Elliptic Curves

Lectured by Prof Tom Fisher
Typed by David Kurniadi Angdinata

Michaelmas 2020

Syllabus

Contents

1 Fermat's method of infinite descent

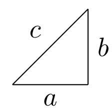
Lecture 1
Friday
09/10/20

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 $c = u^2 + v^2$. □

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 $y = w/v^2$. □

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). □

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

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

Lecture 2 Monday 12/10/20

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

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

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*

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

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

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

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

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

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

- The **degree** of ϕ is
$$\deg \phi = \left[K(C_1) : \phi^* K(C_2)\right].$$
- 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

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

where $f_0, \dots, f_n \in K(C)$ are 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

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

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*

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

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

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

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

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

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 $\psi(P) = [D]$.

$\square$

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.

$\square$

4.2 Explicit formulae for the group law

Lecture 5 Monday 19/10/20

We consider E in Weierstrass form

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

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 $\mathcal{O} \neq T \in E[2]$. 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 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
$$\begin{array}{cccccc} \phi_* & : & \mathrm{Div}^0 E_1 & \longrightarrow & \mathrm{Div}^0 E_2 \\ & & \sum_{P \in E} n_P(P) & \longmapsto & \sum_{P \in E} n_P(\phi(P)) \end{array}.$$

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

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

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

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

□

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 $P, Q, P+Q, P-Q \neq \mathcal{O}$. 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 of degree at most two in* x_2 *such that* $(1 : x_3 + x_4 : x_3 x_4) = (w_0 : w_1 : w_2)$.

Proof. By direct calculation,

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

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

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

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

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

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 $w_0(t - x_3)(t - x_4) = w(t) = w_0 t^2 - w_1 t + w_2$, so $(1 : x_3 + x_4 : x_3 x_4) = (w_0 : w_1 : w_2)$. ☐

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 $\mathcal{O} \ne T \in E(K)[2]$. Suppose $\operatorname{ch} K \ne 2$. 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
$$\begin{array}{rccl} \phi & : & E & \longrightarrow & E' \\ & & (x, y) & \longmapsto & \left(\left(\frac{y}{x}\right)^2 : \frac{y\left(x^2 - b\right)}{x^2} : 1\right) \\ & & \mathcal{O}_E & \longmapsto & (0 : 1 : 0) \end{array}.$$
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 $0 \neq \omega \in \Omega_C$. Let $P \in C$ be a smooth point and $t \in K(C)$ a uniformiser at P. Then $\omega = f\mathrm{d}t$ 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 $\mathrm{ord}_P\,f = n \neq 0$. 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

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

the space of **regular differentials**.

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

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

Lemma 6.1. *Assume $\mathrm{ch}\,K \neq 2$. Let E be $y^2 = (x - e_1)(x - e_2)(x - e_3)$ for e_1, e_2, e_3 distinct. Then $\omega = \mathrm{d}x/y$ 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), $\mathrm{div}(\mathrm{d}x/y) = 0$. ☐

6.3 The invariant differential

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

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

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

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

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

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

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

Proof. Write $E = E_2$. Let

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

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

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

For $Q \in E$ let

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

Applying ι_Q^* to (6) gives

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

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

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

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

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

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

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

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

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 $\mathrm{ch}\, K \nmid n$, then $[n]$ is separable. By Theorem 2.8, $\#[n]^{-1} Q = \deg [n]$ for all but finitely many $Q \in E$. Since $[n]$ is a group homomorphism, $\#[n]^{-1} Q = \#E[n]$ for all $Q \in E$, so $\#E[n] = \deg [n] = n^2$, by Corollary 5.8. By group theory,

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

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

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 $x \neq 0$ 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 $n = -2q(x) \neq 0$ 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 $\mathrm{ch}\,\mathbb{F}_q = p$. Then $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ 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, $(1-\phi)^*\omega = \omega - \phi^*\omega \neq 0$, so $1-\phi$ is separable. By Theorem 2.8 and the fact that $1-\phi$ is a group homomorphism, $\#\ker(1-\phi) = \deg(1-\phi)$, so $\#E(\mathbb{F}_q) = \deg(1-\phi)$. By Theorem 5.6, $\deg : \mathrm{End}\,E = \mathrm{Hom}(E, E) \to \mathbb{Z}$ 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 $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on $C(\overline{\mathbb{F}_q})$, 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

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

Lecture 10
Friday
30/10/20

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

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

We define

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

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

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

Proof. See example sheet 2. □

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

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

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 $\mathrm{Tr}\, \phi = a$ 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 $n \ge 0$, so

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

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

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

Thus

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

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

Remark. By Hasse's theorem, $|a| \le 2\sqrt{q}$. 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 $q^s = \alpha, \beta$. Thus $\Re s = \frac{1}{2}$ by (7).

8 Formal groups

8.1 Complete rings

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

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

Definition. R is **complete** if

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

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

Example.

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

Lemma 8.1 (Hensel's lemma)**.** *Let R be an integral domain, complete with respect to an ideal I. Let $F \in R[X]$ and $s \geq 1$. Suppose $a \in R$ satisfies $F(a) \equiv 0 \mod I^s$ 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 $n \geq 0$. 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 $(x_n)_{n \geq 0}$ 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. ☐

8.2 A nonstandard affine piece

Let E be

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

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

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

We apply Lemma 8.1 with

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

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

$$A_1 = a_1, \qquad A_2 = a_1^2 + a_2, \qquad A_3 = a_1^3 + 2a_1a_2 + a_3, \qquad A_4 = a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + a_4, \qquad \dots.$$

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 $K = \operatorname{Frac} R$. 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

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

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 $n \ge 2$ 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 $f(T) = f(g(h(T))) = h(T)$. ☐

Proof of Theorem 8.3.

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

   - Uniqueness. Let
   $$p(T) = \frac{\mathrm{d}}{\mathrm{d}T}(\log T) = 1 + a_2 T + a_3 T^2 + \dots.$$
   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.

□

Notation. Let $\mathcal{F}$, such as $\widehat{\mathbb{G}_a}, \widehat{\mathbb{G}_m}, \widehat{E}$, 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, $\widehat{\mathbb{G}_a}(I) = (I,+)$ and $\widehat{\mathbb{G}_m}(I) = (1+I,\times)$, 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. □

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 $\operatorname{ch} K = 0$ and $\operatorname{ch} k = p$.

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 $x = u^2 x'$ 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 $\operatorname{ch} k \neq 2, 3$ 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 $v(\text{LHS}) < 0$ and $v(\text{RHS}) \geq 0$, a contradiction, so $x, y \in \mathcal{O}_K$.

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

□

9.2 A 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
$$\dots \subset E_2(K) \subset E_1(K).$$
More generally for $\mathcal{F}$ a formal group over $\mathcal{O}_K$
$$\dots \subset \mathcal{F}\left(\pi^2\mathcal{O}_K\right) \subset \mathcal{F}(\pi\mathcal{O}_K).$$

We show that $\mathcal{F}(\pi^r \mathcal{O}_K) \cong (\mathcal{O}_K, +)$ for r sufficiently large and $\mathcal{F}(\pi^r \mathcal{O}_K)/\mathcal{F}\left(\pi^{r+1}\mathcal{O}_K\right) \cong (k, +)$ for all $r \geq 1$.

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 $\exp x$ and $\log x$ 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 $\mathrm{v}_p(n!) \leq (n-1)/(p-1)$, since

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

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

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

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 $\mathcal{F}(\pi^r \mathcal{O}_K)/\mathcal{F}\left(\pi^{r+1}\mathcal{O}_K\right) \cong (k, +)$ for all $r \geq 1$.*

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

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

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

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

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

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

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

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 $\left[\widetilde{u}; \widetilde{r}, \widetilde{s}, \widetilde{t}\right]$ 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 nonsingular, 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 $v(\Delta) \geq 12$, 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

- $\widetilde{E}_{\mathrm{ns}}\cong\mathbb{G}_{\mathrm{a}}$, 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 the coefficient of X^2 gives $t_1+t_2+t_3=0$.

9.4 The subgroup of nonsingular reduction

Lecture 14 Monday 09/11/20

Definition.

$$E_0(K)=\left\{P\in E(K)\;\middle|\;\widetilde{P}\in\widetilde{E}_{\mathrm{ns}}(k)\right\}.$$

Proposition 9.5. *$E_0(K)$ is a subgroup of $E(K)$, and reduction modulo π is a surjective group homomorphism $E_0(K)\to\widetilde{E}_{\mathrm{ns}}(k)$.*

Proof.

- A line l in $\mathbb{P}^2$ defined over K has equation $aX+bY+cZ=0$ for $a,b,c\in K$. We may assume $\min(v(a),v(b),v(c))=0$. Reduction modulo π gives the line $\widetilde{l}$, $\widetilde{a}X+\widetilde{b}Y+\widetilde{c}Z=0$. If $P_1,P_2,P_3\in E(K)$ with $P_1+P_2+P_3=\mathcal{O}$ then these points lie on a line l, so $\widetilde{P_1},\widetilde{P_2},\widetilde{P_3}\in\widetilde{E}(k)$ lie on the line $\widetilde{l}$. If $\widetilde{P_1},\widetilde{P_2}\in\widetilde{E}_{\mathrm{ns}}(k)$ then $\widetilde{P_3}\in\widetilde{E}_{\mathrm{ns}}(k)$. So if $P_1,P_2\in E_0(K)$ then $P_3\in E_0(K)$ and $\widetilde{P_1}+\widetilde{P_2}+\widetilde{P_3}=\mathcal{O}$. Check this still works if $\#\left\{\widetilde{P_1},\widetilde{P_2},\widetilde{P_3}\right\}<3$. [1]

[1] Exercise

- For surjectivity, let
$$f(x,y) = y^2 + a_1xy + a_3y - \left(x^3 + a_2x^2 + a_4x + a_6\right).$$
Let $\widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(k) \setminus \{\mathcal{O}\}$ say $\widetilde{P} = (\widetilde{x_0}, \widetilde{y_0})$ for some $x_0, y_0 \in \mathcal{O}_K$. Since $\widetilde{P}$ is nonsingular, either
  1. $\frac{\partial f}{\partial x}(x_0,y_0) \not\equiv 0 \mod \pi$, or
  2. $\frac{\partial f}{\partial y}(x_0,y_0) \not\equiv 0 \mod \pi$.

  If 1 we put $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$. Then $g(x_0) \equiv 0 \mod \pi$ and $g'(x_0) \in \mathcal{O}_K^\times$. By Hensel's lemma, there exists $b \in \mathcal{O}_K$ such that $g(b) = 0$ and $b \equiv x_0 \mod \pi$. Then $P = (b, y_0) \in E(K)$ has reduction $\widetilde{P}$. Case 2 is similar.

□

Recall for $r \geq 1$ we have
$$E_r(K) = \{(x,y) \in E(K) \mid v(x) \leq -2r,\ v(y) \leq -3r\} \cup \{\mathcal{O}\}.$$
If $r > e/(p-1)$,
$$\begin{tikzcd}
E_r(K) \arrow[d, phantom, sloped, "\cong"] & \subset \cdots \subset & E_2(K) \arrow[d, phantom, sloped, "\cong"] & \subset \arrow[dd, no head, "\cdot/\cdot"] & E_1(K) \arrow[d, phantom, sloped, "\cong"] & \subset \arrow[dd, no head, "\cdot/\cdot"] & E_0(K) & \subset \arrow[dd, no head, "\cdot/\cdot"] & E(K), \\
(\mathcal{O}_K,+) & & \widehat{E}\left(\pi^2\mathcal{O}_K\right) & & \widehat{E}(\pi\mathcal{O}_K) & & & & . \\
& & & (k,+) & & \widetilde{E}_{\mathrm{ns}}(k) & & ? &
\end{tikzcd}$$

Lemma 9.6. *If $|k| < \infty$ then $E_0(K) \subset E(K)$ has finite index.*

The proof is a compactness argument. See below.

Theorem 9.7. *If $[K : \mathbb{Q}_p] < \infty$ then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.*

Proof. $|k| < \infty$, so this follows from the above. □

Lemma 9.8. *If $|k| < \infty$ then $\mathbb{P}^n(K)$ is compact, with respect to the π-adic topology.*

Proof. Since $|k| < \infty$, $\mathcal{O}_K/\pi^r\mathcal{O}_K$ is finite for all $r \geq 1$, so
$$\mathcal{O}_K \xrightarrow{\sim} \varprojlim_r \mathcal{O}_K/\pi^r\mathcal{O}_K$$
is compact. Then $\mathbb{P}^n(K)$ is the union of compact sets
$$\{(a_0 : \dots : a_{i-1} : 1 : a_{i+1} : \dots : a_n) \mid a_j \in \mathcal{O}_K\},$$
and hence compact. □

Proof of Lemma 9.6. $E(K) \subset \mathbb{P}^2(K)$ is closed subset, so $(E(K), +)$ is a compact topological group. If $\widetilde{E}$ has singular point $(\widetilde{x_0}, \widetilde{y_0})$ then
$$E(K) \setminus E_0(K) = \{(x,y) \in E(K) \mid v(x - x_0) \geq 1,\ v(y - y_0) \geq 1\}$$
is a closed subset of $E(K)$, so $E_0(K)$ is an open subgroup of $E(K)$. The cosets of $E_0(K)$ are an open cover of $E(K)$, so $[E(K) : E_0(K)] < \infty$. □

The **Tamagawa number** is
$$\mathrm{c}_K(E) = [E(K) : E_0(K)].$$

Remark.

