3 + a_1 tw + a_2 t^2 w + a_3 w^2 + a_4 tw^2 + a_6 w^3.$$

We apply Lemma 8.1 with

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

Check that $F(0) = -f(t,0) = -t^3 \equiv 0 \mod I^3$ and $F'(0) = 1 - a_1 t - a_2 t^2 \in R^\times$. 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 $w(t) \equiv 0 \mod t^3$. Following the proof of Lemma 8.1 with $u = 1$ gives

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

Lecture 11 Monday 02/11/20

In fact $w(t) = t^3 \left(1 + A_1 t + A_2 t^2 + A_3 t^3 + A_4 t^4 + \dots\right)$, where

$$A_1 = a_1, \qquad A_2 = a_1^2 + a_2, \qquad A_3 = a_1^3 + 2a_1 a_2 + a_3, \qquad A_4 = a_1^4 + 3a_1^2 a_2 + 3a_1 a_3 + a_2^2 + a_4, \qquad \dots.$$

Lemma 8.2. *Let R be an integral domain, complete with respect to an ideal I, let $a_1, \dots, a_6 \in R$, and let $K = \mathrm{Frac}\, R$. Then*

$$\widehat{E}(I) = \{(t, w) \in E(K) \mid t, w \in I\} = \{(t, w(t)) \in E(K) \mid t \in I\}$$

is a subgroup of $E(K)$.

Proof. The two descriptions of $\widehat{E}(I)$ agree, since given $t \in I$, Hensel's lemma shows there exists a unique $w \in I$ such that $(t, w) \in I$. Taking $(t, w) = (0, 0)$ shows $\mathcal{O}_E \in \widehat{E}(I)$. So it suffices to show that if $P_1, P_2 \in \widehat{E}(I)$ then $P_3 = -P_1 - P_2 \in \widehat{E}(I)$. Let $w = \lambda t + \nu$ be the line through $P_1 = (t_1, w_1)$, $P_2 = (t_2, w_2)$, and $P_3 = (t_3, w_3)$. Then

$$w(t) = \sum_{n=2}^{\infty} A_{n-2} t^{n+1}, \qquad \lambda = \begin{cases} \dfrac{w(t_2) - w(t_1)}{t_2 - t_1} & t_1 \neq t_2 \\ w'(t_1) & t_1 = t_2 \end{cases}.$$

If $P_1, P_2 \in \widehat{E}(I)$, then $t_1, t_2 \in I$, so

$$\lambda = \sum_{n=2}^{\infty} A_{n-2}\left(t_1^n + \dots + t_2^n\right) \in I, \qquad \nu = w_1 - \lambda t_1 \in I.$$

Substituting $w = \lambda t + \nu$ into $w = f(t, w)$ gives

$$\lambda t + \nu = t^3 + a_1 t(\lambda t + \nu) + a_2 t^2 (\lambda t + \nu) + a_3 (\lambda t + \nu)^2 + a_4 t (\lambda t + \nu)^2 + a_6 (\lambda t + \nu)^3.$$

Let

$$A = 1 + a_2 \lambda + a_4 \lambda^2 + a_6 \lambda^3$$

be the coefficient of t^3, and let

$$B = a_1 \lambda + a_2 \nu + a_3 \lambda^2 + 2a_4 \lambda \nu + 3a_6 \lambda^2 \nu$$

be the coefficient of t^2. We have $A \in R^\times$ and $B \in I$, so $t_3 = -B/A - t_1 - t_2 \in I$ and $w_3 = \lambda t_3 + \nu \in I$. $\square$

8.3 Formal groups

Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t]]$ and $I = \langle t \rangle$, by Lemma 8.2, there exists $\iota \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ with $\iota(0) = 0$ such that

$$[-1](t, w(t)) = (\iota(t), w(\iota(t))).$$

Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$ and $I = \langle t_1, t_2 \rangle$ there exists $F \in \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$ with $F(0, 0) = 0$ such that

$$(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2))).$$

In fact

$$\iota(X) = -X - a_1 X^2 - a_2 X^3 - \left(a_1^3 + a_3\right) X^4 + \dots, \qquad F(X, Y) = X + Y - a_1 XY - a_2\left(X^2 Y + XY^2\right) + \dots.$$

