University of Cambridge

Mathematics Tripos

Part III

Elliptic Curves

Michaelmas, 2019

Lectures by

T. A. Fisher

Notes by

Qiangru Kuang

Contents

1 Fermat's method of infinite descent **2**
1.1 A variant for polynomials 3

2 Some remarks on algebraic curves **5**
2.1 Order of vanishing 6
2.2 Degree of a morphism 8

3 Weierstrass equations **10**

4 The group law **13**
4.1 Explicit formula for the group law 14

5 Isogenies **17**

6 Invariant differential **22**

7 Elliptic curves over finite fields **25**
7.1 Zeta function 26

8 Formal groups **28**

9 Elliptic curves over local fields **33**

10 Elliptic curves over number fields **39**

11 Kummer theory **42**

12 Elliptic curves over number fields II **45**

13 Heights **47**

14 Dual isogenies & Weil pairing **51**

15 Galois cohomology **54**

16 Descent by cyclic isogeny **58**

Index **63**

1 Fermat's method of infinite descent

Let $\Delta = (a, b, c)$ be a right angle triangle with sides a, b, c where c is the hypotenuse.

Definition. Δ is rational if $a, b, c \in \mathbb{Q}$. Δ is primitive if $a, b, c \in \mathbb{Z}$ and coprime.

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

Proof. a and b cannot be both even. They cannot be both odd as then $c^2 = 2 \mod 4$. Thus wlog a is odd and b is even, so c odd. Then

$$\left(\frac{b}{2}\right)^2 = \frac{c+a}{2} \cdot \frac{c-a}{2}$$

and the two terms on RHS are coprime positive integers. By unique factorisation in $\mathbb{Z}$, there exist $u, v \in \mathbb{Z}$ such that

$$\frac{c+a}{2} = u^2$$
$$\frac{c-a}{2} = v^2$$

Rearrange. □

Definition. $D \in \mathbb{Q}_{>0}$ is a *congruent number* if there exists a right angle triangle whose area is D.

Note. Suffices to consider $D \in \mathbb{Z}_{>0}$ square-free.

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

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

Proof. Lemma 1 shows that D is congruent if and only if $Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}, w \neq 0$. Let $x = \frac{u}{v}, y = \frac{w}{v^2}$. □

Fermat showed that 1 is not a congruent number.

Theorem 1.3. *There are no solutions to*

$$w^2 = uv(u-v)(u+v) \tag{$*$}$$

for $u, v, w \in \mathbb{Z}, w \neq 0$.

Proof. wlog u, v coprime, $u > 0, w > 0$. If $v < 0$ then replace (u, v, w) by $(-v, u, w)$. If $u = v \mod 2$ then replace (u, v, w) by $(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2})$. Then $u, v, u - v, u + v$ are positive coprime integers whose product is a square. By unique prime factorisation, $u = a^2, v = b^2, u + v = c^2, u - v = d^2$ for some $a, b, c, d \in \mathbb{Z}_{>0}$. As $u \neq v \mod 2$, c, d are both odd. Consider a new triangle with sides $\frac{c+d}{2}, \frac{c-d}{2}$. Then

$$\left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2 + d^2}{2} = u = a^2$$

so this is another primitive triangle. Its area is

$$\frac{c^2 - d^2}{8} = \frac{v}{4} = \left(\frac{b}{2}\right)^2.$$

Let $w_1 = \frac{b}{2}$ so by lemma 1

$$w_1^2 = u_1 v_1 (u_1 - v_1)(u_1 + v_1),$$

i.e. we have a new solution to $(*)$. But $4w_1^2 = b^2 = v \mid w^2$ so $w_1 \leq \frac{1}{2}w$. So by Fermat's method of infinite descend, there is no solution to $(*)$. □

1.1 A variant for polynomials

Let K be a field with $\operatorname{char} K \neq 2$. Let $\overline{K}$ be an algebraic closure of k.

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

Proof. wlog $K = \overline{K}$. Changing coordinates on $\mathbb{P}^1$, we may assume the ratio $(\alpha : \beta)$ are $(1 : 0), (0 : 1), (1 : -1), (1 : -\lambda)$ for some $\lambda \in K \setminus \{0, 1\}$. Thus we have

$$\begin{aligned} u &= a^2 \\ v &= b^2 \\ u - v &= (a - b)(a + b) \\ u - \lambda v &= (a - \mu b)(a + \mu b) \end{aligned}$$

where $\mu = \sqrt{\lambda}$. Use unqiue factorisation in $K[t]$, as a, b are coprime, $a + b, a - b, a - \mu b, a + \mu b$ are squares. But

$$\max(\deg(a), \deg(b)) \leq \frac{1}{2} \max(\deg(u), \deg(v))$$

so by Fermat's method of infinite descend, $u, v \in K$. □

> **Definition** (elliptic curve)**.**
>
> 1. An *elliptic curve* E/K is the projective closure of a plane affine curve $y^2 = f(x)$ where $f \in K[x]$ is a monic cubic polynomial with distinct roots in $\overline{K}$. The equation $y^2 = f(x)$ is called a *Weierstrass function.*

2. For L/K a field extension,

$$E(L) = \{(x, y) \in L^2 : y^2 = f(x)\} \cup \{0\}$$

where 0 is the point at infinity in the projective closure.

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

In this course we study $E(L)$ for L finite field, local field (meaning $L/\mathbb{Q}_p$ finite in this course) or number field ($L/\mathbb{Q}$ finite).

Theorem 1.5. *If $E : y^2 = x^3 - x$ then $E(\mathbb{Q}) = \{0, (0, 0), (\pm 1, 0)\}$.*

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

Proof. wlog $K = \overline{K}$. By a change of coordinates we may assume

$$E : y^2 = x(x - 1)(x - \lambda)$$

for some $\lambda \in K \setminus \{0, 1\}$. Suppose $(x, y) \in E(K(t))$. Write $x = \frac{u}{v}$ where $u, v \in K[t]$ coprime. Then

$$w^2 = uv(u - v)(u - \lambda v)$$

for some $w \in K[t]$. Using same unique factorisation argument as before, $u, v, u - v, u - \lambda v$ are all squares so by lemma $u, v \in K$ so $x, y \in K$. $\square$

2 Some remarks on algebraic curves

Let $K = \overline{K}, \operatorname{char} K \neq 2$.

Definition (rational plane curve)**.** A plane algebraic curve (always assumed to be irreducible)

$$C = \{f(x, y) = 0\} \subseteq \mathbb{A}^2$$

is *rational* if it has a rational parameterisation, i.e. there exist $\phi, \psi \in K(t)$ such that

1. $\mathbb{A}^1 \to \mathbb{A}^2, t \mapsto (\phi(t), \psi(t))$ is injective on $\mathbb{A}^1 \setminus \{\text{finite set}\}$.
2. $f(\phi(t), \psi(t)) = 0$.

Example.

1. Any nonsingular plane conic is rational. For example $x^2 + y^2 = 1$. Pick a point $(-1, 0)$. Putting a line through the point with slope t, i.e. $y = t(x + 1)$. Solve for the intersection. In general we will get a root, which is not rational. But in the quadratic case we already have one solution so the other solution can be expressed as a rational function. we have

   $$x^2 + t^2(x + 1)^2 = 1$$

   which is saying

   $$(x + 1)(x - 1 + t^2(x + 1)) = 0$$

   so $x = -1$ or $x = \frac{1-t^2}{1+t^2}$. Similarly one can solve y. Then we get rational parameterisation

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

2. Any singular plane curve is rational. Two examples: $y^2 = x^3, y^2 = x^2(x + 1)$. Same recipe as before except that we have to pick the singular point, which is the origin in both cases. The line $y = tx$ intersects the curve. We get rational parameterisation $(x, y) = (t^2, t^3)$ for the first one. The second is an exercise.
3. Corollary 1.6 shows that elliptic curves are *not* rational.

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

1. if $k = \mathbb{C}$ then $g(C)$ is the genus of the Riemann surface.
2. a smooth plane curve $C \subseteq \mathbb{P}^2$ of degree d has genus $g(C) = \frac{(d-1)(d-2)}{2}$.

Proposition 2.1. *Let C be a smooth projective curve.*

1. *C is rational if and only if $g(C) = 0$.*
2. *C is an elliptic curve if and only if $g(C) = 1$.*

Proof.

1. Omitted.
2. For only if, check the projective closure is smooth and use remark. For if, see later.

□

2.1 Order of vanishing

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

Some facts: $\text{ord}_P(f) : K(C)^* \to \mathbb{Z}$ is a discrete valuation, i.e.

$$\begin{aligned}\text{ord}_P(f_1 f_2) &= \text{ord}_P(f_1) + \text{ord}_P(f_2) \\ \text{ord}_P(f_1 + f_2) &\geq \min(\text{ord}_P(f_1), \text{ord}_P(f_2))\end{aligned}$$

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

Example. Let $C = \{g = 0\} \subseteq \mathbb{A}^2$ for some $g \in K[x, y]$ irreducible. Then

$$K(C) = \text{Frac}\, \frac{K[x, y]}{(g)}.$$

Write

$$g = g_0 + g_1(x, y) + g_2(x, y) + \dots$$

where g_i is homogeneous of degree i. Suppose $P = (0, 0) \in C$ is smooth, i.e. $g_0 = 0, g_1(x, y) = \alpha x + \beta y$ where α, β not both zero. (Picture). Let $\gamma, \delta \in K$. It is a fact that $\gamma x + \delta y \in K(C)$ is a uniformiser at P if and only if $\alpha\delta - \beta\gamma \neq 0$.

Example. Consider $\{y^2 = x(x-1)(x-\lambda)\} \subseteq \mathbb{A}^2$ where $\lambda \neq 0, 1$. Its projective closure is $\{Y^2 Z = X(X - Z)(X - \lambda Z)\} \subseteq \mathbb{P}^2$, then we get one point $P = (0 : 1 : 0)$ at infinity. We can compute $\text{ord}_P(x)$ and $\text{ord}_P(y)$. We work on the affine piece $\{Y \neq 0\}$. Put $w = \frac{Z}{Y}, t = \frac{X}{Y}$, then the equation becomes

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

Now P is the point $(t, w) = (0, 0)$. This is a smooth point and using the fact in the above example,

$$\text{ord}_P(t) = \text{ord}_P(t - w) = \text{ord}_P(t - \lambda w) = 1,$$

so $\text{ord}_P(w) = 3$. Finally,

$$\begin{aligned}\text{ord}_P(x) &= \text{ord}_P \frac{X}{Z} = \text{ord}_P \frac{t}{w} = -2 \\ \text{ord}_P(y) &= \text{ord}_P \frac{Y}{Z} = \text{ord}_P \frac{1}{w} = -3\end{aligned}$$

Let C be a smooth projective curve.

Definition (divisor)**.** A *divisor* is a formal sum of points on C, say $D = \sum_{P\in C} n_P P$ with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many P. The *degree* of D is

$$\deg D = \sum n_P.$$

Definition (effective divisor)**.** A divisor D is *effective*, written $D \geq 0$, if $n_P \geq 0$ for all P.

If $f \in K(C)^*$ then we write

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

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

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

i.e. the K-vector space of rational functions on C with "pole no worse than specified by D".

Riemann-Roch for genus 1 curve says that

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

Example. Let us revisit some of the previous example. Consider $\{y^2 = x(x-1)(x-\lambda)\} \subseteq \mathbb{A}^2$ and let P the point at infinity. We calculated $\operatorname{ord}_P(x) = -2, \operatorname{ord}_P(y) = -3$. Then

$$\begin{aligned} \mathcal{L}(2P) &= \langle 1, x\rangle \\ \mathcal{L}(3P) &= \langle 1, x, y\rangle \end{aligned}$$

Proposition 2.2. *Let $C \subseteq \mathbb{P}^2$ be a smooth plane cubic and $P \in C$ a point of inflection. Then we can change coordinates such that $C : Y^2Z = X(X-Z)(X-\lambda Z)$ and $P = (0:1:0)$.*

Fact. The points of inflection on $C = \{F = 0\} \subseteq \mathbb{P}^2$ are given by

$$F = \det \frac{\partial^2 F}{\partial x_i \partial x_j} = 0.$$

Proof. We change coordinates such that $P = (0:1:0)$ and $T_pC = \{Z = 0\}$, where $C = \{F(X,Y,Z) = 0\}$. $P \in C$ is a point of inflection, meaning that the intersection of the tangent at P with C has multiplicity 3, so $F(t,1,0)$ is a constant multiple of t^3. Thus there is no X^2Y, XY^2 and Y^3 term, so

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

The coefficient of X^3 is nonzero as otherwise $\{Z = 0\} \subseteq C$. The coefficient of Y^2Z is nonzero as otherwise $P \in C$ is singular. We are free to rescale X, Y, Z and F, so wlog C is defined by

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

Making substitutions $Y \mapsto Y - \frac{1}{2}a_1X - \frac{1}{2}a_3X$, w may asssume $a_1 = a_3 = 0$. Now $C : Y^2Z = Z^3f(X/Z)$ where f is a monic cubic polynomial. As C is smooth, f has distinct roots so wlog $0, 1, \lambda$ so C is

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

□

The equation

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

is called *Weierstrass form* and

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

is called *Legendre form*.

2.2 Degree of a morphism

Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Let $\phi^* : K(C_2) \to K(C_1)$ be the pullback by ϕ.

Definition (degree of morphism)**.** The *degree* of ϕ is

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

the degree of the field extension. ϕ is *separable* if the corresponding field extension is separable (which is automatic if $\operatorname{char} K = 0$).

Fact. $\deg \phi = 1$ if and only if ϕ is an isomorphism.

Definition (ramification index)**.** Suppose $P \in C_1, Q \in C_2$ are such that $\phi(P) = Q$. Let $t \in K(C_2)$ be an uniformiser at Q. The *ramification index* of ϕ at P is

$$e_\phi(P) = \operatorname{ord}_P(\phi^* t).$$

It is independent of the choice of uniformiser and is always greater than 0.

Theorem 2.3. *Let $\phi : C_1 \to C_2$ be a nonconstant morphism of smooth projective curves. Then*

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

for all $Q \in C_2$.

Moreover, if ϕ is separable then $e_\phi(P) = 1$ for all but finitely many

$P \in C_1$.

In particular,

1. ϕ is surjective (note that we are working over algebraically closed fields).
2. $\#\phi^{-1}(Q) \leq \deg \phi$ with equality for all but finitely many $Q \in C_2$.

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

$$\begin{aligned} \phi : C &\dashrightarrow \mathbb{P}^n \\ P &\mapsto (f_0(P) : f_1(P) : \cdots : f_n(P)) \end{aligned}$$

where $f_0, \ldots, f_n \in K(C)$ not all zero.

Fact. If C is smooth then $\phi : C \dashrightarrow \mathbb{P}^n$ is a morphism.

3 Weierstrass equations

We assume K is a perfect field with algebraic closure $\overline{K}$ in this chapter.

Definition (elliptic curve)**.** An *elliptic curve* E over K is a smooth projective curve of genus 1 defined over K with a specified K-rational point 0_E.

Example. $\{X^3 + pY^3 + p^2Z^3 = 0\} \subseteq \mathbb{P}^2$ is smooth but is *not* an elliptic curve over $\mathbb{Q}$ since it has no $\mathbb{Q}$-rational pionts.

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

Remark. Proposition 2.7 treated the special case E is a smooth plane cubic and 0_E is a point of inflection.

Fact. If $D \in \mathrm{Div}(E)$ is defined over K (i.e. it is fixed by $\mathrm{Gal}(\overline{K}/K)$) then $\mathcal{L}(D)$ has a basis in $K(E)$ (not just $\overline{K}(E)$.

Proof. We have $\mathcal{L}(2 \cdot 0_E) \subseteq \mathcal{L}(3 \cdot 0_E)$ with dimension 2 and 3 respectively. Pick basis $1, x$ for $\mathcal{L}(2 \cdot 0_E)$ and $1, x, y \in \mathcal{L}(3 \cdot 0_E)$. Note that this implies $\mathrm{ord}_{0_E}(x) = 2, \mathrm{ord}_{0_E}(y) = 3$. The seven elements $1, x, y, x^2, xy, x^3, y^2$ in the 6-dim vector space $\mathcal{L}(6 \cdot 0_E)$ must satisfy a dependence relation. Leaving out x^3 or y^2 gives a basis for $\mathcal{L}(6 \cdot 0_E)$ since each term has a different order of pole at 0_E, so coefficients of x^3 and y^2 are nonzero. Rescaling x and y, we get

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

By the fact above, we can take $a_i \in K$.