- If good reduction, then $\mathrm{c}_K(E) = 1$, but the converse is false.
- It can be shown that either $\mathrm{c}_K(E) = v(\Delta)$ or $\mathrm{c}_K(E) \leq 4$. Essential we work with a minimal Weierstrass equation.

9.5 Unramified extensions of local fields

Let $[K : \mathbb{Q}_p] < \infty$ and let L/K be a finite extension with residue fields k' and k. Let $f = [k' : k]$. Then

$$\begin{tikzcd} K^* \arrow[r, two heads, "v_K"] \arrow[d, phantom, "\cap"] & \mathbb{Z} \arrow[d, "\cdot e"] \\ L^* \arrow[r, two heads, "v_L"'] & \mathbb{Z} \end{tikzcd}.$$

Fact. $[L : K] = ef$. If L/K is Galois then there is a natural group homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k'/k)$. This map is surjective with kernel of order e.

Definition. L/K is **unramified** if $e = 1$.

Fact. For each integer $m \ge 1$

- k has a unique extension of degree m, say k_m,
- K has a unique unramified extension of degree m, say K_m.

These extensions are Galois with cyclic Galois group.

Definition. The **maximal unramified extension** is

$$K^{\mathrm{ur}} = \bigcup_{m \ge 1} K_m \subset \overline{K}.$$

Notation.

- $[n]^{-1} P = \left\{Q \in E\left(\overline{K}\right) \mid nQ = P\right\}$.
- $K(\{P_1, \dots, P_r\}) = K(x_1, \dots, x_r, y_1, \dots, y_r)$ with $P_i = (x_i, y_i)$.

Theorem 9.9. *Let $[K : \mathbb{Q}_p] < \infty$. Suppose E/K has good reduction and $p \nmid n$. If $P \in E(K)$ then $K\left([n]^{-1} P\right)/K$ is unramified.*

Proof. For each $m \ge 1$ there is a short exact sequence

$$0 \to E_1(K_m) \to E(K_m) \to \widetilde{E}(k_m) \to 0.$$

Taking union over $m \ge 1$ gives a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & E_1(K^{\mathrm{ur}}) \arrow[r] \arrow[d, "\cdot n"] & E(K^{\mathrm{ur}}) \arrow[r] \arrow[d, "\cdot n"] & \widetilde{E}\left(\overline{k}\right) \arrow[r] \arrow[d, "\cdot n"] & 0 \\ 0 \arrow[r] & E_1(K^{\mathrm{ur}}) \arrow[r] & E(K^{\mathrm{ur}}) \arrow[r] & \widetilde{E}\left(\overline{k}\right) \arrow[r] & 0 \end{tikzcd}.$$

The left map is an isomorphism by Corollary 8.5, noting that $p \nmid n$, so $n \in \mathcal{O}_K^\times$. Since K^{ur} is not complete we must apply Corollary 8.5 over each K_m. The right map is surjective by Theorem 2.8 with kernel isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ by Theorem 6.5, noting that $p \nmid n$. By the snake lemma,

$$E(K^{\mathrm{ur}})[n] = (\mathbb{Z}/n\mathbb{Z})^2, \qquad E(K^{\mathrm{ur}})/nE(K^{\mathrm{ur}}) = 0.$$

So if $P \in E(K)$ then there exists $Q \in E(K^{\mathrm{ur}})$ such that $nQ = P$ and $[n]^{-1} P = \{Q + T \mid T \in E[n]\} \subset E(K^{\mathrm{ur}})$, so $K\left([n]^{-1} P\right) \subset K^{\mathrm{ur}}$. Thus $K\left([n]^{-1} P\right)/K$ is unramified. ☐

Lecture 15 Wednesday 11/11/20

Corollary 9.10. *Let E/K be an elliptic curve with $[K : \mathbb{Q}_p] < \infty$. Then $E(K)_{\mathrm{tors}}$ is finite.*

Proof. In Theorem 9.7 we saw there exists a finite index subgroup $E_r(K) \subset E(K)$ with $E_r(K) \cong (\mathcal{O}_K, +)$. Since $E_r(K)$ is torsion free $E(K)_{\mathrm{tors}} \hookrightarrow E(K)/E_r(K)$, which is finite. ☐

10 Elliptic curves over number fields I: the torsion subgroup

Let $[K : \mathbb{Q}] < \infty$, and let E/K be an elliptic curve.

10.1 Primes of good and bad reduction

Notation. If $\mathfrak{p}$ is a prime of K, that is of $\mathcal{O}_K$, then $K_\mathfrak{p}$ is the $\mathfrak{p}$-adic completion of K and $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$.

Definition. $\mathfrak{p}$ is a **prime of good reduction** for E/K if $E/K_\mathfrak{p}$ has good reduction.

Lemma 10.1. *E/K has only finitely many primes of bad reduction.*

Proof. Take a Weierstrass equation for E with $a_1, \dots, a_6 \in \mathcal{O}_K$. Since E is nonsingular, $0 \neq \Delta \in \mathcal{O}_K$. Write $\langle \Delta \rangle = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_r^{\alpha_r}$, a factorisation into prime ideals. Let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$. If $\mathfrak{p} \notin S$ then $\mathrm{v}_\mathfrak{p}(\Delta) = 0$, so $E/K_\mathfrak{p}$ has good reduction. Thus the set of bad primes for E is in S. ☐

Remark. If K has class number one, such as $K = \mathbb{Q}$, then we can always find a Weierstrass equation for E with $a_1, \dots, a_6 \in \mathcal{O}_K$ which is minimal at all primes $\mathfrak{p}$.

Lemma 10.2. *$E(K)_{\mathrm{tors}}$ is finite.*

Proof. Take any prime $\mathfrak{p}$. Then $K \subset K_\mathfrak{p}$, so $E(K)_{\mathrm{tors}} \subset E(K_\mathfrak{p})_{\mathrm{tors}}$, which is finite by Corollary 9.10. ☐

10.2 Reduction modulo $\mathfrak{p}$

Lemma 10.3. *Let $\mathfrak{p}$ be a prime of good reduction with $\mathfrak{p} \nmid n$. Then reduction modulo $\mathfrak{p}$ gives an injective group homomorphism $E(K)[n] \hookrightarrow \widetilde{E}(k_\mathfrak{p})[n]$.*

Proof. By Proposition 9.5, $E(K_\mathfrak{p}) \to \widetilde{E}(k_\mathfrak{p})$ is a group homomorphism with kernel $E_1(K_\mathfrak{p})$. By Corollary 8.5 and $\mathfrak{p} \nmid n$, $E_1(K_\mathfrak{p})$ has no n-torsion. ☐

Example. Let $E/\mathbb{Q}$ be $y^2 + y = x^3 - x^2$. Then $\Delta = -11$, so E has good reduction at all $p \nmid 11$, and

p	2	3	5	7	11	13
$\#\widetilde{E}(\mathbb{F}_p)$	5	5	5	10	–	10

By Lemma 10.3, $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 5 \cdot 2^a$ for some $a \geq 0$ and $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 5 \cdot 3^b$ for some $b \geq 0$, so $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 5$. Let $T = (0,0) \in E(\mathbb{Q})$. By calculation, $5T = \mathcal{O}$, so $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/5\mathbb{Z}$.

Example. Let $E/\mathbb{Q}$ be $y^2 + y = x^3 + x^2$. Then $\Delta = -43$, so E has good reduction at all $p \neq 43$, and

p	2	3	5	7	11	13
$\#\widetilde{E}(\mathbb{F}_p)$	5	6	10	8	9	19

So $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 5 \cdot 2^a$ for some $a \geq 0$ and $\#E(\mathbb{Q})_{\mathrm{tors}} \mid 9 \cdot 11^b$ for some $b \geq 0$, so $E(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}\}$. Thus $P = (0,0) \in E(\mathbb{Q})$ is a point of infinite order, so $\operatorname{rk} E(\mathbb{Q}) \geq 1$.

Example. Let E_D be $y^2 = x^3 - D^2 x$ for $D \in \mathbb{Z}$ a squarefree integer. Then $\Delta = 2^6 D^6$, and $E_D(\mathbb{Q})_{\mathrm{tors}} \supset \{\mathcal{O}, (0,0), (\pm D, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$. Let $f(x) = x^3 - D^2 x$. If $p \nmid 2D$ then

$$\#\widetilde{E_D}(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p^2} \left(\left(\frac{f(x)}{p} \right) + 1 \right).$$

If $p \equiv 3 \mod 4$ then since $f(x)$ is an odd function

$$\left(\frac{f(-x)}{p} \right) = \left(\frac{-f(x)}{p} \right) = \left(\frac{-1}{p} \right) \left(\frac{f(x)}{p} \right) = -\left(\frac{f(x)}{p} \right),$$

so $\#\widetilde{E_D}(\mathbb{F}_p) = p + 1$. Let $m = \#E_D(\mathbb{Q})_{\mathrm{tors}}$. We have $4 \mid m \mid p + 1$ for all sufficiently large primes p with $p \equiv 3 \mod 4$, where $p \nmid 2D$ and $p \nmid m$. So $m = 4$, since otherwise this contradicts Dirichlet's theorem on primes in arithmetic progressions, so $E_D(\mathbb{Q})_{\mathrm{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$. Thus $\operatorname{rk} E_D(\mathbb{Q}) \geq 1$ if and only if there exist $x, y \in \mathbb{Q}$ with $y \neq 0$ such that $y^2 = x^3 - D^2 x$, if and only if D is a congruent number.

10.3 The Lutz-Nagell theorem

Lemma 10.4. *Let $E/\mathbb{Q}$ be given by a Weierstrass equation with $a_1, \ldots, a_6 \in \mathbb{Z}$. Suppose $\mathcal{O} \neq T = (x, y) \in E(\mathbb{Q})_{\mathrm{tors}}$. Then*

1. *$4x, 8y \in \mathbb{Z}$, and*
2. *if $2 \mid a_1$ or $2T \neq \mathcal{O}$ then $x, y \in \mathbb{Z}$.*

Proof.

1. The Weierstrass equation defines a formal group $\widehat{E}$ over $\mathbb{Z}$. For $r \geq 1$ we have

$$\widehat{E}(p^r\mathbb{Z}_p) = \{(x, y) \in E(\mathbb{Q}_p) \mid \mathrm{v}_p(x) \leq -2r,\ \mathrm{v}_p(y) \leq -3r\} \cup \{\mathcal{O}\}.$$

By Theorem 9.2, $\widehat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ if $r > 1/(p-1)$, so $\widehat{E}(4\mathbb{Z}_2)$ and $\widehat{E}(p\mathbb{Z}_p)$ for p odd are torsion free. Since $\mathcal{O} \neq T \in E(\mathbb{Q})_{\mathrm{tors}}$ it follows that $\mathrm{v}_2(x) \geq -2$ and $\mathrm{v}_2(y) \geq -3$, and $\mathrm{v}_p(x) \geq 0$ and $\mathrm{v}_p(y) \geq 0$ for all odd primes p. This proves 1.

2. Suppose $T \in \widehat{E}(2\mathbb{Z}_2)$, that is $\mathrm{v}_2(x) = -2$ and $\mathrm{v}_2(y) = -3$. Since $\widehat{E}(2\mathbb{Z}_2)/\widehat{E}(4\mathbb{Z}_2) \cong (\mathbb{F}_2, +)$ and $\widehat{E}(4\mathbb{Z}_2)$ is torsion free we get $2T = \mathcal{O}$. Also $(x, y) = T = -T = (x, -y - a_1x - a_3)$, so $2y + a_1x + a_3 = 0$, so $8y + 4xa_1 + 4a_3 = 0$. Then $8y$ is odd, $4x$ is odd, and $4a_3$ is even, so a_1 is odd. So if $2T \neq \mathcal{O}$ or a_1 is even then $T \notin \widehat{E}(2\mathbb{Z}_2)$, so $x, y \in \mathbb{Z}$.

$\square$

Example. $y^2 + xy = x^3 + 4x + 1$ has $\left(-\frac{1}{4}, \frac{1}{8}\right) \in E(\mathbb{Q})[2]$.