By properties of the group law we deduce

1. $F(X,Y) = F(Y,X)$,
2. $F(X,0) = X$ and $F(0,Y) = Y$,
3. $F(X, F(Y,Z)) = F(F(X,Y), Z)$, and
4. $F(X, \iota(X)) = 0$.

Definition. Let R be a ring. A **formal group** over R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying 1, 2, and 3.

Exercise. Show that for any formal group there exists a unique $\iota(X) = -X + \dots \in R[[X]]$ such that $F(X, \iota(X)) = 0$.

Example.

- $F(X,Y) = X + Y$ is $\widehat{\mathbb{G}_{\mathrm{a}}}$.
- $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$ is $\widehat{\mathbb{G}_{\mathrm{m}}}$.
- F as above is $\widehat{E}$.

Definition. Let $\mathcal{F}$ and $\mathcal{G}$ be formal groups over R given by power series F and G.

- A **morphism** $f : \mathcal{F} \to \mathcal{G}$ is a power series $f \in R[[T]]$ such that $f(0) = 0$ satisfying $f(F(X,Y)) = G(f(X), f(Y))$.
- $\mathcal{F} \cong \mathcal{G}$ if there exists $f : \mathcal{F} \to \mathcal{G}$ and $g : \mathcal{G} \to \mathcal{F}$ morphisms such that $f(g(X)) = g(f(X)) = X$.

Theorem 8.3. *If $\operatorname{ch} R = 0$ then any formal group $\mathcal{F}$ over R is isomorphic to $\widehat{\mathbb{G}_{\mathrm{a}}}$ over $R \otimes \mathbb{Q}$. More precisely*

1. *there is a unique power series*
$$\log T = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots, \qquad a_i \in R,$$
such that
$$\log F(X,Y) = \log X + \log Y, \tag{11}$$
2. *there is a unique power series*
$$\exp T = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \dots, \qquad b_i \in R,$$
such that $\exp \log T = \log \exp T = T$.

We use the following.

Lecture 12
Wednesday
04/11/20

Lemma 8.4. *Let $f(T) = aT + \dots \in R[[T]]$ with $a \in R^\times$. Then there exists a unique $g(T) = a^{-1}T + \dots \in R[[T]]$ such that $f(g(T)) = g(f(T)) = T$.*

Proof. We construct polynomials $g_n(T) \in R[T]$ such that
$$f(g_n(T)) \equiv T \mod T^{n+1}, \qquad g_{n+1}(T) \equiv g_n(T) \mod T^{n+1}.$$
Then $g(T) = \lim_{n\to\infty} g_n(T)$ satisfies $f(g(T)) = T$. To start the induction set $g_1(T) = a^{-1}T$. Now suppose $n \geq 2$ and $g_{n-1}(T)$ exists, so $f(g_{n-1}(T)) \equiv T + bT^n \mod T^{n+1}$. We put $g_n(T) = g_{n-1}(T) + \lambda T^n$ for $\lambda \in R$ to be chosen later. Then
$$f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n) \equiv f(g_{n-1}(T)) + \lambda a T^n \equiv T + (b + \lambda a) T^n \mod T^{n+1}.$$
We take $\lambda = -b/a$, using again that $a \in R^\times$. We get $g(T) = a^{-1}T + \dots \in R[[T]]$ such that $f(g(T)) = T$. Applying the same argument to g gives $h(T) = aT + \dots \in R[[T]]$ such that $g(h(T)) = T$. Then $f(T) = f(g(h(T))) = h(T)$. $\square$

Proof of Theorem 8.3.