Let E' be the projective closure of the curve defined by Weierstrass form. There is a morphism

$$\begin{aligned} \phi : E &\to E' \\ p &\mapsto (x(P) : y(P) : 1) \end{aligned}$$

Left to show ϕ is an isomorphism, i.e. $\deg \phi = 1$. We have

$$[K(E) : K(x)] = \deg(x : E \to \mathbb{P}^1) = \mathrm{ord}_{0_E}(\frac{1}{x}) = 2$$
$$[K(E) : K(y)] = \deg(y : E \to \mathbb{P}^1) = \mathrm{ord}_{0_E}(\frac{1}{y}) = 3$$

So by tower law

$$[K(E) : K(x, y)] = 1.$$

As $K(x, y) = \phi^*K(E')$ so $\deg \phi = 1$ so σ is birational. If E' is singular then (? genus 0) E and E' are both rational. So E' is nonsingular and ϕ^{-1} is a morphism.

To find the image of 0_E, we cannot simply plug 0_E in as x, y both have poles at infinity. Instead, we multiply through to get

$$\begin{aligned} \phi : E &\to E' \\ P &\mapsto (\frac{x}{y}(P) : 1 : \frac{1}{y}(P)) \end{aligned}$$

so $\phi(0_E) = (0 : 1 : 0)$. □

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 equations are related by a change of variables*

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

where $u, r, s, t \in K, u \neq 0$.

Proof. We check the process of putting a single elliptic curve in Weierstrass form and see what choices we can make. Suppose

$$\begin{aligned} \langle 1, x \rangle &= \mathcal{L}(2 \cdot 0_E) = \langle 1, x' \rangle \\ \langle 1, x, y \rangle &= \mathcal{L}(3 \cdot 0_E) = \langle 1, x', y' \rangle \end{aligned}$$

so

$$\begin{aligned} x &= \lambda x' + r \\ y &= \mu y' + \sigma x' + t \end{aligned}$$

where $\lambda, r, \mu, \sigma, t \in K, \lambda, \mu \neq 0$. Looking at coefficients of x^3 and y^2, must have $\lambda^3 = \mu^2$ so $(\lambda, \mu) = (u^2, u^3)$ for some $u \in K^*$. Finally put $s = \sigma/u^2$. □

A Weierstrass equation defines an elliptic curve if and only if it defines a smooth curve, if and only if $\Delta(a_1, \dots a_6) \neq 0$ where $\Delta \in \mathbb{Z}[a_1, \dots, a_6]$ is a certain polynomial. Details can be found out in the lecture handout.

If $\operatorname{char} K \neq 2, 3$ then we can reduce the curve to $E : y^2 = x^3 + ax + b$ with discriminant $\Delta = -16(4a^3 + 27b^2)$.

Corollary 3.3. *Assume* $\operatorname{char} k \neq 2, 3$. *Elliptic curves*

$$\begin{aligned} E &: y^2 = x^3 + ax + b \\ E' &: y^2 = x^3 + a'x + b' \end{aligned}$$

are isomorphic over K if and only if

$$\begin{aligned} a' &= u^4 a \\ b' &= u^6 b \end{aligned}$$

for some $u \in K^*$.

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

Definition (j-invariant)**.** The *j-invariant* of an elliptic curve E is

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

This is just the ratio $(a^3 : b^2)$ up to a Möbius transform.

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

Proof. $E \cong E'$ if and only if $a' = u^4 a, b' = u^6 b$ for some $u \in K^*$, which implies that $(a^3 : b^2) = ((a')^3 : (b')^2)$, which holds if and only if $j(E) = j(E')$. If $K = \overline{K}$ then we can extract roots and the converse of the second implication holds. □

4 The group law

Let $E \subseteq \mathbb{P}^2$ be a smooth plane cubic and $0_E \in E(K)$. E meets each line in 3 points, counted with multiplicity. Given $P, Q \in E$, let S be the third point of intersection of PQ and E. Let R be the third point of intersection of $0_E S$ and E. We define

$$P \oplus Q = R.$$

If $P = Q$ then take the tangent at P instead of PQ. This is the "chord and tangent process".

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

Here we recall a convention: if we don't specify the field extension the we mean the algebraic claosure. In notation: $E = E(\overline{K})$.

Proof.

1. $P \oplus Q = Q \oplus P$.
2. 0_E is the identity.
3. For inverse, let S be the point of intersection of $T_{0_E}E$ and E, Q the third point of intersection of PS and E. Then $P \oplus Q = 0_E$.
4. Associativity is much harder, and we'll prove it using divisors.

□

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

This is an equivalence relation and we define

Definition (Picard group)**.** The *Picard group* is defined to be

$$\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim.$$

Definition. We let

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

and

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim.$$

Proposition 4.2. *Let*

$$\begin{aligned} \phi : E &\to \mathrm{Pic}^0(E) \\ P &\mapsto [P - 0_E] \end{aligned}$$

then

1. $\phi(P \oplus Q) = \phi(P) + \phi(Q)$.

2. ϕ is a bijection.

Proof.

1. Let ℓ be the line PQ and m the curve $0_E S$. Then

$$\operatorname{div}(\frac{\ell}{m}) = (P)+(S)+(Q)-(R)-(S)-(0_E) = (P)+(Q)-(P\oplus Q)-(0_E)$$

so $(P)+(Q) \sim (P\oplus Q)+(0_E)$ and so

$$(P)-(0_E)+(Q)-(0_E) = (P\oplus Q)-(0_E)$$

so $\phi(P\oplus Q) = \phi(P)+\phi(Q)$.

2. For injectivity, suppose $\phi(P) = \phi(Q)$ for $P \neq Q$. Then exists $f \in \overline{K}(E)^*$ such that $\operatorname{div}(f) = P - Q$. Then

$$\deg(f : E \to \mathbb{P}^1) = \operatorname{ord}_P(f) = 1$$

so $E \cong \mathbb{P}^1$, absurd.

For surjectivity, let $[D] \in \operatorname{Pic}^0(E)$. Then $D+(0_E)$ has degree 1. Riemann-Roch tells us that $\mathcal{L}(D+(0_E)) = 1$ so exists $f \in \overline{K}(E)^*$ such that

$$\operatorname{div}(f) + D + (0_E) \geq 0$$

and furthermore LHS has degree 1. Thus it has to be (P) for some $P \in E$. It follows that $(P)-(0_E) \sim D$.

□

In a nutshell, ϕ identifies $(E,\oplus)$ with $(\operatorname{Pic}^0(E),+)$ so $\oplus$ is associative.

4.1 Explicit formula for the group law

We consider E in Weierstrass form and 0_E the point at infinity.

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Remark. 0_E is a point of inflection so now we can characterise the group law as $P_1 \oplus P_2 \oplus P_3 = 0_E$ if and only if P_1, P_2, P_3 are colinear.

The inverse of $P = (x_1, y_1)$ is the intersection of $P0_E$, which is the vertical line, and E so is given by

$$\ominus P = (x_1, -(a_1x_1 + a_3) - y_1).$$

Given $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$, want to find an expression for $P_3 = P_1 \oplus P_2$. Let P_1P_2 intersect E at $P' = (x', y')$. Then $P_3 = P_1 \oplus P_2 = \ominus P'$. Substitute $y = \lambda x + \nu$ into * and looking at the coefficient of x^2 gives

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x'$$

which gives

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(a_1x' + a_3) - (\lambda x' + \nu) = -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

It remains to find formula for λ and ν. If $x_1 = x_2$ and $P_1 \neq P_2$ then $P_1 \oplus P_2 = 0_E$. For the general case $x_1 \neq x_2$, have

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ \nu &= y_1 - \lambda x_1 = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1} \end{aligned}$$

Finally the case $P_1 = P_2$ is left as an exercise.

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

Proof. It is a subgroup of E:

- identity: $0_E \in E(K)$ by definition,
- closure/inverses: see formula above.
- associativity/commutativity: inherited.

□

Theorem 4.4. *Elliptic curves are group varieties, i.e.* $[-1] : E \to E, + : E \times E \to E$ *are morphisms of algebraic varieties.*

Proof. The above formulae show $[-1]$ and $+$ are rational maps. $[-1] : E \to E$ is a map from a smooth curve to a projective variety so is a morphism. Unfortunately there is no such result for surfaces. Instead, the formulae also show $+$ is regular on

$$U = \{(P, Q) \in E \times E : P, Q, P + Q, P - Q \neq 0_E\}.$$

For $P \in E$, let $\tau_P : E \to E, X \mapsto P + X$ be translation by P. τ_P is a rational map so a morphism. We factor $+$ as

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

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

Definition (torsion subgroup)**.** For $n \in \mathbb{Z}$, let $[n] : E \to E$ be the "n times" map. The *n-torsion subgroup* of E is $E[n] = \ker([n] : E \to E)$.

Lemma 4.5. *Assume* char $k \neq 2$ *and* $E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$ *where* $e_i \in \overline{K}$ *distinct. Then*

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

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

Elliptic curves over C Let $\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}$ be a lattice, where ω_1, ω_2 is a basis for $\mathbb{C}$ as an $\mathbb{R}$-vector space. The the set of meromorphic functions on the Riemann surface $\mathbb{C}/\Lambda$ is the same as Λ-invariant meromorphisc functions on $\mathbb{C}$. This field is generated by $\wp(z)$ and $\wp'(z)$ where

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

They satisfy

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

for some $g_2, g_3 \in \Lambda$ depending on Λ. One shows $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ where E is the elliptic curve

$$y_2 = 4x^3 - g_2x - g_3.$$

The isomorphism is understood as isomorphism of Riemann surfaces and isomorphism of groups.

Theorem 4.6. *Every elliptic curve over $\mathbb{C}$ arises this way.*

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

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

We'll show 2 holds for any field K, and 1 holds if $\operatorname{char} k \nmid n$.

Statement of results

1. If $K = \mathbb{C}$ then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \cong \mathbb{R}/\mathbb{Z}$.
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 $|E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$. This is Hasse's theorem.
4. If $[K : \mathbb{Q}_p] < \infty$ with rings 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 $E(K)$ is a finitely generated abelian group. This is Mordell-Weil theorem.

Remark. The isomorphisms in 1, 2 and 4 resepcted the relevant topologies.

5 Isogenies

Let K be any perfect field in this chapter.

Let E_1, E_2 be elliptic curves.

Definition (isogeny)**.** An *isogeny* $\phi : E_1 \to E_2$ is a nonconstant morphism with $\phi(0_{E_1}) = 0_{E_2}$. We say E_1 and E_2 are *isogenous* if there exists an isogeny from E_1 to E_2.

We define $\mathrm{Hom}(E_1, E_2)$ to the be set of all isogenies $E_1 \to E_2$ plus 0. This is a group under

$$(\phi + \psi)(P) = \phi(P) + \psi(P).$$

Note that nonconstant implies that surjectivity on $\overline{K}$-points. The composition of isogenies is an isogeny.

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

Proof. We have checked that $[n]$ is a morphism. We must show $[n] \neq 0$. There is a trick that we can use, if we assume $\operatorname{char} K \neq 2$. If $n = 2$ then we computed last time that $\mathbb{E}[2]$ has 4 points so $[2] \neq 0$. If n is odd then let $T \in E[2]$ be nonzero then $nT = T \neq 0$ so again $[n] \neq 0$. Now use $[mn] = [m] \circ [n]$.

If $\operatorname{char} K = 2$, we can compute $E[3]$ as in the lemma before. □

Corollary 5.2. $\mathrm{Hom}(E_1, E_2)$ *is torsion-free as a $\mathbb{Z}$-module.*

Lemma 5.3. *Let $\phi : E_1 \to E_2$ be an isogeny. Then $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E$.*

Sketch proof. ϕ induces a map

$$\begin{aligned} \phi_* : \mathrm{Div}^0(E_1) &\to \mathrm{Div}^0(E_2) \\ \sum n_P P &\mapsto \sum n_P \phi(P) \end{aligned}$$

Recall we have a field extension $\phi^* : K(E_2) \to K(E_1)$ so there is a norm map $N_{K(E_1)/K(E_2)} : K(E_1) \to K(E_2)$. It is a fact that if $f \in K(E_1)^*$ then

$$\mathrm{div}(N_{K(E_1)/K(E_2)} f) = \phi_*(\mathrm{div}\, f)$$

so ϕ_* takes principal divisors to principal divisors. Since $\phi(0_{E_1}) = 0_{E_2}$, we have a commutative diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \downarrow \cong & & \downarrow \cong \\ \mathrm{Pic}^0(E_1) & \xrightarrow{\phi_*} & \mathrm{Pic}^0(E_2) \end{array}$$

As ϕ_* is a group homomorphism, so is ϕ. □

Example. Let E/K be an elliptic curve. Suppose $\operatorname{char} K \neq 2$ and exists $0 \neq T \in E(K)[2]$. wlog assume $E : y^2 = x(x^2 + ax + b)$ with $a, b \in K, b(a^2 - 4b) \neq 0$ so $T = (0, 0)$. If $P = (x, y)$ and $P' = P + T = (x', y')$ then

$$\begin{aligned} x' &= \left(\frac{y}{x}\right)^2 - a - x = \frac{b}{x} \\ y' &= -\left(\frac{y}{x}\right) x' = \frac{-by}{x^2} \end{aligned}$$

We define two variables that remain unchanged under (?) swapping

$$\begin{aligned} \xi &= x + x' + a = \left(\frac{y}{x}\right)^2 \\ \eta &= y + y' = \frac{y}{x}(x - \frac{b}{x}) \end{aligned}$$

Then

$$\begin{aligned} \eta^2 &= \left(\frac{y}{x}\right)^2 ((x + \frac{b}{x})^2 - 4b) \\ &= \zeta((\zeta - a)^2 - 4b) \\ &= \zeta(\zeta^2 - 2a\zeta + a^2 - 4b) \end{aligned}$$

Let $E' : y^2 = (x^2 + a'x + b')$ where $a' = -2a, b' = a^2 - 4b$. Then there is an isogeny

$$\begin{aligned} \phi : E &\to E' \subseteq \mathbb{P}^2 \\ (x, y) &\mapsto (\xi : \eta : 1) \end{aligned}$$

Left to show $\phi(0_E) = 0_{E'}$. The three coordinates has a pole of order $-2, -3, 0$ respectively at 0_E so multiply by uniformiser to the power of three we get $(0 : 1 : 0)$.

Lemma 5.4. *Let $\phi : E_1 \to E_2$ be an isogeny. Then exists morphism ξ making the following diagram commute*

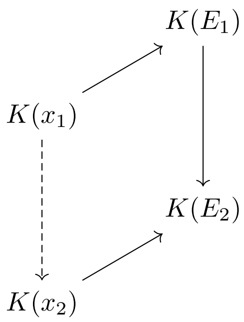
$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ \big\downarrow{\scriptstyle x_1} & & \big\downarrow{\scriptstyle x_2} \\ \mathbb{P}^1 & \xrightarrow{\xi} & \mathbb{P}^1 \end{array}$$

where x_i is the x coordinate on a Weierstrass equation for E_i. Moreover if $\xi(t) = \frac{r(t)}{s(t)}$ where $r, s \in K[t]$ coprime then

$$\deg \phi = \deg \xi = \max(\deg(r), \deg(s)).$$

Example. In the example above we just have $\xi = \frac{x^2+ax+b}{x}$ so in particular it has degree 2.

Proof. For $i = 1, 2$, $K(E_i)/K(x_i)$ is a degree 2 Galois extension with Galois group generated by $[-1]^*$.



If $f \in K(x_2)$ then $[-1]^* f = f$ so

$$[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f$$

so indeed $\phi^* f \in K(x_1)$. Taking $f = x_2$ gives $\phi^* x_2 = \xi(x_1)$ for some rational function ξ. By tower law $\deg \phi = \deg \xi$. Now $K(x_2) \hookrightarrow K(x_1), x_2 \mapsto \xi(x_1) = \frac{r(x_1)}{s(x_1)}$ for some $r, s \in K[t]$ coprime. Claim 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 $f(x_1) = 0$. f is irreducible in $k[x_2, t]$ (since r, s are corpime) so by Gauss' lemma f is irreducible in $K(x_2)[t]$. Therefore

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

□

The lemma shows that the example ϕ above has degree 2. We say ϕ is a 2-*isogeny.*

Lemma 5.5. $\deg[2] = 4$.

Proof. Assume $\operatorname{char} K \neq 2, 3$ so write $E : y^2 = f(x) = x^3 + ax + b$. If $P = (x, y)$ then

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

The numerator and the denominator are coprime. Indeed otherwise exists $\theta \in \overline{K}$ with $f(\theta) = f'(\theta) = 0$, so f has a multiple root, absurd. Therefore by the lemma $\deg[2] = max(4, 3) = 4$. □

We will show that $\deg[n] = n^2$ by showing that deg is a quadratic form. This will also be useful when we prove Hasse's theorem later.

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

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

Lemma 5.6. *$q : A \to \mathbb{Z}$ is a quadratic form if and only if it satisfies the parallelogram law*

$$q(x+y) + q(x-y) = 2q(x) + 2q(y)$$

for all $x, y \in A$.