Lecture 16 Friday 13/11/20

Theorem 10.5 (Lutz-Nagell)**.** *Let $E/\mathbb{Q}$ be $y^2 = f(x) = x^3 + ax + b$ for $a, b \in \mathbb{Z}$. Suppose $\mathcal{O} \neq T = (x, y) \in E(\mathbb{Q})_{\mathrm{tors}}$. Then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 \mid 4a^3 + 27b^2$.*

Proof. By Lemma 10.4, $x, y \in \mathbb{Z}$. If $2T = \mathcal{O}$ then $y = 0$. Otherwise $\mathcal{O} \neq 2T = (x_2, y_2) \in E(\mathbb{Q})_{\mathrm{tors}}$. By Lemma 10.4, $x_2, y_2 \in \mathbb{Z}$. But $x_2 = (f'(x)/2y)^2 - 2x$, so $y \mid f'(x)$. Since E is nonsingular, $f(X)$ and $f'(X)$ are coprime, so $f(X)$ and $f'(X)^2$ are coprime. Then there exist $g, h \in \mathbb{Q}[X]$ such that $g(X)f(X) + h(X)f'(X)^2 = 1$. Doing this calculation and clearing denominators gives

$$\left(3X^2 + 4a\right)f'(X)^2 - 27\left(X^3 + aX - b\right)f(X) = 4a^3 + 27b^2.$$

Since $y \mid f'(x)$ and $y^2 = f(x)$ we get $y^2 \mid 4a^3 + 27b^2$. $\square$

Remark. Mazur showed that if $E/\mathbb{Q}$ is an elliptic curve

$$E(\mathbb{Q})_{\mathrm{tors}} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 12,\ n \neq 11 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & 1 \leq n \leq 4 \end{cases}.$$

Moreover all fifteen possibilities occur.

11 Kummer theory

Let K be a field, and let $\operatorname{ch} K \nmid n$. Assume $\mu_n \subset K$.

11.1 The Kummer theorem

Lemma 11.1. *Let $\Delta \subset K^* / (K^*)^n$ be a finite subgroup. Let $L = K\left(\sqrt[n]{\Delta}\right)$. Then L/K is Galois and*

$$\operatorname{Gal}(L/K) \cong \operatorname{Hom}(\Delta, \mu_n).$$

Proof. L/K is Galois since $\mu_n \subset K$ and $\operatorname{ch} K \nmid n$. Define the **Kummer pairing**

$$\begin{array}{rccc} \langle , \rangle & : \operatorname{Gal}(L,K) \times \Delta & \longrightarrow & \mu_n \\ & (\sigma, x) & \longmapsto & \dfrac{\sigma\left(\sqrt[n]{x}\right)}{\sqrt[n]{x}} \end{array}.$$

- Well-defined. If $\alpha, \beta \in L$ with $\alpha^n = \beta^n = x$, then $(\alpha/\beta)^n = 1$. Then $\alpha/\beta \in \mu_n \subset K$, so $\sigma(\alpha)/\alpha = \sigma(\beta)/\beta$.
- Bilinear, since

$$\langle \sigma\tau, x \rangle = \frac{\sigma\left(\tau\left(\sqrt[n]{x}\right)\right)\tau\left(\sqrt[n]{x}\right)}{\tau\left(\sqrt[n]{x}\right)\sqrt[n]{x}} = \langle \sigma, x \rangle \langle \tau, x \rangle, \qquad \langle \sigma, xy \rangle = \frac{\sigma\left(\sqrt[n]{xy}\right)}{\sqrt[n]{xy}} = \frac{\sigma\left(\sqrt[n]{x}\right)\sigma\left(\sqrt[n]{y}\right)}{\sqrt[n]{x}\sqrt[n]{y}} = \langle \sigma, x \rangle \langle \sigma, y \rangle.$$

- Nondegenerate. Let $\sigma \in \operatorname{Gal}(L/K)$. If $\langle \sigma, x \rangle = 1$ for all $x \in \Delta$ then $\sigma\left(\sqrt[n]{x}\right) = \sqrt[n]{x}$ for all $x \in \Delta$, so σ fixes L pointwise, that is $\sigma = \mathrm{id}$. Let $x \in \Delta$. If $\langle \sigma, x \rangle = 1$ for all $\sigma \in \operatorname{Gal}(L/K)$ then $\sigma\left(\sqrt[n]{x}\right) = \sqrt[n]{x}$ for all $\sigma \in \operatorname{Gal}(L/K)$, so $\sqrt[n]{x} \in K^*$, so $x \in (K^*)^n$, that is $x(K^*)^n$ is trivial in Δ.

We get injective group homomorphisms

1. $\operatorname{Gal}(L/K) \hookrightarrow \operatorname{Hom}(\Delta, \mu_n)$, and
2. $\Delta \hookrightarrow \operatorname{Hom}(\operatorname{Gal}(L/K), \mu_r)$.

By 1, $\operatorname{Gal}(L/K)$ is abelian and of exponent dividing n, where the exponent is the least integer m such that $g^m = 1$ for all g. Note that if G is a finite abelian group of exponent dividing n then $\operatorname{Hom}(G, \mu_n) \cong G$, noncanonically. So $|\operatorname{Gal}(L/K)| \le |\Delta| \le |\operatorname{Gal}(L/K)|$ by 1 and 2, so 1 and 2 are isomorphisms. ☐

Example. $\operatorname{Gal}\left(\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{5}\right)/\mathbb{Q}\right) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

Theorem 11.2. *There is a bijection*

$$\begin{array}{rcl} \{\textit{finite subgroups } \Delta \subset K^*/(K^*)^n\} & \longleftrightarrow & \{\textit{finite abelian extensions } L/K \textit{ of exponent dividing } n\} \\ \Delta & \longmapsto & K\left(\sqrt[n]{\Delta}\right) \\ ((L^*)^n \cap K^*)/(K^*)^n & \longleftarrow & L \end{array}.$$

Proof.

- Let L/K be a finite abelian extension of exponent dividing n. Let $\Delta = ((L^*)^n \cap K^*)/(K^*)^n$. Then $K\left(\sqrt[n]{\Delta}\right) \subset L$ and we aim to show equality. Let $G = \operatorname{Gal}(L/K)$. The Kummer pairing gives an injection $\Delta \hookrightarrow \operatorname{Hom}(G, \mu_n)$. Claim that this is a surjection. Given the claim $\Delta \cong \operatorname{Hom}(G, \mu_n)$, so by Lemma 11.1 $\left[K\left(\sqrt[n]{\Delta}\right) : K\right] = |\Delta| = |G| = [L : K]$. But $K\left(\sqrt[n]{\Delta}\right) \subset L$, so $L = K\left(\sqrt[n]{\Delta}\right)$. To prove the claim, let $\chi : G \to \mu_n$ be a group homomorphism. Distinct automorphisms are linearly independent, so there exists $a \in L$ such that $y = \sum_{\tau \in G} \chi(\tau)^{-1} \tau(a) \neq 0$. Let $\sigma \in G$. Then

$$\sigma(y) = \sum_{\tau \in G} \chi(\tau)^{-1} \sigma(\tau(a)) = \sum_{\tau \in G} \chi\left(\sigma^{-1}\tau\right) \sigma(a) = \chi(\sigma) \sum_{\tau \in G} \chi\left(\sigma^{-1}\tau\right) \sigma(a) = \chi(\sigma) y, \tag{12}$$

so $\sigma(y^n) = y^n$ for all $\sigma \in G$. Let $x = y^n$. Then $x \in K^* \cap (L^*)^n$, that is $x \in \Delta$. Also by (12), $\chi : \sigma \mapsto \sigma(y)/y = \sigma(\sqrt[n]{x})/\sqrt[n]{x}$, so

$$\begin{array}{ccc} \Delta & \longrightarrow & \mathrm{Hom}(G, \mu_n) \\ x & \longmapsto & \chi \end{array}.$$

This proves the claim.

- Let $\Delta \subset K^*/(K^*)^n$ be a finite subgroup. Let $L = K\left(\sqrt[n]{\Delta}\right)$ and $\Delta' = ((L^*)^n \cap K^*)/(K^*)^n$. We must show $\Delta' = \Delta$. Clearly $\Delta \subset \Delta'$, so $L = K\left(\sqrt[n]{\Delta}\right) \subset K\left(\sqrt[n]{\Delta'}\right) \subset L$. Then $K\left(\sqrt[n]{\Delta}\right) = K\left(\sqrt[n]{\Delta'}\right)$, so by Lemma 11.1, $|\Delta| = |\Delta'|$. Since $\Delta \subset \Delta'$ it follows that $\Delta = \Delta'$.

$\square$

11.2 Unramified Kummer extensions

Lecture 17 Monday 16/11/20

Proposition 11.3. *Let K be a number field such that $\mu_n \subset K$. Let S be a finite set of primes of K. There are only finitely many extensions L/K such that*

- *L/K is abelian of exponent dividing n, and*
- *L/K is unramified at all primes $\mathfrak{p} \notin S$.*

Proof. By Theorem 11.2, $L = K\left(\sqrt[n]{\Delta}\right)$ for some $\Delta \subset K^*/(K^*)^n$ a finite subgroup. Let $\mathfrak{p}$ be a prime of K such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ for $\mathfrak{P}_i$ a prime in $\mathcal{O}_L$. If $x \in K^*$ represents an element of Δ then $n\mathrm{v}_{\mathfrak{P}_i}(\sqrt[n]{x}) = \mathrm{v}_{\mathfrak{P}_i}(x) = e_i \mathrm{v}_{\mathfrak{p}}(x)$. If $\mathfrak{p} \notin S$ then all $e_i = 1$, so $\mathrm{v}_{\mathfrak{p}}(x) \equiv 0 \mod n$. Thus $\Delta \subset K(S, n)$ where

$$K(S, n) = \{x \in K^*/(K^*)^n \mid \forall \mathfrak{p} \notin S,\ \mathrm{v}_{\mathfrak{p}}(x) \equiv 0 \mod n\},$$

and the proof is completed by Lemma 11.4. $\square$

Lemma 11.4. *$K(S, n)$ is finite.*

Proof. The map

$$\begin{array}{ccc} K(S, n) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^{|S|} \\ x & \longmapsto & (\mathrm{v}_{\mathfrak{p}}(x) \mod n)_{\mathfrak{p} \in S} \end{array}$$

is a group homomorphism with kernel $K(\emptyset, n)$. Since $|S| < \infty$, it suffices to prove Lemma 11.4 with $S = \emptyset$. If $x \in K^*$ represents an element of $K(\emptyset, n)$ then $\langle x \rangle = \mathfrak{a}^n$ for some ideal $\mathfrak{a}$. There is an exact sequence

$$0 \to \mathcal{O}_K^\times/\left(\mathcal{O}_K^\times\right)^n \to K(\emptyset, n) \xrightarrow{x(K^*)^n \mapsto [\mathfrak{a}]} \mathrm{Cl}_K[n] \to 0.$$

Since $|\mathrm{Cl}_K| < \infty$ and $\mathcal{O}_K^\times$ is finitely generated, by Dirichlet's unit theorem, $K(\emptyset, n)$ is finite. $\square$

12 Elliptic curves over number fields II: the Mordell-Weil theorem

12.1 The weak Mordell-Weil theorem

Lemma 12.1. *Let E/K be an elliptic curve, and let L/K be a finite Galois extension. Then the map $E(K)/nE(K) \to E(L)/nE(L)$ has finite kernel.*

Proof. For each element in the kernel we pick a coset representative $P \in E(K)$ and then $Q \in E(L)$ with $nQ = P$. Note that for any $\sigma \in \mathrm{Gal}(L/K)$, $n(\sigma(Q) - Q) = \sigma(P) - P = 0$. Since $\mathrm{Gal}(L/K)$ is finite and $E[n]$ is finite, there are only finitely many possibilities for the map

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \longrightarrow & E[n] \\ \sigma & \longmapsto & \sigma(Q) - Q \end{array}.$$

But if $P_1, P_2 \in E(K)$ such that $P_i = nQ_i$ for $Q_1, Q_2 \in E(L)$ and $\sigma(Q_1) - Q_1 = \sigma(Q_2) - Q_2$ for all $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(Q_1 - Q_2) = Q_1 - Q_2$ for all $\sigma \in \mathrm{Gal}(L/K)$. Then $Q_1 - Q_2 \in E(K)$, so $P_1 - P_2 \in nE(K)$. ☐

Theorem 12.2 (Weak Mordell-Weil)**.** *Let K be a number field, let E/K be an elliptic curve, and let $n \geq 2$ be an integer. Then $E(K)/nE(K)$ is finite.*

Proof. By Lemma 12.1, we may replace K by a finite Galois extension. So without loss of generality $\mu_n \subset K$ and $E[n] \subset E(K)$. Let

$$S = \{\mathfrak{p} \mid n\} \cup \{\text{primes of bad reduction for } E/K\}.$$

For each $P \in E(K)$ the extension $K\left([n]^{-1} P\right)/K$ is unramified outside S, by Theorem 9.9. Let $Q \in [n]^{-1} P$. Since $E[n] \subset E(K)$, $K(Q) = K\left([n]^{-1} P\right)$. This is a Galois extension of K. Let

$$\begin{array}{ccc} \mathrm{Gal}(K(Q)/K) & \longrightarrow & E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \\ \sigma & \longmapsto & \sigma(Q) - Q \end{array}.$$

This is

- a group homomorphism, since

$$\sigma\tau(Q) - Q = \sigma(\tau(Q) - Q) + \sigma(Q) - Q = \tau(Q) - Q + \sigma(Q) - Q,$$

- injective, since if $\sigma(Q) = Q$ then σ fixes $K(Q)$ pointwise, that is $\sigma = \mathrm{id}$.

