# Elliptic Curves

Cambridge Part III, Lent 2023
Taught by Tom Fisher
Notes taken by Leonard Tomczak

# Contents

# 1 Fermat's Method of Infinite Descent

We consider a right angle triangle $\Delta$ with side lengths $a, b, c > 0$ such that $a^2 + b^2 = c^2$ and area $\frac{1}{2}ab$. $\Delta$ is *rational* if $a, b, c \in \mathbb{Q}$. $\Delta$ is *primitive* if $a, b, c \in \mathbb{Z}$ are coprime.

**Lemma 1.1.** *Every primitive triangle is of the form $\{a, b\} = \{u^2 - v^2, 2uv\}, c = u^2 + v^2$ for some integers $u > v > 0$.*

*Proof.* It is easy to see that exactly one of $a, b$ (wlog say $b$) is even. So $(b/2)^2 = \frac{c+a}{2}\frac{c-a}{2}$. The factors on the right are coprime positive integers. By unique factorization in $\mathbb{Z}$ we get that $\frac{c+a}{2} = u^2, \frac{c-a}{2} = v^2$ for suitable $u, v \in \mathbb{Z}$. The claim follows. □

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

N.B. It suffices to consider $D \in \mathbb{Z}_{>0}$ squarefree.

E.g. $D = 5, 6$ are congruent.

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

*Proof.* The first lemma shows that $D$ is congruent iff $Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}, w \neq 0$. Then put $x = u/v, y = w/v^2$. □

Fermat showed that 1 is not a congruent number:

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

$$w^2 = uv(u + v)(u - v) \qquad (*)$$

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

*Proof.* Wlog $u, v$ coprime, $u > 0, w > 0$. If $v < 0$, then replace $(u, v, w)$ by $(-v, u, w)$. If $u \equiv v \bmod 2$, 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 pairwise positive integers with product a square. By unique factorization in $\mathbb{Z}$ $u = a^2, v = b^2, u+v = c^2, u - v = d^2$ for some $a, b, c, d \in \mathbb{Z}_{>0}$. Since $u \not\equiv v \bmod 2$, both $c$ and $d$ are odd. Hence

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

This is a primitive triangle. Its area is $\frac{c^2-d^2}{8} = \frac{v}{4} = (b/2)^2$. Let $w_1 = b/2$. By the first lemma we get again $w_1^2 = u_1 v_1 (u_1 + v_1)(u_1 - v_1)$ for some $u_1, v_1 \in \mathbb{Z}$. So 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 descent, there is no solution to $(*)$ □

## 1.1 A Variant for Polynomials

Let $K$ be a field of characteristic not equal to 2 with algebraic closure $K^{\text{alg}}$.

**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 $K = K^{\text{alg}}$. Changing coordinates on $\mathbb{P}^1$ we may assume the ratios $(\alpha : \beta)$ are $(1:0), (0:1), (1:-1), (1:-\lambda)$ for some $\lambda \in K \setminus \{0, 1\}$. We have $u = a^2, v = b^2, u - v = (a+b)(a-b), u - \lambda v = (a + \mu b)(a - \mu b)$ where $\mu = \sqrt{\lambda}$. By unique factorization in $K[t]$ we get that $a+b, a-b, a+\mu b, a-\mu b$ are all squares. But $\max(\deg a, \deg b)) \leq \frac{1}{2}\max(\deg u, \deg v)$. So by Fermat's method of infinite descent $u, v \in K$. □

**Definition.**

*(i) (Preliminary definition) An* elliptic curve *$E/K$ is the projective closure of the plane affine curve defined by*

$$y^2 = f(x)$$

*where $f \in K[x]$ is a monic cubic separable polynomial.*

*(ii) For $L/K$ any field extension we let*

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

*where $O = (0 : 1 : 0)$ is the point at infinity.*

The previous results show that for $E : y^2 = x^3 - x$ we have $E(\mathbb{Q}) = \{O, (0,0), (\pm 1, 0)\}$.

**Corollary 1.5.** *Let $E/K$ be an elliptic curve. Then $E(K(t)) = E(K)$.*

*Proof.* Wlog $K = K^{\text{alg}}$. 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 $x = u/v$ where $u, v \in K[t]$ are coprime. Then we get $w^2 = uv(u-v)(u-\lambda v)$ for some $w \in K[t]$. By unique factorization in $K[t]$, the four polynomials $u, v, u-v, u-\lambda v$ are squares. So by our previous result $u, v \in K$, so $x, y \in K$. □

This shows that elliptic curves are not rational.

# 2 Some Remarks on Algebraic Curves

For this section we assume $K = K^{\text{alg}}$.

**Proposition 2.1.** *Let $C$ be a smooth projective curve and $g(C)$ its genus.*

*(i) $C$ is rational iff $g(C) = 0$.*

*(ii) $C$ is an elliptic curve (in our sense) iff $g(C) = 1$.*

Recall that a *uniformizer* of a curve $C$ at a smooth point $P$ is a function $t \in K(C)^*$ such that $\operatorname{ord}_P t = 1$.

**Example.** Let $C = \{g = 0\} \subseteq \mathbb{A}^2$ be a plane curve with $g \in K[x, y]$ irreducible. Suppose $P = (0, 0) \in C$ and write $g = g_0 + g_1(x, y) + g_2(x, y) + \dots$ and where $g_i$ is homogeneous of degree $i$. Write $g_1(x, y) = \alpha x + \beta y$. Assume that $C$ is non-singular so that $\alpha, \beta$ are not both zero. Then $\gamma x + \delta y \in K(C)$ is a uniformizer at $P$ iff $\alpha\delta - \beta\gamma \neq 0$.

**Example.** Let $\{y^2 = x(x - 1)(x - \lambda)\} \subseteq \mathbb{A}^2$ where $\lambda \neq 0, 1$. The projective closure is

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

where $x = X/Z, y = Y/Z$. $P = (0 : 1 : 0)$. Put $t = X/Y, w = Z/Y$. Then $w = t(t - w)(t - \lambda w)$ (dehomogenize w.r.t. $y$) Now $P$ is the point $(t, w) = (0, 0)$. This is a smooth point with $\operatorname{ord}_p(t) = \operatorname{ord}_p(t - w) = \operatorname{ord}_p(t - \lambda w) = 1$, so $\operatorname{ord}_p(w) = 3$. Then $\operatorname{ord}_p(x) = \operatorname{ord}_p(t/w) = -2, \operatorname{ord}_p(y) = -3$.

Recall the Riemann-Roch Theorem for smooth curves of genus 1. If $D$ is a divisor, then:

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

Assume $K = K^{\text{alg}}$ and $\operatorname{char} K \neq 2$.

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

*Proof.* We may change coordinates such that $P = (0 : 1 : 0)$ and $T_p C = \{Z = 0\}$. Let $C$ be defined by $F(X, Y, Z)$. $P$ is a point of inflection, so $F(t, 1, 0) = t^3$, i.e. $F$ has no terms

$X^2Y, XY^2, Y^3$. Therefore $F \in \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \rangle$. The monomials $Y^2Z, X^3$ must appear in $F$, as $P$ is non-singular and $\{Z = 0\} \not\subseteq C$. We are free to rescale $X, Y, Z$ and $F$. Wlog $C$ is defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \quad \text{“Weierstraß equation”}$$

Substituing $Y \mapsto Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$ we may assume $a_1 = a_3 = 0$. Now $C : Y^2Z = Z^3f(X/Z)$ for some monic cubic polynomial $f$. Since $C$ is smooth, $f$ has distinct roots, wlog $0, 1, \lambda$. Then $C$ has the equation

$$Y^2Z = X(X - Z)(X - \lambda Z). \quad \text{“Legendre form”}$$

$\square$

Remark: It can be shown that the points of inflection on a plane curve $C = \{F(X_1, X_2, X_3) = 0\} \subseteq \mathbb{P}^2$ are given by

$$F = 0 = \det \left( \frac{\partial^2 F}{\partial X_i \partial X_j} \right).$$

# 3 Weierstraß Equations

In this chapter, $K$ is a perfect field with algebraic closure $K^{\text{alg}}$.

**Definition.** *An* elliptic curve $E/K$ *is a smooth projective curve of genus* 1 *defined over* $K$*, with a specified* $K$*-rational point* $O_E$*.*

*A morphisms of elliptic curves is a morphism of algebraic curves preserving the base point* $O$*.*

**Example.** $\{X^3 + pY^3 + p^2Z^3 = 0\} \subseteq \mathbb{P}^2$ is a smooth projective curve of genus 1 defined over $\mathbb{Q}$, but it is not an elliptic curve over $\mathbb{Q}$, since it has no $\mathbb{Q}$-rational points.

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

Fact: If $D \in \text{Div}(E)$ is defined over $K$ (i.e. fixed by $\text{Gal}(K^{\text{alg}}/K)$), then $\mathcal{L}(D)$ has a basis in $K(E)$.

*Proof.* Pick bases $1, x$ resp. $1, x, y$ of $\mathcal{L}(2O_E) \subseteq \mathcal{L}(3O_E)$. Note that $\text{ord}_{O_E}(x) = -2$ and $\text{ord}_{O_E}(y) = -3$. The seven elements $1, x, y, x^2, xy, x^3, y^2$ in the 6-dimensional vector space $\mathcal{L}(6O_E)$ must satisfy a dependence relation. Leaving out $x^3$ or $y^2$ gives a basis for $\mathcal{L}(6O_E)$ since each term has a different order pole at $O_E$. Therefore the coefficients of $x^3$ and $y^2$ are non-zero. Rescaling $x, y$ and the whole equation we get

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

for some $a_i \in K$. Let $\phi : E \to E' \subseteq \mathbb{P}^2, P \mapsto (x(P), y(P) : 1)$. This is a morphism and $\phi(P) = ((x/y)(P) : 1 : (1/y)(P))$, hence $\phi(O_E) = (0 : 1 : 0)$. We have $\deg \phi = [K(E) : \phi^*K(E')]$ and $\phi^*K(E') = K(x, y)$. Since $x, y$ have degree 2 resp. 3, we see that $\deg \phi = 1$, so $\phi$ is birational.

If $E'$ is singular, then $E, E'$ are rational, so $E'$ is non-singular and $\phi$ is thus an isomorphism. □

**Proposition 3.2.** *Let* $E, E'$ *be elliptic curves over* $K$ *in Weierstraß form. Then* $E \cong E'$ *over* $K$ *iff the equations are related by a change of variables of the form*

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

*for some* $u, r, s, t \in K$*,* $u \neq 0$*.*

*Proof.* $\langle 1, x\rangle = \mathcal{L}(2, O_E) = \langle 1, x'\rangle$, so $x = \lambda x' + r$ for some $\lambda, r \in K, \lambda \neq 0$. Similarly for $y$, we get that $y = \mu y' + \sigma x' + t$ for some $\mu, \sigma, t \in K, \mu \neq 0$. looking at the coefficients of $x^3, y^2$ we see that $\lambda^3 = \mu^2$, so $\lambda = u^2, \mu = u^3$ for some $u \neq 0$. Put $s = \sigma/u^2$. □

A Weierstraß equation defines an elliptic curve iff it defines a smooth curve which is the case iff

$$\Delta(a_1, \dots, a_6) \neq 0$$

where $\Delta \in \mathbb{Z}[a_1, \dots, a_6]$ is a certain polynomial.

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

**Corollary 3.3.** *Assume* $\operatorname{char} K \neq 2, 3$. *Then two elliptic curves*

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

*are isomorphic over $K$ iff $a' = u^4 a, b' = u^6 b$ for some $u \in K^*$.*

*Proof.* $E$ and $E'$ are related by a substitution as in the proposition with $r = s = t = 0$. □

**Definition.** *The $j$-invariant of $E$ is* $j(E) = \frac{1728(4a^3)}{4a^3+27b^2}$.

**Corollary 3.4.** $E \cong E' \implies j(E) = j(E')$. *The converse holds if $K = K^{\text{alg}}$.*

*Proof.* By the the previous corollary

$$\begin{aligned} E \cong E' &\Leftrightarrow a' = u^4 a, b' = u^6 b \text{ for some } u \in K^* \\ &\Rightarrow (a^3 : b^2) = ((a')^3 : (b')^2) \\ &\Leftrightarrow j(E) = j(E') \end{aligned}$$

and the converse holds if $K = K^{\text{alg}}$. □

# 4 The Group Law

Let $E \subseteq \mathbb{P}^2$ be a smooth plane cubic. $E$ meets any line in 3 points counted with multiplicity. Let $O_E, P, Q \in E$. Let $S$ be the third point of intersection of $E$ and $PQ$. Let $R$ be the third point of intersection of $E$ and $O_E S$. Define $P \oplus Q := R$. If $P = Q$, then take the tangent line $T_P E$ at $P$ instead of $PQ$, etc.

This is called "the cord and tangent process".

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

*Proof.*

(i) commutativity of $\oplus$ is clear.

(ii) $O_E$ is the identity.

(iii) Inverses: Let $S$ be the third point of $\cap$ of $E$ and $T_{O_E}E$. Let $Q$ be the third point of $\cap$ of $E$ and $PS$. Then $P \oplus Q = O_E$.