1. The notation is $F_1(X,Y) = \frac{\partial F}{\partial X}(X,Y)$.

   - Uniqueness. Let
   $$p(T) = \tfrac{\mathrm{d}}{\mathrm{d}T}(\log T) = 1 + a_2 T + a_3 T^2 + \dots.$$
   Differentiating (11) with respect to X gives
   $$p(F(X,Y))\, F_1(X,Y) = p(X) + 0.$$
   Putting $X = 0$ gives
   $$p(Y)\, F_1(0,Y) = 1.$$
   Then $p(Y) = F_1(0,Y)^{-1}$, so p, and hence log, is unique.
   - Existence. Let $p(T) = F_1(0,T)^{-1} = 1 + a_2 T + a_3 T^2 + \dots$ for some $a_i \in R$. Let
   $$\log T = T + \frac{a_2}{2} T^2 + \frac{a_3}{3} T^3 + \dots.$$
   Differentiating $F(F(X,Y),Z) = F(X,F(Y,Z))$ with respect to X,
   $$F_1(F(X,Y),Z)\, F_1(X,Y) = F_1(X,F(Y,Z)).$$
   Putting $X = 0$,
   $$F_1(Y,Z)\, F_1(0,Y) = F_1(0,F(Y,Z)).$$
   Then $F_1(Y,Z)\, p(Y)^{-1} = p(F(Y,Z))^{-1}$, so $F_1(Y,Z)\, p(F(Y,Z)) = p(Y)$. Integrating with respect to Y,
   $$\log F(Y,Z) = \log Y + h(Z),$$
   for some power series h. By symmetry of Y and Z we see $h(Z) = \log Z$.

2. Theorem 8.3.2 now follows from Lemma 8.4, except for showing $b_n \in R$, not just in $R \otimes \mathbb{Q}$. See example sheet 2.

$\square$

Notation. Let $\mathcal{F}$, such as $\widehat{\mathbb{G}_{\mathrm{a}}}, \widehat{\mathbb{G}_{\mathrm{m}}}, \widehat{E}$, be a formal group, given by $F \in R[[X,Y]]$. Suppose R is complete with respect to an ideal I. For $x, y \in I$ put $x \oplus_{\mathcal{F}} y = F(x,y) \in I$. Then $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ is an abelian group. For example, $\widehat{\mathbb{G}_{\mathrm{a}}}(I) = (I,+)$ and $\widehat{\mathbb{G}_{\mathrm{m}}}(I) = (1+I,\times)$, and by Lemma 8.2 $\widehat{E}(I) \subset E(K)$, which explains the earlier notation.

Corollary 8.5. *Let $\mathcal{F}$ be a formal group over R, and $n \in \mathbb{Z}$. Suppose $n \in R^\times$. Then*

- *$[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism, and*
- *If R is complete with respect to an ideal I then $\cdot n : \mathcal{F}(I) \to \mathcal{F}(I)$ is an isomorphism.*

In particular $\mathcal{F}(I)$ has no n-torsion.

Proof. We have $[1](T) = T$ and $[n](T) = F([n-1]T, T)$ for all $n \geq 2$. For $n < 0$ use $[-1](T) = \iota(T)$. By induction, $[n](T) = nT + \dots \in R[[T]]$. Lemma 8.4 shows that if $n \in R^\times$ then $[n]$ is an isomorphism. $\square$

9 Elliptic curves over local fields

Let K be a field, complete with respect to a discrete valuation $v : K^* \to \mathbb{Z}$. The **valuation ring**, or **ring of integers**, is

$$\mathcal{O}_K = \{x \in K^* \mid v(x) \geq 0\} \cup \{0\}.$$

with unit group $\mathcal{O}_K^\times$ where $v(x) = 0$ and maximal ideal $\pi\mathcal{O}_K$ where $v(\pi) = 1$. The residue field is $k = \mathcal{O}_K/\pi\mathcal{O}_K$. We assume $\mathrm{ch}\, K = 0$ and $\mathrm{ch}\, k = p$.