Then $K(Q)/K$ is an abelian extension of exponent dividing n, unramified outside S. By Proposition 11.3, there are only finitely many possibilities for $K(Q)$, as we vary $P \in E(K)$. Let L be the composite of all such extensions of K, that is for all $P \in E(K)$. Then L/K is finite, and Galois, and $E(K)/nE(K) \to E(L)/nE(L)$ is the zero map. By Lemma 12.1, $|E(K)/nE(K)| < \infty$. ☐

Remark. If $K = \mathbb{R}, \mathbb{C}$ or $[K : \mathbb{Q}_p] < \infty$ then $|E(K)/nE(K)| < \infty$, yet $E(K)$ is not finitely generated, indeed uncountable.

12.2 The Mordell-Weil theorem

Let E/K be an elliptic curve over a number field.

Fact. There exists a quadratic form, the canonical height, $\widehat{\mathrm{h}} : E(K) \to \mathbb{R}_{\geq 0}$ with the property that

$$\#\left\{P \in E(K) \;\middle|\; \widehat{\mathrm{h}}(P) \leq B\right\} < \infty, \qquad B \geq 0. \tag{13}$$

Theorem 12.3 (Mordell-Weil)**.** *Let K be a number field, and let E/K be an elliptic curve. Then $E(K)$ is a finitely generated abelian group.*

Proof. Fix any integer $n \geq 2$. By weak Mordell-Weil, $|E(K)/nE(K)| < \infty$. Pick coset representatives $P_1, \dots, P_m$. Let

$$\Sigma = \left\{P \in E(K) \;\middle|\; \widehat{\mathrm{h}}(P) \leq \max_{1 \leq i \leq m} \widehat{\mathrm{h}}(P_i)\right\}.$$

Claim that Σ generates $E(K)$. If not there exists $P \in E(K) \setminus \{\text{subgroup generated by } \Sigma\}$ of minimal height, which exists by (13). Then $P = P_i + nQ$ for some $1 \leq i \leq m$ and $Q \in E(K)$. Note that $Q \in E(K) \setminus \{\text{subgroup generated by } \Sigma\}$. By the minimal choice of P,

$$4\widehat{\mathrm{h}}(P) \leq 4\widehat{\mathrm{h}}(Q) \leq n^2\widehat{\mathrm{h}}(Q) = \widehat{\mathrm{h}}(nQ) = \widehat{\mathrm{h}}(P - P_i) \leq \widehat{\mathrm{h}}(P - P_i) + \widehat{\mathrm{h}}(P + P_i) = 2\widehat{\mathrm{h}}(P) + 2\widehat{\mathrm{h}}(P_i),$$

by the parallelogram law, so $\widehat{\mathrm{h}}(P) \leq \widehat{\mathrm{h}}(P_i)$. By definition of Σ, $P \in \Sigma$, a contradiction to the choice of P. This proves the claim. But by (13), Σ is finite. □

Lecture 18
Wednesday
18/11/20

Remark. The structure theorem for finitely generated abelian groups shows

$$E(K) \cong E(K)_{\mathrm{tors}} \times \mathbb{Z}^r, \qquad r \geq 0,$$

where r is called the **rank**. There is no known algorithm proven to compute $\operatorname{rk} E(K)$ in all cases.

13 Heights

For simplicity take $K = \mathbb{Q}$.

13.1 Naive heights on projective space

Write $P \in \mathbb{P}^n(\mathbb{Q})$ as $P = (a_0 : \dots : a_n)$ where $a_0, \dots, a_n \in \mathbb{Z}$ such that $\gcd(a_0, \dots, a_n) = 1$.

Definition. The **height** is

$$\mathrm{H}(P) = \max_{0 \le i \le n} |a_i|.$$

Lemma 13.1. *Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be coprime homogeneous polynomials of degree d. Let*

$$\begin{array}{cccccc} F & : & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \\ & & (x_1 : x_2) & \longmapsto & (f_1(x_1, x_2) : f_2(x_1, x_2)) \end{array}.$$

Then there exist $c_1, c_2 > 0$ such that

$$c_1 \mathrm{H}(P)^d \le \mathrm{H}(F(P)) \le c_2 \mathrm{H}(P)^d, \qquad P \in \mathbb{P}^1(\mathbb{Q}).$$

Proof. Without loss of generality $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$.

- Upper bound. Write $P = (a : b)$ for $a, b \in \mathbb{Z}$ coprime. Then

$$\mathrm{H}(F(P)) \le \max(|f_1(a, b)|, |f_2(a, b)|) \le c_2 \max\left(|a|^d, |b|^d\right),$$

where c_2 is the maximum of the sum of absolute values of coefficients of f_1 and f_2, so $\mathrm{H}(F(P)) \le c_2 \mathrm{H}(P)^d$.

- Lower bound. We claim there exist $g_{ij} \in \mathbb{Z}[X_1, X_2]$ homogeneous polynomials of degree $d - 1$ and $\kappa \in \mathbb{Z}_{>0}$ such that

$$\sum_{j=1}^{2} g_{ij} f_j = \kappa X_i^{2d-1}, \qquad i = 1, 2. \tag{14}$$

Indeed running Euclid's algorithm on $f_1(X, 1)$ and $f_2(X, 1)$ gives $r, s \in \mathbb{Q}[X]$ of degree less than d such that $r(X) f_1(X, 1) + s(X) f_2(X, 1) = 1$. Homogenising and clearing denominators gives (14) with $i = 2$. Likewise for $i = 1$. Write $P = (a_1 : a_2)$ for $a_1, a_2 \in \mathbb{Z}$ coprime. By (14),

$$\sum_{j=1}^{2} g_{ij}(a_1, a_2) f_j(a_1, a_2) = \kappa a_i^{2d-1}, \qquad i = 1, 2,$$

so $\gcd(f_1(a_1, a_2), f_2(a_1, a_2))$ divides $\gcd\left(\kappa a_1^{2d-1}, \kappa a_2^{2d-1}\right) = \kappa$. But also

$$\left|\kappa a_i^{2d-1}\right| \le \max_{j=1,2} |f_j(a_1, a_2)| \sum_{j=1}^{2} |g_{ij}(a_1, a_2)| \le \kappa \mathrm{H}(F(P)) \gamma_i \mathrm{H}(P)^{d-1},$$

where γ_i is the sum of absolute values of coefficients of g_{i1} and g_{i2}. Then

$$\kappa |a_i|^{2d-1} \le \gamma_i \kappa \mathrm{H}(F(P)) \mathrm{H}(P)^{d-1}, \qquad i = 1, 2,$$

so

$$\mathrm{H}(P)^{2d-1} \le \max(\gamma_1, \gamma_2) \mathrm{H}(F(P)) \mathrm{H}(P)^{d-1}.$$

Thus

$$c_1 \mathrm{H}(P)^d = \frac{1}{\max(\gamma_1, \gamma_2)} \mathrm{H}(P)^d \le \mathrm{H}(F(P)).$$

□

Notation. For $x \in \mathbb{Q}$

$$\mathrm{H}(x) = \mathrm{H}((x : 1)) = \max(|u|, |v|), \qquad x = \frac{u}{v}, \qquad u, v \in \mathbb{Z} \text{ coprime}.$$

13.2 Naive heights on elliptic curves

Definition. The **height** is

$$\begin{array}{rcccl} \mathrm{H} & : & E(\mathbb{Q}) & \longrightarrow & \mathbb{R}_{\geq 1} \\ & & P & \longmapsto & \begin{cases} \mathrm{H}(x) & P = (x, y) \\ 1 & P = \mathcal{O}_E \end{cases} \end{array}.$$

The **logarithmic height** is

$$\begin{array}{rcccl} \mathrm{h} & : & E(\mathbb{Q}) & \longrightarrow & \mathbb{R}_{\geq 0} \\ & & P & \longmapsto & \log \mathrm{H}(P) \end{array}.$$

Lemma 13.2. *Let E and E' be elliptic curves over $\mathbb{Q}$, and let $\phi : E \to E'$ be an isogeny defined over $\mathbb{Q}$. Then there exists $c > 0$ such that*

$$|\mathrm{h}(\phi(P)) - (\deg \phi)\,\mathrm{h}(P)| \leq c, \qquad P \in E(\mathbb{Q}).$$

Note that c depends on E, E', ϕ but not on P.

Proof. Recall, by Lemma 5.3,

$$\begin{tikzcd} E \arrow[r, "\phi"] \arrow[d, "x"'] & E' \arrow[d, "x"] \\ \mathbb{P}^1 \arrow[r, "\xi"'] & \mathbb{P}^1 \end{tikzcd},$$

where $\deg \phi = \deg \xi = d$, say. By Lemma 13.1, there exist $c_1, c_2 \geq 0$ such that

$$c_1 \mathrm{H}(P)^d \leq \mathrm{H}(\phi(P)) \leq c_2 \mathrm{H}(P)^d, \qquad P \in \mathbb{P}^1(\mathbb{Q}).$$

Taking logarithms gives

$$|\mathrm{h}(\phi(P)) - d\mathrm{h}(P)| \leq \max(\log c_2, -\log c_1) = c.$$

∎

Example. Let $\phi = [2] : E \to E$. Then there exists $c > 0$ such that

$$|\mathrm{h}(2P) - 4\mathrm{h}(P)| \leq c, \qquad P \in E(\mathbb{Q}). \tag{15}$$

13.3 The canonical height quadratic form

Definition. The **canonical height** is

$$\widehat{\mathrm{h}}(P) = \lim_{n \to \infty} \frac{1}{4^n} \mathrm{h}(2^n P).$$

We check convergence. Let $m \geq n$. Then

$$\begin{aligned} \left| \frac{1}{4^m} \mathrm{h}(2^m P) - \frac{1}{4^n} \mathrm{h}(2^n P) \right| &\leq \sum_{r=n}^{m-1} \left| \frac{1}{4^{r+1}} \mathrm{h}\left(2^{r+1} P\right) - \frac{1}{4^r} \mathrm{h}(2^r P) \right| \\ &= \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} |\mathrm{h}(2(2^r P)) - 4\mathrm{h}(2^r P)| \leq c \sum_{r=n}^{\infty} \frac{1}{4^{r+1}} && \text{by (15)} \\ &= \frac{c}{4^{n+1}} \cdot \frac{1}{1 - \frac{1}{4}} = \frac{c}{3 \cdot 4^n} \to 0, && n \to \infty. \end{aligned}$$

So the sequence is Cauchy and $\widehat{\mathrm{h}}(P)$ exists.

Lemma 13.3. *$\left|\mathrm{h}(P) - \widehat{\mathrm{h}}(P)\right|$ is bounded for $P \in E(\mathbb{Q})$.*

Proof. Putting $n = 0$ in the above calculation

$$\left|\frac{1}{4^m}\mathrm{h}(2^m P) - \mathrm{h}(P)\right| \le \frac{c}{3}.$$

Take the limit as $m \to \infty$. ☐

Corollary 13.4. *For any $B > 0$, $\#\left\{P \in E(\mathbb{Q}) \;\middle|\; \widehat{h}(P) \le B\right\}$ is finite.*

Proof. If $\widehat{\mathrm{h}}(P)$ is bounded, then by Lemma 13.3, $\mathrm{h}(P)$ is bounded, so there are only finitely many possibilities for x. Each x leaves at most two choices for y. ☐

Lemma 13.5. *Let $\phi : E \to E'$ be an isogeny over $\mathbb{Q}$. Then*

$$\widehat{\mathrm{h}}(\phi(P)) = (\deg\phi)\,\widehat{\mathrm{h}}(P), \qquad P \in E(\mathbb{Q}).$$

Proof. By Lemma 13.2 there exists $c > 0$ such that $|\mathrm{h}(\phi(P)) - (\deg\phi)\,\mathrm{h}(P)| \le c$ for all $P \in E(\mathbb{Q})$. Replace P by $2^n P$, divide by 4^n, and take the limit as $n \to \infty$. ☐

Lecture 19
Friday
20/11/20

Remark.

- H and h depend on a choice of Weierstrass equation, but Lemma 13.5, with $\deg\phi = 1$, shows $\widehat{\mathrm{h}}$ does not.
- Taking $\phi = [n] : E \to E$ shows $\widehat{\mathrm{h}}(nP) = n^2\widehat{\mathrm{h}}(P)$ for all $n \in \mathbb{Z}$.