(iv) Associativity: Harder! □

Define $\psi : E \to \mathrm{Pic}^0(E)$ by $P \mapsto [(P) - (O_E)]$.

**Proposition 4.2.**

*(i)* $\psi(P \oplus Q) = \psi(P) + \psi(Q)$.

*(ii)* $\psi$ *is a bijection.*

*Proof.*

(i) Let $l$ resp. $m$ be the linear forms whose zero sets are the lines $PQ$ resp. $O_E S$. Then $\mathrm{div}(l/m) = (P) + (S) + (Q) - (O_E) - (S) - (R) = (P) + (Q) - (O_E) - (P \oplus Q)$. Therefore $(P \oplus Q) - (O_E) \sim (P) - (O_E) + (Q) - (O_E)$, i.e. $\psi(P \oplus Q) = \psi(P) + \psi(Q)$.

(ii) Injective: Suppose $\psi(P) = \psi(Q)$, for $P \neq Q$. So there exists $f \in K^{\mathrm{alg}}(E)$ such that $\mathrm{div}\, f = (P) - (Q)$. Then the map $f : E \to \mathbb{P}^1$ has degree 1, so $E$ is rational, a contradiction.

Surjective: Let $[D] \in \mathrm{Pic}^0(E)$. Then $D + (O_E)$ has degree 1, so by Riemann-Roch, $\dim \mathcal{L}(D + (O_E)) = 1$, so there exists $f \in K^{\mathrm{alg}}(E)^*$ such that $\mathrm{div}\, f + D + (O_E) \geq 0$. The divisor on the left has degree 1, so $\mathrm{div}\, f + D + (O_E) = (P)$ for some $P \in E$ and hence $\psi(P) = [D]$. □

So $\psi$ identifies $(E, \oplus)$ with $(\mathrm{Pic}^0(E), +)$, hence $\oplus$ is associative.

## 4.1 Formulae for $E$ in Weierstraß Form

Let

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{$*$}$$

Let $P_1, P_2, P_3, P'$ be points such that $P'$ is the third point of intersection of $E$ with $P_1P_2$ and $P_3$ is the third point of intersection of $E$ with $P'O_E$. Write $P_i = (x_i, y_i), i = 1, 2, 3, P' = (x', y')$.

The inverse $\ominus P_1$ of $P_1$ is the third point of intersection of $P_1O_E$ with $E$. So $\ominus P_1 = (x_1, -(a_1x_1 + a_3) - y_1)$.

Suppose the line through $P_1, P_2$ has equation $y = \lambda x + \nu$. Substituting this into $(*)$ and looking at the coefficient of $x^2$ gives

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

Note that $x' = x_3$, so

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

Formulae for $\lambda, \nu$:

- Case I: $x_1 = x_2$ and $P_1 \neq P_2$, then $P_1 \oplus P_2 = O_E$.
- Case II: $x_1 \neq x_2$. Then $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = y_1 - \lambda x_1 = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}$.
- Case III: $P_1 = P_2$. See formula sheet.

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

*Proof.* It is a subgroup $(E, \oplus)$. We need to check that it is closed under $\oplus, \ominus$. This follows from the explicit formulas (they only involve the coefficients of the Weierstraß equation which lie in $K$). □

**Theorem 4.4.** *Elliptic curves are group varieties, i.e. the maps $[-1] : E \to E, P \mapsto \ominus P$ and $\oplus : E \times E \to E, (P, Q) \mapsto P \oplus Q$ are morphisms.*

*Proof.* The above formula show that $[-1] : E \to E$ is a rational map, hence extends to a morphism (and this extension still agrees with $[-1]$).

The above formulae show that $\oplus : E \times E \to E$ is a rational map, regular on

$$U = \{(P, Q) \in E \times E \mid P, Q, P \oplus Q, P \ominus Q \neq O_E\}.$$

For $P \in E$ let $\tau_P : E \to E$ be translation by $P$. $\tau_P$ is rational map and thus extends to a morphism (which still agrees with $\tau_P$). We factor $\oplus$ as

$$E \times E \xrightarrow{\tau_{\ominus A} \times \tau_{\ominus B}} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{A \oplus B}} E$$

This shows that $\oplus$ is regular on $(\tau_A \times \tau_B)(U)$ for all $A, B \in E$. Thus $\oplus$ is regular on $E \times E$. □

## 4.2 Statement of Results on $E(K)$

(i) $K = \mathbb{C}$. Then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for a lattice $\Lambda$.

(ii) $K = \mathbb{R}$. Then $E(\mathbb{R}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \text{if } \Delta > 0, \\ \mathbb{R}/\mathbb{Z} & \text{if } \Delta < 0. \end{cases}$

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

(iv) $[K : \mathbb{Q}_p] < \infty$. Then $E(K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

(v) $[K : \mathbb{Q}] < \infty$. Then $E(K)$ is finitely generated.

In the subsequent chapters we will prove (iii), (iv) and (v).

# 5 Isogenies

Let $E_1, E_2$ be elliptic curves.

**Definition.**

*(i) An* isogeny $\phi : E_1 \to E_2$ *is a nonconstant morphism with* $\phi(O_{E_1}) = \phi(O_{E_2})$.

*(ii) We say* $E_1, E_2$ *are* isogenous *if there is an isogeny* $E_1 \to E_2$.

By basic theorems about curves, $\phi : E_1 \to E_2$ is nonconstant iff it is surjective on $K^{\text{alg}}$-points. Hence if $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ are isogenies, then so is $\psi\phi : E_1 \to E_3$. Furthermore, $\deg(\psi\phi) = \deg\psi \deg\phi$ which also holds if we allow $\phi = 0$ and set $\deg 0 = 0$.

**Definition.** $\text{Hom}(E_1, E_2) = \{$*isogenies* $E_1 \to E_2\} \cup \{0\}$. *This is an abelian group with pointwise operations.*

**Definition.** *For* $n \in \mathbb{Z}$ *let* $[n] : E \to E$ *be defined by* $P \mapsto P + \cdots + P$ *(n times) if* $n > 0$ *and* $[-n] = [-1] \circ [n]$ *for* $n < 0$.

*The n-torsion subgroup of E is* $E[n] = \ker(E \xrightarrow{[n]} E)$.

If $K = \mathbb{C}$, then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, so (1) $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and (2) $\deg[n] = n^2$ in this case.

We will show that (2) holds over any field $K$ and (1) holds if $\text{char}\, K \nmid n$

**Lemma 5.1.** *Assume* $\text{char}\, K \neq 2$ *and let E be given by* $y^2 = f(x) = (x-e_1)(x-e_2)(x-e_3)$ *with* $e_i \in K^{\text{alg}}$. *Then* $E[2] = \{O, (e_1, 0), (e_2, 0), (e_3, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$.

*Proof.* Let $P = (x, y) \in E \setminus \{O\}$. Then $[2]P = O$ iff $P = -P$ iff $(x, y) = (x, -y)$ iff $y = 0$. □

**Proposition 5.2.** *If* $0 \neq n \in \mathbb{Z}$, *then* $[n] : E \to E$ *is an isogeny.*

*Proof.* $[n]$ is a morphism since the group law is given by a morphism, so we must show $[n] \neq [0]$. Assume that $\text{char}\, K \neq 2$.

- Case $n = 2$: By the previous Lemma we have $E[2] \neq E$, so $[2] \neq 0$.
- Case $n$ odd: By the Lemma there exists $O \neq T \in E[2]$. Then $[n]T = T \neq 0$, so $[n] \neq [0]$.
- General case: Write $[n] = [2^k][m]$ with $m$ odd.

If $\operatorname{char} K = 2$, then we could replace the Lemma with an explicit lemma about 3-torsion points. □

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

**Theorem 5.3.** *Let* $\phi : E_1 \to E_2$ *be an isogeny. Then* $\phi$ *is a group homomorphism.*

*Proof.* $\phi$ induces a map $\phi_* : \operatorname{Div}^0(E_1) \to \operatorname{Div}^0(E_2)$, $\sum_{P \in E_1} n_P P \mapsto \sum_{P \in E_1} n_P \phi(P)$. Fact: If $f \in K(E_1)^*$, then $\operatorname{div} N_{K(E_1)/K(E_2)}(f) = \phi_*(\operatorname{div} f)$. So $\phi_*$ sends principal divisors to principal divisors and hence descends to a map $\operatorname{Pic}^0(E_1) \to \operatorname{Pic}^0(E_2)$. Since $\phi(O_{E_1}) = O_{E_2}$, the following diagram commutes:

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

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

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

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

*Here* $x_i$ *is an* $x$*-coodinate of a Weierstraß equation for* $E_i$*.*

*Moreover if* $\xi(t) = \frac{r(t)}{s(t)}$ *with* $r, s \in K[t]$ *coprime, then* $\deg \phi = \deg \xi = \max(\deg r, \deg s)$.

*Proof.* For $i = 1, 2$, $K(E_i)/K(x_i)$ is a degree 2 Galois extension with with Galois group generated by $[-1]^*$. By the theorem $\phi[-1] = [-1]\phi$. So if $f \in K(x_2)$, then $[-1]^*\phi^* f = \phi^*[-1]^* f = \phi^* f$, so $\phi^* f \in K(x_1)$. Now under the field embedding $K(x_2) \hookrightarrow K(x_1)$ induced by $\phi^*$, $x_2$ maps to some $\xi(x_1)$. This $\xi$ defines a morphism $\mathbb{P}^1 \to \mathbb{P}^1$ making the above diagram commute. Then $2 \deg \phi = 2 \deg \xi$, so $\deg \phi = \deg \xi$. Write $\xi(x_1) = \frac{r(x_1)}{s(x_1)}$ with $r, s \in K[t]$ coprime. We claim that the minimal polynomial of $x_1$ over $K(x_2)$ is $f(t) = r(t) - s(t)x_2 \in K(x_2)[t]$. Since $r, s$ are coprime, $f$ is irreducible in $K[x_2, t]$. By Gauss' Lemma it is irreducible in $K(x_2)[t]$, hence $\deg \phi = \deg \xi = [K(x_1) : K(x_2)] = \deg_t f = \max(\deg r, \deg s)$. □

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

*Proof.* Assume $\operatorname{char} K \neq 2, 3$. $E : y^2 = x^3 + ax + b = f(x)$. If $P = (x, y)$, then $x(2P) = \left(\frac{3x^2+a}{2y}\right)^2 - 2x = \frac{(3x^2+a)^2 - 8xf(x)}{4f(x)} = \frac{x^4+\dots}{4f(x)}$. So we have to prove that numerator and denominator are coprime. Indeed, otherwise there would be $\theta \in K^{\mathrm{alg}}$ with $f(\theta) = 0 = 3x^2 + a = f'(\theta)$ which is not possible, hence $\deg[2] = \max(4, 3) = 4$. $\square$

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

*(i) $q(nx) = n^2 q(x)$ for all $n \in \mathbb{Z}, x \in A$,*

*(ii) $(x, y) \mapsto q(x + y) - q(x) - q(y)$ is $\mathbb{Z}$-bilinear.*

**Lemma 5.6.** *$q : A \to \mathbb{Z}$ is a quadratic form iff it satisfies the parallelogram law, i.e. $q(x + y) + q(x - y) = 2q(x) + 2q(y)$ for all $x, y \in A$.*

*Proof.* "$\Rightarrow$" Let $\langle x, y\rangle = q(x + y) - q(x) - q(y)$. Then $\langle x, x\rangle = q(2x) - 2q(x) = 2q(x)$. But by (ii), $q(x+y)+q(x-y) = \frac{1}{2}\langle x+y, x+y\rangle + \frac{1}{2}\langle x-y, x-y\rangle = \langle x, x\rangle + \langle y, y\rangle = 2q(x)+2q(y)$.

"$\Leftarrow$" On Example Sheet 2. $\square$

**Theorem 5.7.** $\deg : \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$ *is a quadratic form (N.B. we define* $\deg 0 = 0$*).*

*Proof.* We assume that $\operatorname{char} K \neq 2, 3$, so that we can write $E_2 : y^2 = x^3 + ax + b$. Let $P, Q \in E_2$ with $P, Q, P + Q, P - Q \neq 0$. Let $x_1, \dots, x_4$ be their $x$-coordinates.

**Lemma 5.8.** *There exist polynomials $W_0, W_1, W_2 \in \mathbb{Z}[a, b][x_1, x_2]$ of degree $\leq 2$ in $x_1$ and degree $\leq 2$ and $x_2$ such that $(1 : x_3 + x_4 : x_3x_4) = (W_0 : W_1 : W_2)$.*

*Proof.* Method 1: Direct calculation, $W_0 = (x_1 - x_2)^2, W_1 = \dots, W_2 = \dots$, see formula sheet.

Method 2: Let $y = \lambda x + \nu$ be the equation of the line through $P, Q$. Then $x^3 + ax + b - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3) = x^3 - s_1x^2 + s_2x - s_3$.