Proof. Only if is an easy exercise. If will be on example sheet 2. □

Theorem 5.7. $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ *is a quadratic form.*

Here by convention the 0 map has degree 0.

For the proof we assume char $K \neq 2, 3$ and write $E_2 : y^2 = f(x) = x^3 + ax + b$. Let $P, Q \in E_2$ with $P, Q, P+Q, P-Q \neq 0$. Let $x_1, \dots, x_4$ be the x coordinates of these four points.

Lemma 5.8. *There exist $W_0, W_1, W_2 \in \mathbb{Z}[a, b][x_1, x_2]$ of degree ≤ 2 in x_1 and of degree ≤ 2 in x_2 such that*

$$(1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2).$$

Proof. Method 1 is to calculate directly and get $W_0 = (x_1 - x_2)^2, \dots$. See formula sheet.

Method 2: let $y = \lambda x + \nu$ be the line through P and Q so

$$f(x) - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3).$$

By comparing coefficients we get

$$\begin{aligned} \lambda^2 &= s_1 \\ -2\lambda\nu &= s_2 - a \\ \nu^2 &= s_3 + b \end{aligned}$$

where s_i is the ith elementary symmetric polynomial in x_1, x_2, x_3. Eliminating λ and μ gives

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

where F has degree ≤ 2 in each x_i. x_3 is a root of the quadratic $W(t) = F(x_1, x_2, t)$. Repeating for line through P and $-Q$ shows x_4 is also a root of $W(t)$. Write $W(t) = W_0 t^2 - W_1 t + W_2$ and then

$$(1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2).$$

□

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 $\phi, \psi, \phi + \psi, \phi - \psi \neq 0$ as the other cases are trivial or we may use $\deg[2] = 4$. Let the x coordinate of $\phi(x, y), \psi(x, y), (\phi + \psi)(x, y), (\phi - \psi)(x, y)$

be $\xi_1(x), \dots, \xi_4(x)$ respectively. Put $\xi_i = \frac{r_i}{s_i}$ where $r_i, s_i \in K[x]$ coprime and use the above lemma, we get

$$(s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = ((r_1 s_2 - r_2 s_1)^2 : \cdots).$$

Note that the three coordinates on LHS are coprime. We have

$$\begin{aligned}
&\deg(\phi + \psi) + \deg(\phi - \psi) \\
&= \max(\deg(r_3), \deg(s_3)) + \max(\deg(r_4), \deg(s_4)) \\
&= \max(\deg(s_3 s_4), \deg(r_3 s_4 + r_4 s_3), \deg(r_3 r_4)) \quad \text{case checking} \\
&\le 2\max(\deg(r_1), \deg(s_1)) + 2\max(\deg(r_2), \deg(s_2)) \quad \text{as terms on LHS are coprime} \\
&= 2\deg(\phi) + 2\deg(\psi)
\end{aligned}$$

Now replace ϕ, ψ by $\phi + \psi$ and $\phi - \psi$ to get

$$\deg(2\phi) + \deg(2\psi) \le 2\deg(\phi + \psi) + 2\deg(\phi - \psi)$$

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

$$2\deg(\phi) + 2\deg(\psi) \le \deg(\phi + \psi) + \deg(\phi - \psi)$$

Together they show deg satisfies the parallelogram law, so deg is a quadratic form.

Corollary 5.9. $\deg(n\phi) = n^2 \deg(\phi)$ *for all* $n \in \mathbb{Z}, \phi \in \mathrm{Hom}(E_1, E_2)$. *In particular* $\deg[n] = n^2$.

6 Invariant differential

We want to find out when a morphism is separable so we may apply Riemann-Hurwitz. To do so we use differentials.

Let C be an algebraic curve over $K = \overline{K}$. The space of differentials Ω_C is the $K(C)$-vector spaces generated by df for $f \in K(C)$ subject to the relations

1. $d(f+g) = df + dg$,
2. $d(fg) = fdg + gdf$,
3. $da = 0$ for all $a \in K$.

Fact. Ω_C is a 1-dimensional $K(C)$-vector space.

Let $0 \neq \omega \in \Omega_C$. Let $P \in C$ be a smooth point with uniformiser $t \in K(C)$. It is a fact that $dt \neq 0$ so we may write $\omega = f dt$ for some $f \in K(C)^*$. We define $\mathrm{ord}_p(\omega) = \mathrm{ord}_p(f)$. This is independent of choice of t.

Fact. Suppose $f \in K(C)^*$ and $\mathrm{ord}_P(f) = n \neq 0$. If $\mathrm{char}\, K \nmid n$ then $\mathrm{ord}_P(df) = n - 1$.

We now assume C is a smooth projective curve.

Fact. $\mathrm{ord}_p(\omega) = 0$ for all but finitely many $P \in C$.

Definition. We define $\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P \in \mathrm{Div}(C)$.

Definition. We define the genus of C to be

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

the dimension of the space of *regular differentials*.

As a consequence of Riemann-Roch, we have if $0 \neq \omega \in \Omega_C$ then $\deg(\mathrm{div}(\omega)) = 2g(C) - 2$.

Lemma 6.1. *Assume* $\mathrm{char}\, k \neq 2$ *and* $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$. *Then* $\omega = \frac{dx}{y}$ *is a differential on* E *with no zeros or poles. In particular* $g(E) = 1$ *and the* K*-vector space of regular differentials on* E *is* 1*-dimensional, spanned by* ω.

Proof. Let $T_i = (e_i, 0)$ and we know $E[2] = \{0, T_1, T_2, T_3\}$. We have

$$\mathrm{div}(y) = (T_1) + (T_2) + (T_3) - 3(0_E)$$

T_i appears with multiplicity 1 in $\mathrm{div}\, y$ since we know $\deg \mathrm{div}\, y = 0$. If $P \in E \backslash \{0\}$ then

$$\mathrm{div}(x - x_P) = (P) + (-P) - 2(0_E).$$

If $P \in E \setminus E[2]$ then $\mathrm{ord}_P(x - x_P) = 1$ so $\mathrm{ord}_P(dx) = 0$. If $P = T_i$ then $\mathrm{ord}_P(x - x_P) = 2$ so $\mathrm{ord}_P(dx) = 1$. Finally if $P = 0_E$ then $\mathrm{ord}_P(x) = -2$ so $\mathrm{ord}_P(dx) = -3$. Therefore

$$\mathrm{div}(dx) = (T_1) + (T_2) + (T_3) - 3(0_E).$$

It follows that $\mathrm{div}(\frac{dx}{y}) = 0$. □

Definition. If $\phi : C_1 \to C_2$ is a nonconstant morphism then we have *pullback of differentials* defined by

$$\begin{aligned}\phi^* : \Omega_{C_2} &\to \Omega_{C_1} \\ fdg &\mapsto (\phi^* f) d(\phi^* g)\end{aligned}$$

Lemma 6.2. *Let $P \in E$ and $\tau_P : E \to E, X \mapsto P + X$. If $\omega = \frac{dx}{y}$ then $\tau_P^* \omega = \omega$. ω is called the* invariant differential*.*

Proof. $\tau_p^* \omega$ is again a regular differential on E so $\tau_P^* \omega = \lambda_P \omega$ for some $\lambda_P \in K^*$. The map $E \to \mathbb{P}^1, P \mapsto \lambda_P$ (after a calculation we know the map is rational) is a morphism of smooth projective curve but *not* surjective, as it misses $0, \infty$. Therefore it is constant. Thus exists $\lambda \in K^*$ such that $\tau_P^* \omega = \lambda \omega$ for all $P \in E$. Taking $P = 0_E$ shows $\lambda = 1$. □

Remark. If $K = \mathbb{C}$ then remember we have an isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C}), z \mapsto (\wp(z), \wp'(z))$ so

$$\frac{dx}{y} = \frac{\wp'(z) dz}{\wp'(z)} = dz,$$

which is manifestly invariant under $z \mapsto z +$ constant.

Lemma 6.3. *Let $\phi, \psi \in \operatorname{Hom}(E_1, E_2)$ and ω the invariant differential on E_2. Then $(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$.*

Proof. Write $E = E_2$. We have three maps

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

As $E \times E$ is 2-dimensional, it is a fact that $\Omega_{E \times E}$ is a 2-dimensional $K(E \times E)$-vector space with basis $\pi_1^* \omega, \pi_2^* \omega$. Then $\mu^* \omega = f \pi_1^* \omega + g \pi_2^* \omega$ for some $f, g \in K(E \times E)$. For $Q \in E$ let $\iota_Q : E \to E \times E, P \mapsto (P, Q)$. Applying ι_Q^* gives

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

i.e.

$$\tau_Q^* \omega = (\iota_Q^* f) \omega + 0$$

so $\iota_Q^* f = 1$ for all $Q \in E$, so $f(P, Q) = 1$ for all $P, Q \in E$. Similarly $g(P, Q) = 1$. Thus $\mu^* \omega = \pi_1^* \omega + \pi_2^* \omega$. Now pullback by $E \to E \times E, P \mapsto (\phi(P), \psi(P))$ to get

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

□

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

Proof. Omitted. □

Example. Consider the group variety $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} = \mathbb{P}^1 \setminus \{0, \infty\}$ with group law being multiplication. Let $n \geq 2$ be an intger and consider $\phi(x) = x^n$. We know from Galois theory that if $\operatorname{char} K \nmid n$ then $\ker \phi$ has n elements. This can also be deducted geometrically using differentials: $\phi^*(dx) = dx^n = nx^{n-1}dx$ so if $\operatorname{char} K \nmid n$ then ϕ is separable. Then $\#\phi^{-1}(Q) = \deg \phi$ for all but finitely many $Q \in \mathbb{G}_m$. ϕ is a group homomorphism so $\#\phi^{-1}(Q) = \ker \phi$ for all $Q \in \mathbb{G}_m$ so in fact $\# \ker \phi = \deg \phi = n$. Thus K (which is algebraically closed) contains exactly n nth roots of unity.

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

Proof. By induction $[n]^*\omega = n\omega$ so if $\operatorname{char} K \nmid n$ then $[n] : E \to E$ is separable. Thus by the theorem $\#[n]^{-1}(Q) = \deg[n]$ for all but finitely many $Q \in E$. But $[n]$ is a group homomorphism so $\#[n]^{-1}(Q) = \#E[n]$ for all $Q \in E$. Thus

$$\#E[n] = \deg[n] = n^2.$$

By classification of finitely generated abelian groups,

$$E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_t\mathbb{Z}$$

with $d_1 \mid d_2 \mid \cdots \mid d_t \mid n$ and $\prod d_i = n^2$. 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 $t = 2$ and $d_1 \mid d_2 \mid n$, $d_1 d_2 = n^2$ so $d_1 = d_2 = n$. □

Remark. If $\operatorname{char} K = p$ then $[p]$ is inseparable. It can be shown that either $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$, or $E[p^r] = 0$ for all $r \geq 1$. They are called ordinary and supersingular.

7 Elliptic curves over finite fields

We begin by proving a form of Cauchy-Schwarz.

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*

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

Notation. $\langle x, y\rangle = q(x+y) - q(x) - q(y)$ and note that $\langle x, x\rangle = 2q(x)$.

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

$$\begin{aligned} 0 &\leq q(mx+ny) \\ &\frac{1}{2}\langle mx+ny, mx+ny\rangle \\ &= m^2 qx + mn\langle x, y\rangle + n62q(y) \\ &= q(x)(m + \frac{n\langle x, y\rangle}{2q(x)})^2 + n^2(q(y) - \frac{\langle x, y\rangle^2}{4q(x)} \end{aligned}$$

Take $m = \langle x, y\rangle, n = -2q(x)$ to deduce

$$\langle x, y\rangle^2 \leq 4q(x)q(y).$$

□

Let $\mathbb{F}_q$ be the field with q elements where $q = p^m$ for some p prime. 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*

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

Proof. Let E have Weierstrass equation with coefficients $a_1, \dots, a_6 \in \mathbb{F}_q$ so $a_i^q = a_i$ for all i. Define the *Frobenius endomorphism* $\phi : E \to E, (x, y) \mapsto (x^q, y^q)$ which is an isogeny of degree q. Then

$$E(\mathbb{F}_q) = \{P \in E : \phi(P) = P\} = \ker(1 - \phi).$$

Note ϕ is not separable as

$$\phi^*\omega = \phi^*(\frac{dx}{y}) = \frac{dx^q}{y^q} = \frac{qx^{q-1}dx}{y^q} = 0$$

but

$$(1-\phi)^*\omega = \omega - \phi^*\omega = \omega \neq 0$$

so $1 - \phi$ is separable. Same as before, we have $\#\ker(1-\phi) = \deg(1-\phi)$.

Recall that $\deg : \mathrm{End}(E) \to \mathbb{Z}$ is a positive definite quadratic form so by Cauchy-Schwarz

$$|\deg(1-\phi) - \deg[1] - \deg[\phi]| \leq 2\sqrt{\deg[1]\deg[\phi]}$$

so

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

as required. □

7.1 Zeta function

For K a number field, define

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

For K a function field, i.e. $K = \mathbb{F}_q(C)$ where $C/\mathbb{F}_q$ is a smoth projective curve, we define

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

where $|C|$ is the set of closed points of C, and is the same as the orbits of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ on $C(\overline{F}_q)$. Have $Nx = q^{\deg x}$ where $\deg x$ is the size of the orbit.

We have $\zeta_K(s) = F(q^{-s})$ for some $F \in \mathbb{Q}[[T]]$. Explicitly

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

Take logarithm of the formal power series, we get

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

Now reverse the process,

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

We define $\mathrm{tr} : \mathrm{End}(E) \to \mathbb{Z}, \phi \mapsto \langle \phi, 1\rangle$.

Lemma 7.3. *If* $\phi \in \mathrm{End}(E)$ *then*

$$\phi^2 - (\mathrm{tr}\,\phi)\phi + \deg\phi = 0.$$

Proof. Example sheet 2. □

Definition (zeta function)**.** The *zeta function* of a variety $V/\mathbb{F}_q$ is the formal power series (?)

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

Lemma 7.4. *Suppose $E/\mathbb{F}_q$ is an elliptic curve, $\#E(\mathbb{F}_q) = q+1-a$. Then*

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

Proof. Let $\phi : E \to E$ be the q-power Frobenius. By the proof of Hasse's theorem

$$\#E(\mathbb{F}_q) = \deg(1-\phi) = q + 1 - \operatorname{tr}\phi$$

so $a = \operatorname{tr}\phi$ and $\deg\phi = q$. By the above lemma $\phi^2 - a\phi + q = 0$ so $\phi^{n+2} - a\phi^{n+1} + q\phi^n = 0$. Upon taking trace,

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

This second order difference equation with initial condition $\operatorname{tr} 1 = 2, \operatorname{tr}\phi = q$ has solution $\operatorname{tr}\phi^n = \alpha^n + \beta^n$ where $\alpha, \beta \in \mathbb{C}$ ar roots of $X^2 - aX + q = 0$. Then

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

Thus the zeta function is

$$Z_V(T) = \exp\sum_{n=1}^{\infty} \frac{1}{n}(T^n + (qT)^n - (\alpha T)^n - (\beta T)^n) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$$

using $-\log(1-x) = \sum_{m=1}^{\infty} \frac{x^m}{m}$. Expand. □

Remark. Hasse's theorem as Riemann hypothesis for finite fields: Hasse's theorem gives a bound $|a| \leq 2\sqrt{q}$ so $\alpha = \overline{\beta}$. As $\alpha\beta = q$, have $|\alpha| = |\beta| = sqrtq$. Let $K = \mathbb{F}_q(E)$. Then $\zeta_K(s) = 0$ if and only if $Z_E(q^{-s}) = 0$, so $q^s = \alpha$ or β so $q^{\operatorname{Re} s} = \sqrt{q}$, i.e. $\operatorname{Re} s = \frac{1}{2}$. Thus we have proven the Riemann hypothesis.

8 Formal groups

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

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

Definition. R is *complete* if

1. $\bigcap_{n\geq 0} I^n = \{0\}$ (Hausdorff condition),
2. every Cauchy sequence converges.

Remark. Suppose R is complete. If $x \in I$ then $\frac{1}{1-x} = 1 + x + x^2 + \cdots$ so $1 - x \in R^*$.

Example.

1. $R = \mathbb{Z}_p$ with $I = p\mathbb{Z}_p$. This is complete by construction.
2. $R = \mathbb{Z}[[t]]$ with $I = (t)$.

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

Proof. Let $u \in R^\times$ with $F'(a) = u \pmod I$. Replacing F by $\frac{X+A}{u}$, we may assume $a = 0$ and $F'(0 = 1 \pmod I$. We define

$$x_0 = 0, \quad x_{n+1} = x_n - F(x_n).$$

An easy induction shows $x_n = 0 \pmod{I^s}$ for all n. Also

$$F(X) - F(Y) = (X - Y)(F'(0) + XG(X, Y) + YH(X, Y))$$

for some $G, H \in R[X, Y]$. Claim that $x_{n+1} = x_n \pmod{I^{n+s}}$ for all $n \geq 0$.