Example. $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$, and $k = \mathbb{F}_p$.

9.1 Integral Weierstrass equations

Let E/K be an elliptic curve.

Definition. A Weierstrass equation for E with coefficients $a_1, \dots, a_6 \in K$ is **integral** if $a_1, \dots, a_6 \in \mathcal{O}_K$, and **minimal** if $v(\Delta)$ is minimal among all integral Weierstrass equations for E.

Remark.

- Putting $x = u^{x\prime}$ and $y = u^3 y'$ gives $a_i = u^i a_i'$, so integral Weierstrass equations exist.
- Since $a_1, \dots, a_6 \in \mathcal{O}_K$, $\Delta \in \mathcal{O}_K$, so $v(\Delta) \geq 0$, so minimal Weierstrass equations exist.
- If $\mathrm{ch}\, k \neq 2, 3$ then there exists a minimal Weierstrass equation of the form $y^2 = x^3 + ax + b$.

Lemma 9.1. *Let E/K have an integral Weierstrass equation*

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

Let $\mathcal{O} \neq P = (x, y) \in E(K)$. Then either $x, y \in \mathcal{O}_K$ or $v(x) = -2s$ and $v(y) = -3s$ for some $s \geq 1$.

Compare to example sheet 1, question 5.

Proof.

$v(x) \geq 0$. If $v(y) < 0$ then $v(\mathrm{LHS}) < 0$ and $v(\mathrm{RHS}) \geq 0$, a contradiction, so $x, y \in \mathcal{O}_K$.

$v(x) < 0$. $v(\mathrm{LHS}) \geq \min(2v(y), v(x) + v(y), v(y))$ and $v(\mathrm{RHS}) = 3v(x)$, so $v(y) < v(x)$. But $v(\mathrm{LHS}) = 2v(y)$. Thus $3v(x) = 2v(y)$, so $v(x) = -2s$ and $v(y) = -3s$ for some $s \geq 1$.

□

9.2 The filtration of formal groups

Since K complete, $\mathcal{O}_K$ is complete with respect to the ideal $\pi^r\mathcal{O}_K$, for any $r \geq 1$. Fix a minimal Weierstrass equation for E/K, which gives a formal group $\widehat{E}$ over $\mathcal{O}_K$. Taking $I = \pi^r\mathcal{O}_K$ in Lemma 8.2

$$\begin{aligned}
\widehat{E}(\pi^r\mathcal{O}_K) &= \left\{(x, y) \in E(K) \;\middle|\; -\frac{x}{y}, -\frac{1}{y} \in \pi^r\mathcal{O}_K\right\} \cup \{\mathcal{O}\} \\
&= \left\{(x, y) \in E(K) \;\middle|\; v\left(\frac{x}{y}\right) \geq r,\ v\left(\frac{1}{y}\right) \geq r\right\} \cup \{\mathcal{O}\} \\
&= \{(x, y) \in E(K) \mid \exists s \geq r,\ v(x) = -2s,\ v(y) = -3s\} \cup \{\mathcal{O}\} \\
&= \{(x, y) \in E(K) \mid v(x) \leq -2r,\ v(y) \leq -3r\} \cup \{\mathcal{O}\},
\end{aligned}$$

using Lemma 9.1. By Lemma 8.2 this is a subgroup of $E(K)$, say $E_r(K)$, so

$$\cdots \subset E_2(K) \subset E_1(K).$$

More generally for $\mathcal{F}$ a formal group over $\mathcal{O}_K$

$$\cdots \subset \mathcal{F}\left(\pi^2\mathcal{O}_K\right) \subset \mathcal{F}(\pi\mathcal{O}_K).$$

We show that $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K, +)$ for r sufficiently large and $\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$. Lecture 13 Friday 06/11/20