Lemma 13.6. *Let $E/\mathbb{Q}$ be an elliptic curve $y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Z}$. Then there exists $c > 0$ such that*

$$\mathrm{H}(P+Q)\,\mathrm{H}(P-Q) \le c\mathrm{H}(P)^2\,\mathrm{H}(Q)^2, \qquad P, Q \in E(\mathbb{Q}), \qquad P, Q, P \pm Q \ne \mathcal{O}_E.$$

Proof. Let $P, Q, P+Q, P-Q$ have x-coordinates $x_1, \dots, x_4$. By Lemma 5.7 there exist $w_1, w_2, w_3 \in \mathbb{Z}[x_1, x_2]$ of degree at most two in x_1 and of degree at most two in x_2 such that $(1 : x_3 + x_4 : x_3 x_4) = (w_0 : w_1 : w_2)$. Write $x_i = r_i/s_i$ for $r_i, s_i \in \mathbb{Z}$ coprime. Then

$$(s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = \left((r_1 s_2 - r_2 s_1)^2 : w_1(r_1, s_1, r_2, s_2) : w_2(r_1, s_1, r_2, s_2)\right),$$

where $s_3 s_4, r_3 s_4 + r_4 s_3, r_3 r_4$ are coprime, so

$$\begin{aligned} \mathrm{H}(P+Q)\,\mathrm{H}(P-Q) &= \max(|r_3|, |s_3|)\max(|r_4|, |s_4|) \le 2\max(|s_3 s_4|, |r_3 s_4 + r_4 s_3|, |r_3 r_4|) \\ &\le 2\max\left(|r_1 s_2 - r_2 s_1|^2, |w_1(r_1, s_1, r_2, s_2)|, |w_2(r_1, s_1, r_2, s_2)|\right) \le c\mathrm{H}(P)^2\,\mathrm{H}(Q)^2, \end{aligned}$$

where c depends on E, but not on P and Q. ☐

Theorem 13.7. *$\widehat{\mathrm{h}} : E(\mathbb{Q}) \to \mathbb{R}_{\ge 0}$ is a quadratic form.*

Proof. By Lemma 13.6 and since $|\mathrm{h}(2P) - 4\mathrm{h}(P)|$ is bounded,

$$\mathrm{h}(P+Q) + \mathrm{h}(P-Q) \le 2\mathrm{h}(P) + 2\mathrm{h}(Q) + c, \qquad P, Q \in E(\mathbb{Q}).$$

Replacing P and Q by $2^n P$ and $2^n Q$, dividing by 4^n, and taking the limit as $n \to \infty$ gives

$$\widehat{\mathrm{h}}(P+Q) + \widehat{\mathrm{h}}(P-Q) \le 2\widehat{\mathrm{h}}(P) + 2\widehat{\mathrm{h}}(Q).$$

Replacing P and Q by $P+Q$ and $P-Q$ and using $\widehat{\mathrm{h}}(2P) = 4\widehat{\mathrm{h}}(P)$ gives the reverse inequality. Thus $\widehat{\mathrm{h}}$ satisfies the parallelogram law, so $\widehat{\mathrm{h}}$ is a quadratic form. ☐

13.4 Heights on number fields

The **places** of a number field K are

- the finite places, or primes, $\left|x\right|_{\mathfrak{p}} = c^{-\mathrm{v}_{\mathfrak{p}}(x)}$ for some fixed $c > 1$, and
- the infinite places, or real and complex embeddings, $\left|x\right|_{\sigma} = \left|\sigma\left(x\right)\right|^{d}$ for some fixed $d > 0$.

For each place v we may chose a normalisation $\left|\cdot\right|_v$, that is make a choice of c and d, such that

$$\prod_v \left|\lambda\right|_v = 1, \qquad \lambda \in K^*,$$

the **product formula**.

Remark. For K a number field let $P = (a_0 : \dots : a_n) \in \mathbb{P}^n\left(K\right)$. Define

$$\mathrm{H}\left(P\right) = \prod_v \max_{0 \le i \le n} \left|a_i\right|_v .$$

This is well-defined by the product formula. All results in this section generalise from $\mathbb{Q}$ to K.

Remark. Let $\pi_i : E \times E \times E \to E$ be projection onto the i-th factor. Let $\pi_{ij} = \pi_i + \pi_j$ and $\pi_{123} = \pi_1 + \pi_2 + \pi_3$. The **theorem of the cube**, proof omitted, says that if $D \in \operatorname{Div} E$ then

$$\pi_{123}^* D + \pi_1^* D + \pi_2^* D + \pi_3^* D \sim \pi_{12}^* D + \pi_{13}^* D + \pi_{23}^* D.$$

This can be used to give alternative proofs of Theorem 5.6 and Theorem 13.7.

14 Dual isogenies and the Weil pairing

14.1 Dual isogenies

Let K be a perfect field, and let E/K be an elliptic curve.

Proposition 14.1. *Let $\Phi \subset E\left(\overline{K}\right)$ be a finite $\mathrm{Gal}\left(\overline{K}/K\right)$-stable subgroup. Then there exist an elliptic curve E'/K and a separable isogeny $\phi : E \to E'$ defined over K with kernel Φ such that every isogeny $\psi : E \to E''$ with $\Phi \subset \ker \psi$ factors uniquely in ϕ, so*

$$\begin{tikzcd} E \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & E'' \\ & E' \arrow[ur, dashed, "\exists!"'] & \end{tikzcd}.$$

Proof. Omitted. Silverman, Chapter III, Proposition 4.12. ☐

Proposition 14.2. *Let $\phi : E \to E'$ be an isogeny of degree n. Then there exists a unique isogeny $\widehat{\phi} : E' \to E$ such that $\widehat{\phi} \circ \phi = [n]$. Then $\widehat{\phi}$ is called the* ***dual isogeny****.*

Proof.

- If ϕ is separable, then $|\ker \phi| = n$, so $\ker \phi \subset E[n]$. Apply Proposition 14.1 with $\psi = [n]$.
- The case ϕ is inseparable is omitted. See Silverman, Chapter III, Theorem 6.1. For uniqueness, if $\psi_1 \circ \phi = \psi_2 \circ \phi = [n]$, then $(\psi_1 - \psi_2) \circ \phi = 0$. Since ϕ is nonconstant, so surjective on $\overline{K}$ points, $\psi_1 - \psi_2 = 0$, so $\psi_1 = \psi_2$.

☐

Remark.

- Let $E_1 \sim E_2$ if and only if E_1 and E_2 are isogenous. Then $\sim$ is an equivalence relation.
- $\deg [n] = n^2$, so $\deg \phi = \deg \widehat{\phi}$ and $\widehat{[n]} = [n]$.
- $\phi \circ \widehat{\phi} \circ \phi = \phi \circ [n]_E = [n]_{E'} \circ \phi$, so $\phi \circ \widehat{\phi} = [n]_{E'}$. In particular $\widehat{\widehat{\phi}} = \phi$.
- If $\psi : E_1 \to E_2$ and $\phi : E_2 \to E_3$ then $\widehat{\phi \circ \psi} = \widehat{\psi} \circ \widehat{\phi}$.
- If $\phi \in \mathrm{End}\, E$ then by example sheet 2, $\phi^2 - [\mathrm{Tr}\, \phi]\, \phi + [\deg \phi] = 0$, so $([\mathrm{Tr}\, \phi] - \phi) \circ \phi = [\deg \phi]$. Thus $[\mathrm{Tr}\, \phi] = \phi + \widehat{\phi}$.

Lemma 14.3. *If $\phi, \psi \in \mathrm{Hom}\,(E, E')$ then*

$$\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}.$$

Proof.

1. If $E = E'$ then this follows from $\mathrm{Tr}\,(\phi + \psi) = \mathrm{Tr}\, \phi + \mathrm{Tr}\, \psi$.
2. In general let $\alpha : E' \to E$ be any isogeny, such as $\widehat{\phi}$. By 1, $\widehat{\alpha \circ \phi + \alpha \circ \psi} = \widehat{\alpha \circ \phi} + \widehat{\alpha \circ \psi}$, so $\widehat{\alpha \circ (\phi + \psi)} = \widehat{\phi} \circ \widehat{\alpha} + \widehat{\psi} \circ \widehat{\alpha}$. Thus $\widehat{\phi + \psi} \circ \widehat{\alpha} = \left(\widehat{\phi} + \widehat{\psi}\right) \circ \widehat{\alpha}$, so $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi}$.

☐

Remark. In Silverman's book he proves Lemma 14.3 first, and uses this to show $\deg : \mathrm{Hom}\,(E, E') \to \mathbb{Z}$ is a quadratic form.

14.2 The Weil pairing

Lecture 20 Monday 23/11/20

Definition. The **sum** is

$$\begin{array}{ccccc} \mathrm{Sum} & : & \mathrm{Div}\, E & \longrightarrow & E \\ & & \sum_P n_P(P) & \longmapsto & \sum_P n_P P \end{array},$$

adding up a formal sum using the group law.

Recall there is an isomorphism

$$\begin{array}{ccc} E & \longrightarrow & \mathrm{Pic}^0 E \\ P & \longmapsto & [(P) - (\mathcal{O}_E)] \\ \sum_P n_P P & \longmapsto & \sum_P n_P(P) - \left(\sum_P n_P\right)(\mathcal{O}_E) \end{array},$$

so $\mathrm{Sum}\, D \mapsto [D]$ for all $D \in \mathrm{Div}^0 E$.

Lemma 14.4. *Let $D \in \mathrm{Div}\, E$. Then $D \sim 0$ if and only if $\deg D = 0$ and $\mathrm{Sum}\, D = \mathcal{O}_E$.*

Let $\phi : E \to E'$ be an isogeny of degree n with dual isogeny $\widehat{\phi} : E' \to E$. Assume $\mathrm{ch}\, K \neq n$, so ϕ and ϕ' are separable. We define the **Weil pairing**

$$\mathrm{e}_\phi : E[\phi] \times E'\left[\widehat{\phi}\right] \to \mu_n.$$

Let $T \in E'\left[\widehat{\phi}\right]$. Then $nT = \mathcal{O}$. So there exists $f \in \overline{K}(E')^*$ such that

$$\mathrm{div}\, f = n(T) - n(\mathcal{O}).$$

Pick $T_0 \in E(K)$ with $\phi(T_0) = T$. Then

$$\phi^*(T) - \phi^*(\mathcal{O}) = \sum_{P \in E[\phi]} (P + T_0) - \sum_{P \in E[\phi]} (P)$$

has sum $nT_0 = \widehat{\phi}(\phi(T_0)) = \widehat{\phi}(T) = \mathcal{O}$. So there exists $g \in \overline{K}(E)^*$ such that

$$\mathrm{div}\, g = \phi^*(T) - \phi^*(\mathcal{O}).$$

Now

$$\mathrm{div}(\phi^* f) = \phi^*(\mathrm{div}\, f) = n(\phi^*(T) - \phi^*(\mathcal{O})) = \mathrm{div}\, g^n,$$

so $\phi^* f = cg^n$ for some $c \in \overline{K}^*$. Rescaling f, without loss of generality $c = 1$, that is $\phi^* f = g^n$. If $S \in E[\phi]$ then $\phi \circ \tau_S = \phi$, so $\tau_S^* \circ \phi^* = \phi^*$. Then $\tau_S^*(\mathrm{div}\, g) = \mathrm{div}\, g$, so $\tau_S^* g = \zeta g$ for some $\zeta \in \overline{K}^*$. Thus

$$\zeta = \frac{g(X+S)}{g(X)}, \qquad X \in E\left(\overline{K}\right) \setminus \{\text{zeros and poles of } g\}.$$

Now

$$\zeta^n = \frac{g(X+S)^n}{g(X)^n} = \frac{f(\phi(X+S))}{f(\phi(X))} = 1,$$

since $S \in E[\phi]$, so $\zeta \in \mu_n$. We define

$$\mathrm{e}_\phi(S, T) = \frac{g(X+S)}{g(X)}.$$

Proposition 14.5. e_ϕ *is bilinear and nondegenerate.*

Proof.

- Linearity in first argument, since

$$\mathrm{e}_\phi(S_1 + S_2, T) = \frac{g(X + S_1 + S_2)}{g(X + S_2)} \cdot \frac{g(X + S_2)}{g(X)} = \mathrm{e}_\phi(S_1, T)\, \mathrm{e}_\phi(S_2, T).$$

- Linearity in second argument. Let $T_1, T_2 \in E'\left[\widehat{\phi}\right]$, and let
$$\operatorname{div} f_1 = n\left(T_1\right) - n\left(\mathcal{O}\right), \qquad \operatorname{div} f_2 = n\left(T_2\right) - n\left(\mathcal{O}\right), \qquad \phi^* f_1 = g_1^n, \qquad \phi^* f_2 = g_2^n.$$
There exists $h \in \overline{K}\left(E'\right)^*$ such that
$$\operatorname{div} h = \left(T_1\right) + \left(T_2\right) - \left(T_1 + T_2\right) - \left(\mathcal{O}\right).$$
Then put $f = f_1 f_2 / h^n$ and $g = g_1 g_2 / \phi^* h$. Check that
$$\operatorname{div} f = n\left(T_1 + T_2\right) - n\left(\mathcal{O}\right), \qquad \phi^* f = \frac{\phi^* f_1 \phi^* f_2}{\left(\phi^* h\right)^n} = \left(\frac{g_1 g_2}{\phi^* h}\right)^n = g^n,$$
so
$$\mathrm{e}_\phi\left(S, T_1 + T_2\right) = \frac{g\left(X + S\right)}{g\left(X\right)} = \frac{g_1\left(X + S\right)}{g_1\left(X\right)} \cdot \frac{g_2\left(X + S\right)}{g_2\left(X\right)} \cdot \frac{h\left(\phi\left(X\right)\right)}{h\left(\phi\left(X + S\right)\right)} = \mathrm{e}_\phi\left(S, T_1\right) \mathrm{e}_\phi\left(S, T_2\right),$$
since $S \in E\left[\phi\right]$.