Proof. Induction on n. $n = 0$ holds. Suppose $x_n = x_{n-1} \pmod{I^{n+s-1}}$. Then

$$F(x_n) - F(x_{n-1}) = (x_n - x_{n-1})(1 + c)$$

for some $c \in I$. Modulo I^{n+s}, get

$$F(x_n) - F(x_{n-1}) = x_n - x_{n-1} \pmod{I^{n+s]}}.$$

Rearrange to get

$$x_{n+1} = x_n - F(x_n) = x_{n-1} - F(x_{n-1}) = x_n \pmod{I^{n+s}}.$$

□

Thus by completeness $x_n \to b$ as $n \to \infty$ for some $b \in R$. Taking limit of the recurrence relation and use the continuity of F to get $F(b) = 0$. Taking limit in $x_n = 0 \pmod{I^s}$ gives $b = 0 \pmod{I^s}$. Uniqueness follows from the assumption R is an integral domain. $\square$

Consider $E : Y^2Z + a_1XYZ + a_3yZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. We want to study the behaviour near 0_E so use the affine piece $Y \neq 0$. Let $t = -X/Y, w = -Z/Y$. Then

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

Apply Hensel's lemma to $R = \mathbb{Z}[a_1, \dots, a_6][[t]], I = (t)$ and $F(X) = X - f(t, X)$. The approximate root is $a = 0$ for $s = 3$. Check $F(0) = -t^3, F'(0) = 1 - a_1t - a_2t^2 \in R^\times$. Then there exists a unique $w(t) \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ such that $w(t) = f(t, w(t))$ and $w(t) = 0 \pmod{t^3}$.

To see $w(t)$ explicitly, we follow the proof of Hensel's lemma (with $u = 1$) and get $w(t) = \lim_{n\to\infty} w_n(t)$ where

$$w_0(t) = 0, \quad w_{n+1}(t) = f(t, w_n(t)).$$

In fact

$$\omega(t) = t^3(1 + A_1t + A_2t^2 + \dots) = \sum_{n=2}^{\infty} A_{n-2}t^{n+1}$$

where $A_1 = a_1, A_2 = a_1^2 + a_2, A_3 = a_1^3 + 2a_1a_2 + a_3, \dots$

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 K the field of fraction of R. Then*

$$\hat{E}(I) = \{(t, w) \in E(K) : t, w \in I\}$$

is a subgroup of $E(K)$.

Remark. By unqiueness in Hensel's lemma (with $s = 1$), we can also describe $\hat{E}(I)$ as

$$\hat{E}(I) = \{(t, w(t)) \in E(K) : t \in I\}.$$

Proof. Taking $(t, w) = (00)$ shows $0_E \in \hat{E}(I)$, so suffices to show if $P_1, P_2 \in \hat{E}(I)$ then $-P_1 - P_2 \in \hat{E}(I)$. Suppose $P_i = (t_i, w_i)$. The line P_1P_2 is given by $\omega = \lambda t + \nu$ where

$$\lambda = \begin{cases} \frac{w(t_2) - w(t_1)}{t_2 - t_1} & t_1 \neq t_2 \\ w'(t_1) & t_1 = t_2 \end{cases}$$

so

$$\begin{aligned} \lambda &= \sum_{n=2}^{\infty} A_{n-2}(t_1^n + t_1^{n-1}t_2 + \dots + t_2^n) \in I \\ \nu &= w_1 - \lambda t_1 \in I \end{aligned}$$

Subsituting $w = \lambda t + \nu$ into $w = f(t, w)$, we get

$$\begin{aligned} A &= \text{ coefficient of } t^3 = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3 \\ B &= \text{ coefficient of } t^2 = a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu \end{aligned}$$

we have $A \in R^\times, B \in I$ so $t_3 = -B/A - t_1 - t_2 \in I$ and $w_3 = \lambda t_3 + \nu \in I$. $\square$

Taking $R = \mathbb{Z}[a_1, \dots, a_t][[t]], I = (t)$. The lemma shows that there exists $\iota(t) \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ with $\iota(0) = 0$ such that $[-1](t, w(t)) = (\iota(t), w(\iota(t)))$. Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]], I = (t_1, t_2)$, the lemma says there exists $F \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ 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

$$\begin{aligned}\iota(X) &= -X - a_1 X^2 - a_2 X^3 - (a_1^3 + a_3) X^4 + \dots \\ F(X, Y) &= X + Y - a_1 XY - a_2 (X^2 Y + XY^2) + \dots\end{aligned}$$

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. $F(F(X, Y), Z) = F(X, F(Y, Z))$.
4. $F(X, \iota(X)) = 0$.

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

A question on example sheet 2 shows that for any formal group, there exists a unique $\iota(t) = -t + \cdots \in R[[t]]$ satisfying 4.

Example.

1. $F(X, Y) = X + Y$. We call this formal group $\hat{\mathbb{G}}_a$.
2. $F(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1$ so is secretly the same as above. We call this formal group $\hat{\mathbb{G}_m}$.
3. F arising from an elliptic curve. We call it $\hat{E}$.

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

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

Theorem 8.3. *If* $\operatorname{char} R = 0$ *then every formal group* $\mathbb{F}$ *over* R *is isomorphic to* $\hat{\mathbb{G}}_a$ *over* $R \otimes \mathbb{Q}$*. More precisely,*

1. *there is a unique power series* $\log(T) = T + \frac{a_2}{2} T^2 + \frac{a_3}{3} T^3 + \cdots$ *with* $a_i \in R$ *such that*

$$\log F(X, Y) = \log(X) + \log(Y). \qquad (*)$$

2. *there is a unique power series* $\exp(T) = T + \frac{b_2}{2!} T^2 + \frac{b_3}{3!} T^3 + \cdots$ *with*

> $b_i \in R$ *such that*
> $$\exp\log(T) = \log\exp(T) = T.$$

Proof.

1. Write $F_1(X,Y) = \frac{\partial F}{\partial X}(X,Y)$. For uniqueness, let
$$p(T) = \frac{d}{dT}\log T = 1 + a_2T + a_3T^2 + \dots.$$
Differentiating $(*)$ with respect to X gives
$$p(F(X,Y))F_1(X,Y) = p(X).$$
Putting $X = 0$ gives $p(Y)F_1(0,Y) = 1$ so $p(Y) = F_1(0,Y)^{-1}$ is unqiue. Thus log is unique.
For existence, let $p(T) = F_1(0,T)^{-1} = 1 + a_2T + a_3T^2 + \dots$ for some $a_i \in R$. Let $\log T = T + \frac{a_2}{2}T^2 + \dots$. Differentiate the associativity law with respect to X we get
$$F_1(F(X,Y),Z)F_1(X,Y) = F_1(X,F(Y,Z)).$$
Sub $X = 0$ and use identity law,
$$F_1(Y,Z)F_1(0,Y) = F_1(0,F(Y,Z))$$
so
$$F_1(Y,Z)p(F(Y,Z)) = p(Y).$$
Integrate with repsect to Y to get
$$\log(F(Y,Z)) = \log Y + h(Z)$$
for some power series h. By symmetry in Y,Z have $h(Z) = \log Z$.

2. We use

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

Proof. We construct polynomials $g_n(T)$ such that $f(g_n(T)) = T \pmod{T^{n+1}}$ and $g_{n+1}(T) = g_n(T) \pmod{T^{n+1}}$. Then $g(T) = \lim_{n\to\infty} g_n(T)$ exists and satisfies $f(g(T)) = T$.
To start the induction set $g_1(T) = a^{-1}T$. Now suppose $n \geq 2$ and $g_{n-1}(T)$ exists so $f(g_{n-1}(T)) = T + bT^n \pmod{T^{n+1}}$ for some $b \in R$. We put $g_n(T) = g_{n-1}(T) + \lambda T^n$ for some $\lambda \in R$ to be chosen later. Then
$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &= f(g_{n-1}(T)) + \lambda a T^n \pmod{T^{n+1}} \\ &= T + (b + \lambda a)T^n \pmod{T^{n+1}} \end{aligned}$$
so we take $\lambda = -b/a$.

We get $g(T) = a^{-1}T + \cdots \in R[[T]]$ such that $f(g(T)) = T$. Applying the same argument to g gives $h(T) = aT + \cdots \in R[[T]]$ such that $g(h(T)) = T$. Then

$$f(T) = f(g(h(T))) = h(T).$$

□

The theorem then follows except for showing $b_n \in R$ (not just $R \otimes \mathbb{Q}$). This is on example sheet 2.

□

Notation. Let $\mathcal{F}$ (e.g. $\hat{\mathbb{G}_a}, \hat{\mathbb{G}_m}, \hat{E}$) be a formal group given by $F \in R[[X, Y]]$. Suppose R is complete with respect to 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 $\hat{\mathbb{G}(I)} = (I, +), \hat{\mathbb{G}_m(I)} \cong (1 + I, \times)$ and $\hat{E}(I) \subseteq E(K)$ as in lemma 8.2. This also explains the earlier choice of notation.

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

1. *$[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.*
2. *If R is complete with respect to an ideal I then $\times n : \mathcal{F}(I) \to \mathcal{F}(I)$ is an isomorphism. In particular $\mathcal{F}(I)$ has no n-torsion.*

Proof. We first explain the notation $[n]$. We inductively define $[1](T) = T, [n](T) = F([n-1]T, T)$ for $n \geq 2$ (for $n < 0$, use $[-1](T) = \iota(T)$). An easy induction show $[n](T) = nT + \cdots \in R[[T]]$ so by Lemma 8.4 it is an isomorphism. □

9 Elliptic curves over local fields

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

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

with unit group

$$\mathcal{O}_K^* = \{x \in K^* : v(x) = 0\}$$

and maximal ideal $\pi\mathcal{O}_K$ where $v(\pi) = 1$. It has residue field $k = \mathcal{O}_k/\pi\mathcal{O}_K$. We assume $\operatorname{char} K = 0, \operatorname{char} k = p > 0$. For example $K = \mathbb{Q}_p, \mathcal{O}_K = \mathbb{Z}_p, k = \mathbb{F}_p$.

Let E/K be an elliptic curve.

Definition (integral/minimal Weierstrass equation)**.** 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 is *minimal* if $v(\Delta)$ is minimal among all integral equations for E.

Remark.

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

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $0 \neq P \in E(K)$, say $P = (x, y)$. Then either $x, y \in \mathcal{O}_K$ or $v(x) = -2s, v(y) = -3s$ for some $s \geq 1$.

Proof. First we deal with the case $v(x) \geq 0$ (or $x = 0$). If $v(y) < 0$ then $v(\text{LHS}) = 0$ while $v(\text{RHS}) > 0$, absurd so $x, y \in \mathcal{O}_K$.

Now suppose $v(x) < 0$. Then

$$v(\text{LHS}) \geq \min(2v(y), v(x) + v(y), v(y)), \quad v(\text{RHS}) = 3v(x).$$

In each of the three cases, $v(y) < v(x)$ so $2v(y) = 3v(x)$. □

Remark. See example sheet 1.

Fix a minimal Weierstrass equation for E/K, we get a formal group $\hat{E}$ over $\mathcal{O}_K$, and

$$\begin{aligned}\hat{E}(\pi^r\mathcal{O}_K) &= \{(x, y) \in E(K) : -\frac{x}{y}, -\frac{1}{y} \in \pi^r\mathcal{O}_K\} \cup \{0\} \\ &= \{(x, y) \in E(K) : v(\frac{x}{y}) \geq r, v(\frac{1}{y}) \geq r\} \cup \{0\} \\ &= \{(x, y) \in E(K) : v(x) \leq -2r, v(y) \leq -2r\} \cup \{0\}\end{aligned}$$

by using the lemma. This is a π-neighbourhood of 0. By theorem 8.2 this is a subgroup of $E(K)$, say $E_r(K)$. Then we have a nested sequence of groups

$$E_1(K) \supseteq E_2(K) \supseteq \cdots$$

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

$$\mathcal{F}(\pi\mathcal{O}_K) \supseteq \mathcal{F}(\pi^2\mathcal{O}_K) \supseteq \cdots$$

We will show that $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K, +)$ for r sufficiently large and

$$\frac{\mathcal{F}(\pi^r\mathcal{O}_K)}{\mathcal{F}(\pi^{r+1}\mathcal{O}_K)} \cong (k, +)$$

for all $r \geq 1$.

A reminder we are working over $\operatorname{char} K = 0, \operatorname{char} k = p$.

Proposition 9.2. *Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. Let $e = v(p)$. If $r > \frac{e}{p-1}$ then*

$$\log : \mathcal{F}(\pi^r\mathcal{O}_K) \to \hat{\mathbb{G}}_a(\pi^r\mathcal{O}_K)$$

is an isomorphism with inverse exp.

Proof. For $x \in \pi^r\mathcal{O}_K$ we must show that the power series exp and log in theorem 8.3 converge. Recall $\exp(T) = T + \frac{b_2}{2!}T^2 + \dots$ where $b_n \in \mathcal{O}_K$. Note that while a "big" denominator is good in Archimedean analysis, the situation is the opposite in the non-Archimedean case. Claim $v_p(n!) = \frac{n-1}{p-1}$.

Proof.

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

so $(p-1)v_p(n!) < n$. By noting that it is integer valued we get the required inequality. □

Now

$$v(\frac{b_n x^n}{n!} \geq nr - e\left(\frac{n-1}{p-1}\right) = (n-1)\underbrace{(r - \frac{e}{p-1})}_{>0} + r$$

This is always $\geq r$ and goes to infinity as $n \to \infty$ so $\exp x$ converges and belongs to $\pi^r\mathcal{O}_K$. $\log x$ is similar but easier. □

Proposition 9.3. *For $r \geq 1$,*

$$\frac{\mathcal{F}(\pi^r\mathcal{O}_K)}{\mathcal{F}(\pi^{r+1}\mathcal{O}_K)} \cong (k, +).$$

Proof. Recall $F(X,Y) = X + Y + XY(\cdots)$ so if $x, y \in \mathcal{O}_K$,

$$F(\pi^r x, \pi^r y) = \pi^r(x+y) \pmod{\pi^{r+1}}.$$

Thus

$$\begin{aligned} \mathcal{F}(\pi^r\mathcal{O}_K) &\to (k, +) \\ \pi^r x &\mapsto x \pmod{\pi} \end{aligned}$$

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

Corollary 9.4. *If k is finite then $\mathcal{F}(\pi\mathcal{O}_K)$ contains a subgroup of finite index and is isomorphic to $(\mathcal{O}_K, +)$.*

Notation. We denote reduction mod π by $x \mapsto \tilde{x}$.

Proposition 9.5. *Suppose E/K is an elliptic curve. The reduction mod π of two minimal Weierstrass equations for E define isomorphic curves over k.*

Proof. Say Weierstrass equations are related by $[u; r, s, t]$ where $u \in K^\times, r, s, t \in K$. Then $\Delta_1 = u^{12}\Delta_2$. Minimality of equations implies that $u \in \mathcal{O}_K^*$. By transformation formula for a_i and b_i, we conclude $r, s, t \in \mathcal{O}_K$. Then the Weierstrass equation for the reductions mod π are related by $[\tilde{u}; \tilde{r}, \tilde{s}, \tilde{t}]$. Note that all these are to ensure that things work in characteristic 2 or 3. ☐

Definition (reduction)**.** The *reduction* $\widetilde{E}/k$ of E/K is defined to be the reduction of a minimal Weierstrass equation.

E has *good reduction* if $\widetilde{E}$ is nonsingular (and so is an elliptic curve), otherwise *bad reduction.*

For an integral Weierstras equation, $v(\Delta) = 0$ is a sufficient condition for good reduction. On the other hand if $0 < v(\Delta) < 12$ then by $\Delta_1 = u^{12}\Delta_2$ we have bad reduction. If $v(\Delta) \geq 12$ then the equation might not be minimal.