Theorem 9.2. *Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. Let $e = v(p)$. If $r > e/(p-1)$ then $\log : \mathcal{F}(\pi^r\mathcal{O}_K) \xrightarrow{\sim} \widehat{\mathbb{G}_{\mathrm{a}}}(\pi^r\mathcal{O}_K)$ is an isomorphism with inverse $\exp : \widehat{\mathbb{G}_{\mathrm{a}}}(\pi^r\mathcal{O}_K) \xrightarrow{\sim} \mathcal{F}(\pi^r\mathcal{O}_K)$.*

Remark. $\widehat{\mathbb{G}_{\mathrm{a}}}(\pi^r\mathcal{O}_K) = (\pi^r\mathcal{O}_K, +) \cong (\mathcal{O}_K, +)$.

Proof. For $x \in \pi^r\mathcal{O}_K$ we must check the power series exp and log converge. Recall $\exp T = T + (b_2/2!)T^2 + (b_3/3!)T^3 + \dots$ for $b_i \in \mathcal{O}_K$. Claim that $\mathrm{v}_p(n!) \le (n-1)/(p-1)$, since

$$\mathrm{v}_p(n!) = \sum_{r=1}^{\infty} \left\lfloor \frac{n}{p^r} \right\rfloor < \sum_{r=1}^{\infty} \frac{n}{p^r} = n\frac{\frac{1}{p}}{1-\frac{1}{p}} = \frac{n}{p-1},$$

so $(p-1)\mathrm{v}_p(n!) < n$, so $(p-1)\mathrm{v}_p(n!) \le n-1$, since the left hand side is in $\mathbb{Z}$. Now

$$v\left(\frac{b_n x^n}{n!}\right) \ge nr - e\left(\frac{n-1}{p-1}\right) = (n-1)\left(r - \frac{e}{p-1}\right) + r.$$

This is always at least r and tends to infinity as $n \to \infty$, so $\exp x$ converges and belongs to $\pi^r\mathcal{O}_K$. The same method works for log. $\square$

Lemma 9.3. *We have $\mathcal{F}(\pi^r\mathcal{O}_K)/\mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$ for all $r \ge 1$.*

Proof. By definition of formal groups $F(X,Y) = X + Y + XY(\dots)$. So if $x, y \in \mathcal{O}_K$ then $F(\pi^r x, \pi^r y) \equiv \pi^r(x+y) \mod \pi^{r+1}$. Therefore

$$\begin{array}{ccc} \mathcal{F}(\pi^r\mathcal{O}_K) & \longrightarrow & (k, +) \\ \pi^r x & \longmapsto & x \mod \pi \end{array}$$

is a surjective group homomorphism, with kernel $\mathcal{F}(\pi^{r+1}\mathcal{O}_K)$. $\square$

Thus for $r > e/(p-1)$,

$$(\mathcal{O}_K, +) \cong \mathcal{F}(\pi^r\mathcal{O}_K) \subset \dots \subset \mathcal{F}(\pi^2\mathcal{O}_K) \subset \mathcal{F}(\pi\mathcal{O}_K),$$

where the quotients are isomorphic to $(k, +)$, so if $|k| < \infty$ then $\mathcal{F}(\pi\mathcal{O}_K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

9.3 Reduction modulo π

Notation. Reduction modulo π is

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\pi\mathcal{O}_K = k \\ x & \longmapsto & \widetilde{x} \end{array}.$$

Proposition 9.4. *Let E/K be an elliptic curve. The reduction modulo π of any two minimal Weierstrass equations for E define isomorphic curves over k.*

Proof. Say Weierstrass equations are related by $[u; r, s, t]$ for $u \in K^*$ and $r, s, t \in K$. Then $\Delta_1 = u^{12}\Delta_2$. Since both equations are minimal, $v(\Delta_1) = v(\Delta_2)$, so $u \in \mathcal{O}_K^\times$. By the transformation formulae for a_i and b_i and since $\mathcal{O}_K$ is integrally closed, $r, s, t \in \mathcal{O}_K$. The Weierstrass equations for the reduction modulo π are related by $[\widetilde{u}; \widetilde{r}, \widetilde{s}, \widetilde{t}]$ for $\widetilde{u} \in k^*$ and $\widetilde{r}, \widetilde{s}, \widetilde{t} \in k$. $\square$

Definition. The reduction $\widetilde{E}/k$ of E/K is defined by the reduction of a minimal Weierstrass equation. Then E has **good reduction** if $\widetilde{E}$ is non-singular, and so an elliptic curve, otherwise it has **bad reduction**.