- e_ϕ is nondegenerate. Fix $T \in E'\left[\widehat{\phi}\right]$. Suppose $\mathrm{e}_\phi\left(S, T\right) = 1$ for all $S \in E\left[\phi\right]$, so $\tau_S^* g = g$ for all $S \in E\left[\phi\right]$. Then $\overline{K}\left(E\right) / \phi^*\left(\overline{K}\left(E'\right)\right)$ is a Galois extension with Galois group $E\left[\phi\right]$. Note that $S \in E\left[\phi\right]$ acts as τ_S^*. Then $g = \phi^* h$ for some $h \in \overline{K}\left(E'\right)$, so $\phi^* f = g^n = \left(\phi^* h\right)^n = \phi^* h^n$, so $f = h^n$, so $\operatorname{div} h = \left(T\right) - \left(\mathcal{O}\right)$, so $T = \mathcal{O}$. We have shown the injection
$$\begin{array}{rcl} E'\left[\widehat{\phi}\right] & \longrightarrow & \operatorname{Hom}\left(E\left[\phi\right], \mu_n\right) \\ T & \longmapsto & \left(S \mapsto \mathrm{e}_\phi\left(S, T\right)\right) \end{array}.$$
This map is an isomorphism since $\# E\left[\phi\right] = \# E'\left[\widehat{\phi}\right] = n$.

$\square$

Remark.

- If E, E', ϕ are defined over K then e_ϕ is **Galois equivariant**, that is
$$\mathrm{e}_\phi\left(\sigma\left(S\right), \sigma\left(T\right)\right) = \sigma\left(\mathrm{e}_\phi\left(S, T\right)\right), \qquad \sigma \in \operatorname{Gal}\left(\overline{K} / K\right), \qquad S \in E\left[\phi\right], \qquad T \in E'\left[\widehat{\phi}\right].$$

- Taking $\phi = \left[n\right] : E \to E$, so $\widehat{\phi} = \left[n\right]$, gives
$$\mathrm{e}_n : E\left[n\right] \times E\left[n\right] \to \mu_n,$$
since e_n is bilinear.

Corollary 14.6. *If $E\left[n\right] \subset E\left(K\right)$ then $\mu_n \subset K$.*

Proof. Since e_n is nondegenerate, there exist $S, T \in E\left[n\right]$ such that $\mathrm{e}_n\left(S, T\right)$ is a primitive n-th root of unity, say ζ_n. To see this pick $T \in E\left[n\right]$ of order n. The group homomorphism
$$\begin{array}{rcl} E\left[n\right] & \longrightarrow & \mu_n \\ S & \longmapsto & \mathrm{e}_n\left(S, T\right) \end{array}$$
has image μ_d for some $d \mid n$. Then $\mathrm{e}_n\left(S, dT\right) = 1$ for all $S \in E\left[n\right]$. Since e_n is nondegenerate, $dT = 0$, so $d = n$. Then
$$\sigma\left(\zeta_n\right) = \mathrm{e}_n\left(\sigma\left(S\right), \sigma\left(T\right)\right) = \mathrm{e}_n\left(S, T\right) = \zeta_n, \qquad \sigma \in \operatorname{Gal}\left(\overline{K} / K\right),$$
by Galois equivariance and since $S, T \in E\left(K\right)$. Thus $\zeta_n \in K$. $\square$

Example. There does not exist $E / \mathbb{Q}$ such that $E\left(\mathbb{Q}\right)_{\text{tors}} \cong \left(\mathbb{Z} / 3\mathbb{Z}\right)^2$.

Remark. In fact the Weil pairing e_n is **alternating**, that is $\mathrm{e}_n\left(T, T\right) = 1$ for all $T \in E\left[n\right]$. In particular expanding $\mathrm{e}_n\left(S + T, S + T\right)$, show $\mathrm{e}_n\left(S, T\right) = \mathrm{e}_n\left(T, S\right)^{-1}$.

15 Galois cohomology

15.1 Group cohomology

Lecture 21 Wednesday 25/11/20

Let G be a group, and let A be a G-**module**, that is an abelian group with an action of G via group homomorphisms, or a $\mathbb{Z}[G]$-module.

Definition. The **zeroth cohomology group** is

$$\mathrm{H}^0(G, A) = A^G = \{a \in A \mid \forall \sigma \in G,\ \sigma(a) = a\}.$$

The **cochains**

$$\mathrm{C}^1(G, A) = \{\text{maps } G \to A\}$$

contains the **cocycles**

$$\mathrm{Z}^1(G, A) = \left\{(a_\sigma)_{\sigma \in G} \mid a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\right\},$$

which contains the **coboundaries**

$$\mathrm{B}^1(G, A) = \left\{(\sigma(b) - b)_{\sigma \in G} \mid b \in A\right\}.$$

The **first cohomology group** is

$$\mathrm{H}^1(G, A) = \mathrm{Z}^1(G, A) / \mathrm{B}^1(G, A).$$

Remark. If G acts trivially on A then $\mathrm{H}^1(G, A) = \mathrm{Hom}(G, A)$.

Theorem 15.1. *A short exact sequence of G-modules*

$$0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0$$

gives rise to a long exact sequence of abelian groups

$$0 \to A^G \xrightarrow{\phi} B^G \xrightarrow{\psi} C^G \xrightarrow{\delta} \mathrm{H}^1(G, A) \xrightarrow{\phi_*} \mathrm{H}^1(G, B) \xrightarrow{\psi_*} \mathrm{H}^1(G, C).$$

Proof. Omitted except the definition of δ. Let $c \in C^G$. There exists $b \in B$ such that $\psi(b) = c$. Then $\psi(\sigma(b) - b) = \sigma(c) - c = 0$ for all $\sigma \in G$, so $\sigma(b) - b = \phi(a_\sigma)$ for some $a_\sigma \in A$. Then

$$\phi(a_{\sigma\tau} - \sigma(a_\tau) - a_\sigma) = \sigma\tau(b) - b - \sigma(\tau(b) - b) - (\sigma(b) - b) = 0,$$

so $a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma$. Thus $(a_\sigma)_{\sigma \in G} \in \mathrm{Z}^1(G, A)$. We define

$$\delta(c) = \left[(a_\sigma)_{\sigma \in G}\right] \in \mathrm{H}^1(G, A).$$

□

Theorem 15.2. *Let A be a G-module and $H \lhd G$ a normal subgroup. There is an* ***inflation-restriction*** *exact sequence*

$$0 \to \mathrm{H}^1\left(G/H, A^H\right) \xrightarrow{\mathrm{inf}} \mathrm{H}^1(G, A) \xrightarrow{\mathrm{res}} \mathrm{H}^1(H, A).$$

Proof. Omitted. □

15.2 Galois cohomology

Let K be a perfect field. Then $\mathrm{Gal}\left(\overline{K}/K\right)$ is a topological group with basis of open subgroups the $\mathrm{Gal}\left(\overline{K}/L\right)$ for $[L : K] < \infty$. If $G = \mathrm{Gal}\left(\overline{K}/K\right)$ we modify the definition of $\mathrm{H}^1(G, A)$ by insisting

- the stabiliser of each $a \in A$ is an open subgroup of G, and
- all cochains $G \to A$ are continuous where A is given the discrete topology.

Then

$$\mathrm{H}^1\left(\mathrm{Gal}\left(\overline{K}/K\right), A\right) = \varinjlim_{L/K \text{ finite Galois extension}} \mathrm{H}^1\left(\mathrm{Gal}(L/K), A^{\mathrm{Gal}\left(\overline{K}/L\right)}\right),$$

where the direct limit is with respect to inflation maps.

Theorem (Hilbert's theorem 90). *Let L/K be a finite Galois extension. Then*
$$\mathrm{H}^1\left(\mathrm{Gal}\left(L/K\right), L^*\right) = 0.$$

Proof. Let $G = \mathrm{Gal}\left(L/K\right)$. Let $\left(a_\sigma\right)_{\sigma \in G} \in \mathrm{Z}^1\left(G, L^*\right)$. Distinct automorphisms are linearly independent, so there exists $y \in L$ such that $x = \sum_{\tau \in G} a_\tau^{-1} \tau\left(y\right) \ne 0$. For $\sigma \in G$, $a_{\sigma\tau} = \sigma\left(a_\tau\right) a_\sigma$, so $\sigma\left(a_\tau\right)^{-1} = a_\sigma a_{\sigma\tau}^{-1}$. Then
$$\sigma\left(x\right) = \sum_{\tau \in G} \sigma\left(a_\tau\right)^{-1} \sigma\tau\left(y\right) = a_\sigma \sum_{\tau \in G} a_{\sigma\tau}^{-1} \sigma\tau\left(y\right) = a_\sigma x,$$
so $a_\sigma = \sigma\left(x\right)/x$. Thus $\left(a_\sigma\right)_{\sigma \in G} \in \mathrm{B}^1\left(G, L^*\right)$, so $\mathrm{H}^1\left(G, L^*\right) = 0$. ☐

A corollary is
$$\mathrm{H}^1\left(\mathrm{Gal}\left(\overline{K}/K\right), \overline{K}^*\right) = 0.$$

15.3 Application to Kummer theory

Assume $\mathrm{ch}\, K \nmid n$. There is an exact sequence of $\mathrm{Gal}\left(\overline{K}/K\right)$-modules
$$0 \to \mu_n \to \overline{K}^* \xrightarrow{x \mapsto x^n} \overline{K}^* \to 0.$$

The long exact sequence is
$$K^* \xrightarrow{x \mapsto x^n} K^* \to \mathrm{H}^1\left(\mathrm{Gal}\left(\overline{K}/K\right), \mu_n\right) \to \mathrm{H}^1\left(\mathrm{Gal}\left(\overline{K}/K\right), \overline{K}^*\right) = 0,$$
by Hilbert 90, so $\mathrm{H}^1\left(\mathrm{Gal}\left(\overline{K}/K\right), \mu_n\right) \cong K^*/\left(K^*\right)^n$. If $\mu_n \subset K$ then
$$\mathrm{Hom}_{\mathrm{cts}}\left(\mathrm{Gal}\left(\overline{K}/K\right), \mu_n\right) \cong K^*/\left(K^*\right)^n. \tag{16}$$

If L/K is a finite Galois extension then $\pi : \mathrm{Gal}\left(\overline{K}/K\right) \twoheadrightarrow \mathrm{Gal}\left(L/K\right)$, so there is an injection
$$\begin{array}{rcl} \mathrm{Hom}\left(\mathrm{Gal}\left(L/K\right), \mu_n\right) & \longrightarrow & \mathrm{Hom}_{\mathrm{cts}}\left(\mathrm{Gal}\left(\overline{K}/K\right), \mu_n\right) \\ \chi & \longmapsto & \chi \circ \pi \end{array}.$$

We claim that every finite subgroup Ξ of $\mathrm{Hom}_{\mathrm{cts}}\left(\mathrm{Gal}\left(\overline{K}/K\right), \mu_n\right)$ arises uniquely in this way for L/K a finite abelian extension of exponent dividing n. So from (16) we recover Theorem 11.2. To prove the claim, consider the pairing
$$\begin{array}{rcl} \mathrm{Gal}\left(\overline{K}/K\right) \times \Xi & \longrightarrow & \mu_n \\ \left(\sigma, \chi\right) & \longmapsto & \chi\left(\sigma\right) \end{array}.$$

This is bilinear, has trivial right kernel, and left kernel is $\bigcap_{\chi \in \Xi} \ker \chi \subset \mathrm{Gal}\left(\overline{K}/K\right)$, an open normal subgroup, so $\bigcap_{\chi \in \Xi} \ker \chi = \mathrm{Gal}\left(\overline{K}/L\right)$ for some L/K finite Galois. We get a nondegenerate pairing $\mathrm{Gal}\left(L/K\right) \times \Xi \to \mu_n$. In particular $\mathrm{Gal}\left(L/K\right) \hookrightarrow \mathrm{Hom}\left(\Xi, \mu_n\right)$, so L/K is abelian of exponent dividing n, and $\Xi \hookrightarrow \mathrm{Hom}\left(\mathrm{Gal}\left(L/K\right), \mu_n\right)$. This proves the claim.

Notation. $\mathrm{H}^1\left(K, -\right)$ means $\mathrm{H}^1\left(\mathrm{Gal}\left(\overline{K}, K\right), -\right)$.

Lemma 15.3. *Let $\left[K : \mathbb{Q}_p\right] < \infty$ with $p \nmid n$. Then*
$$\ker\left(\mathrm{H}^1\left(K, \mu_n\right) \to \mathrm{H}^1\left(K^{\mathrm{ur}}, \mu_n\right)\right) \cong \mathcal{O}_K^\times/\left(\mathcal{O}_K^\times\right)^n.$$

Proof. By Hilbert 90 it suffices to show the sequence
$$0 \to \mathcal{O}_K^\times/\left(\mathcal{O}_K^\times\right)^n \xrightarrow{\alpha} K^*/\left(K^*\right)^n \xrightarrow{\beta} \left(K^{\mathrm{ur}}\right)^*/\left(\left(K^{\mathrm{ur}}\right)^*\right)^n$$
is exact.