Comparing coefficients gives:

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

Eliminating $\lambda, \nu$ gives $(s_2 - a)^2 - 4s_1(s_3 + b) = 0$. The left side is a polynomial in $x_1, x_2, x_3$. We denote it by $F(x_1, x_2, x_3)$. It has degree at most 2 in each $x_i$ (separately). $x_3$ is a root of the quadratic $W(t) = F(x_1, x_2, t)$. Note that the same is true for $x_4$ (as $-Q$ has also $x$-coordinate $x_2$).

So $W_0(t - x_3)(t - x_4) = W(t) = W_0t^2 - W_1t + W_2$. Then $(1 : x_3 + x_4 : x_3x_4) = (W_0 : W_1 : W_2)$. $\square$

We show that if $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, then $\deg(\phi + \psi) + \deg(\phi - \psi) \leq 2 \deg \phi + 2 \deg \psi$. We may assume $\phi, \psi, \phi + \psi, \phi - \psi \neq 0$. Otherwise trivial (or use $\deg[-1] = 1$, $\deg[2] = 4$).

We can write

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

By the Lemma, $(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = ((\xi_1 - \xi_2)^2 : \dots)$. Put $\xi_i = r_i/s_i$ with $r_i, s_i \in K[t]$ coprime. Then $(s_3s_4 : r_3s_4 + r_4s_3 : r_3r_4) = ((r_1s_2 - r_2s_1)^2 : \dots)$. The three polynomials on the left are (not necessarily pairwise) coprime.

Therefore

$$\begin{aligned} \deg(\phi + \psi) + \deg(\phi - \psi) &= \max(\deg r_3, \deg s_3) + \max(\deg r_4, \deg s_4) \\ &= \max(\deg(s_3s_4), \deg(r_3s_4 + r_4s_3), \deg(r_3r_4)) \\ &\leq 2 \max(\deg r_1, \deg s_1) + 2 \max(\deg r_2, \deg s_1) \\ &= 2 \deg \phi + 2 \deg \psi \end{aligned}$$

Now replace $\phi, \psi$ by $\phi + \psi, \phi - \psi$, so that $\deg(2\phi) + \deg(2\psi) \leq 2 \deg(\phi + \psi) + 2 \deg(\phi - \psi)$. Since $\deg[2] = 4$, we get the desired reversed inequality.

Hence deg satisfies the parallelogram law and is thus a quadratic form. $\square$

**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* $\deg[n] = n^2$.

**Example** (2-isogeny)**.** Let $E/K$ be an elliptic curve. Suppose $\mathrm{char}\, K \neq 2$ and $0 \neq T \in E(K)[2]$. WLOG $E : y^2 = x(x^2 + ax + b)$, with $a, b \in K$, $b(a^2 - 4b) \neq 0$ and $T = (0, 0)$. If $P = (x, y)$, then $P' = P + T = (x', y')$ where $x' = (y/x)^2 - a - x = \frac{x^2+ax+b}{x} - a - b = \frac{b}{x}$, and $y' = -(y/x)x' = -\frac{by}{x^2}$. Let

$$\begin{aligned} \xi &= x + x' + a = (y/x)^2, \\ \eta &= y + y' = (y/x)(x - b/x). \end{aligned}$$

Then $\eta^2 = (y/x)^2((x + b/x)^2 - 4b) = \xi((\xi - a)^2 - 4b) = \xi(\xi^2 - 2a\xi + a^2 - 4b)$. Thus $\phi = (\xi, \eta)$ is a map from $E$ to $E' : y^2 = x(x^2 + a'x + b')$ with $a' = -2a, b' = a^2 - 4b$. This is an isogeny: $\phi(x, y) = ((y/x)^2 : (y(x^2 - b))/x^2 : 1)$. The orders of these functions at $O_E$ are $-2, -3, 0$, so by multipliying through by the cube of a uniformizer gives $1, 0, 3$, so $\phi(O_E) = (0 : 1 : 0) = O'_E$. Note that $(y/x)^2 = (x^2 + ax + b)/x$, and $x^2 + ax + b, x$ are coprime as $b \neq 0$. So $\deg \phi = 2$ and we say that $\phi$ is a 2-isogeny.

# 6 The Invariant Differential

Let $C$ be an algebraic curve over $K = K^{\text{alg}}$.

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

*(i)* $d(f+g) = df + dg$,

*(ii)* $d(fg) = fdg + gdf$,

*(iii)* $da = 0$ *for* $a \in K$.

Fact: $\Omega_C$ is a 1-dimensional $K(C)$-vector space.

Let $0 \neq \omega \in \Omega_C$. Let $P \in C$ be a smooth point and $t \in K(C)$ a uniformizer at $P$. Then $\omega = fdt$ for some $f \in K(C)^*$. We define $\text{ord}_P(\omega) = \text{ord}_P(f)$. It is independent of the choice of $t$.

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

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

**Definition.** $\text{div}\, \omega := \sum_{P \in C} \text{ord}_P(\omega) P \in \text{Div}(C)$ *(using that* $\text{ord}_P(\omega) = 0$ *for all but finitely many $P \in C$). The genus is* $g(C) = \dim_K \{\omega \in \Omega_C \mid \text{div}(\omega) \geq 0\}$.

Consequence of Riemann-Roch: If $0 \neq \omega \in \Omega_C$, $\deg \text{div}(\omega) = 2g - 2$.

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

*Proof.* Let $T_i = (e_i, 0)$, $E[2] = \{0, T_1, T_2, T_3\}$. Then $\text{div}(y) = (T_1) + (T_2) + (T_3) - 3(O_E)$. For $O_E \neq P \in E$ we have $\text{div}(x - x_P) = (P) + (-P) - 2(O_E)$. If $P \in E \setminus E[2]$, then $\text{ord}_P(x - x_P) = 1$, so $\text{ord}_P(dx) = 0$. If $P = T_i$, then $\text{ord}_P(x - x_P) = 2$, so $\text{ord}_P(dx) = 1$. If $P = O_E$, then $\text{ord}_P(x) = -2$, so $\text{ord}_P(dx) = -3$. Therefore $\text{div}(dx) = (T_1) + (T_2) + (T_3) - 3(O_E)$. Thus $\text{div}(dx/y) = 0$. □

**Definition.** *For a nonconstant morphism* $\phi : C_1 \to C_2$ *we define* $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ *by* $fdg \mapsto \phi^* f d(\phi^* g)$

**Lemma 6.2.** *Let* $P \in E$ *and* $\tau_P : E \to E, X \mapsto P + X$. *Let* $\omega = dx/y$ *as above. Then* $\tau_P^* \omega = \omega$.

*Proof.* $\tau_P^*\omega$ is a regular differential on $E$, so $\tau_P^*\omega = \lambda_P\omega$ for some $\lambda_P \in K^*$. The map $E \to \mathbb{P}^1, P \mapsto \lambda_P$ is a morphism of smooth projective curves, but not surjective (misses 0 and $\infty$). Hence this morphism is constant. Since $\lambda_{O_E} = 1$, we deduce that $\lambda_P = 1$ for all $P$. $\square$

Remark: If $K = \mathbb{C}$, $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ via $z \mapsto (\wp(z), \wp'(z))$. Then $dx/y = (\wp'(z)dz)/\wp'(z) = dz$.

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

*Proof.* Write $E = E_2$. Define the following maps:

$$\begin{aligned} E \times E &\longrightarrow E, \\ \mu : (P, Q) &\longmapsto P + Q, \\ \mathrm{pr}_1 : (P, Q) &\longmapsto P, \\ \mathrm{pr}_2 : (P, Q) &\longmapsto Q. \end{aligned}$$

Fact: $\Omega_{E\times E}$ is a 2-dimensional $K(E \times E)$-vector space with basis $\mathrm{pr}_1^*\,\omega, \mathrm{pr}_2^*\,\omega$. Therefore $\mu^*\omega = f\,\mathrm{pr}_1^*\,\omega + g\,\mathrm{pr}_2^*\,\omega$ for some $f, g \in K(E \times E)$. For fixed $Q \in E$ let

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

Applying $\iota_Q^*$ to the above equation gives

$$\begin{aligned} (\mu\iota_Q)^*\omega &= (\iota_Q^* f)(\mathrm{pr}_1\,\iota_Q)^*\omega + (\iota_Q^* g)(\underbrace{\mathrm{pr}_2\,\iota_Q}_{\text{constant map}})^*\omega \\ \Rightarrow \tau_Q^*\omega &= (\iota_Q^* f)\omega + 0 \\ \Rightarrow \omega &= (\iota_Q^* f)\omega \end{aligned}$$

Therefore $\iota_Q^* f = 1$ for all $Q \in E$, so $f(P, Q) = 1$ for all $P, Q \in E$. Similarly $g(P, Q) = 1$ for all $P, Q \in E$. Therefore $\mu^*\omega = \mathrm{pr}_1^*\,\omega + \mathrm{pr}_2^*\,\omega$. Now pullback by $E_1 \to E_2 \times E_2, P \mapsto (\phi(P), \psi(P))$ to get $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$. $\square$

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

*Proof.* Omitted. $\square$

**Example.** Let $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$ be the multiplicative group. Consider the map $\phi : \mathbb{G}_m \to \mathbb{G}_m, x \mapsto x^n$. Then $\phi^*(dx) = d(x^n) = nx^{n-1}dx$. So if $\mathrm{char}\, K \nmid n$, then $\phi$ is separable, so $\#\phi^{-1}(Q) = \deg\phi$ for all but finitely many $Q \in \mathbb{G}_m$. Since $\phi$ is a group homomorphism, $\#\phi^{-1}(Q) = \#\ker\phi$ for all $Q \in \mathbb{G}_m$. Therefore $\#\ker\phi = \deg\phi = n$. So $K$ contains exactly $n$ $n$-th roots of unity (unsurprisingly).

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

*Proof.* By Lemma 6.3 and induction we get $[n]^*\omega = n\omega$. Since $\operatorname{char} K \nmid n$, we get that $[n]$ is separable, so $\#[n]^{-1}(Q) = \deg[n]$ for all but finitely many $Q \in E$. As in the example above, since $[n]$ is a group homomorphism, $\#[n]^{-1}(Q) = \#E[n]$ for all $Q \in E$, so $\#E[n] = \deg[n] = n^2$. We know that $E[n] = \mathbb{Z}/d_1\mathbb{Z} \times \ldots \mathbb{Z}/d_t\mathbb{Z}$ with $d_1 \mid \cdots \mid d_t \mid n$. If $p$ is a prime with $p \mid d_1$, then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$. But what we just proved is also true for $p$, i.e. $\#E[p] = p^2$, hence $t = 2$ and then $d_1 = d_2 = n$. □

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 $r \geq 1$. In the first case $E$ is "ordinary", in the second "supersingular".

# 7 Elliptic Curves over Finite Fields

**Lemma 7.1.** *Let $A$ be an abelian group and $q : A \to \mathbb{Z}$ be a positive definite quadratic form. Then $|q(x+y) - q(x) - q(y)| \leq 2\sqrt{q(x)q(y)}$.*

*Proof.* We denote $\langle x, y\rangle = q(x+y) - q(x) - q(y)$. We may assume $x \neq 0$, so that $q(x) > 0$. Let $m, n \in \mathbb{Z}$. Then $0 \leq q(mx+ny) = \frac{1}{2}\langle mx+ny, mx+ny\rangle = m^2 q(x) + mn\langle x,y\rangle + n^2 q(y) = q(x)(m + \frac{\langle x,y\rangle}{2q(x)}n)^2 + (q(y) - \frac{\langle x,y\rangle^2}{4q(x)})n^2$. Now take $m = -\langle x,y\rangle, n = 2q(x)$ to deduce $4q(x)q(y) \geq \langle x,y\rangle^2$. □

**Theorem 7.2.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$.*

*Proof.* Recall $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q)$ is topologically generated by the Frobenius $x \mapsto x^q$. Define the Frobenius endomorphism $\phi : E \to E, (x,y) \mapsto (x^q, y^q)$ (after fixing a Weierstraß equation). It is an isogeny of degree $q$. Then $E(\mathbb{F}_q) = \{P \in E \mid \phi(P) = P\} = \ker(1-\phi)$. Note that $\phi^*\omega = \phi^*(dx/y) = d(x^q)/y^q = qx^{q-1}dx/y^q = 0$. By Lemma 6.3 $(1-\phi)^*\omega = \omega - \phi^*\omega = \omega \neq 0$, so $1-\phi$ is separable. Hence $\#E(\mathbb{F}_q) = \#\ker(1-\phi) = \deg(1-\phi)$. Now $\deg : \mathrm{Hom}(E,E) \to \mathbb{Z}$ is a positive definite quadratic form, so by the lemma we get