There is a well-defined map

$$\begin{aligned} \mathbb{P}^2(K) &\to \mathbb{P}^2(k) \\ (x : y : z) &\mapsto (\tilde{x} : \tilde{y} : \tilde{z}) \end{aligned}$$

where we choose representatives with $\min(v(x), v(y), v(z)) = 0$ to ensure we do not get $(0 : 0 : 0)$. We restrict to get $E(K) \to E(k), P \mapsto \widetilde{P}$. If $P = (x, y) \in E(K)$ then either $x, y \in \mathcal{O}_K$ so $\widetilde{P} = (\tilde{x}, \tilde{y})$, or $v(x) = -2s, v(y) = -3s$ and we choose $P = (\pi^{3s}x : \pi^{3s}y : \pi^{3s})$ which reduces to $\widetilde{P} = (0 : 1 : 0)$. Thus

$$E_1(K) = \hat{E}(\pi\mathcal{O}_K) = \{P \in E(K) : \widetilde{P} = 0\}$$

is the *kernel of reduction.*

Let $\widetilde{E}_{\text{ns}}$ be the set of nonsingular points on $\widetilde{E}$. If E has good reduction then this is the same as $\widetilde{E}$. Otherwise we delete the singular points. The chord and tangent process still defines a group law on $\widetilde{E}_{\text{ns}}$ (since the third intersection point only has multiplicity 1). In case of bad reduction $\widetilde{E}_{\text{ns}} \cong \mathbb{G}_a$ or $\mathbb{G}_m$ (over $\overline{k}$), called additive reduction or multiplicative reduction. For simpicity suppose $\operatorname{char} k \neq 2$ and we have $\widetilde{E} : y^2 = f(x)$. Then $\widetilde{E}$ is singular if and only if f has a repeated root. For double root $(y^2 = x^2(x + 1))$ we have a curve with a node and we use multiplicative reduction. For triple root $(y^2 = x^3)$ we have a curve with a cusp and we use additive reduction

$$\begin{aligned} \widetilde{E}_{\text{ns}} &\to \mathbb{G}_a \\ (x, y) &\mapsto \frac{x}{y} \\ (t^{-2}, t^{-3}) &\leftarrow\!\shortmid t \\ \infty &\leftarrow\!\shortmid 0 \end{aligned}$$

We check this is a group homomorphism. Let P_1, P_2, P_3 be on the line $ax+by = 1$. Write $P_i = (x_i, y_i), t_i = \frac{x_i}{y_u}$. Then $x_i^3 = y_i^2 = y_i^2(ax_i + by_i)$ so t_1, t_2, t_3 are roots of $X^3 - aX - b = 0$. Looking at the coefficient of X^2 gives $t_1 + t_2 + t_3 = 0$.

The node case is on example sheet.

Definition. We define

$$E_0(K) = \{P \in E(K) : \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(k)\},$$

the points that do not become singular upon reduction.

Proposition 9.6. *$E_0(K)$ is a subgroup of $E(K)$ and reduction mod π is a surjective group homomorphism $E_0(K) \to \widetilde{E}_{\mathrm{ns}}(k)$.*

Proof. First check this is a group homomorphism. A line ℓ in $\mathbb{P}^2$ defined over K has equation $aX + bY + cZ = 0$ where $a, b, c \in K$. We may assume $\min(v(a), v(b), v(c)) = 0$. Reduction mod π given the line $\tilde{\ell}$ $\tilde{a}X + \tilde{b}Y + \tilde{c}Z = 0$. If $P_1, P_2, P_3 \in E(K)$ with $P_1 + P_2 + P_3 = 0$ then they lie on a line ℓ. Then $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3$ lie on $\tilde{\ell}$. 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 $\widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3 = 0$. It is an exercise to check that this still works when $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3$ are not necessarily distinct.

Now we show surjectivity. Let $f(x, y) = y^2 + a_1xy + a_3y - (x^3 + \dots)$ be the Weierstrass equation. Let $\widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(k) \setminus \{0\}$, say $\widetilde{P} = (\tilde{x}_0, \tilde{y}_0)$ for some $x_0, y_0 \in \mathcal{O}_K$. $\widetilde{P}$ nonsingular implies that either $\frac{\partial f}{\partial x}(x_0, y_0) \neq 0 \pmod{\pi}$ or $\frac{\partial f}{\partial y}(x_0, y_0) \neq 0 \pmod{\pi}$. In the first case put $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$. Then

$$g(x_0) = 0 \pmod{\pi}, \quad g'(x_0) \in \mathcal{O}_K^*$$

so by Hensel's lemma exists $b \in \mathcal{O}_K$ such that $g(b) = 0, b = x_0 \pmod{\pi}$. Then $P = (b, y_0) \in E(K)$ has reduction $\widetilde{P}$. The second case is similar. □

Recall that for $r \geq 1$ we put

$$E_r(K) = \{(x, y) \in E(K) : v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}$$

and we have a nested sequence of groups

$$(\mathcal{O}_K, +) \cong E_r(K) \subseteq \cdots \subseteq E_2(K) \subseteq E_1(K) \subseteq E_0(K) \subseteq E(K)$$

for $r > \frac{e}{p-1}$. The quotient $\frac{E_0(K)}{E_1(K)} \cong \widetilde{E}_{\mathrm{ns}}(K)$ and all quotients $\frac{E_{t+1}}{E_t} \cong (k, +)$. What about $E_0(K) \subseteq E(K)$? There are much to be said about this but we only cover a special case here. More can be found is Silverman's sequel.

Lemma 9.7. *If $|k| < \infty$ then $\mathbb{P}^n(K)$ is compact (with respect to π-adic topology).*

Proof. If $|k| < \infty$ then $\frac{\mathcal{O}_K}{\pi^r\mathcal{O}_K}$ is finite for $r \geq 1$ so $\mathcal{O}_K \cong \varprojlim_r \mathcal{O}_K/\pi^r\mathcal{O}_K$ is compact. $\mathbb{P}^n(K)$ is the union of compact sets

$$\{(a_0 : a_1 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n) : a_j \in \mathcal{O}_K\}$$

and hence compact. □

Lemma 9.8. *If $|k| < \infty$ then $E_0(K) \subseteq E(K)$ has finite index.*

Proof. $E(K) \subseteq \mathbb{P}^2(K)$ is a closed subset so $(E(K), +)$ is a compact topological group. If $\widetilde{E}$ has singular point $(\tilde{x}_0, \tilde{y}_0)$ then

$$E(K) \setminus E_0(K) = \{(x, y) \in E(K) : v(x - x_0) \geq 1, v(y - y_0) \geq 1\}$$

(?) is a closed subset of $E(K)$ and so $E_0(K)$ is an open subgroup of $E(K)$. The cosets of $E_0(K)$ are an open cover of $E(K)$, and thus $E_0(K)$ has finite index in $E(K)$ by compactness. The index is called *Tamagawa number* and is denoted $c_K(E)$. □

Remark. Good reduction implies that $c_K(E) = 1$ but the converse is false.

Fact. For these facts it is essential that E is defined by a minimal Weierstrass equation, but we don't need $|k| < \infty$.

Either $c_K(E) = v(\Delta)$ or $c_K(E) \leq 4$

Theorem 9.9. *If $[K : \mathbb{Q}_p] < \infty$ then $E(K)$ contains a subgroup $E_r(K)$ of finite index with $E_r(K) \cong (\mathcal{O}_K, +)$.*

Proof. We have $|k| < \infty$. Combine all results in this chapter. □

Corollary 9.10. $E(K)_{\text{tors}}$ *injects into $\frac{E(K)}{E_r(K)}$ and is therefore finite.*

We now quote some results from algebraic number theory. Let $[K : \mathbb{Q}_p] < \infty$ and L/K a finite extension. Then $[L : K] = ef$ where $v_L|_{K^*} = ev_K$ and $f = [k' : k]$ where k' and k are the residue fields of L and K respectively. If L/K is Galois then there is a natural group homomorphism $\text{Gal}(L/K) \to \text{Gal}(k'/k)$. This map is surjective with kernel of order e.

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

Fact. For each integer $m \geq 1$,

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

Definition (maximal unramified extension)**.** We define the *maximal unramified extension* to be $K^{\text{nr}} = \bigcup_{m \geq 1} K_m$ (inside $\overline{K}$).

Theorem 9.11. *Suppose $[K : \mathbb{Q}_p] < \infty$, E/K an elliptic curve with good reduction and $p \nmid n$. If $P \in E(K)$ then $K([n]^{-1}P)/K$ is unramified.*

Recall that when we do not specify a base field then we refer to the algebraic closure so

$$[n]^{-1}P = \{Q \in E(\overline{K}) = nQ = P\}.$$

Also we denote

$$K(\{P_1, \dots, P_r\}) = K(X_1, \dots, x_r, y_1, \dots, y_r)$$

where $P_i = (x_i, y_i)$.

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

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

Taking union over all $m \geq 1$ gives a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K^{\mathrm{nr}}) & \longrightarrow & E(K^{\mathrm{nr}}) & \longrightarrow & \widetilde{E}(\overline{k}) & \longrightarrow & 0 \\ & & \downarrow n & & \downarrow n & & \downarrow n & & \\ 0 & \longrightarrow & E_1(K^{\mathrm{nr}}) & \longrightarrow & E(K^{\mathrm{nr}}) & \longrightarrow & \widetilde{E}(\overline{k}) & \longrightarrow & 0 \end{array}$$

The left vertical map is an isomorphism by corollary 8.5, which applies since $p \nmid n$ implies $n \in \mathcal{O}_K^*$. The right vertical map is surjective by Theorem 2.8 and has kernel isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ by theorem 6.5. Then by snake lemma

$$E(K^{\mathrm{nr}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2, \frac{E(K^{\mathrm{nr}})}{nE(K^{\mathrm{nr}})} = 0$$

so if $P \in E(K)$ then $P = nQ$ for some $Q \in E(K^{\mathrm{nr}})$ so

$$[n]^{-1}P = \{Q + T : T \in E[n]\} \subseteq E(K^{\mathrm{nr}})$$

so $K([n]^{-1}P) \subseteq K^{\mathrm{nr}}$ so $K([n]^{-1}P)/K$ is unramified. $\square$

10 Elliptic curves over number fields

Suppose $[K : \mathbb{Q}] < \infty$ and E/K is an elliptic curve. Throughout we let $\mathfrak{p}$ be a prime of K (i.e. of $\mathcal{O}_K$), $K_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of K and $k_\mathfrak{p} = \mathcal{O}_k/\mathfrak{p}$.

Definition (prime of good reduction)**.** $\mathfrak{p}$ 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 coefficients $a_1, \ldots, a_6 \in \mathcal{O}_K$. E is nonsingular implies that $0 \neq \Delta \in \mathcal{O}_K$. Write $(\Delta) = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ for the factorisation into prime ideals. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. If $\mathfrak{p} \notin S$ then $v_\mathfrak{p}(\Delta) = 0$ so $E/K_\mathfrak{p}$ has good reduction. □

Remark. If K has class number 1 (e.g. $K = \mathbb{Q}$) then we can always find a Weierstrass equation for $a_1, \ldots, a_6 \in \mathcal{O}_K$ which is minimal at all primes $\mathfrak{p}$.

Lemma 10.2. *$E(K)_{\text{tor}}$ is finite.*

Proof. Take any $\mathfrak{p}$. Note $K \subseteq K_\mathfrak{p}$ and apply theorem 9.8. □

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

Proof. Proposition 9.5 says that $E(K_\mathfrak{p}) \to \widetilde{E}(k_\mathfrak{p})$ is a group homomorphism with kernel $E_1(K_\mathfrak{p})$. Then corollary 8.5 implies that $E_1(K_\mathfrak{p})$ has no n-torsion. □

Example. Let $E/\mathbb{Q} : y^2 + y = x^3 - x^2$. $\Delta = -11$. E has good reduction at all primes $p \neq 11$. so by looking at 2 and 3, $\#E(\mathbb{Q})_{\text{tor}} \mid 5 \cdot 2^a$ for some $a \geq 0$.

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

$\#E(\mathbb{Q})_{\text{tor}} \mid 5 \cdot 3^b$ for some $b \geq 0$, so $\#E(\mathbb{Q})_{\text{tor}} \mid 5$. Let $T = (0, 0) \in E(\mathbb{Q})$. We can check that $5T = 0$ so $E(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/5\mathbb{Z}$.

Example. Let $E/\mathbb{Q} : y^2 + y = x^3 + x$. $\Delta = -43$. E has good reduction at all $p \neq 43$. By considering $p = 2, 11$ we show $E(\mathbb{Q})_{\text{tor}} = \{0\}$. Thus $P = (0, 0) \in$

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

$E(\mathbb{Q})$ is a point of infinite order. Thus rank of $E(\mathbb{Q}) \geq 1$.

Example. Let $E_D : y^2 = y^2 = x^3 - D^2 x$ where $D \in \mathbb{Z}$ square free and $\Delta = 2^6 D^6$. We know the torsion group contains $\{0, (0, 0), (\pm d, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Let $f(x) = x^3 - D^2x$. We can count the number of points using Legendre symbol. If $p \nmid 2D$ then

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

If $p = 3 \pmod 4$ 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 $m = \#E_D(\mathbb{Q})_{\text{tor}}$. We have $4 \mid m \mid (p+1)$ for all sufficiently large primes p with $p = 3 \pmod 4$. Then by $m = 4$ as otherwise we will get a contradiction to Dirichlet's theorem on primes in arithmetic progression. Thus $E_D(\mathbb{Q})_{\text{tor}} \cong (\mathbb{Z}/2\mathbb{Z})^2$. Thus rank $E_D(\mathbb{Q}) \geq 1$ if and only if there exists $x, y \in \mathbb{Q}$ with $y \neq 0$ and $y^2 = x^3 - D^2x$, if and only if D is a congruent number.

Lemma 10.4. *Let $E/\mathbb{Q}$ be given by a Weierstrass equation with $a_1, \dots, a_6 \in \mathbb{Z}$. Suppose $0 \neq T = (x, y) \in E(\mathbb{Q})_{\text{tor}}$. Then*

1. $4x, 8y \in \mathbb{Z}$,
2. *if* $2 \mid a_1$ *or* $2T \neq 0$ *then* $x, y \in \mathbb{Z}$.

Proof.

1. The Weierstrass equation defines a formal group $\hat{E}$ over $\mathbb{Z}$. For $r \geq 1$, recall

$$\hat{E}(p^r\mathbb{Z}_p) = \{(x, y) \in E(\mathbb{Q}_p) : v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{0\}.$$

Proposition 9.2 says $\hat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ if $r > \frac{1}{p-1}$. Thus $\hat{E}(4\mathbb{Z}_2)$ and $\hat{E}(p\mathbb{Z}_p)$ for p odd are torsion free. Thus if $0 \neq T = (x, y) \in E(\mathbb{Q})_{\text{tors}}$ then $T \notin \hat{E}(4\mathbb{Z}_2)$, so $v_2(x) \geq -2, v_2(y) \geq -3$. $T \notin \hat{E}(p\mathbb{Z}_p)$ so $v_p(X) \geq 0, v_p(y) \geq 0$.

2. Suppose $T \in \hat{E}(2\mathbb{Z}_2)$, i.e. $v_2(x) = -2, v_3(y) = -3$. Since $\frac{\hat{E}(2\mathbb{Z}_2)}{\hat{E}(4\mathbb{Z}_2)} \cong (\mathbb{F}_2, +)$ and $\hat{E}(4\mathbb{Z}_2)$ is torsion free, we get $2T = 0$. Also

$$(x, y) = T = -T = (x, -y - a_1x - a_3)$$

so $2y + a_1x + a_3 = 0$. Thus $8y + a_1(4x) + 4a_3 = 0$, and $8y, 4x$ are both odd and $4a_3 = 0$ so a_1 is odd. Thus if $2T \neq 0$ or a_1 is even then $T \in \hat{E}(2\mathbb{Z}_2)$ and so $x, y \in \mathbb{Z}$.

□

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

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

Proof. Lemma 10.4 implies $x, y \in \mathbb{Z}$. If $2T = 0$ then $y = 0$. Otherwise $0 \neq 2T = (x_2, y_2)$ is torsion so $x_2, y_2 \in \mathbb{Z}$. Then $x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x$. Everything is integer so $y \mid f'(x)$. E is nonsingular so $f(X)$ and $f'(X)$ are coprime. $f(X)$ and $f'(X)^2$ are coprime so exists $g, h \in \mathbb{Q}[X]$ such that $g(X)f(X) + h(X)f'(X)^2 = 1$. A calculation gives

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

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

Remark. Mazur has shown that if $E/\mathbb{Q}$ is an elliptic curve then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the below:

$$\mathbb{Z}/n\mathbb{Z} \text{ for } 1 \leq n \leq 12, n \neq 11 \text{ or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } 1 \leq n \leq 4.$$

Moreover all 15 possibilities occur.

11 Kummer theory

Let K be a field with $\operatorname{char} K \nmid n$. Assume $\mu_n \subseteq K$.