$\mathrm{im}\,\alpha \subset \ker\beta$. Let $a \in \mathcal{O}_K^\times$. If $f\left(x\right) = x^n - a \in \mathcal{O}_K\left[x\right]$ then $\widetilde{f}\left(x\right) = x^n - \widetilde{a} \in k\left[x\right]$ has distinct roots in $\overline{k}$, using $p \nmid n$ here. Then $K\left(\sqrt[n]{a}\right)/K$ is unramified, so $a \in \left(\left(K^{\mathrm{ur}}\right)^*\right)^n$.

$\ker\beta \subset \mathrm{im}\,\alpha$. Let $x\left(K^*\right)^n \in \ker\beta$. Write $x = u\pi^r$ with $u \in \mathcal{O}_K^\times$ and $r \in \mathbb{Z}$. Since the discrete valuation in K extends to K^{ur} we have $r \equiv 0 \mod n$, so $x\left(K^*\right)^n = u\left(K^*\right)^n$.

☐

15.4 The Selmer and Tate-Shafarevich groups

Lecture 22 Friday 27/11/20

Let $\phi : E \to E'$ be an isogeny of elliptic curves over K. There is a short exact sequence of $\mathrm{Gal}\left(\overline{K}/K\right)$-modules

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0.$$

The long exact sequence is

$$E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} \mathrm{H}^1(K, E[\phi]) \to \mathrm{H}^1(K, E) \xrightarrow{\phi_*} \mathrm{H}^1(K, E').$$

We get a short exact sequence

$$0 \to E'(K)/\phi(E(K)) \xrightarrow{\delta} \mathrm{H}^1(K, E[\phi]) \to \mathrm{H}^1(K, E)[\phi_*] \to 0.$$

Now take K a number field. For each place v fix an embedding $\overline{K} \subset \overline{K_v}$. Then $\mathrm{Gal}\left(\overline{K_v}/K_v\right) \subset \mathrm{Gal}\left(\overline{K}/K\right)$, so

$$\begin{tikzcd}
0 \arrow[r] & E'(K)/\phi(E(K)) \arrow[r, "\delta"] \arrow[d] & \mathrm{H}^1(K, E[\phi]) \arrow[r] \arrow[d, "\mathrm{res}_v"'] \arrow[dr, dashed] & \mathrm{H}^1(K, E)[\phi_*] \arrow[r] \arrow[d, "\mathrm{res}_v"] & 0 \\
0 \arrow[r] & \prod_v E'(K_v)/\phi(E(K_v)) \arrow[r, "\delta_v"'] & \prod_v \mathrm{H}^1(K_v, E[\phi]) \arrow[r] & \prod_v \mathrm{H}^1(K_v, E)[\phi_*] \arrow[r] & 0
\end{tikzcd}.$$

Definition. The **ϕ-Selmer group** is

$$\begin{aligned} \mathrm{S}^{(\phi)}(E/K) &= \ker\left(\mathrm{H}^1(K, E[\phi]) \to \prod_v \mathrm{H}^1(K_v, E)\right) \\ &= \left\{\alpha \in \mathrm{H}^1(K, E[\phi]) \;\middle|\; \forall v,\ \mathrm{res}_v(\alpha) \in \operatorname{im}\delta_v\right\}. \end{aligned}$$

The **Tate-Shafarevich group** is

$$Ш(E/K) = \ker\left(\mathrm{H}^1(K, E) \to \prod_v \mathrm{H}^1(K_v, E)\right).$$

We get a short exact sequence

$$0 \to E'(K)/\phi(E(K)) \to \mathrm{S}^{(\phi)}(E/K) \to Ш(E/K)[\phi_*] \to 0.$$

Taking $\phi = [n]$ gives

$$0 \to E(K)/nE(K) \to \mathrm{S}^{(n)}(E/K) \to Ш(E/K)[n] \to 0.$$

Re-organising the proof of weak Mordell-Weil gives the following.

Theorem 15.4. *$\mathrm{S}^{(n)}(E/K)$ is finite.*

Proof. For L/K a finite Galois extension there is an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(\mathrm{Gal}(L/K), E(L)[n]) \arrow[r, "\mathrm{inf}"] & \mathrm{H}^1(K, E[n]) \arrow[r, "\mathrm{res}"] & \mathrm{H}^1(L, E[n]) \\
& & \mathrm{S}^{(n)}(E/K) \arrow[r] \arrow[u, phantom, "\cup"] & \mathrm{S}^{(n)}(E/L) \arrow[u, phantom, "\cup"]
\end{tikzcd},$$

where $\mathrm{H}^1(\mathrm{Gal}(L/K), E(L)[n])$ is finite. By extending our field we may assume $E[n] \subset E(K)$, and hence $\mu_n \subset K$, so $E[n] \cong \mu_n \times \mu_n$ as a Galois module. By Hilbert 90,

$$\mathrm{H}^1(K, E[n]) \cong \mathrm{H}^1(K, \mu_n) \times \mathrm{H}^1(K, \mu_n) \cong K^*/(K^*)^n \times K^*/(K^*)^n.$$

Let

$$S = \{\text{primes of bad reduction for } E/K\} \cup \{v \mid n\infty\}.$$

Note that this is a finite set of places. Define the subgroup of $\mathrm{H}^1(K, A)$ unramified outside S by

$$\mathrm{H}^1(K, A; S) = \ker\left(\mathrm{H}^1(K, A) \to \prod_{v \notin S} \mathrm{H}^1(K_v^{\mathrm{ur}}, A)\right).$$

There is a commutative diagram with exact rows

$$\begin{array}{ccccc} E(K_v) & \xrightarrow{\cdot n} & E(K_v) & \xrightarrow{\delta_v} & \mathrm{H}^1(K_v, E[n]) \\ \cap & & \cap & & \downarrow{\scriptstyle \mathrm{res}} \\ E(K_v^{\mathrm{ur}}) & \xrightarrow[\cdot n]{} & E(K_v^{\mathrm{ur}}) & \xrightarrow[0]{} & \mathrm{H}^1(K_v^{\mathrm{ur}}, E[n]) \end{array}.$$

The map $\cdot n : E(K_v^{\mathrm{ur}}) \to E(K_v^{\mathrm{ur}})$ is surjective for all $v \notin S$, by the proof of Theorem 9.9, so $\operatorname{im} \delta_v \subset \ker \mathrm{res}$. Then

$$\begin{aligned} \mathrm{S}^{(n)}(E/K) &= \left\{\alpha \in \mathrm{H}^1(K, E[n]) \;\middle|\; \forall v,\ \mathrm{res}_v(\alpha) \in \operatorname{im} \delta_v\right\} \\ &\subset \mathrm{H}^1(K, E[n]; S) \cong \mathrm{H}^1(K, \mu_n; S) \times \mathrm{H}^1(K, \mu_n; S) \cong K(S, n) \times K(S, n), \end{aligned}$$

by Lemma 15.3, noting that $\{v \mid n\} \subset S$. But $K(S, n)$ is finite by Lemma 11.4, so $\mathrm{S}^{(n)}(E/K)$ is finite. ☐

Remark. $\mathrm{S}^{(n)}(E/K)$ is finite and effectively computable. It is conjectured that $|Ш(E/K)| < \infty$. This would imply that $\operatorname{rk} E(K)$ is effectively computable.

16 Descent by cyclic isogeny

16.1 Descent by n-isogeny

Let E and E' be elliptic curves over a number field K, and let $\phi : E \to E'$ be an isogeny of degree n. Suppose $E'\left[\widehat{\phi}\right] \cong \mathbb{Z}/n\mathbb{Z}$ is generated by $T \in E'(K)$. Then there is an isomorphism of Galois modules

$$\begin{array}{rcl} E[\phi] & \longrightarrow & \mu_n \\ S & \longmapsto & \mathrm{e}_\phi(S,T) \end{array}.$$

The short exact sequence of $\mathrm{Gal}\left(\overline{K}/K\right)$-modules

$$0 \to \mu_n \to E \xrightarrow{\phi} E' \to 0$$

gives a long exact sequence

$$\begin{tikzcd} E(K) \arrow[r] & E'(K) \arrow[r, "\delta"] \arrow[dr, "\alpha"'] & \mathrm{H}^1(K,\mu_n) \arrow[r] \arrow[d, "\sim"', "\text{Hilbert 90}"] & \mathrm{H}^1(K,E) \\ & & K^*/(K^*)^n & \end{tikzcd}.$$

Theorem 16.1. *Let $f \in K(E')$ and $g \in K(E)$ with $\operatorname{div} f = n(T) - n(\mathcal{O})$ and $\phi^* f = g^n$. Then*

$$\alpha(P) = f(P) \mod (K^*)^n, \qquad P \in E'(K) \setminus \{\mathcal{O}, T\}.$$

Proof. Let $Q \in \phi^{-1}(P)$. Then $\delta(P)$ is represented by the cocycle $\sigma \mapsto \sigma(Q) - Q \in E[\phi] \cong \mu_n$. For any $X \in E$ not a zero or pole of g, then taking $X = Q$,

$$\mathrm{e}_\phi(\sigma(Q) - Q, T) = \frac{g(\sigma(Q) - Q + X)}{g(X)} = \frac{g(\sigma(Q))}{g(Q)} = \frac{\sigma(g(Q))}{g(Q)} = \frac{\sigma\left(\sqrt[n]{f(P)}\right)}{\sqrt[n]{f(P)}},$$

noting that $f(P) = g(Q)^n$. Then $\delta(P)$ is represented by the cocycle $\sigma \mapsto \sigma\left(\sqrt[n]{f(P)}\right) / \sqrt[n]{f(P)}$. But there is an isomorphism

$$\begin{array}{rcl} K^*/(K^*)^n & \longrightarrow & \mathrm{H}^1(K,\mu_n) \\ x & \longmapsto & \left(\sigma \mapsto \dfrac{\sigma\left(\sqrt[n]{x}\right)}{\sqrt[n]{x}}\right) \end{array},$$

so $\alpha(P) = f(P) \mod (K^*)^n$. ☐

16.2 Descent by 2-isogeny

Lecture 23 Monday 30/11/20

Let E be $y^2 = x\left(x^2 + ax + b\right)$ where $b\left(a^2 - 4b\right) \neq 0$, let E' be $y^2 = x\left(x^2 + a'x + b'\right)$ where $a' = -2a$ and $b' = a^2 - 4b$, and let

$$\begin{array}{rrcl} \phi : & E & \longrightarrow & E' \\ & (x,y) & \longmapsto & \left(\left(\dfrac{y}{x}\right)^2, \dfrac{y\left(x^2 - b\right)}{x^2}\right) \end{array}, \qquad \begin{array}{rrcl} \widehat{\phi} : & E' & \longrightarrow & E \\ & (x,y) & \longmapsto & \left(\dfrac{1}{4}\left(\dfrac{y}{x}\right)^2, \dfrac{y\left(x^2 - b\right)}{8x^2}\right) \end{array}.$$

Then $E[\phi] = \{\mathcal{O}, T\}$ where $T = (0,0) \in E(K)$ and $E'\left[\widehat{\phi}\right] = \{\mathcal{O}, T'\}$ where $T' = (0,0) \in E'(K)$.

Proposition 16.2. *There is a group homomorphism*

$$\begin{array}{rcl} E'(K) & \longrightarrow & K^*/(K^*)^2 \\ (x,y) & \longmapsto & \begin{cases} x \mod (K^*)^2 & x \neq 0 \\ b' \mod (K^*)^2 & x = 0 \end{cases} \end{array},$$

with kernel $\phi(E(K))$.

Proof. Either apply Theorem 16.1 with $f = x \in K(E')$ and $g = y/x \in K(E)$, or direct calculation. See example sheet 4. ☐

Let

$$\alpha_E : E(K)/\widehat{\phi}(E'(K)) \hookrightarrow K^*/(K^*)^2, \qquad \alpha_{E'} : E'(K)/\phi(E(K)) \hookrightarrow K^*/(K^*)^2.$$

Lemma 16.3.

$$2^{\operatorname{rk} E(K)} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4}.$$

Proof. If $f : A \to B$ and $g : B \to C$ are homomorphisms of abelian groups then there is an exact sequence

$$0 \to \ker f \to \ker gf \xrightarrow{f} \ker g \to \operatorname{coker} f \xrightarrow{g} \operatorname{coker} gf \to \operatorname{coker} g \to 0.$$

Since $\widehat{\phi} \circ \phi = [2]_E$ we get an exact sequence

$$\begin{tikzcd}
 & \mathbb{Z}/2\mathbb{Z} & & \mathbb{Z}/2\mathbb{Z} \\
0 \arrow[r] & E(K)[\phi] \arrow[u, phantom, "\wr\|"] \arrow[r] & E(K)[2] \arrow[r, "\phi"] & E'(K)\left[\widehat{\phi}\right] \arrow[u, phantom, "\wr\|"] \arrow[dll, rounded corners] \\
 & E'(K)/\phi(E(K)) \arrow[r, "\widehat{\phi}"'] \arrow[d, phantom, "\cong"] & E(K)/2E(K) \arrow[r] & E(K)/\widehat{\phi}(E'(K)) \arrow[r] \arrow[d, phantom, "\cong"] & 0 \\
 & \operatorname{im}\alpha_{E'} & & \operatorname{im}\alpha_E
\end{tikzcd},$$

so $|E(K)/2E(K)|/|E(K)[2]| = |\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|/2 \cdot 2$. By the Mordell-Weil theorem, $E(K) \cong \Delta \times \mathbb{Z}^r$ for Δ a finite group and $r = \operatorname{rk} E(K)$, so $E(K)/2E(K) \cong \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r$ and $E(K)[2] \cong \Delta[2]$. Then $\Delta/2\Delta$ and $\Delta[2]$ have the same order, since Δ is finite. Thus $|E(K)/2E(K)|/|E(K)[2]| = 2^r$. ☐

Lemma 16.4. *If K is a number field and $a, b \in \mathcal{O}_K$ then $\operatorname{im}\alpha_E \subset K(S, 2)$ where $S = \{$primes dividing $b\}$.*

Proof. Must show that if $x, y \in K$ such that $y^2 = x\left(x^2 + ax + b\right)$ and $v_{\mathfrak{p}}(b) = 0$ then $v_{\mathfrak{p}}(x) \equiv 0 \mod 2$.