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

□

## 7.1 Zeta Functions

For $K$ a function field, i.e. $K = \mathbb{F}_q(C)$ where $C/\mathbb{F}_q$ is a smooth projective curve, we define $\zeta_K(s) = \prod_{x\in|C|}(1-(Nx)^{-s})^{-1}$ where $|C|$ is the set of closed points on $C$ (i.e. orbits of $\mathrm{Gal}(\mathbb{F}_q^{\mathrm{alg}}/\mathbb{F}_q)$ on $C(\mathbb{F}_q^{\mathrm{alg}})$) and $Nx = q^{\deg x}$ where $\deg x$ is the size of the orbit. We have $\zeta_K(s) = F(q^{-s})$ for $F(T) = \prod_{x\in|C|}(1-T^{\deg x})^{-1} \in \mathbb{Q}[\![t]\!]$. Then

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

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

$$= \sum_{n=1}^{\infty} \Big( \sum_{\substack{x \in |C| \\ \deg x | n}} \deg x \Big) T^n$$

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

Thus we get

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

**Definition.** *The* zeta function *of a smooth projective curve $C/\mathbb{F}_q$ is*

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

**Definition.** *For $\phi, \psi \in \operatorname{End} E$ we put $\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg \phi - \deg \psi$ and $\operatorname{tr}(\phi) = \langle \phi, 1 \rangle$.*

**Lemma 7.3.** *If $\psi \in \operatorname{End}(E)$, then $\psi^2 - [\operatorname{tr} \psi]\psi + [\deg \psi] = 0$.*

*Proof.* See Exercise Sheet 2. □

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

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

*Proof.* Let $\phi : E \to E$ be the $q$-power Frobenius map. By the proof of Hasse's theorem $\#E(\mathbb{F}_q) = \deg(1 - \phi) = q + 1 - \operatorname{tr}(\phi)$ and $\operatorname{tr}(\phi) = a$, $\deg \phi = q$. By the lemma we have $\phi^2 - a\phi + q = 0$, hence $\operatorname{tr}(\phi^{n+2}) - a \operatorname{tr}(\phi^{n+1}) + q \operatorname{tr}(\phi^n) = 0$. This second order difference equation with initial conditions $\operatorname{tr}(1) = 2, \operatorname{tr}(\phi) = a$ has solution $\operatorname{tr}(\phi^n) = \alpha^n + \beta^n$ where $\alpha, \beta \in \mathbb{C}$ are the roots of $X^2 - aX + q = 0$. Then $\#E(\mathbb{F}_{q^n}) = \deg(1 - \phi^n) = 1 + \deg(\phi^n) - \operatorname{tr}(\phi^n) = 1 + q^n - \alpha^n - \beta^n$. We then obtain

$$\begin{aligned} Z_E(T) &= \exp\left( \sum_{n=1}^{\infty} \Big( \frac{T^n}{n} + \frac{(qT)^n}{n} - \frac{(\alpha T)^n}{n} - \frac{(\beta T)^n}{n} \Big) \right) \\ &= \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)} \\ &= \frac{1 - aT + qT^2}{(1 - T)(1 - qT)}. \end{aligned}$$

□

# 8 Formal Groups

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

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

*$R$ is ($I$-adically)* complete *if*

*(i)* $\bigcap_{n \geq 0} I^n = \{0\}$,

*(ii) every Cauchy sequence converges.*

Useful remark: If $R$ is complete and $x \in I$, then $\frac{1}{1-x} = 1 + x + x^2 + \cdots \in R$, so $1 - x \in R^\times$.

**Examples.** The following rings are $I$-adically complete:

- $R = \mathbb{Z}_p, I = p\mathbb{Z}_p$.
- $R = \mathbb{Z}[\![t]\!], I = (t)$.

**Lemma 8.1** (Hensel's Lemma)**.** *Let $R$ be complete w.r.t. an ideal $I$. Let $F \in R[X]$, $s \geq 1$. Suppose $a \in R$ satisfies $F(a) \equiv 0 \bmod I^s$ and $F'(a) \in R^\times$. Then there exists a unique $b \in R$ such that $F(b) = 0$ and $a \equiv b \bmod I^s$.*

*Proof.* Let $u \in R^\times$ with $F'(a) \equiv u \bmod I$. Replacing $F(X)$ by $F(X+a)/u$ we may assume $a = 0$ and $F'(0) \equiv 1 \bmod I$. We put $x_0 = 0$ and $x_{n+1} = x_n - F(x_n)$. An easy induction shows that $x_n \equiv 0 \bmod I^s$ for all $n$. Also $F(X) - F(Y) = (X - Y)(F'(0) + XG(X, Y) + YH(X, Y))$ for some polynomials $G, H \in R[X, Y]$.

Claim: $x_{n+1} \equiv x_n \bmod I^{n+s}$ for all $n \geq 0$. Proof: By induction on $n$, the case $n = 0$ is clear. Suppose $x_n \equiv x_{n-1} \bmod I^{n+s-1}$. By the above we get $F(x_n) - F(x_{n-1}) = (x_n - x_{n-1})(1+c)$ for some $c \in I$. Hence $F(x_n) - F(x_{n-1}) \equiv x_n - x_{n-1} \bmod I^{n+s}$. Rearranging this gives the claim.

Hence $(x_n)_{n \geq 0}$ is Cauchy, so $x_n \to b$ as $n \to \infty$ for some $b \in R$ since $R$ is complete. Taking the limit $n \to \infty$ in $x_{n+1} = x_n - F(x_n)$ shows $f(b) = 0$. Also we get $b \equiv 0 \bmod I^s$.

Uniqueness: Use $F(X) - F(Y) = (X - Y)(F'(0) + XG(X, Y) + YH(X, Y))$ and the useful remark (need $R$ domain for uniqueness ?). □

Consider an elliptic curve with Weierstraß equation

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

On the affine piece $Y \neq 0$ we set $t = -X/Y, w = -Z/Y$ and get the equation

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

We apply Hensel's Lemma with $R = \mathbb{Z}[a_1, \dots, a_6][\![t]\!]$, $I = (t)$ and $F(X) = X - f(t, X) \in R[X]$, $s = 3, a = 0$. We check $F(0) = -f(t, 0) = -t^3 \equiv 0 \bmod I^3$ and $F'(0) = 1 - a_1t - a_2t^2 \in R^\times$. Therefore there exists a unique $w(t) \in \mathbb{Z}[a_1, \dots, a_6][\![t]\!]$ such that $w(t) = f(t, w(t))$ and $w(t) \equiv 0 \bmod t^3$.

Remarks:

(i) In fact $w(t) = t^3(1 + A_1t + A_2t^2 + \dots)$ where

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

(ii) Taking $u = 1$ in the proof of Hensel's Lemma gives $w(t) = \lim_{n\to\infty} w_n(t)$, where $w_0(t) = 0, w_{n+1}(t) = f(t, w_n(t))$.

**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 $K = \operatorname{Frac} R$. Then $\widehat{E}(I) = \{(t, w) \in E(K) \mid t, w \in I\}$ is a subgroup of $E(K)$.*

N.B. By the uniqueness in Hensel's lemma this set is $\{(t, w(t)) \mid t \in I\}$.

*Proof.* Taking $(t, w) = (0, 0)$ shows $O_E \in \widehat{E}(I)$. So its suffices to show that if $P_1, P_2 \in \widehat{E}(I)$, then $-P_1 - P_2 \in \widehat{E}(I)$. Let

$$\begin{aligned}\lambda &= \begin{cases} \frac{w(t_2)-w(t_1)}{t_2-t_1}, & t_1 \neq t_2 \\ w'(t_1), & t_1 = t_2 \end{cases} \\ &= \sum_{n=2}^{\infty} A_{n-2} \frac{t_1^{n+1} - t_2^{n+1}}{t_1 - t_2} \\ &= \sum_{n=2}^{\infty} A_{n-2}(t_1^n + t_1^{n-1}t_2 + \dots + t_2^n) \in I\end{aligned}$$

Let $\nu = w - \lambda t \in I$. Substituting $w = \lambda t + \nu$ in $w = f(t, w)$ gives

$$\lambda t + \nu = t^3 + a_1t(\lambda t + \nu) + a_2t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4t(\lambda t + \nu)^2 + a_6(\lambda t + \nu)^3$$

Let

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

Note that $A \in R^\times, B \in R$. Then $t_3 = -\frac{B}{A} - t_1 - t_2 \in I$ and $w_3(t_3) = \lambda t_3 + \nu \in I$. □

We apply this:

- $R = \mathbb{Z}[a_1, \ldots, a_6][\![t]\!], I = (t)$, then the Lemma shows that there exists $\iota \in \mathbb{Z}[a_1, \ldots, a_6][\![t]\!]$ with $\iota(0) = 0$ and $[-1](t, w(t)) = (\iota(t), w(\iota(t)))$.
- $R = \mathbb{Z}[a_1, \ldots, a_6][\![t_1, t_2]\!], I = (t_1, t_2)$, then the Lemma shows that there exists $F \in \mathbb{Z}[a_1, \ldots, a_6][\![t_1, t_2]\!]$ with $F(0,0) = 0$ and $(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2)))$.

In fact

$$\iota(X) = -X - a_1 X^2 - a_2 X^3 - (a_1^3 + a_3) X^4 + \ldots$$
$$F(X, Y) = X + Y - a_1 XY - a_2 (X^2 Y + XY^2) + \ldots$$

The group law implies the following properties:

(i) $F(X, Y) = F(Y, X)$

(ii) $F(X, 0) = X$ and $F(0, Y) = Y$

(iii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$

(iv) $F(X, \iota(X)) = 0$.

**Definition.** *Let $R$ be a ring. A* formal group *over $R$ is a power series $F \in R[\![X, Y]\!]$ satisfiying (i), (ii), (iii) above.*

N.B. One can show that property (iv) is automatically satisfied (see Example Sheet 2).

**Examples.**

(i) $F(X, Y) = X + Y$, the additive group $\widehat{\mathbb{G}}_a$.

(ii) $F(X, Y) = (1 + X)(1 + Y) - 1 = X + Y + XY$, the multiplicative group $\widehat{\mathbb{G}}_m$.

(iii) The power series $F$ associated to an elliptic curve $E$ as above.

**Definition.** *Let $\mathcal{F}, \mathcal{G}$ be formal groups over $R$ given by power series $F$ and $G$. A* morphism *$f : \mathcal{F} \to \mathcal{G}$ is a power series $f \in R[\![t]\!]$ with $f(0) = 0$ satisfying $f(F(X, Y)) = G(f(x), f(y))$. $\mathcal{F}$ and $\mathcal{G}$ are isomorphic if there exist morphisms $\mathcal{F} \xrightarrow{f} \mathcal{G}$, $\mathcal{G} \xrightarrow{g} \mathcal{F}$ such that $g(f(X)) = X = f(g(X))$.*

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

*(i) There is a unique power series*

$$\log(T) = T + \frac{a_2}{2} T^2 + \frac{a_3}{3} T^2 + \ldots$$

*with $a_i \in R$ such that $\log(F(X, Y)) = \log X + \log Y$.*

*(ii) There is a unique power series*

$$\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \dots$$

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

*Proof.* Notation: $F_1(X,Y) = \frac{\partial F}{\partial X}(X,Y)$.

(i) Uniqueness: Let $p(T) = \frac{d}{dT}\log T = 1 + a_2 T + a_3 T^2 + \dots$. Differentiating $\log F(X,Y) = \log X + \log Y$ w.r.t. $X$ gives $p(F(X,Y)) \cdot F_1(X,Y) = p(X)$. Then plug in $X = 0$ to get $p(Y)F_1(0,Y) = 1$, so $p(Y) = F_1(0,Y)^{-1}$.

Existence: Let $p(T) = F_1(0,T)^{-1} = 1 + a_2 T + a_3 T^2 + \dots$ for some $a_i \in R$. Then let $\log(T) = \int p(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots$. We know $F(F(X,Y),Z) = F(X,F(Y,Z))$. Differentiate w.r.t. $X$ to get $F_1(F(X,Y),Z)F_1(X,Y) = F_1(X,F(Y,Z))$ and put $X = 0$, so $F_1(Y,Z)F_1(0,Y) = F_1(0,F(Y,Z))$. So $F_1(Y,Z)p(Y)^{-1} = p(F(Y,Z))^{-1}$, so $F_1(Y,Z)p(F(Y,Z)) = p(Y)$. Integrate w.r.t. $Y$ and get $\log F(Y,Z) = \log Y + h(Z)$ for some power series $h$. By symmetry we see that $h(Z) = \log Z$.

(ii) This part follows from Q12 on Example Sheet 2 and the following Lemma:

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

*Proof.* We construct polynomials $g_n(T) \in R[T]$ such that $f(g_n(T)) \equiv T \bmod T^{n+1}$ and $g_{n+1}(T) \equiv g_n(T) \bmod T^{n+1}$. Then set $g(T) = \lim_{n\to\infty} g_n(T)$ satisfies $f(g(T)) = T$. To start the induction set $g_1(T) = a^{-1}T$. Now suppose $n \geq 2$ and $g_{n-1}(T)$ exists, so $f(g_{n-1}(T)) \equiv T + bT^n \bmod T^{n+1}$ 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

$$\begin{aligned} f(g_n(T)) &= f(g_{n-1}(T) + \lambda T^n) \\ &\equiv f(g_{n-1}(T)) + \lambda a T^n \bmod T^{n+1} \\ &\equiv T + (b + \lambda a)T^n \bmod T^{n+1} \end{aligned}$$

So take $\lambda = -b/a$ using $a \in R^\times$.