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

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

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

$$\begin{aligned} \langle \cdot, \cdot \rangle : \operatorname{Gal}(L/K) \times \Delta &\to \mu_n \\ (\sigma, x) &\mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}} \end{aligned}$$

Check this is well-defined: if $\alpha, \beta \in L$ with $\alpha^n = \beta^n = x$ then $(\frac{\alpha}{\beta})^n = 1$ so $\frac{\alpha}{\beta} \in \mu_n \subseteq K$ so $\sigma(\frac{\alpha}{\beta}) = \frac{\alpha}{\beta}$ so $\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\beta)}{\beta}$. It is bilinear:

$$\begin{aligned} \langle \sigma\tau, x \rangle &= \frac{\sigma(\tau \sqrt[n]{x})}{\tau \sqrt[n]{x}} \frac{\tau \sqrt[n]{x}}{\sqrt[n]{x}} = \langle \sigma, x \rangle \langle \tau, x \rangle \\ \langle \sigma, xy \rangle &= \frac{\sigma \sqrt[n]{xy}}{\sqrt[n]{xy}} = \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}} \frac{\sigma \sqrt[n]{y}}{\sqrt[n]{y}} = \langle \sigma, x \rangle \langle \sigma, y \rangle \end{aligned}$$

The pairing is nondegenerate in both arguments: let $\sigma \in \operatorname{Gal}(L/K)$. If $\langle \sigma, x \rangle = 1$ for all $x \in \Delta$ then $\sigma \sqrt[n]{x} = \sqrt[n]{x}$ for all $x \in \Delta$ so σ fixes L pointwise so $\sigma = 1$. Conversely let $x \in \Delta$. If $\langle \sigma, x \rangle = 1$ for all $\sigma \in \operatorname{Gal}(L/K)$ then $\sigma \sqrt[n]{x} = \sqrt[n]{x}$ for all σ so $\sqrt[n]{x} \in K^*$ so $x \in (K^*)^n$.

To put it in another way $\operatorname{Gal}(L/K)$ and Δ are dual groups to each other and we have two injective group homomorphisms

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

Statement 1 implies $\operatorname{Gal}(L/K)$ is an abelian group of exponent dividing n. Now similar to the fact that the dual group of a finite abelian group has the same size, we have $|\operatorname{Hom}(\Delta, \mu_n)| = |\Delta|$ and same for the other so

$$|\operatorname{Gal}(L/K)| \le |\Delta| \le |\operatorname{Gal}(L/K)|$$

so 1 and 2 are isomorphisms. □

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

Theorem 11.2. *There is a bijection*

$$\left\{ \begin{array}{c} \textit{finite subgroups} \\ \Delta \subseteq K^*/(K^*)^n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{finite abelian extensions} \\ L/K \textit{ of exponent} \\ \textit{dividing } n \end{array} \right\}$$

$$\Delta \mapsto K(\sqrt[n]{\Delta})$$

$$\frac{(L^*)^n \cap K^*}{(K^*)^n} \leftarrow\!\shortmid L$$

Proof. Let $\Delta \subseteq K^*/(K^*)^n$ be a finite subgroup. Let $L = K(\sqrt[n]{\Delta})$ and $\Delta' = \frac{(L^*)^n \cap K^*}{(K^*)^n}$. Clearly $\Delta \subseteq \Delta'$. To show equality,

$$L = K(\sqrt[n]{\Delta}) \subseteq K(\sqrt[n]{\Delta'}) \subseteq L$$

so $K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\Delta'})$ so $|\Delta| = |\Delta'|$ by the lemma. Thus equality.

Conversely let L/K be a finite abelian extension of exponent dividing n. Let Δ be as defined in the statement. Then $K(\sqrt[n]{\Delta}) \subseteq L$. We aim to show equality by showing $[K(\sqrt[n]{\Delta}) : K] = [L : K]$. Let $G = \mathrm{Gal}(L/K)$. The Kummer pairing defines an injective group homomorphism $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$. Claim this is surjective.

Proof. Let $\chi : G \to \mu_n$ be a group homomorphism. From basic Galois theory distinct automorphisms are linearly independent so exists $a \in L$ such that $y = \sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \neq 0$. Let $\sigma \in G$. Then

$$\sigma(y) = \sum_{\tau \in G} \chi(\tau)^{-1}\sigma\tau(a) = \sum_{\tau \in G} \chi(\sigma^{-1}\tau)^{-1}\tau(a) = \chi(\sigma)y$$

Thus $\sigma(y^n) = y^n$ for all $\sigma \in G$ so $x = y^n \in K^* \cap (L^*)^n$. Then $x \in \Delta$ and $\chi : \sigma \mapsto \frac{\sigma(y)}{y} = \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}}$. □

Now

$$[K(\sqrt[n]{\Delta}) : K] = |\Delta| = |\mathrm{Hom}(G, \mu_n)| = |G| = [L : K].$$

□

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

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

Proof. By 11.2 $L = K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subseteq K^*/(K^*)^n$. Let $\mathfrak{p}$ be a prime of K with

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

for distinct primes $\mathfrak{P}_i$ of L. If $x \in K^*$ represents an element of Δ then

$$n v_{\mathfrak{P}_i}(\sqrt[n]{x}) = v_{\mathfrak{P}_i}(x) = e_i v_{\mathfrak{p}}(x).$$

If $\mathfrak{p} \notin S$ then $e_i = 1$ for all i so $v_{\mathfrak{p}}(x) = 0 \pmod n$. Thus $\Delta \subseteq K(S, n)$ where

$$K(S, n) = \{x \in K^*/(K^*)^n : v_{\mathfrak{p}}(x) = 0 \pmod n \text{ for all } \mathfrak{p} \notin S\}.$$

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

Proof. The map

$$\begin{aligned} K(S,n) &\to (\mathbb{Z}/n\mathbb{Z})^{|S|} \\ x &\mapsto (v_{\mathfrak{p}}(x) \pmod n)_{\mathfrak{p}\in S} \end{aligned}$$

is a group homomorphism with kernel $K(\emptyset,n)$ so suffice to prove the lemma with $S=\emptyset$. If $x\in K^*$ represents an element of $K(\emptyset,n)$ then $(x)=\mathfrak{a}^n$ for some ideal $\mathfrak{a}$. There is an exact sequence

$$0 \longrightarrow \mathcal{O}_K^*/(\mathcal{O}_K^*)^n \longrightarrow K(\emptyset,n) \longrightarrow \mathrm{Cl}_K[n] \longrightarrow 0$$

From algebraic number theory $|\mathrm{Cl}_K|<\infty$ and $\mathcal{O}_K^*$ is finitely generated (Dirichlet's unit theorem) so $K(\emptyset,n)$ is finite. □

□

12 Elliptic curves over number fields II

Mordell-Weil Theorem

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

Proof. For each element in the kernel we pick a coset representative $P \in E(K)$ and then exists $Q \in E(L)$ such that $nQ = P$. $\mathrm{Gal}(L/K)$ is finite and $E[n]$ is finite so there are only finitely many possibilities for the map $\mathrm{Gal}(L/K) \to E[n], \sigma \mapsto \sigma Q - Q$. But if $P_1, P_2 \in E(K)$ with $P_i = nQ_i$ and $\sigma Q_1 - Q_2 = \sigma Q_2 - Q_2$ for all $\sigma \in \mathrm{Gal}(L/K)$ then $\sigma(Q_1 - Q_2) = Q_2 - Q_2$ so $Q_1 - Q_2 \in E(K)$, and hence $P_1 - P_2 \in nE(K)$. □

Theorem 12.2 (weak Mordell-Weil theorem)**.** *Let K be a number field and E/K an elliptic curve. Then for $n \geq 2$, $|\frac{E(K)}{nE(K)}| < \infty$.*

Proof. By lemma wlog we can assume $\mu_n \subseteq K$ and $E[n] \subseteq E(K)$. Let $S = \{\mathfrak{p} \mid n\} \cup \{\text{primes of bad reduction for } E\}$. For each $P \in E(K)$ the extension $K([n]^{-1}P)/K$ is unramified outside S by theorem 9.9.

Let $Q \in [n]^{-1}P$. Since $E[n] \subseteq E(K)$, $K(Q) = K([n]^{-1}P)$ is a Galois extension of K. Define

$$\begin{aligned} \mathrm{Gal}(K(Q)/K) &\to E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \\ \sigma &\mapsto \sigma Q - Q \end{aligned}$$

Check this is a homomorphism:

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

It is injective as $\sigma Q = Q$ implies σ fixes $K(Q)$ so $\sigma = 1$. Thus $K(Q)/K$ is an abelian extension of exponent dividing n, unramified outside S. By 11.3 only there are only finitely many possibilities for $K(Q)$. Let L be the composite of all such extensions (i.e. for all $P \in E(K)$). Then L/K is finite (and Galois) and $\frac{E(K)}{nE(K)} \to \frac{E(L)}{nE(L)}$ is the zero map. Apply lemma 12.1. □

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

Fact. Let E/K be a elliptic curve over a number field. Then there exists a quadratic form, called *canonical height* $\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$ with the property that for any $B \geq 0$, $\{P \in E(K) : \hat{h}(P) \leq B\}$ is finite.

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

Proof. Fix an integer $n \geq 2$. Weak Mordell-Weil implies that $|\frac{E(K)}{nE(K)}| < \infty$. Pick coset representatives $P_1, \dots, P_m$. Let $\Sigma = \{P \in E(K) : \hat{h}(P) \leq \max_{1 \leq i \leq n} \hat{h}(P_i)\}$. Claim Σ generates $E(K)$.

Proof. Suppose not. Then exists $P \in E(K) \setminus \{\text{subgroup generated by } \Sigma\}$ of minimal height. Then $P = P_i + nQ$ for some $1 \leq i \leq m$ where $Q \in E(K) \setminus \{\text{subgroup generated by } \Sigma\}$. Then $\hat{h}(P) \leq \hat{h}(Q)$. Then

$$\begin{aligned} 4\hat{h}(P) &\leq 4\hat{h}(Q) \\ &\leq n^2\hat{(}Q) \\ &= \hat{h}(nQ) \\ &= \hat{h}(P - P_2) \\ &\leq \hat{h}(P - P_i) + \hat{h}(P + P_i) \\ &= 2\hat{h}(P) + 2\hat{h}(P_1) \text{ parallalogram law} \end{aligned}$$

so $\hat{h}(P) \in \hat{h}(P_i)$ so $P \in \Sigma$, contradiction. □

Σ is finite so done. □

13 Heights

For simplicity take $K = \mathbb{Q}$. Write $P \in \mathbb{P}^n(\mathbb{Q})$ as $P = (a_1 : \cdots : a_n)$ where $a_0, \dots, a_n \in \mathbb{Z}, \gcd(a_0, \dots, a_n) = 1$.

Definition (height)**.** We define the *height* of P to be

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

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

$$\begin{aligned} F : \mathbb{P}^1 &\to \mathbb{P}^1 \\ (x_1 : x_2) &\mapsto (f_1(x_1, x_2) : f_2(x_1, x_2)) \end{aligned}$$

Then exists $c_1, c_2 > 0$ such that

$$c_1 H(P)^d \le H(F(P)) \le c_2 H(P)^d$$

for all $P \in \mathbb{P}^1(\mathbb{Q})$.

Proof. wlog $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$. We prove the upper bound first. Write $P = (a : b)$ where $a, b \in \mathbb{Z}$ coprime. Then

$$H(F(P)) \le \max(|f_1(a,b)|, |f_2(a,b)|) \le c_2 \max(|a|^d, |b|^d) = c_2 H(P)^d$$

where c_2 is the maximum of the sum of absolute values of coefficients of f_1 and f_2.

For the lower bound, we claim exists $g_{ij} \in \mathbb{Z}[X_1, X_2]$ homogeneous of degree $d-1$ and $\kappa \in \mathbb{Z}_{>0}$ such that

$$\sum_{j=1}^{2} g_{ij} f_j = \kappa X_i^{2d-1}. \tag{†}$$

Proof. Indeed running Euclid's algorihm on $f_1(X, 1)$ and $f_2(X, 1)$ gives $r, s \in \mathbb{Q}[X]$ such that

$$r(X) f_1(X, 1) + s(X) f_2(X, 1) = 1.$$

Homgogenising and clearing denominators gives (†) for $i = 2$ Likewise for $i = 1$. □

Write $P = (a_1 : a_2)$ where $a_1, a_2 \in \mathbb{Z}$ coprime. Then (†) gives

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

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

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

where γ_i is the sum over j of absolute values of coefficients of g_{ij}. Thus

$$|a_i|^{2d-1} \leq \gamma_i H(F(P))H(P)^{d-1}$$

for $i = 1, 2$. Thus

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

Take $c_1 = \max(\gamma_1, \gamma_2)^{-1}$. □

Notation. For $x \in \mathbb{Q}$ we define $H(x) = H((x : 1)) = \max(|u|, |v|)$ where $x = \frac{u}{v}$ for $u, v \in \mathbb{Z}$ coprime.

Let $E/\mathbb{Q}$ be an elliptic curve of the form $y^2 = x^3 + ax + b$.

Definition (height)**.** The *height* is defined as the map

$$\begin{aligned} H : E(\mathbb{Q}) &\to \mathbb{R}_{\geq 1} \\ P &\mapsto \begin{cases} H(x) & P = (x, y) \\ 1 & P = 0_E \end{cases} \end{aligned}$$

We define the *logarithmic height* to be $h = \log H$.

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

$$|h(\phi(P)) - \deg(\phi)h(P)| \leq c$$

for all $P \in E(\mathbb{Q})$. Note that c depends on E, E' and ϕ.

Proof. Recall (Lemma 5.4) we have commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \big\downarrow{\scriptstyle x} & & \big\downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow{\xi} & \mathbb{P}^1 \end{array}$$

and $\deg \phi = \deg \xi = d$, say. Lemma 13.1 says that there exist $c_1, c_2 > 0$ such that

$$c_1 H(P)^d \leq H(\phi(P)) \leq c_2 H(P)^d$$

for all $P \in E(\mathbb{Q})$. Taking logs gives

$$|h(\phi(P)) - dh(P)| \leq \max(\log c_2, -\log c_1).$$

□

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

$$|h(2P) - 4h(P)| < c$$

for all $P \in E(\mathbb{Q})$.

Definition (canonical height)**.** The *canonical height* is

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

Check convergence: for $m \geq n$,

$$\begin{aligned}
|\frac{1}{4^m}h(2^m P) - \frac{1}{4^n}h(2^n P)| &\leq \sum_{r=n}^{m-1} |\frac{1}{4^{r+1}}h(2^{r+1}P) - \frac{1}{4^r}h(2^r P)| \\
&\leq \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} |h(2^{r+1}P) - 4h(2^r P)| \\
&\leq c \sum_{r=n}^{\infty} \frac{1}{4^{r+1}} \\
&\to 0
\end{aligned}$$

as $n \to \infty$ so the sequence is Cauchy so $\hat{h}(P)$ exists.

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

Proof. Put $n = 0$ in the above calcultion to give

$$|\frac{1}{4^m}h(2^m P) - h(P)| \leq \frac{c}{3}.$$

Take limit as $m \to \infty$. ☐

Corollary 13.4. *For any $B > 0$, $\#\{P \in E(\mathbb{Q}) : \hat{h}(P) < B\} < \infty$.*

Proof. By the lemma $\hat{h}(P)$ is bounded implies $h(P)$ is bounded, so only finitely many possibilities for x. Each x leaves at most 2 choices for y. ☐

Lemma 13.5. *Suppose $\phi : E \to E'$ is an isogeny defined over $\mathbb{Q}$. Then*

$$\hat{h}(\phi P) = (\deg \phi)\hat{h}(P)$$

for all $P \in E(\mathbb{Q})$.

Proof. By lemma 13.2 exists $c > 0$ such that

$$|h(\phi P) - (\deg \phi)h(P)| < c$$

for all $P \in E(\mathbb{Q})$. Replace P by $2^n P$, divide by 4^n and take limit as $n \to \infty$. ☐

Remark.

1. The case $\deg \phi = 1$ shows that $\hat{h}$, unlike h, is independent of the choice of Weierstrass equation.
2. Taking $\phi = [n] : E \to E$ gives $\hat{h}(nP) = n^2\hat{h}(P)$ for all $P \in E(\mathbb{Q})$.

(Going to prove $\hat{h}$ is a quadratic form by showing that it satisfies the parallelogram law).

Lemma 13.6. *Let $E/\mathbb{Q}$ be an ellitpic curve. There exists $c > 0$ such that*

$$H(P+Q)H(P-Q) \le cH(P)^2H(Q)^2$$

for all $P, Q, P+Q, P-Q \neq 0_E$.