$v_{\mathfrak{p}}(x) < 0$. By Lemma 9.1, $v_{\mathfrak{p}}(x) = -2r$ and $v_{\mathfrak{p}}(y) = -3r$ for some $r \geq 1$.

$v_{\mathfrak{p}}(x) > 0$. Since $v_{\mathfrak{p}}\left(x^2 + ax + b\right) = 0$, $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}\left(y^2\right) = 2v_{\mathfrak{p}}(y)$.

☐

Lemma 16.5. *If $b_1 b_2 = b$ then $b_1 (K^*)^2 \in \operatorname{im}\alpha_E$ if and only if*

$$w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4 \tag{17}$$

is soluble for $u, v, w \in K$ not all zero.

Proof. If $b_1 \in (K^*)^2$ or $b_2 \in (K^*)^2$ then both conditions are satisfied. So we may assume $b_1, b_2 \notin (K^*)^2$. Then $b_1 (K^*)^2 \in \operatorname{im}\alpha_E$ if and only if there exists $(x, y) \in E(K)$ such that $x = b_1 t^2$ for some $t \in K^*$, so $y^2 = b_1 t^2 \left(\left(b_1 t^2\right)^2 + a b_1 t^2 + b\right)$, so $(y/b_1 t)^2 = b_1 t^4 + a t^2 + b_2$. So (17) has a solution $u = t$, $v = 1$, and $w = y/b_1 t$. Conversely if (u, v, w) is a solution to (17) then $uv \neq 0$ and $\left(b_1 (u/v)^2, b_1 \left(uw/v^3\right)\right) \in E(K)$. ☐

Now take $K = \mathbb{Q}$. Then

$$\begin{tikzcd}
0 \arrow[r] & E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \arrow[r, "\delta"] \arrow[dr, "\alpha_{E'}"'] & \mathrm{S}^{(\phi)}(E/\mathbb{Q}) \arrow[r] \arrow[d, phantom, "\cap"] & Ш(E/\mathbb{Q})[\phi_*] \arrow[r] & 0 \\
 & & \mathbb{Q}^*/(\mathbb{Q}^*)^n & &
\end{tikzcd},$$

so

$$\operatorname{im}\alpha_{E'} = \left\{ b_1 (\mathbb{Q}^*)^2 \;\middle|\; (17)' \text{ is soluble over } \mathbb{Q} \right\}$$

is contained in

$$\mathrm{S}^{(\phi)}(E/\mathbb{Q}) = \left\{ b_1 (\mathbb{Q}^*)^2 \;\middle|\; (17)' \text{ is soluble over } \mathbb{R} \text{ and over } \mathbb{Q}_p \text{ for all primes } p \right\},$$

where $(17)'$ means (17) with a and b replaced by a' and b'.

Fact. If $a, b_1, b_2 \in \mathbb{Z}$ and $p \nmid 2b\left(a^2 - 4b\right)$ then (17) is soluble over $\mathbb{Q}_p$. Uses example sheet 3, question 9 and Hensel's lemma.

Example. Let E be $y^2 = x^3 - x$, so $a = 0$ and $b = -1$. Then $\operatorname{im} \alpha_E = \langle -1 \rangle \subset \mathbb{Q}^* / \left(\mathbb{Q}^*\right)^2$. Let E' be $y^2 = x^3 + 4x$. Then $\operatorname{im} \alpha_{E'} \subset \langle -1, 2 \rangle \subset \mathbb{Q}^* / \left(\mathbb{Q}^*\right)^2$.

- If $b_1 = -1$, then $w^2 = -u^4 - 4v^4$ is insoluble over $\mathbb{R}$.
- If $b_1 = 2$, then $w^2 = 2u^4 + 2v^4$ has solution $(u, v, w) = (1, 1, 2)$.
- If $b_1 = -2$, then $w^2 = -2u^4 - 2v^4$ is insoluble over $\mathbb{R}$.

Thus $\operatorname{im} \alpha_{E'} = \langle 2 \rangle \subset \mathbb{Q}^* / \left(\mathbb{Q}^*\right)^2$. Thus $\operatorname{rk} E(\mathbb{Q}) = 0$, so 1 is not a congruent number.

Lecture 24 Wednesday 02/12/20

Example. Let E be $y^2 = x^3 + px$ for $p \equiv 5 \mod 8$ prime. If $b_1 = -1$, then $w^2 = -u^4 - pv^4$ is insoluble over $\mathbb{R}$. Thus $\operatorname{im} \alpha_E = \langle p \rangle \subset \mathbb{Q}^* / \left(\mathbb{Q}^*\right)^2$. Let E' be $y^2 = x^3 - 4px$. Then $\operatorname{im} \alpha_{E'} \subset \langle -1, 2, p \rangle \subset \mathbb{Q}^* / \left(\mathbb{Q}^*\right)^2$. Note that $\alpha_{E'}\left(T'\right) = -4p\left(\mathbb{Q}^*\right)^2 = -p\left(\mathbb{Q}^*\right)^2$.

- If $b_1 = 2$, then $w^2 = 2u^4 - 2pv^4$. Suppose this is soluble. Without loss of generality $u, v, w \in \mathbb{Z}$ such that $\gcd(u, v) = 1$. If $p \mid u$ then $p \mid w$ and then $p \mid v$, a contradiction. Then $w^2 \equiv 2u^4 \not\equiv 0 \mod p$, so $\left(\frac{2}{p}\right) = 1$, a contradiction since $p \equiv 5 \mod 8$.
- If $b_1 = -2$, then $w^2 = -2u^4 + 2pv^4$. Likewise this has no solution since $\left(\frac{-2}{p}\right) = -1$.
- If $b_1 = p$, then $w^2 = pu^4 - 4v^4$.
  - This is soluble over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right) = 1$, so by Hensel's lemma $-1 \in \left(\mathbb{Z}_p^*\right)^2$.
  - This is soluble over $\mathbb{Q}_2$ since $p - 4 \equiv 1 \mod 8$, so by Hensel's lemma $p - 4 \in \left(\mathbb{Z}_2^*\right)^2$.
  - This is soluble over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$.

  Over $\mathbb{Q}$,

p	5	13	29	37	53
u	1	1	1	5	1
v	1	1	1	3	1
w	1	3	5	151	7

.

Thus $\operatorname{im} \alpha_{E'} \subset \langle -1, p \rangle \subset \mathbb{Q}^* / \left(\mathbb{Q}^*\right)^2$, and

$$\operatorname{rk} E(\mathbb{Q}) = \begin{cases} 0 & \text{this is insoluble over } \mathbb{Q} \\ 1 & \text{this is soluble over } \mathbb{Q} \end{cases}.$$

The conjecture is that $\operatorname{rk} E(\mathbb{Q}) = 1$ for all primes $p \equiv 5 \mod 8$.

Example (Lind). Let E be $y^2 = x^3 + 17x$. Then $\operatorname{im} \alpha_E = \langle 17 \rangle \subset \mathbb{Q}^* / \left(\mathbb{Q}^*\right)^2$. Let E' be $y^2 = x^3 - 68x$. If $b_1 = 2$, then $w^2 = 2u^4 - 34v^2$. Replacing w by $2w$ and dividing by two, let C be $2w^2 = u^4 - 17v^4$. Denote

$$C(K) = \left\{(u, v, w) \in K^3 \setminus \{0\} \;\middle|\; 2w^2 = u^4 - 17v^4\right\} / \sim,$$

where $(u, v, w) \sim \left(\lambda u, \lambda v, \lambda^2 w\right)$ for all $\lambda \in K^*$. Then

- $C(\mathbb{Q}_2) \neq \emptyset$ since $17 \in \left(\mathbb{Z}_2^*\right)^4$,
- $C(\mathbb{Q}_{17}) \neq \emptyset$ since $2 \in \left(\mathbb{Z}_{17}^*\right)^2$, and
- $C(\mathbb{R}) \neq \emptyset$ since $\sqrt{2} \in \mathbb{R}$,

so $C(\mathbb{Q}_v) \neq \emptyset$ for all places v of $\mathbb{Q}$. Suppose $(u, v, w) \in C(\mathbb{Q})$, without loss of generality $u, v, w \in \mathbb{Z}$ such that $\gcd(u, v) = 1$ and $w > 0$. If $17 \mid w$ then $17 \mid u$ and then $17 \mid v$, a contradiction. So if $p \mid w$ then $p \neq 17$ and $\left(\frac{17}{p}\right) = 1$ if p is odd, so $\left(\frac{p}{17}\right) = \left(\frac{17}{p}\right) = 1$, by quadratic reciprocity, but also $\left(\frac{2}{17}\right) = 1$. Thus $\left(\frac{w}{17}\right) = 1$. But $2w^2 \equiv u^4 \mod 17$, so $2 \in \left(\mathbb{F}_{17}^*\right)^4 = \{\pm 1, \pm 4\}$, a contradiction. Thus $C(\mathbb{Q}) = \emptyset$. That is, C is a counterexample to the Hasse principle. It represents a nontrivial element of $\text{Ш}(E/\mathbb{Q})$.

A The Birch Swinnerton-Dyer conjecture

Let $E/\mathbb{Q}$ be an elliptic curve.

Definition. $\mathrm{L}(E,s)=\prod_p \mathrm{L}_p(E,s)$ where

$$\mathrm{L}_p(E,s)=\begin{cases}\left(1-\mathrm{a}_p p^{-s}+p^{1-2s}\right)^{-1} & \text{good reduction}\\ \left(1-p^{-s}\right)^{-1} & \text{split multiplicative reduction}\\ \left(1+p^{-s}\right)^{-1} & \text{nonsplit multiplicative reduction}\\ 1 & \text{additive reduction}\end{cases},$$

and $\#\widetilde{E}(\mathbb{F}_p)=p+1-\mathrm{a}_p$.

By Hasse's theorem, $|\mathrm{a}_p|\le 2\sqrt{p}$, so $\mathrm{L}(E,s)$ converges for $\Re s>\frac{3}{2}$.

Theorem A.1 (Wiles, Breuil, Conrad, Diamond, Taylor)**.** *$\mathrm{L}(E,s)$ is the L-function of a weight two modular form and hence has an analytic continuation to all of $\mathbb{C}$, and a functional equation that relates $\mathrm{L}(E,s)$ and $\mathrm{L}(E,2-s)$.*

Theorem A.2 (Weak BSD)**.**

$$\mathrm{ord}_{s=1}\mathrm{L}(E,s)=\mathrm{rk}\,E(\mathbb{Q}).$$

Theorem A.3 (Strong BSD)**.** *If $r=\mathrm{rk}\,E(\mathbb{Q})$, then*

$$\lim_{s\to 1}\frac{1}{(s-1)^r}\mathrm{L}(E,s)=\frac{\Omega_E\cdot\mathrm{Reg}\,E(\mathbb{Q})\cdot|\text{Ш}(E/\mathbb{Q})|\cdot\prod_p \mathrm{c}_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2},$$

where

- *the Tamagawa number of $E/\mathbb{Q}_p$ is*

$$\mathrm{c}_p=[E(\mathbb{Q}_p):E_0(\mathbb{Q}_p)],$$

- *if $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}\cong\langle P_1,\dots,P_r\rangle$ then the* ***regulator*** *of $E/\mathbb{Q}$ is*

$$\mathrm{Reg}\,E(\mathbb{Q})=\det\left([P_i,P_j]\right)_{i,j=1,\dots,r},$$

  where $[P,Q]=\widehat{\mathrm{h}}(P+Q)-\widehat{\mathrm{h}}(P)-\widehat{\mathrm{h}}(Q)$, and

- *the* ***real period*** *of $E/\mathbb{Q}$ is*

$$\Omega_E=\int_{E(\mathbb{R})}\frac{1}{|2y+a_1x+a_3|}\,\mathrm{d}x,$$

  where a_i are the coefficients of a globally minimal Weierstrass equation.

Theorem A.4 (Kolyvagin)**.** *If $\mathrm{ord}_{s=1}\mathrm{L}(E,s)=0,1$ then weak BSD holds and $|\text{Ш}(E/\mathbb{Q})|<\infty$.*