Hence we get $g(T) = a^{-1}T + \dots \in R[\![T]\!]$ with $f(g(T)) = T$. Applying the same construction to $g$ gives $h(T) = aT + \dots \in R[\![T]\!]$ such that $g(h(T)) = T$, so $f(T) = f(g(h(T))) = h(T)$, hence $g(f(T)) = T$. □

□

Notation: Let $\mathcal{F}$ be a formal group given by a power series $F \in R[\![X,Y]\!]$. Suppose $R$ is complete w.r.t. the ideal $I$. For $x, y \in I$ put $x \oplus_{\mathcal{F}} y = F(x,y) \in I$. Then $\mathcal{F}(I) := (I, \oplus_{\mathcal{F}})$ is an abelian group.

**Examples.**

- $\widehat{\mathbb{G}}_a(I) = (I, +)$,
- $\widehat{\mathbb{G}}_m(I) \cong (1 + I, \times)$,
- $\widehat{E}(I) =$ subgroup of $E(K)$ in Lemma 8.2.

**Corollary 8.4.** *Let $\mathcal{F}$ be a formal group over $R$ and $n \in \mathbb{Z}$. Suppose $n \in R^\times$. Then*

*(i)* $[n] : \mathcal{F} \to \mathcal{F}$ *is an isomorphism of formal groups.*

*(ii) If $R$ is complete w.r.t. an ideal $I$, then $\mathcal{F}(I) \xrightarrow{\times n} \mathcal{F}(I)$ is an isomorphism of groups. In particular, $\mathcal{F}(I)$ has no $n$-torsion.*

*Proof.* We have $[1](T) = T$ and $[n](T) = F([n-1](T), T)$ for $n \geq 2$, for $n < 0$ use $[-1](T) = \iota(T)$. A straightforward induction then shows that $[n](T) = nT + \cdots \in R[\![T]\!]$, so the claim is immediate from the lemma above. □

# 9 Elliptic Curves over Local Fields

Let $K$ be a field, complete w.r.t. a (normalized) discrete valuation $v : K^\times \to \mathbb{Z}$. Let $k$ denote its residue field and $\pi$ a uniformizer. We assume $\operatorname{char} K = 0$ and $\operatorname{char} k = p > 0$ (e.g. $K = \mathbb{Q}_p$).

Let $E/K$ be an elliptic curve.

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

Remarks:

(i) Putting $x = u^2x', y = u^3y'$ gives $a_i = u^ia_i'$. Therefore integral Weierstraß equations exist.

(ii) If $a_1, \ldots, a_6 \in \mathcal{O}_K$, then $\Delta \in \mathcal{O}_K$, so $v(\Delta) \geq 0$, so minimal Weierstraß equations exist.

(iii) If $\operatorname{char} k \neq 2, 3$, then there exist minimal Weierstraß equations 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 $O \neq P = (x, y) \in E(K)$. Then either $x, y \in \mathcal{O}_K$ or $v(x) = -2s, v(y) = -3s$ for some $s \geq 1$.*

*Proof.* It is easy to see that if $v(x) \geq 0$, then $v(y) \geq 0$ and also conversely. So suppose $v(x), v(y) < 0$. Then on LHS and RHS the dominating terms w.r.t. $v$ are $y^2$ and $x^3$, so $v(y^2) = v(x^3)$ and the result follows. □

Since $K$ is complete, $\mathcal{O}_K$ is complete w.r.t. to the ideal $\pi^r\mathcal{O}_K$ for any $r \geq 1$.

Fix a minimal Weierstraß equation for $E/K$, so we get a formal group $\widehat{E}$ over $\mathcal{O}_K$. Taking $I = \pi^r\mathcal{O}_K$ in Lemma 8.2 shows that

$$\begin{aligned}\widehat{E}(\pi^r\mathcal{O}_K) &= \{(x, y) \in E(K) \mid -\frac{x}{y}, -\frac{1}{y} \in \pi^r\mathcal{O}_K\} \cup \{O\} \\ &= \{(x, y) \in E(K) \mid v(x/y) \geq r, \, -v(y) \geq r\} \cup \{O\}\end{aligned}$$

$$= \{(x,y) \in E(K) \mid v(x) = -2s,\ v(y) = -3s,\ s \geq r\} \cup \{O\}$$
$$= \{(x,y) \in E(K) \mid v(x) \leq -2r,\ v(y) \leq -3r\} \cup \{O\}$$

is a subgroup of $E(K)$. We denote it by $E_r(K)$. This gives a filtration $\ldots \subseteq E_3(K) \subseteq E_2(K) \subseteq E_1(K)$. More generally for any formal group $\mathcal{F}$ over $\mathcal{O}_K$ we have $\ldots \subseteq \mathcal{F}(\pi^3\mathcal{O}_K) \subseteq \mathcal{F}(\pi^2\mathcal{O}_K) \subseteq \mathcal{F}(\pi\mathcal{O}_K)$.

We now show that the isomorphism $\mathcal{F} \cong \widehat{\mathbb{G}}_a$ of formal groups induces an isomorphism $\mathcal{F}(\pi^r\mathcal{O}_K) \cong (\mathcal{O}_K, +)$ of genuine groups for $r$ sufficiently large.

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

$$\log : \mathcal{F}(\pi^r\mathcal{O}_K) \xrightarrow{\cong} \widehat{\mathbb{G}}_a(\pi^r\mathcal{O}_K)$$

*is an isomorphism of groups with inverse*

$$\exp : \widehat{\mathbb{G}}_a(\pi^r\mathcal{O}_K) \xrightarrow{\cong} \mathcal{F}(\pi^r\mathcal{O}_K).$$

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

*Proof.* For $x \in \pi^r\mathcal{O}_K$ we must show that the power series $\log x$ and $\exp x$ converge. Recall $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \ldots$ with $b_i \in \mathcal{O}_K$.

Claim: $v_p(n!) \leq \frac{n-1}{p-1}$. Proof of claim:

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

So $(p-1)v_p(n!) < n$, so $(p-1)v_p(n!) \leq n-1$ since the LHS is $\in \mathbb{Z}$.

Now

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

This is always $\geq r$ and goes to $\infty$ as $n \to \infty$. So $\exp x$ converges and belongs to $\pi^r\mathcal{O}_K$. A similar method works for log. □

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

*Proof.* By the definition of a formal group, $F(X,Y) = X + Y + XY(\ldots)$. So if $x, y \in \mathcal{O}_K$,

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

Therefore

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

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

**Corollary.** *If $\#k < \infty$, then $\mathcal{F}(\pi\mathcal{O}_K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.*

We denote the reduction $\mathcal{O}_K \to \mathcal{O}_K/\pi\mathcal{O}_K = k$ by $x \mapsto \widetilde{x}$.

**Proposition 9.4.** *Let $E/K$ be an elliptic curve. Then the reductions mod $\pi$ of any two minimal Weierstraß equations for $E$ define isomorphic curves over $k$.*

*Proof.* Say the Weierstraß equations are related by the usual coordinate change with parameters $u \in K^\times, r, s, t \in K$. Then $\Delta_1 = u^{12}\Delta_2$. Since both equations are minimal, we get $u \in \mathcal{O}_K^\times$. From the transformation formulae for the $a_i$ and $b_i$, one can also see that $r, s, t \in \mathcal{O}_K$. So the coordinate change descends to a valid coordinate change mod $\pi$. □

**Definition.** *The reduction $\widetilde{E}/k$ of $E/K$ is defined by the reduction of a minimal Weierstraß equation.*

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

For an integral Weierstraß equation

$$\begin{aligned} v(\Delta) = 0 &\implies \text{good reduction} \\ 0 < v(\Delta) < 12 &\implies \text{bad reduction} \end{aligned}$$

There is a well-defined map

$$\begin{aligned} \mathbb{P}^2(K) &\longrightarrow \mathbb{P}^2(k) \\ (x : y : z) &\longmapsto (\widetilde{x} : \widetilde{y} : \widetilde{z}) \end{aligned}$$

by choosing $x, y, z$ such that $\min\{v(x), v(y), v(z)\} = 0$.

We restrict to get $E(K) \to \widetilde{E}(k)$, $P \mapsto \widetilde{P}$.

If $P = (x, y) \in E(K)$, then by Lemma 9.1 either $x, y \in \mathcal{O}_K$, so that $\widetilde{P} = (\widetilde{x}, \widetilde{y})$, or $v(x) = -2s, v(y) = -3s$ and $P = (\pi^{3s}x : \pi^{3s}y : \pi^{3s}) \longmapsto \widetilde{P} = (0 : 1 : 0)$.

Therefore $\widehat{E}(\pi\mathcal{O}_K) = E_1(K) = \{P \in E(K) \mid \widetilde{P} = O\}$ is called the *kernel of reduction.*

Let $\widetilde{E}_{ns} = \begin{cases} \widetilde{E} & \text{if } E \text{ has good reduction,} \\ \widetilde{E} \setminus \{\text{singular point}\} & \text{if } E \text{ hs bad reduction.} \end{cases}$

The chord and tangent process still defines a group law on $\widetilde{E}_{ns}$. In cases of bad reduction $\widetilde{E}_{ns} \cong \mathbb{G}_a$ (over $k$) or $\widetilde{E}_{ns} \cong \mathbb{G}_m$ (over $k$ or possibly a quadratic extension of $k$).

For simplicity, suppose $\operatorname{char} k \neq 2$. Then $\widetilde{E} : y^2 = f(x)$ with $\deg f = 3$. Then $\widetilde{E}$ is singular iff $f$ has a repeated root.

If the singularity is a node (resp. a cusp), we get multiplicative (resp. additive) reduction.

Assume that the singularity is a cusp and that $\widetilde{E}$ is given by $y^2 = x^3$. Then consider the map $\widetilde{E}_{ns} \to \mathbb{G}_a$, $(x, y) \mapsto x/y$ with inverse $t \mapsto (t^{-2}, t^{-3})$. Let $P_1, P_2, P_3$ lie on the line $ax + by = 1$. Write $P_i = (x_i, y_i)$, $t_i = x_i/y_i$. Then $x_i^3 = y_i^2 = y_i^2(ax_i + by_i)$. So $t_i^3 - at_i - b = 0$. Then $t_1, t_2, t_3$ are the roots of $T^3 - aT - b = 0$, so $t_1 + t_2 + t_3 = 0$. Hence the map above is a group isomorphism.

The case of a node is an exercise.

**Definition.** $E_0(K) = \{P \in E(K) \mid \widetilde{P} \in \widetilde{E}_{ns}(k)\}$.

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

*Proof.* Group homomorphism: A line $l$ in $\mathbb{P}^2$ defined over $K$ has equation $l : aX+bY+cZ = 0$ with $a, b, c \in K$. We may assume that $\min(v(a), v(b), v(c)) = 0$. Then reducing mod $\pi$ gives a line $\widetilde{l} : \widetilde{a}X + \widetilde{b}Y + \widetilde{c}Z = 0$. If $P_1, P_2, P_3 \in E(K)$ with $P_1 + P_2 + P_3 = O$, then these points lie on a line $l$. Then $\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3$ lie on the line $\widetilde{l}$. If $\widetilde{P}_1, \widetilde{P}_2 \in \widetilde{E}_{ns}(K)$, then $\widetilde{P}_3 \in \widetilde{E}_{ns}(k)$. So if $P_1, P_2 \in E_0(K)$, then $P_3 \in E_0(K)$ and $\widetilde{P}_1 + \widetilde{P}_2 + \widetilde{P}_3 = 0$ (exercise: Show this also works if some of the points are repeated).

Surjective: Let $f(x, y) = y^2 + a_1xy + a_3y - (x^3 + \dots)$. Let $\widetilde{P} \in \widetilde{E}_{ns}(k) \setminus \{O\}$, say $\widetilde{P} = (\widetilde{x}_0, \widetilde{y}_0)$. For some $x_0, y_0 \in \mathcal{O}_K$. Since $\widetilde{P}$ is non-singular, either $\frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \bmod \pi$ or $\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \bmod \pi$. In the first case we put $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$ and apply Hensel's lemma to the approximate root $x_0$, the second case is similar. □

It follows that $E_0(K)/E_1(K) \cong \widetilde{E}_{ns}(k)$.

A compactness argument will show that if $\#k < \infty$, then $E_0(K)$ is of finite index in $E(K)$.

We deduce:

**Theorem 9.6.** *If $[K : \mathbb{Q}_p] < \infty$, then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.*

In the following let $[K : \mathbb{Q}_p] < \infty$. We denote the unique unramified extension of degree $m$ of $K$ by $K_m$. We also let $K^{\text{ur}} = \bigcup_{m \geq 1} K_m$.