Proof. Let E have Weierstrass equation $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$. Let $P, Q, P+Q, P-Q$ has x coordinates $x_1, \ldots, x_4$. By lemma 5.8 there exist $W_0, W_1, W_2 \in \mathbb{Z}[x_1, x_2]$ of degree ≤ 2 in x_1 and degree ≤ 2 in x_2 such that

$$(1 : x_3 + x_4 : x_3x_4) = (W_0 : W_1 : W_2)$$

and $W_0 = (x_1 - x_2)^2$. Write $x_i = \frac{r_i}{s_i}$ where $r_i, s_i \in \mathbb{Z}$ coprime. Then we get

$$(s_3s_4 : r_3s_4 + r_4s_3 : r_3r_4) = ((r_1s_2 - r_2s_1)^2 : \cdots).$$

So

$$\begin{aligned} H(P+Q)H(P-Q) &= \max(|r_3|, |s_3|)\max(|r_4|, |s_4|) \\ &\le 2\max(|s_3s_4|, |r_3s_4 + r_4s_3|, |r_3r_4|) \\ &\le 2\max(|r_1s_2 - r_2s_1|, \cdots) \\ &\le cH(P)^2H(Q)^2 \end{aligned}$$

where c depends on E but not on P and Q. □

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

Proof. Lemma 13.6 and $|h(2P) - 4h(P)|$ bounded implies that

$$h(P+Q) + h(P-Q) \le 2h(P) + 2h(Q) + c$$

for $P, Q \in E(\mathbb{Q})$ (there are several special cases to check). Replacing P, Q by $2^nP, 2^nQ$, dividing by 4^n and taking limit $n \to \infty$ gives

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

Replacing P, Q by $P+Q, P-Q$ and writing $\hat{h}(2P) = 4\hat{h}(P)$ gives the reverse inequality. Thus $\hat{h}$ satisfies the parallelogram law and $\hat{h}$ is a quadratic form. □

Remark. For K a number field, $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n(K)$, define

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

where the product is over all places v and the absolute values $|\cdot|_v$ are normalised such that $\prod_v |\lambda|_v = 1$ for all $\lambda \in K^*$. Then all results in this section generalises to K.

14 Dual isogenies & Weil pairing

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

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

$$\begin{array}{ccc} E & \xrightarrow{\psi} & E'' \\ \downarrow{\scriptstyle \phi} & \nearrow_{\exists!} & \\ E' & & \end{array}$$

Proof. Omitted. See Silverman Chapter 3. □

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

Proof. Case ϕ separable: $|\ker \phi| = n$ so $\ker \phi \subseteq \mathbb{E}[n]$. Apply proposition 14.1 with $\psi = [n]$. The ϕ inseparble case is omitted (see Silverman. Suffice to check for Frobenius map). For uniqueness if $\psi_1\phi = \psi_2\phi = [n]$ then $(\psi_1 - \psi_2)\phi = 0$ so $\psi_1 = \psi_2$ since ϕ nonconstant is surjective. □

Remark.

1. The relation of elliptic curves being isogenous is an equivalence relation.
2. If $\deg \phi = n$ then $\deg[n] = n^2$ implies that $\deg \hat{\phi} = \deg \phi$ and $\widehat{[n]} = [n]$.
3. $\phi\hat{\phi}\phi = \phi[n]_E = [n]_{E'}\phi$ implies that $\phi\hat{\phi} = [n]_{E'}$. In particular $\hat{\hat{\phi}} = \phi$.
4. If $E \xrightarrow{\psi} E' \xrightarrow{\phi} E''$ then $\widehat{\phi\psi} = \hat{\psi}\hat{\phi}$.
5. If $\phi \in \mathrm{End}(E)$ then by example sheet 2

$$\phi^2 - (\mathrm{tr}\,\phi)\phi + \deg \phi = 0$$

so

$$\underbrace{([\mathrm{tr}\,\phi] - \phi)}_{\hat{\phi}}\phi = [\deg \phi]$$

and hence $\mathrm{tr}\,\phi = \phi + \hat{\phi}$.

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

Proof. If $E = E'$ then this follows from $\mathrm{tr}(\phi + \psi) = \mathrm{tr}\,\phi + \mathrm{tr}\,\psi$. In general let $\alpha : E' \to E$ be any isogeny (e.g. $\hat{\phi}$). Thus

$$(\widehat{\alpha\phi + \alpha\psi}) = \widehat{\alpha\phi} + \widehat{\alpha\psi}$$

so

$$\widehat{\phi + \psi}\hat{\alpha} = (\hat{\phi} + \hat{\psi})\hat{\alpha}.$$

□

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.

Definition (sum)**.** The *sum map* is defined as

$$\begin{aligned} \mathrm{sum} : \mathrm{Div}(E) &\to E \\ \sum n_P(P) &\mapsto \sum n_P P \end{aligned}$$

where LHS is a formal sum and RHS is sum using group law.

Recall that we have a group isomorphism $E \to \mathrm{Pic}^0(E), P \mapsto [P - 0]$. Thus $\mathrm{sum}\, D \mapsto [D]$ 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* $\mathrm{sum}\, D = 0$.

Let $\phi : E \to E'$ be an isogeny of degree n with dual isogeny $\hat{\phi} : E' \to E$. Assume $\mathrm{char}\, K \nmid n$. We define the *Weil pairing* $e_\phi : E[\phi] \times E'[\hat{\phi}] \to \mu_n$. Let $T \in E'[\hat{\phi}]$. Then $nT = 0$ so exists $f \in \overline{K}(E')$ such that $\mathrm{div}(f) = n(T) - n(0)$. Pick $T_0 \in E(\overline{K})$ with $\phi(T_0) = T$. Then

$$\phi^*(T) - \phi^*(0) = \sum_{P \in E[\phi]} (P + T_0) - \sum_{P \in E[\phi]} (P)$$

has sum $nT_0 = \hat{\phi}\phi T_0 = \hat{\phi} T = 0$ so exists $g \in \overline{K}(E)$ such that $\mathrm{div}(g) = \phi^*(T) - \phi^*(0)$. Now $\mathrm{div}(\phi^* f) = \phi^*(\mathrm{div}\, f) = n(\phi^*(T) - \phi^*(0)) = \mathrm{div}(g^n)$ so $\phi^* f = c g^n$ for some $c \in \overline{K}^*$. Recaling f, wlog $c = 1$, i.e. $\phi^* f = g^n$.

If $S \in E[\phi]$ then $\tau_S^*(\mathrm{div}\, g) = \mathrm{div}\, g$ so $\mathrm{div}(\tau_S^* g) = \mathrm{div}\, g$ so $\tau_S^* g = \zeta g$ for some $\zeta \in \overline{K}^*$, i.e. $\zeta = \frac{g(X+S)}{g(X)}$ independent of choice of $X \in E(\overline{K})$. Now

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

since $S \in E[\phi]$. Thus $\zeta \in \mu_n$. Finally we define

$$e_\phi(S, T) = \frac{g(X+S)}{g(X)}$$

for any $X \in E$.

Proposition 14.5. e_ϕ *is bliniear and nondegenerate.*

Proof. Linearity in first argument:

$$e_\phi(S_1 + S_2, T) = \frac{g(X + S_1 + S_2)}{g(X + S_2)} \frac{g(X + S_2)}{g(X)} = e_\phi(S_1, T) e_\phi(S_2, T).$$

Linearity in second argument: let $T_1, T_2 \in E'[\hat{\phi}]$. We can find f_i, g_i such that $\mathrm{div}(f_i) = n(T_i) - n(0), \phi^* f_i = g_n^n$. There exists $h \in \overline{K}(E')$ such that

$$\mathrm{div}(h) = (T_1) + (T_2) - (T_1 + T_2) - (0).$$

Then put $f = \frac{f_1 f_2}{h^n}, g = \frac{g_1 g_2}{\phi^*(h)}$. Check

$$\begin{aligned} \mathrm{div}(f) &= n(T_1 + T_2) - n(0) \\ \phi^* f &= \frac{\phi^* f_1 \phi^* f_2}{(\phi^* h)^n} = \left(\frac{g_1 g_2}{\phi^*(h)}\right)^n = g^n \end{aligned}$$

so

$$\begin{aligned} e_\phi(S, T_1 + T_2) &= \frac{g(X+S)}{g(X)} \\ &= \frac{g_1(X+S)}{g_1(X)} \frac{g_2(X+S)}{g_2(X)} \underbrace{\frac{h(\phi(X))}{h(\phi(X+S))}}_{=1} \\ &= e_\phi(S, T_1) e_\phi(S, T_2) \end{aligned}$$

e_ϕ is nondegenerate: fix $T \in E'[\hat{\phi}]$. Suppose $e_\phi(S,T) = 1$ for all $S \in E[\phi]$, so $\tau_S^* g = g$ for all $S \in E[\phi]$. Thus

$$\begin{array}{c} \overline{K}(E) \\ | \\ \phi^* \overline{K}(E') \end{array}$$

is a Galois extension with group $E[\phi]$, with $S \in E[\phi]$ acting as τ_S^*. Thus $g = \phi^* h$ for some $h \in \overline{K}(E')^*$. Thus $\phi^* f = g^n = \phi^* h^n$ so $f = h^n$. Thus $\mathrm{div}\, h = (T) - (0)$ so $T = 0_E$.

For the other direction, we've show $E'[\hat{\phi}] \hookrightarrow \mathrm{Hom}(E[\phi], \mu_n)$. It is an isomorphism by counting. □

Remark.

1. If E, E' and ϕ are defined over K then e_ϕ is Galois equivariant, i.e. $e_\phi(\sigma S, \sigma T) = \sigma(e_\phi(S,T))$.
2. Taking $\phi = [n] : E \to E$ (so $\hat{\phi} = [n]$) gives $e_n : E[n] \times E[n] \to \mu_{n^2} = \mu_n$ since e_n is bilinear.

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

Proof. We claim exists $S, T \in E[n]$ such that $e_n(S,T)$ is a primitive nth root of unit, say ζ_n. We pick $T \in E[n]$ of order n. The group homomorphism $E[n] \to \mu_n, S \mapsto e_n(S,T)$ has image μ_d for some $d \mid n$. Then $e_n(S, dT) = 1$ for all $S \in E[n]$. By nondegeneracy $dT = 0$ so $d = n$, proving the claim. To show $\zeta_n \in K$ we use Galois equivariance: for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$\sigma(\zeta_n)\sigma(e_n(S,T)) = e_n(\sigma S, \sigma T) = e_n(S,T) = \zeta_n$$

so $\zeta_n \in K$. □

Example. There does not exist $E/\mathbb{Q}$ with $E(\mathbb{Q})_{\mathrm{tor}} \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Remark. In fact e_n is alternating, i.e. $e_n(T,T) = 1$ for all $T \in E[n]$. By expanding $e_n(S+T, S+T)$, we have e_n alternating: $e_n(S,T) = e_n(T,S)^{-1}$.

15 Galois cohomology

Let G be a group and A a G-module, i.e. an abelian group with an action of G via group homomorphism (in other words a $\mathbb{Z}[G]$-module). We begin with a very practical definition of group cohomology (or more precisely, H^0 and H^1).

Definition (group cohomology)**.** We define

$$H^0(G,A) = A^G = \{a \in A : \sigma(a) = a \text{ for all } \sigma \in G\}.$$

We define the first cochains, cocyles and coboundaries

$$\begin{aligned} C^1(G,A) &= \{G \to A\} \\ Z^1(G,A) &= \{(a_\sigma)_{\sigma \in G} : a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\} \\ B^1(G,A) &= \{(\sigma b - b)_{\sigma \in G} : b \in A\} \end{aligned}$$

Then we define

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

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

We quote some elementary results from homological algebra:

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

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

gives rise to a long exact sequence of abelian groups

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C)$$

Proof. Omitted. We note the definition of $\delta : C^G \to H^1(G,A)$: given $c \in C^G$, exists $b \in B$ such that $\psi(b) = c$. Then

$$\tau(\sigma b - b) = \sigma c - c = 0$$

for all $\sigma \in G$ so $\sigma b - b = \phi(a_\sigma)$ for some $a_\sigma \in A$. Can show $(a_\sigma)_{\sigma \in G} \in Z^1(G,A)$. We define $\delta(c)$ to be the class of $(a_\sigma)_{\sigma \in G}$ in $H^1(G,A)$. ☐

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

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A)$$

Proof. Omitted. ☐

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

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

Then

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

Here the direct limit is with respect to inflation maps.

Theorem 15.3 (Hilbert theorem 90)**.** *Suppose L/K is a finite Galois extension. Then*

$$H^1(\mathrm{Gal}(L/K), L^*) = 0.$$

Proof. Let $G = \mathrm{Gal}(L/K)$ and $(a_\sigma)_{\sigma \in G} \in Z^1(G, L^*)$. Distinct automorphisms are linearly independent so exists y such that

$$x = \sum_{\tau \in G} a_\tau^{-1} \tau(y) \neq 0.$$

For $\sigma \in G$,

$$\sigma(x) = \sum_{\tau \in G} \sigma(a_\tau)^{-1} \sigma\tau(y) = a_\sigma \sum_{\tau \in G} a_{\sigma\tau}^{-1} \sigma\tau(y) = a_\sigma x.$$

Thus $a_\sigma = \frac{\sigma(x)}{x}$ so $(a_\sigma)_{\sigma \in G} \in B^1(G, L^*)$. Thus $H^1(G, L^*) = 0$. □

Corollary 15.4. $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$.

As an application, assume $\mathrm{char}\, K \nmid n$. There is a short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow \mu_n \longrightarrow \overline{K}^* \xrightarrow{x \mapsto x^n} \overline{K}^* \longrightarrow 0$$

so we have a long exact sequence

$$K^* \xrightarrow{x \mapsto x^n} K^* \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$$

so

$$H^1(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n.$$

Now let's revisit Kummer theory. If $\mu_n \subseteq K$ then

$$\mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mu_n) \cong K^*/(K^*)^n.$$

Finite subgroups of LHS are of the form $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$ for L/K a finite abelian extension of exponent dividing n. Thus we get another proof of Theorem 11.2.

Remark. Every continuous group homomorphism $\chi : \mathrm{Gal}(\overline{K}/K) \to \mu_n$ factorises uniquely as

$$\mathrm{Gal}(\overline{K}/K) \twoheadrightarrow \mathrm{Gal}(L/K) \hookrightarrow \mu_n$$

for L the fixed field of $\ker \chi$.

Notation. Since we are dealing with Galois cohomology, write $H^1(K,-)$ for $H^1(\mathrm{Gal}(\overline{K}/K),-)$.

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

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

which induces a long exact seqeucne

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

from which we get a short exact sequence

$$0 \longrightarrow \tfrac{E'(K)}{\phi E(K)} \longrightarrow H^1(K,E[\phi]) \longrightarrow H^1(K,E)[\phi_*] \longrightarrow 0$$

Now take K a number field. For each place v of K we fix an embedding $\overline{K} \subseteq \overline{K}_v$. Then $\mathrm{Gal}(\overline{K}_V/K_V) \subseteq \mathrm{Gal}(\overline{K}/K)$. We get a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{E'(K)}{\phi E(K)} & \longrightarrow & H^1(K,E[\phi]) & \longrightarrow & H^1(K,E)[\phi_*] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_V} & & \downarrow{\scriptstyle \mathrm{res}_V} & & \\
0 & \longrightarrow & \frac{E'(K_v)}{\phi E(K_v)} & \longrightarrow & H^1(K_v,E[\phi]) & \longrightarrow & H^1(K_v,E)[\phi_*] & \longrightarrow & 0
\end{array}$$

Definition (Selmer group)**.** The *ϕ-Selmer group* $S^{(\phi)}(E/K)$ is the kernel of the dotted arrow in

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{E'(K)}{\phi E(K)} & \longrightarrow & H^1(K,E[\phi]) & \longrightarrow & H^1(K,E)[\phi_*] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_V} & \searrow & \downarrow{\scriptstyle \mathrm{res}_V} & & \\
0 & \longrightarrow & \prod_v \frac{E'(K_v)}{\phi E(K_v)} & \xrightarrow{\delta_v} & \prod_v H^1(K_v,E[\phi]) & \longrightarrow & \prod_v H^1(K_v,E)[\phi_*] & \longrightarrow & 0
\end{array}$$

so

$$\begin{aligned} S^{(\phi)}(E/K) &= \ker(H^1(K,E[\phi]) \to \prod_v H^1(K_v,E)) \\ &= \{\alpha \in H^1(K,E[\phi]) : \mathrm{res}_V(\alpha) \in \mathrm{im}(\delta_v) \text{ for all } v\} \end{aligned}$$

Definition (Tate-Shafarevich group)**.** The *Tate-Shafarevich group* is

$$Ш(E/K) = \ker(H^1(K,E) \to \prod_v H^1(K_v,E)).$$

We get a short exact sequence

$$0 \longrightarrow \tfrac{E'(K)}{\phi E(K)} \longrightarrow S^{(\theta)}(E/K) \longrightarrow (E/K)[\phi_*] \longrightarrow 0$$

In particular we can specialise to $\phi = [n]$. Rearranging our proof of weak Mordell-Weil gives

Theorem 15.5. *$S^{(n)}(E/K)$ is finite.*

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

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(\mathrm{Gal}(L/K), E(L)[n]) & \xrightarrow{\text{inf}} & H^1(K, E[n]) & \xrightarrow{\text{res}} & H^1(L, E[n]) \\ & & & & \big\downarrow\supseteq & & \big\downarrow\supseteq \\ & & & & S^{(n)}(E/K) & \longrightarrow & S^{(n)}(E/K) \end{array}$$

As $H^1(\mathrm{Gal}(L/K), E(L)[n])$ is finite, we we extend our field K and assume $E[n] \subseteq E(K)$ and hence $\mu_n \subseteq K$. Thus $E[n] \cong \mu_n \times \mu_n$ as Galois modules. Thus

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

Let S be the union of primes of bad reduction for E, v such that $v \mid n$ and the infinite places. Note S is a finite set of places.