For an integral Weierstrass equation

- if $v(\Delta) = 0$, then good reduction,
- if $0 < v(\Delta) < 12$, then bad reduction, and
- if $v(\Delta) \ge 12$, then beware the equation might not be minimal.

There is a well-defined map
$$\begin{array}{rcl} \mathbb{P}^2(K) & \longrightarrow & \mathbb{P}^2(k) \\ (x:y:z) & \longmapsto & \widetilde{x}:\widetilde{y}:\widetilde{z} \end{array},$$
choosing the representative of $(x:y:z)$ with $\min(v(x),v(y),v(z))=0$. We restrict to give
$$\begin{array}{rcl} E(K) & \longrightarrow & \widetilde{E}(k) \\ P & \longmapsto & \widetilde{P} \end{array}.$$

If $P=(x,y)\in E(K)$ then by Lemma 9.1 either $x,y\in\mathcal{O}_K$, so $\widetilde{P}=(x,y)$, or $v(x)=-2s$ and $v(y)=-3s$, so $P=\left(\pi^{3s}x:\pi^{3s}y:\pi^{3s}\right)$ and $\widetilde{P}=(0:1:0)$. Thus
$$\widehat{E}(\pi\mathcal{O}_K)=E_1(K)=\left\{P\in E(K)\;\middle|\;\widetilde{P}=\mathcal{O}\right\},$$
the **kernel of reduction**. Let
$$\widetilde{E}_{\mathrm{ns}}=\begin{cases}\widetilde{E} & E \text{ has good reduction} \\ \widetilde{E}\setminus\{\text{singular point}\} & E \text{ has bad reduction}\end{cases}.$$

The chord and tangent process still defines a group law on $\widetilde{E}_{\mathrm{ns}}$. In cases of bad reduction either $\widetilde{E}_{\mathrm{ns}}\cong\mathbb{G}_{\mathrm{a}}$, an **additive reduction**, or $\widetilde{E}_{\mathrm{ns}}\cong\mathbb{G}_{\mathrm{m}}$, a **multiplicative reduction**. The isomorphism is over k, or possibly a quadratic extension of k. For simplicity suppose $\operatorname{ch} k\neq 2$. Then $\widetilde{E}$ is $y^2=f(x)$ for $\deg f=3$, so $\widetilde{E}$ is singular if and only if f has a repeated root. A double root gives a curve $y^2=x^2(x+1)$ with a **node**, which leads to multiplicative reduction. See example sheet 3. A triple root gives a curve $y^2=x^3$ with a **cusp**, which leads to additive reduction. We check
$$\begin{array}{rcl} \widetilde{E}_{\mathrm{ns}} & \longleftrightarrow & \mathbb{G}_{\mathrm{a}} \\ (x,y) & \longmapsto & \dfrac{x}{y} \\ \left(\dfrac{1}{t^2},\dfrac{1}{t^3}\right) & \longleftarrow & t \end{array}$$
is a group homomorphism. Let P_1,P_2,P_3 lie on the line $ax+by=1$. Write $P_i=(x_i,y_i)$ and $t_i=x_i/y_i$. Then $x_i^3=y_i^2=y_i^2(ax_i+by_i)$, so t_1,t_2,t_3 are the roots of $X^3-aX-b=0$. Looking at coefficient of X^2 gives $t_1+t_2+t_3=0$.