**Theorem 9.7.** *Let $[K : \mathbb{Q}_p] < \infty$. Suppose $E/K$ has good reduction and $p \nmid n$. If $P \in E(K)$, then $K([n]^{-1}P)/K$ is unramified. Here $[n]^{-1}P = \{Q \in E(K^{\text{alg}}) : nQ = P\}$.*

*Proof.* For each $m \geq 1$ there is a SES

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

Taking $\bigcup_{m\geq 1}$ gives a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K^{\mathrm{ur}}) & \longrightarrow & E(K^{\mathrm{ur}}) & \longrightarrow & \widetilde{E}(k^{\mathrm{alg}}) & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle \times n} & & \Big\downarrow{\scriptstyle \times n} & & \Big\downarrow{\scriptstyle \times n} & & \\ 0 & \longrightarrow & E_1(K^{\mathrm{ur}}) & \longrightarrow & E(K^{\mathrm{ur}}) & \longrightarrow & \widetilde{E}(k^{\mathrm{alg}}) & \longrightarrow & 0 \end{array}$$

The left vertical map is an isomorphism by Corollary 8.4 (ii) applied over each $K_m$. The right vertical map is surjective with kernel $\cong (\mathbb{Z}/n\mathbb{Z})^2$. By the Snake lemma we get $E(K^{\mathrm{ur}})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ and $E(K^{\mathrm{ur}})/nE(K^{\mathrm{ur}}) = 0$.

So if $P \in E(K)$, there exists $Q \in E(K^{\mathrm{ur}})$ such that $nQ = P$. Then $[n]^{-1}(P) = \{Q + T : T \in E[n]\} \subseteq E(K^{\mathrm{ur}})$. Hence $K([n]^{-1}P) \subseteq K^{\mathrm{ur}}$. □

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

*Proof.* Since $\#k < \infty$, $\mathcal{O}_K/\pi^r\mathcal{O}_K$ is finite for all $r \geq 1$. So $\mathcal{O}_K \cong \varprojlim_r \mathcal{O}_K/\pi^r\mathcal{O}_K$ is a profinite group and hence compact. $\mathbb{P}^n(K)$ is the union of sets $\{(a_0 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots : a_n) \mid a_j \in \mathcal{O}_K\} \cong \mathcal{O}_K^n$, hence compact. $E(K) \subseteq \mathbb{P}^2(K)$ is a closed subset, hence compact. The group operations are continuous. So $E(K)$ is a compact topological group. If $\widetilde{E}$ has singular point $(\widetilde{x}_0, \widetilde{y}_0)$, then $E(K) \setminus E_0(K) = \{(x, y) \in E(K) \mid v(x - x_0) \geq 1, v(y - y_0) \geq 1\}$ is a closed subset of $E(K)$. Therefore $E_0(K)$ is an open subgroup of $E(K)$. As $E(K)$ is compact, this implies that $E_0(K)$ has finite index in $E(K)$. □

The index $[E(K) : E_0(K)] =: c_K(E)$ is called the "Tamagawa number" (of $E$).

Remarks:

(i) If $E$ has good reduction, then $c_K(E) = 1$, but the converse is false.

(ii) It can be shown that either $c_K(E) = v(\Delta)$ or $c_K(E) \leq 4$ (essential that we work with a minimal Weierstraß equation).

# 10 Elliptic Curves over Number Fields - The Torsion Subgroup

Let $K$ be a finite extension of $\mathbb{Q}$, $E/K$ an elliptic curve.

Notation: $\mathfrak{p}$ is a prime of $K$ (i.e. of $\mathcal{O}_K$), write $K_\mathfrak{p}$ for the completion of $K$ at $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ for its valuation ring and $k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$ for its residue field.

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

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

*Proof.* Take a Weierstraß equation for $E$ with coefficients $a_1, \ldots, a_6 \in \mathcal{O}_K$. As $E$ is non-singular, $\Delta \neq 0$. Then $E$ has good reduction at any prime not dividing $\Delta$. □

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

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

*Proof.* Take any prime $\mathfrak{p}$. We saw that $E(K_\mathfrak{p})$ has a subgroup $A$ of finite index with $A \cong (\mathcal{O}_\mathfrak{p}, +)$. In particular $A$ is torsionfree. Then $E(K)_{\text{tors}} \subseteq E(K_\mathfrak{p})_{\text{tors}} \hookrightarrow E(K_\mathfrak{p})/A$. □

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

*Proof.* We know that $E(K_\mathfrak{p}) \to \widetilde{E}(k_\mathfrak{p})$ is a group homomorphism with kernel $E_1(K_\mathfrak{p})$. By corollary 8.4 and $\mathfrak{p} \nmid n$, $E_1(K_\mathfrak{p})$ has no $n$-torsion. □

**Example.** Let $E/\mathbb{Q}$ be defined by $y^2 + y = x^3 - x^2$. Then $\Delta = -11$. So $E$ has good reduction at all $p \neq 11$. We calculate:

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

Thus by the lemma $\#E(\mathbb{Q})_{\text{tors}} \mid 5 \cdot 2^a$ for some $a \geq 0$ and $\#E(\mathbb{Q})_{\text{tors}} \mid 5 \cdot 3^b$ for some $b \geq 0$, hence $\#E(\mathbb{Q})_{\text{tors}} \mid 5$. Let $T = (0,0) \in E(\mathbb{Q})$. Then $5T = O$, so $E(\mathbb{Q})_{\text{tors}} = \langle T \rangle \cong \mathbb{Z}/5\mathbb{Z}$.

**Example.** Let $E/\mathbb{Q}$ be defined by $y^2 + y = x^3 + x^2$. Then $\Delta = -43$. Again we calculate:

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

Therefore $\#E(\mathbb{Q})_{\text{tors}} \mid 5 \cdot 2^a$ for some $a \geq 0$ and $\#E(\mathbb{Q})_{\text{tors}} \mid 9 \cdot 11^b$ for some $b \geq 0$. Hence $E(\mathbb{Q})_{\text{tors}} = \{O\}$. Therefore $P = (0,0)$ must have infinite order. In particular $E(\mathbb{Q})$ is infinite.

**Example.** $E_D : y^2 = x^3 - D^2x$ with $D \in \mathbb{Z}$ squarefree, $\Delta = 2^6D^6$. Then $E_D(\mathbb{Q})_{\text{tors}} \supseteq \{0, (0,0), (\pm D, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^\times$. Let $f(x) = x^3 - D^2x$. If $p \nmid 2D$, then

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

If $p \equiv 3 \bmod 4$, then since $f$ is an odd function, $\left(\frac{f(-x)}{p}\right) = -\left(\frac{f(x)}{p}\right)$. Therefore $\#\widetilde{E}_D(\mathbb{F}_p) = p + 1$. Let $m = \#E_D(\mathbb{Q})_{\text{tors}}$. We have $4 \mid m \mid p + 1$ for all sufficiently large (i.e. $p \nmid 2Dm$) primes $p$ with $p \equiv 3 \bmod 4$. Therefore $m = 4$ since otherwise this contradicts Dirichlet's theorem on primes in arithmetic progressions. So $E_D(\mathbb{Q})_{\text{tors}} \cong (\mathbb{Z}/2\mathbb{Z})^2$. Hence $\operatorname{rank} E_D(\mathbb{Q}) \geq 1$ iff there exist $x, y \in \mathbb{Q}$ with $y \neq 0$ such that $y^2 = x^3 - D^2x$ iff $D$ is a congruent number.

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

*(i)* $4x, 8y \in \mathbb{Z}$.

*(ii) If $2 \mid a_1$ or $2T \neq 0$, then $x, y \in \mathbb{Z}$.*

*Proof.* The Weierstraß equation defines a formal group $\widehat{E}$ over $\mathbb{Z}$. For $r \geq 1$ we have $\widehat{E}(p^r\mathbb{Z}_p) = \{(x, y) \in E(\mathbb{Q}_p) \mid v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{O\}$. By Theorem 9.2, $\widehat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ if $r > \frac{1}{p-1}$. So $\widehat{E}(4\mathbb{Z}_2)$ and $\widehat{E}(p\mathbb{Z}_p)$ for $p$ odd are torsionfree. So if $0 \neq T = (x, y) \in E(\mathbb{Q})_{\text{tors}}$, it follows that $v_2(x) \geq -2, v_2(y) \geq -3$ and $v_p(x) \geq 0, v_p(y) \geq 0$ for odd primes $p$. This proves (i).

For (ii) suppose $T \in \widehat{E}(2\mathbb{Z}_2) \backslash \widehat{E}(4\mathbb{Z}_2)$, i.e. $v_2(x) = -2, v_2(y) = -3$. Since $\widehat{E}(2\mathbb{Z}_2)/\widehat{E}(4\mathbb{Z}_2) \cong (\mathbb{F}_2, +)$ and $\widehat{E}(4\mathbb{Z}_2)$ is torsionfree, we get $2T = 0$. So $(x, y) = T = -T = (x, -y - a_1x - a_3)$, so $2y + a_1x + a_3 = 0$. From this it follows easily that $2 \nmid a_1$.

So if $2T \neq O$ or $a_1$ is even, then $T \notin \widehat{E}(2\mathbb{Z}_2)$. □

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

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

*Proof.* The previous lemma shows that $x, y \in \mathbb{Z}$. If $2T = O$, then $y = 0$, so suppose that $2T \neq O$. Write $2T = (x_2, y_2)$. Then by the lemma again $x_2, y_2 \in \mathbb{Z}$. But $x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x$, so $y \mid f'(x)$. As $E$ is non-singular, $f$ and $f'$ are coprime, so there exist $g, h \in \mathbb{Q}[X]$ such that $g(X)f(X) + h(X)f'(X)^2 = 1$. Doing this calculation and clearing denominators gives

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

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

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

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

# 11 Kummer Theory

Let $K$ be a field, $\operatorname{char} K \nmid n$. 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 $\langle , \rangle : \operatorname{Gal}(L/K) \times \Delta \to \mu_n$, $(\sigma, x) \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$. Note that this is well-defined and bilinear. It is also non-degenerate: If $\sigma \in \operatorname{Gal}(L/K)$ such that $\langle \sigma, x \rangle = 1$ for all $x \in \Delta$, then clearly $\sigma = 1$. If $x \in \Delta$ such that $\langle \sigma, x \rangle = 1$ for all $\sigma \in \operatorname{Gal}(L/K)$, so $\sigma(\sqrt[n]{x}) = \sqrt[n]{x}$ for all $\sigma$ and so $\sqrt[n]{x} \in K$, i.e. $x \in (K^*)^n$.

Thus we get injective group homomorphisms

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

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

By (i) $\operatorname{Gal}(L/K)$ is abelian of exponent dividing $n$.

N.B. If $G$ is a finite abelian group of exponent dividing $n$, then $\operatorname{Hom}(G, \mu_n) \cong G$ (non-canonically). So $\# \operatorname{Gal}(L/K) \leq \# \Delta \leq \# \operatorname{Gal}(L/K)$, hence the injections above 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*

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

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

$$(L^*)^n \cap K^*/(K^*)^n \longleftarrow L.$$

*Proof.* (i) Let $\Delta \subseteq K^*/(K^*)^n$ be a finite subgroup. Let $L = K(\sqrt[n]{\Delta})$ and $\Delta' = (L^*)^n \cap K^*/(K^*)^n$. We must show $\Delta = \Delta'$. Clearly $\Delta \subseteq \Delta'$. So $L = K(\sqrt[n]{\Delta}) \subseteq K(\sqrt[n]{\Delta'}) \subseteq L$. In particular $K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\Delta'})$, so by Lemma 11.1 $\#\Delta = \#\Delta'$. It follows that $\Delta = \Delta'$.

(ii) Let $L/K$ be a finite abelian extension of exponent dividing $n$. Let $\Delta = (L^*)^n \cap K^*/(K^*)^n$. Then $K(\sqrt[n]{\Delta}) \subseteq L$ and we aim to prove this is an equality. Let $G = \operatorname{Gal}(L/K)$.

The Kummer pairing gives an injection $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$. **Claim**: This is a surjection. From this we would get $[K(\sqrt[n]{\Delta}) : K] = \#\Delta = \#G$, so $L = K(\sqrt[n]{\Delta})$. Proof of claim: Let $\chi : G \to \mu_n$ be a homomorphism. Distinct automorphisms are linearly independent, so there exists $a \in L$ such that $y := \sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \neq 0$. Let $\sigma \in G$. Then

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

Therefore $\sigma(y^n) = y^n$ for all $\sigma \in G$, so $y^n \in K^*$. Let $x = y^n$. Then $x \in K^* \cap (L^*)^n$. Note that $\chi : \sigma \mapsto \frac{\sigma(y)}{y} = \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$. So the map $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$ sends $x$ to $\chi$ which proves the claim. □

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

*(i) $L/K$ is finite abelian of exponent dividing $n$.*

*(ii) $L/K$ is unramified at all $\mathfrak{p} \notin S$.*

*Proof.* Let $L$ be such an extension. By Theorem 11.2, $L = K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subseteq K^*/(K^*)^n$. Let $\mathfrak{p}$ be a prime of $K$. Write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$. If $x \in K^*$ represents an element of $\Delta$. Then $nv_{\mathfrak{P}_i}(\sqrt[n]{x}) = v_{\mathfrak{P}_i}(x) = e_i v_{\mathfrak{p}}(x)$. If $\mathfrak{p} \notin S$, then all $e_i = 1$, so $n \mid v_{\mathfrak{p}}(x)$. So $\Delta \subseteq K(S, n)$ where $K(S, n) = \{x \in K^*/(K^*)^n \mid v_{\mathfrak{p}}(x) \equiv 0 \bmod n \,\forall \mathfrak{p} \notin S\}$. The claim then follows from the following Lemma. □

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

*Proof.* The map $K(S, n) \to (\mathbb{Z}/n\mathbb{Z})^{\#S}$, $x \mapsto (v_{\mathfrak{p}}(x) \bmod n)_{\mathfrak{p} \in S}$ is a group homomorphism with kernel $K(\emptyset, n)$. So it suffices to prove that $K(\emptyset, n)$ is finite, i.e. we may assume $S = \emptyset$.