Definition. The subgroup of $H^1(K, A)$ unramified outside S is

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

There is a commutative diagram with exact rows

$$\begin{array}{ccccc} E(K_v) & \xrightarrow{\times n} & E(K_v) & \xrightarrow{\delta_v} & H^1(K_v, E[n]) \\ \big\downarrow & & \big\downarrow & & \big\downarrow \text{res} \\ E(K_v^{\mathrm{nr}}) & \xrightarrow{\times n} & E(K_v^{\mathrm{nr}}) & \xrightarrow{0} & H^1(K_v^{\mathrm{nr}}, E[n]) \end{array}$$

Multiplication by n on the second row is surjective for all $v \notin S$ (Thm 9.9). Thus

$$\begin{aligned} S^{(n)}(E/K) &= \{\alpha \in H^1(K, E[n]) : \mathrm{res}_v(\alpha) \in \mathrm{im}(\delta_v) \text{ for all } v\} \\ &\subseteq H^1(K, E[n]; S) \\ &\cong H^1(K, \mu_n; S) \times H^1(K, \mu_n; S) \end{aligned}$$

(?using the fact that $\mathrm{res} \circ \delta_v = 0$) But

$$H^1(K, \mu_n; S) = \ker(K^*/(K^*)^n \to \prod_{v \notin S} (K_v^{\mathrm{nr}})^*/(K_v^{\mathrm{nr}})^{*n}) = K(S, n)$$

which is finite. □

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

16 Descent by cyclic isogeny

Let E, E' be elliptic curves over a number field K. Let $\phi : E \to E'$ be an isogeny of degree n. Suppose $E'[\hat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$ is generated by $T \in E'(K)$. Then $E[\phi] \cong \mu_n, S \mapsto e_\phi(S,T)$ as a $\text{Gal}(\overline{K}/K)$-module. We have a short exact sequence of $\text{Gal}(\overline{K}/K)$-modules

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

giving rise to long exact sequence

$$\begin{array}{ccccccc} E(K) & \longrightarrow & E'(K) & \xrightarrow{\delta} & H^1(K, \mu_n) & \longrightarrow & H^1(K, E) \\ & & & \searrow^{\alpha} & \downarrow \cong & & \\ & & & & K^*/(K^*)^n & & \end{array}$$

Theorem 16.1. *Let $f \in K(E')$ and $g \in K(E)$ with $\text{div}(f) = n(T) - n(0)$ and $\phi^* f = g^n$. Then $\alpha(P) = f(P) \pmod{(K^*)^n}$ for all $P \in E'(K) \setminus \{0, T\}$.*

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

$$e_\phi(\sigma Q - Q, T) = \frac{g(\sigma Q - Q + X)}{g(X)} = \frac{g(\sigma Q)}{g(Q)} = \frac{\sigma(g(Q))}{g(Q)} = \frac{\sigma(\sqrt[n]{f(P)})}{\sqrt[n]{f(P)}}$$

But

$$\begin{aligned} H^1(K, \mu_n) &\cong K^*/(K^*)^n \\ \sigma \mapsto \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}} &\leftarrow\!\shortmid x \end{aligned}$$

so $\alpha(P) = f(P) \pmod{(K^*)^n}$. □

Descent by 2-isogeny Let $E : y^2 = x(x^2 + ax + b), E' : y^2 = x(x^2 + a'x + b')$ where $b(a^2 - 4b) \neq 0, a' = -2a, b' = a^2 - 4b$. Define

$$\begin{aligned} &\phi : E \to E' \\ &(x, y) \mapsto ((\frac{y}{x})^2, \frac{y(x^2 - b)}{x^2}) \\ &\hat{\phi} : E' \to E \\ &(x, y) \mapsto (\frac{1}{4}(\frac{y}{x})^2, \frac{y(x^2 - b')}{8x^2}) \end{aligned}$$

Check they are dual to each other. Have $E[\phi] = \{0, T\}, E'[\hat{\phi}] = \{0, T'\}$ where $T = (0, 0) \in E(K), E' = (0, 0) \in E'(K)$.

Proposition 16.2. *There is a group homomorphism*

$$E'(K) \to K^*/(K^*)^2$$
$$(x, y) \mapsto \begin{cases} x \pmod{(K^*)^2} & x \neq 0 \\ b' \pmod{(K^*)^2} & x = 0 \end{cases}$$

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

Proof. Either apply theorem 16.1 with $f = x \in K(E'), g = \frac{y}{x} \in K(E)$, or direct calculation, see example sheet 4. □

Let

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

Lemma 16.3. $2^{\operatorname{rank} E(K)} = \frac{1}{4}|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|$.

Proof. Since $\hat{\phi}\phi = [2]_E$ there is an exact sequence

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K)[2] \xrightarrow{\phi} E'(K)[\hat{\phi}] \hookrightarrow \frac{E'(K)}{\phi E(K)} \xrightarrow{\hat{\phi}} \frac{E(K)}{2E(K)} \longrightarrow \frac{E(K)}{\hat{E}'(K)} \longrightarrow 0$$

so the alternative product of group orders is 1. Thus

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

By Mordell-Weil $E(K) \cong \Delta \times \mathbb{Z}^r$ where Δ is finite and r is the rank of $E(K)$. Thus

$$\frac{E(K)}{2E(K)} \cong \frac{\Delta}{2\Delta} \times (\mathbb{Z}/2\mathbb{Z})^r, E(K)[2] \cong \Delta[2].$$

Since Δ is finite, $\frac{\Delta}{2\Delta}$ and $\Delta[2]$ have the same order. The result thus follows. □

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

Proof. Must show if $x, y \in K$, $y^2 = x(x^2 + ax + b)$ and $v_\mathfrak{p}(b) = 0$ then $v_\mathfrak{p}(x)$ is even. If $v_\mathfrak{p}(x) < 0$ then by lemma 9.1 $v_\mathfrak{p}(x) = -2r, v_\mathfrak{p}(y) = -3r$ for some $r \geq 1$. If $v_\mathfrak{p}(x) > 0$ then $v_\mathfrak{p}(x^2 + ax + b) = 0$ so $v_\mathfrak{p}(x) = v_\mathfrak{p}(y^2) = 2v_\mathfrak{p}(y)$. □

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

$$w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$$

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 may assume $b_1, b_2 \notin (K^*)^2$. $b_1(K^*)^2 \in \operatorname{im}\alpha_E$ if and only if exists $(x,y) \in E(K)$ such that $x = b_1 t^2$ for some $t \in K^*$, so

$$y^2 = b_1 t^2 ((b_1 t^2)^2 + a b_1 t^2 + b)$$

so

$$(\frac{y}{b_1 t})^2 = b_1 t^4 + a t^2 + b_2$$

so have solution $(u,v,w) = (t, 1, \frac{w}{b_1 t})$.

Conversely if (u,v,w) is a solution then $uv \neq 0$. Check $(b_1(\frac{u}{v})^2, b_1\frac{uw}{v^3}) \in E(K)$. ☐

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

Example. $E : y^2 = x^3 - x$. By lemma 16.4, $\operatorname{im}\alpha_E \subseteq \langle -1 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. But we know $(0,0) \in \operatorname{im}\alpha_E$, equality. $E' : y^2 = x^3 + 4x$, $\operatorname{im}\alpha_{E'} \subseteq \langle -1, 2 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Need to check

$$\begin{aligned} b_1 &= 1, w^2 = -u^4 - 4u^4 \\ b_1 &= 2, w^2 = 2u^4 + 2v^4 \\ b_1 &= -2, w^2 = -2u^4 - 2v^4 \end{aligned}$$

The first and third are not soluble over $\mathbb{R}$. The second has solution $(u,v,w) = (1,1,2)$ so $\operatorname{im}\alpha_{E'} = \langle 2 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Thus $\operatorname{rank} E(\mathbb{Q}) = 0$ so 1 is not a congruent number.

Example. $E : y^2 = x^3 + px$ where p is a prime, $p = 5 \pmod 8$. $b_1 = -1, w^2 = -u^4 - pv^4$ is insoluble over $\mathbb{R}$ so $\operatorname{im}\alpha_E = \langle p \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. $E' : y^2 = x^3 - 4px$ so $\operatorname{im}\alpha_{E'} \subseteq \langle -1, 2, p \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Note $\alpha_{E'}(T') = (-4p)(\mathbb{Q}^*)^2 = (-p)(\mathbb{Q}^*)^2$ so only need to consider

$$\begin{aligned} b_1 &= 2, w^2 = 2u^4 - 2pv^4 \\ b_1 &= -2, w^2 = -2u^4 + 2pv^4 \\ b_1 &= p, w^2 = pu^4 - 4v^4 \end{aligned}$$

Suppose equation 1 is soluble. wlog $u, v, w \in \mathbb{Z}, \gcd(u,v) = 1$. If $p \mid u$ then $p \mid w$ and then $p \mid v$, absurd. Thus $w^2 = 2u^4 \neq 0 \pmod p$ so $\left(\frac{2}{p}\right) = 1$, contradicting $p = 5 \pmod 8$.

Likewise 2 has no solution since $\left(\frac{-2}{p}\right) = -1$.

To recall, for $E : y^2 = x(x^2 + ax + b)$, $\phi : E \to E'$ a 2-isogeny. $w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4 (*)$. Have a short exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E'(\mathbb{Q})}{\phi E(\mathbb{Q})} & \longrightarrow & S^{(\phi)}(E/\mathbb{Q}) & \longrightarrow & Ш(E/\mathbb{Q})[\phi_*] & \longrightarrow & 0 \\ & & & \searrow^{\alpha_{E'}} & & & & & \\ & & & & \mathbb{Q}^*/(\mathbb{Q}^*)^2 & & & & \end{array}$$

$$\begin{aligned} \operatorname{im}\alpha_{E'} &= \{b_1(\mathbb{Q}^*)^2 : * \text{ is soluble over } \mathbb{Q}\} \\ \subseteq S^{(\phi)}(E/\mathbb{Q}) &= \{b_1(\mathbb{Q}^*)^2 : * \text{ is soluble over } \mathbb{R} \text{ and over } \mathbb{Q}_p \text{ for all } p\} \end{aligned}$$

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

Example (example 2 continued)**.** $E : y^2 = x^3 + px$, $p = 5 \pmod 8$, $w^2 = pu^4 - 4v^4 \dagger$. $E(\mathbb{Q})$ has rank 0 if ($\dagger$) is insoluble over $\mathbb{Q}$ and rank 1 if soluble. By the fact we only have to look at p- and 2-adics.

- $\dagger$ is soluble over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right) = 1$ so $-1 \in (\mathbb{Z}_p^*)^2$ (by Hensel's lemma).
- soluble over $\mathbb{Q}_2$ since $p - 4 = 1 \pmod 8$ so $p - 4 \in (\mathbb{Z}_2^*)^2$.
- soluble over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$.

We can try to spot solutions:

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

Conjecture: $\text{rank}(E(\mathbb{Q})) = 1$ for all primes $p = 5 \pmod 8$.

Example (Lind)**.** $E : y^2 = x^3 + 17x$. $\operatorname{im} \alpha_E = \langle 17 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. $E' : y^2 = x^3 - 68x$. $\operatorname{im} \alpha_{E'} \subseteq \langle -1, 2, 17 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Consider $b_1 = 2$. $w^2 = 2u^4 - 34v^4$. Replace w by $2w$ and divide through by 2 to get $C : 2w^2 = u^4 - 17v^4$. Denote by

$$C(K) = \{(u, v, w) \in K^3 \setminus \{0\} \text{ satisfying } C\}/\sim$$

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

$C(\mathbb{Q}_2) \neq \emptyset$ as $17 \in (\mathbb{Z}_2^*)^4$. $C(\mathbb{Q}_{17}) \neq \emptyset$ since $2 \in (\mathbb{Z}_{17}^*)^2$. $C(\mathbb{R}) \neq \emptyset$ since $\sqrt{2} \in \mathbb{R}$. Thus $C(\mathbb{Q}_v) \neq \emptyset$ for all places of $\mathbb{Q}$. However it has no solution over $\mathbb{Q}$: suppose $(u, v, w) \in C(\mathbb{Q})$. wlog $u, v \in \mathbb{Z}, \gcd(u, v) = 1$, then $w \in \mathbb{Z}$ and can assume $w > 0$. If $17 \mid w$ then $17 \mid u$ and then $17 \mid v$, absurd. So if $p \mid w$ then $p \neq 17$ and $\left(\frac{17}{p}\right) = 1$ so by quadratic reciprocity $\left(\frac{p}{17}\right) = \left(\frac{17}{2}\right) = 1$ (for p odd. For $p = 2$ have $\left(\frac{2}{17}\right) = 1$. Thus $\left(\frac{w}{17}\right) = 1$. But $2w^2 = u^4 \pmod{17}$ so $2 \in (\mathbb{F}_{17}^*)^4 = \{\pm 1, \pm 4\}$, absurd. Thus $C(\mathbb{Q}) = \emptyset$. C is a counterexample to the Hasse principle. It representes a non-trivial element in $Ш(E/\mathbb{Q})$.

Birch Swinnerton-Dyer conjecture Let $E/\mathbb{Q}$ be an elliptic curve.

Definition (l-function)**.** The *L-function* of E is $L(E, s) = \prod_p L_p(E, s)$ where

$$L_p(E, s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1} & \text{good reduction} \\ (1 - p^{-s})^{-1} & \text{split multiplicative reduction} \\ (1 + p^{-s})^{-1} & \text{nonsplit multiplicative reduction} \\ 1 & \text{additive reduction} \end{cases}$$

where $\#(\mathbb{F}_p) = p + 1 - a_p$.

Hasse's theorem says that $|a_p| < s\sqrt{p}$ so $L(E, s)$ converges for $\operatorname{Re} s > \frac{3}{2}$.

Theorem 16.6 (Wiles, Breuil, Conrad, Diamond, Taylor)**.** *$L(E,s)$ is the L-function of a weight 2 modular form and hence has an analytic continuation to all of $\mathbb{C}$ (and a functional equation relating $L(E,s)$ and $L(E,2-s)$).*

Conjecture (weak Birch Swinnerton-Dyer conjecutre)**.** $\operatorname{ord}_{s=1} L(E,s) = \operatorname{rank} E(\mathbb{Q})$.

Assuming weak BSD and let $r = \operatorname{ord}_{s=1} L(E,s)$ be the analytic rank, we have

Conjecture (strong Birch Swinnerton-Dyer conjecutre)**.**

$$\lim_{s\to 1} \frac{1}{(s-1)^r} L(E,s) = \frac{\Omega_E |Ш(E/\mathbb{Q})| \operatorname{Reg} E(\mathbb{Q}) \prod_P c_p}{|E(\mathbb{Q})_{\text{tors}}|^2}$$

where

- $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)] =$ *tamagawa number of* $E/\mathbb{Q}_p$*, if* $\frac{E(\mathbb{Q})}{E(\mathbb{Q})_{\text{tors}}} = \langle P_1, \dots, P_r \rangle$ *then*
$$\operatorname{Reg} E(\mathbb{Q}) = \det([P_i, P_j])_{ij}$$
where $[P,Q] = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$.
- $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{|2y + a_1 x + a_3|}$ *where a_i is the coefficient of a globally minimal Weierstrass equation for E.*

Best result so far:

Theorem 16.7 (Kolvragin)**.** *If $\operatorname{ord}_{s=1} L(E,s) = 0$ or 1 then weak BSD is trus and $|Ш(E/\mathbb{Q})| < \infty$.*

Index

I-adic topology, 28
L-function, 61
j-invariant, 11

Birch Sinnerton-Dyer conjecture, 61

canonical height, 45, 49

divisor, 7
- effective, 7
- linearly equivalent, 13

dual isogeny, 51

elliptic curve, 10
ellptic curve, 3

formal group, 30
Frobenius endomorphism, 25

good reduction, 39
group cohomology, 54

Hasse's theorem, 25
height, 47, 48
Hensel's lemma, 28
Hilbert theorem 90, 55

inflation-restriciton exact sequence, 54
invariant differential, 23
isogeny, 17

kernel of reduction, 35
Kummer pairing, 42

maximal unramified extension, 37
Mordell-Weil theorem, 45

Picard group, 13

ramification index, 8
rational plane curve, 5
reduction, 35

Selmer group, 56
sum, 52

Tate-Shafarevich group, 56
torsion subgroup, 15

uniformiser, 6
unramified extension, 37

Weierstrass equation, 8
- integral, 33
- minimal, 33

Weierstrass function, 3
Weil pairing, 52

zeta function, 26