If $x \in K^*$ represents an element of $K(\emptyset, n)$, then $(x) = \mathfrak{a}^n$ for some fractional ideal $\mathfrak{a}$. There is a short exact sequence

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

We know that $\mathrm{Cl}_K$ is finite and $\mathcal{O}_K^*$ is finitely generated, so it follows that $K(\emptyset, n)$ is finite. □

# 12 Elliptic Curves over Number Fields - The Mordell-Weil Theorem

Let $K$ be a field.

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

*Proof.* For each element in the kernel we pick a coset representative $P \in E(K)$, and then $Q \in E(L)$ with $nQ = P$. For any $\sigma \in \mathrm{Gal}(L/K)$ we have $n(\sigma Q - Q) = \sigma P - P = O$, so $\sigma Q - Q \in E[n]$. Since $\mathrm{Gal}(L/K)$ and $E[n]$ are finite, there are only finitely many possibilities for the map $\mathrm{Gal}(L/K) \to E[n]$, $\sigma \mapsto \sigma Q - Q$. But if $P_1, P_2 \in E(K)$, $P_i = nQ_i, Q_i \in E(L)$ for $i = 1, 2$ and $\sigma Q_1 - Q_1 = \sigma Q_2 - Q_2$ for all $\sigma \in \mathrm{Gal}(L/K)$, then $\sigma(Q_1 - Q_2) = Q_1 - Q_2$, so $Q_1 - Q_2 \in E(K)$, hence $P_1 - P_2 = n(Q_1 - Q_2) \in nE(K)$. □

**Lemma 12.2.** *Let $E/K$ be an elliptic curve. If $P \in E(K)$, then $K([n]^{-1}P)/K$ is a Galois extension, and moreover if $E[n] \subseteq E(K)$, the Galois group is abelian of exponent dividing $n$.*

*Proof.* Since $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ acts on $[n]^{-1}(P)$, we see that $\mathrm{Gal}(K^{\mathrm{alg}}/K([n]^{-1}P))$ is a normal subgroup of $\mathrm{Gal}(K^{\mathrm{alg}}/K)$, so the extension $K([n]^{-1}P)/K$ is Galois.

Suppose that $E[n] \subseteq E(K)$. Pick $Q \in [n]^{-1}P$. Then $[n]^{-1}P = \{Q + T \mid T \in E[n]\}$. So $K([n]^{-1}P) = K(Q)$. There is a map $\mathrm{Gal}(K(Q)/K) \to E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, $\sigma \mapsto \sigma Q - Q$. This is a group homomorphism as $\sigma\tau Q - Q = \sigma(\tau Q - Q) + \sigma Q - Q = (\tau\sigma - Q) + \sigma Q - Q$ and injective: If $\sigma Q - Q = O$, then $\sigma Q = Q$, so $\sigma$ fixes $K(Q)$, so $\sigma = 1$. Hence $\mathrm{Gal}(K(Q)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^2$. □

**Theorem 12.3** (Weak Mordell-Weil Theorem)**.** *Let $K$ be a number field, $E/K$ an elliptic curve, $n \geq 2$ an integer. Then $E(K)/nE(K)$ is finite.*

*Proof.* By Lemma 12.1 we may replace $K$ by a finite Galois extension, and thus wlog assume $\mu_n \subseteq K$ and $E[n] \subseteq E(K)$. The field extensions $K([n]^{-1}P)/K$ as $P$ runs over $E(K)$ are abelian of exponent dividing $n$ and unramified outside the finite set of primes

$$S = \{\mathfrak{p} \mid n\} \cup \{\text{primes of bad reduction}\}$$

by Theorem 9.7. By Proposition 11.3 there are only finitely many such extensions. The composite ($L$ say) of all these field extensions is therefore a finite Galois extension of $K$.

By construction of $L$ the map $E(K)/nE(K) \to E(L)/nE(L)$ is the zero map. By Lemma 12.1 again its kernel, which is $E(K)/nE(K)$, is finite. $\square$

Remark: If $K = \mathbb{R}$ or $\mathbb{C}$ or $[K : \mathbb{Q}_p] < \infty$, then $\#(E(K)/nE(K)) < \infty$, yet $E(K)$ is uncountable and so not finitely generated. For an example of a field $K$ and an elliptic curve $E/K$ for which $E(K)/2E(K)$ is not finitely generated, see Example Sheet 4.

Fact: If $K$ is a number field, there exists a quadratic form (= canonical height), $\widehat{h} : E(K) \to \mathbb{R}_{\geq 0}$ with the property that for any $B \geq 0$, the set $\{P \in E(K) \mid \widehat{h}(P) \leq B\}$ is finite. We will show this in the next chapter.

**Theorem 12.4** (The Mordell-Weil Theorem)**.** *Let $K$ be a number field, $E/K$ an elliptic curve. Then $E(K)$ is a finitely generated abelian group.*

*Proof.* Fix an integer $n \geq 2$. By Weak Mordell-Weil $E(K)/nE(K)$ is finite, so let $P_1, \ldots, P_m \in E(K)$ be a finite list of coset representatives. Let $\Sigma = \{P \in E(K) \mid \widehat{h}(P) \leq \max_{1 \leq i \leq m} \widehat{h}(P_i)\}$. Claim: $\Sigma$ generates $E(K)$. If not, there exists $P \in E(K)$ of minimal height which is not in the subgroup $A$ generated by $\Sigma$. Then $P = P_i + nQ$ for some $1 \leq i \leq m$ and $Q \in E(K)$. Note that $Q \notin A$, so by minimality of $\widehat{h}(P)$, we get $\widehat{h}(P) \leq \widehat{h}(Q)$, hence

$$\begin{aligned} 4\widehat{h}(P) \leq 4\widehat{h}(Q) &\leq n^2\widehat{h}(Q) \\ &= \widehat{h}(P - P_i) \\ &\leq \widehat{h}(P - P_i) + \widehat{h}(P + P_i) = 2\widehat{h}(P) + 2\widehat{h}(P_i). \end{aligned}$$

So $\widehat{h}(P) \leq \widehat{h}(P_i)$. Then $P \in \Sigma \subseteq A$, a contradiction.

Hence $\Sigma$ generates $E(K)$ and thus $E(K)$ is finitely generated. $\square$

# 13 Heights

For simplicity take $K = \mathbb{Q}$. Write $P \in \mathbb{P}^n(\mathbb{Q})$ as $P = (a_0 : a_1 : \cdots : a_n)$ where $a_0, \ldots, a_n \in \mathbb{Z}$ with $\gcd(a_0, \ldots, a_n) = 1$. The *height* of $P$ is $H(P) := \max_{0 \le i \le n} |a_i|$.

**Lemma 13.1.** *Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be coprime homogeneous polynomials of the same 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 there exist $c_1, c_2 > 0$ such that $c_1 H(P)^d \le H(F(P)) \le c_2 H(P)^d$.*

*Proof.* WLOG $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$. For the upper bound write $P = (a : b)$ with $a, b \in \mathbb{Z}$ coprime. Then $H(F(P)) \le \max(|f_1(a,b)|, |f_2(a,b)|) \le c_2 \max\{|a|^d, |b|^d\}$ where $c_2 = \max_{i=1,2}$(sum of absolute values of coeffs. of $f_i$). Hence $H(F(P)) \le c_2 H(P)^d$.

Lower bound: We claim there exist homogeneous polynomials $g_{ij} \in \mathbb{Z}[X_1, X_2]$ of degree $d-1$ and $\kappa \in \mathbb{Z}_{>0}$ such that $\sum_{j=1}^{2} g_{ij} f_j = \kappa X_i^{2d-1}$ for $i = 1, 2$. Indeed, running Euclid's algorithm on $f_1(X, 1)$ and $f_2(X, 1)$ gives $r, s \in \mathbb{Q}[X]$ of degree $< d$ such that $r(X) f_1(X, 1) + s(X) f_2(X, 1) = 1$. Homogenizing and clearing denominators gives the claim with $i = 2$. Likewise with $i = 1$. Write $P = (a_1 : a_2)$ with $a_1, a_2 \in \mathbb{Z}$ coprime. Then $\sum_{j=1}^{2} g_{ij}(a_1, a_2) f_j(a_1, a_2) = \kappa a_i^{2d-1}$ for $i = 1, 2$. Therefore $\gcd(f_1(a_1, a_2), f_2(a_1, a_2))$ divides $\gcd(\kappa a_1^{2d-1}, \kappa a_2^{2d-1}) = \kappa$. Also

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

where $\gamma_i = \sum_{j=1}^{2}$(sum of absolute values of coeffs. of $g_{ij}$). Therefore $H(P)^{2d-1} \le \max(\gamma_1, \gamma_2) H(F(P)) H(P)^{d-1}$ and so $c_1 H(P)^d \le H(F(P))$ where $c_1 = \frac{1}{\max(\gamma_1, \gamma_2)}$. $\square$

Notation: For $x \in \mathbb{Q}$, let $H(x) = H((x : 1)) = \max(|a|, |b|)$ where $x = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ coprime.

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

**Definition.** *The* height *on $E$ is*

$$H : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\ge 1}$$

$$P \longmapsto \begin{cases} H(x) & \textit{if } P = (x,y), \\ 1 & \textit{if } P = O_E. \end{cases}$$

*The* logarithmic height *is*

$$h : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0},$$
$$P \longmapsto \log H(P).$$

**Lemma 13.2.** *Let $E, E'$ be elliptic curves over $\mathbb{Q}$, $\phi : E \to E'$ an isogeny defined over $\mathbb{Q}$. Then there exists $c > 0$ such that $|h(\phi(P)) - (\deg \phi)h(P)| \leq c$ for all $P \in E(\mathbb{Q})$.*

*Proof.* Recall that by Lemma 5.4 there is a map $\xi : \mathbb{P}^1 \to \mathbb{P}^1$ such that

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

commutes. By Lemma 13.1 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 $P \in E(\mathbb{Q})$ where $d = \deg \xi = \deg \phi$. Taking log gives

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

□

Let $\phi = [2] : E \to E$. Then there exists $c > 0$ such that $|h(2P) - 4h(P)| \leq C$ for all $P \in E(\mathbb{Q})$.

The canonical height is

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

We check that this converges: Let $m \geq n$, then

$$\begin{aligned} |4^{-m}h(2^m P) - 4^{-n}h(2^n P)| &\leq \sum_{r=n}^{m-1} |4^{-(r+1)}h(2^{r+1}P) - 4^{-r}h(2^r P)| \\ &= \sum_{r=n}^{m-1} 4^{-(r+1)}|h(2(2^r P)) - 4h(2^r P)| \\ &\leq C \sum_{r=n}^{\infty} 4^{-(r+1)} \\ &= \frac{C}{3 \cdot 4^n} \to 0 \text{ as } n \to \infty \end{aligned}$$

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

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

*Proof.* Putting $n = 0$ in the above calculation gives $|4^{-m}h(2^m P) - h(P)| \leq \frac{C}{3}$, hence $|\widehat{h}(P) - h(P)| \leq \frac{C}{3}$. ☐

**Corollary 13.4.** *For any $B > 0$, the set $\{P \in E(\mathbb{Q}) \mid \widehat{h}(P) \leq B\}$ is finite.*

*Proof.* By the previous lemma we can replace $\widehat{h}$ by $h$. It is clear that there are only finitely many $x$ with $H(x) \leq B$, each such $x$ leaves at most 2 choices for $y$. ☐

**Lemma 13.5.** *Let $\phi : E \to E'$ be an isogeny defined over $\mathbb{Q}$. Then $\widehat{h}(\phi P) = (\deg \phi)\widehat{h}(P)$ for all $P \in E(\mathbb{Q})$.*

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

Remark: This shows that $\widehat{h}$ (unlike $h$) does not depend on the choice of Weierstraß equation for $E$.

Taking $\phi = [n]$ shows $\widehat{h}(nP) = n^2\widehat{h}(P)$ for all $P \in E(\mathbb{Q}), n \in \mathbb{Z}$.

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

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

*for all $P, Q \in E(\mathbb{Q})$ with $P, Q, P + Q, P - Q \neq O$.*

*Proof.* Let $P, Q, P + Q, P - Q$ have $x$ coordinates $x_1, \ldots, x_4$. Write $x_i = \frac{r_i}{s_i}$ with $r_i, s_i \in \mathbb{Z}$ coprime. As in the proof of Theorem 5.7 there are polynomials $W_0, W_1, W_2$ such that $(s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = (W_0 : W_1 : W_2)$. The $W_0, W_1, W_2$ have degree 2 in $r_1, s_1$ and degree 2 in $r_2, s_2$.

Then

$$\begin{aligned} H(P + Q)H(P - Q) &= \max(|r_3|, |s_3|) \max(|r_4|, |s_4|) \\ &\leq 2 \max(|s_3 s_4|, |r_3 s_4 + r_4 s_3|, |r_3 r_4|) \\ &\leq 2 \max(|W_0|, |W_1|, |W_2|) \\ &\leq (\text{const.}) \max(|r_1|, |s_1|)^2 \max(|r_2|, |s_2|)^2 \\ &= (\text{const.}) H(P)^2 H(Q)^2. \end{aligned}$$

☐

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

*Proof.* Using Lemma 13.6 and that $|h(2P) - 4h(P)|$ is bounded (in one of the exceptional cases where the lemma does not apply) we get $h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + C$ for some constant $C$ for all $P, Q \in E(\mathbb{Q})$. Then replace $P, Q$ by $2^n P, 2^n Q$, divide by $4^n$ and take the limit $n \to \infty$. We get $\widehat{h}(P+Q) + \widehat{h}(P-Q) \leq 2\widehat{h}(P) + 2\widehat{h}(Q)$ Replacing $P, Q$ by $P+Q, P-Q$ and using $\widehat{h}(2P) = 4\widehat{h}(P)$ we get the reverse inequality.

So $\widehat{h}$ satisfies the parallelogram law and is thus a quadratic form. □

Remark: Over a general number field $K$, define the height $H(P)$ of $P = (a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n(K)$ by

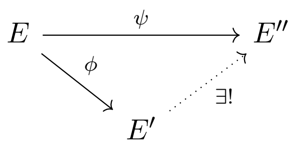
$$H(P) = \prod_v \max_{0 \leq i \leq n} |a_i|_v$$

where the product ranges over the places $v$ of $K$ (using a suitable normalization of $|\cdot|_v$). This is well-defined by the product formula. All results in this section generalize from $\mathbb{Q}$ to $K$.

# 14 Dual Isogenies and the Weil Pairing

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

**Proposition 14.1.** *Let $\Phi \subseteq E(K^{\text{alg}})$ be a finite $\text{Gal}(K^{\text{alg}}/K)$-stable subgroup. Then there exists an elliptic curve $E'/K$ and a separable isogeny $\phi : E \to E'$ defined over $K$, with kernel $\Phi$. Moreover, every isogeny $\psi : E \to E''$ with $\Phi \subseteq \ker\psi$ uniquely factors through $\phi$.*




*Proof.* Omitted, see Silverman AEC, Chapter III, Corollary 11 and Proposition 4.12. □

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

*Proof.* Uniqueness: $\psi_1\phi = \psi_2\phi = [n]$, so $(\psi_1 - \psi_2)\phi = 0$, so $\psi_1 = \psi_2$ as $\phi$ is surjective. Case $\phi$ is separable: $\#\ker\phi = n$, so $\ker\phi \subseteq E[n]$. Apply the proposition to $\psi = [n]$.

Case $\phi$ inseparable: Omitted (Silverman AEC, Chapter III, Theorem 6). □

Remarks:

(i) Write $E_1 \sim E_2$ if $E_1, E_2$ are isogenous. Then $\sim$ is an equivalence relation.

(ii) $\deg[n] = n^2$, so $\deg\phi = \deg\widehat{\phi}$ and $\widehat{[n]} = [n]$.

(iii) If $E_1 \xrightarrow{\psi} E_2 \xrightarrow{\phi} E_3$, then $\widehat{\phi\psi} = \widehat{\psi}\widehat{\phi}$.

(iv) $\phi\widehat{\phi}\phi = \phi[n]_E = [n]_{E'}\phi$, hence $\phi\widehat{\phi} = [n]_{E'}$. In particular $\widehat{\widehat{\phi}} = \phi$. If $\phi \in \text{End}(E)$, then $\phi^2 - [\operatorname{tr}\phi]\phi + [\deg\phi] = 0$, so $([\operatorname{tr}\phi] - \phi)\phi = [\deg\phi]$. So $\widehat{\phi} = [\operatorname{tr}\phi] - \phi$ and so $[\operatorname{tr}\phi] = \phi + \widehat{\phi}$.

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

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

*Proof.*

(i) If $E = E'$, this follows from $\operatorname{tr}(\phi + \psi) = \operatorname{tr}\phi + \operatorname{tr}\psi$.

(ii) In general, let $\alpha : E' \to E$ be any isogeny (e.g. $\alpha = \widehat{\phi}$). Then by (i), $\widehat{\alpha(\phi+\psi)} = \widehat{\alpha\phi+\alpha\psi} = \widehat{\alpha\phi} + \widehat{\alpha\psi}$. So $\widehat{\phi+\psi}\widehat{\alpha} = (\widehat{\phi}+\widehat{\psi})\widehat{\alpha}$. The claim follows.

□

Remark: In Silverman's AEC, the lemma is used to show that $\deg : \mathrm{Hom}(E, E')$ is a quadratic form.

Let $\mathrm{sum} : \mathrm{Div}(E) \to E$, $\sum n_P(P) \mapsto \sum n_P P$. Recall $E \xrightarrow{\sim} \mathrm{Pic}^0(E)$ via $P \mapsto [(P) - (O_E)]$ and $\mathrm{sum}(D) \mapsto [D]$ if $\deg D = 0$.

We deduce:

**Lemma 14.4.** *Let $D \in \mathrm{Div}(E)$. Then $D \sim 0$ iff $\deg D = 0$ and $\mathrm{sum}\, D = O_E$.*

Let $\phi : E \to E'$ be an isogeny of degree $n$ with dual isogeny $\widehat{\phi} : E' \to E$. Assume $\mathrm{char}\, K \nmid n$ (so both $\phi$ and $\widehat{\phi}$ are separable). We define the Weil pairing

$$E[\phi] \times E'[\widehat{\phi}] \to \mu_n.$$

Let $T \in E'[\widehat{\phi}]$. Then $nT = 0$, so there exists $f \in K^{\mathrm{alg}}(E')^*$ such that $\mathrm{div}(f) = n(T) - n(O)$. Pick $T_0 \in E(K^{\mathrm{alg}})$ such that $\phi T_0 = T$. Then $\phi^*(T) - \phi^*(O) = \sum_{P \in E[\phi]}(P + T_0) - \sum_{P\in E[\phi]}(P)$ has sum $nT_0 = \widehat{\phi}\phi T_0 = \widehat{\phi} T = 0$. So there is $g \in K^{\mathrm{alg}}(E)^*$ such that

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

Now $\mathrm{div}(\phi^* f) = \phi^*(\mathrm{div}\, f) = \phi^*(n(T) - n(O)) = n(\phi^*(T) - \phi^*(O)) = \mathrm{div}(g^n)$. So $\phi^* f = cg^n$ for some $c \in K^{\mathrm{alg}*}$. Rescaling $f$ we may assume $c = 1$, so $\phi^* f = g^n$.

If $S \in E[\phi]$, then $\phi \circ \tau_S = \phi$, so $\tau_S^*(\mathrm{div}\, g) = \mathrm{div}\, g$. Then $\mathrm{div}(\tau_S^* g) = \mathrm{div}(g)$ and so $\tau_S^* g = \zeta g$ for some $\zeta \in K^{\mathrm{alg}*}$. Therefore

$$\zeta = \frac{g(X+S)}{g(X)} \quad \text{for all } X \in E(K^{\mathrm{alg}}) \text{ where this is defined.}$$

Now $\zeta^n = \frac{g(X+S)^n}{g(X)^n} = \frac{f(\phi(X+S))}{f(\phi(X))} = 1$ since $S \in E[\phi]$. So $\zeta \in \mu_n$. We define $e_\phi(S, T) = \zeta = \frac{g(X+S)}{g(X)}$.

**Proposition 14.5.** *$e_\phi$ is bilinear and non-degenerate.*

*Proof.* (i) Linearity in first argument:

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

(ii) Linearity in second argument: Let $T_1, T_2 \in E'[\widehat{\phi}]$, we get $f_1, f_2, g_1, g_2$ with $\mathrm{div}(f_i) = n(T_i) - n(O)$ and $\phi^* f_i = g_i^n$, $i = 1, 2$. There exists $h \in K^{\mathrm{alg}}(E')^*$ such that $\mathrm{div}(h) =$

$(T_1)+(T_2)-(T_1+T_2)-(O)$. Then put $f=\frac{f_1 f_2}{h^n}$. Then $\operatorname{div}(f)=\operatorname{div}(f_1)+\operatorname{div}(f_2)-n\operatorname{div}(h)=n(T_1+T_2)-n(O)$ and $\phi^* f=\frac{g_1^n g_2^n}{(\phi^* h)^n}$, so set $g=\frac{g_1 g_2}{\phi^* h}$. Then

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

(iii) Nondegeneracy: For $T\in E'[\widehat{\phi}]$ suppose $e_\phi(S,T)=1$ for all $S\in E[\phi]$. Then $\tau_S^* g=g$ for all $S\in E[\phi]$. Note that $K^{\mathrm{alg}}(E)/\phi^* K^{\mathrm{alg}}(E')$ is Galois with Galois group $E[\phi]$ (where $S\in E[\phi]$ acts as $\tau_S^*$). Then $g=\phi^* h$ for some $h\in K^{\mathrm{alg}}(E')$ (see also Proposition 14.1). Then $\phi^* f=g^n=\phi^*(h^n)$, so $f=h^n$ and thus $\operatorname{div}(h)=(T)-(O)$. Then $T=O$. Hence $E'[\widehat{\phi}]\to\operatorname{Hom}(E[\phi],\mu_n)$ is injective. Since $\#E[\phi]=\#E'[\widehat{\phi}]=n$, this map is an isomorphism. □

Remarks:

(i) If $E,E',\phi$ are defined over $K$, then $e_\phi$ is Galois equivariant, i.e. $e_\phi(\sigma S,\sigma T)=\sigma(e_\phi(S,T))$ for all $\sigma\in\operatorname{Gal}(K^{\mathrm{alg}}/K), S\in E[\phi], T\in E'[\widehat{\phi}]$.

(ii) Taking $\phi=[n]:E\to E$ (so $\widehat{\phi}=n$) gives $e_n:E[n]\times E[n]\to\mu_n$ (note that since $E[n]$ is $n$-torsion the image is actually in $\mu_n\subseteq\mu_{n^2}$).

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

*Proof.* $e_n$ is nondegenerate, so there exists $S,T\in E[n]$ such that $e_n(S,T)$ is a primitive $n$-th root of unity $\zeta_n$. Then $\sigma(\zeta_n)=\sigma(e_n(S,T))=e_n(\sigma S,\sigma T)=e_n(S,T)$ for all $\sigma\in\operatorname{Gal}(K^{\mathrm{alg}}/K)$, hence $\zeta_n\in K$. □

Remark: In fact the Weil pairing $e_n$ is alternating, i.e. $e_n(T,T)=1$ for all $T\in E[n]$.

# 15 Galois Cohomology

Let $G$ be a group, $A$ a $G$-module.

**Definition.**

$$\begin{aligned} H^0(G,A) &= A^G = \{a \in A \mid \sigma a = a \,\forall \sigma \in G\} \\ C^1(G,A) &= \{\text{maps } G \to A\} \\ Z^1(G,A) &= \{(a_\sigma)_{\sigma \in A} \in C^1(G,A) \mid a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\} \\ B^1(G,A) &= \{(\sigma b - b)_{\sigma \in G} \mid b \in A\} \\ H^1(G,A) &= Z^1(G,A)/B^1(G,A) \end{aligned}$$

*Elements in $C^1(G,A)$ (resp. $Z^1(G,A)$, $B^1(G,A)$) are called* cochains *(resp.* cocycles*,* coboundaries*).*

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

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

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

*induces a long exact sequence of abelian groups:*

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

*Proof.* Omitted (straightforward, Snake lemma). □

Definition of $\delta$: Let $c \in C^G$. Then there exists $b \in B$ such that $\psi(b) = c$. Then $\psi(\sigma b - b) = \sigma c - c$ for all $\sigma \in G$, so $\sigma b - b = \phi(a_\sigma)$ for some $a_\sigma \in A$. Then $(a_\sigma)_{\sigma \in G} \in Z^1(G,A)$. We define $\delta(c) = (a_\sigma)_{\sigma \in G} + B^1(G,A) \in H^1(G,A)$.

**Theorem 15.2.** *Let $A$ be a $G$-module, $H$ a normal subgroup of $G$. There is an inflation-restriction exact sequence:*

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

*Proof.* Omitted (straightforward). □

Let $K$ be a perfect field. Then $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ is a topological group. If $G = \mathrm{Gal}(K^{\mathrm{alg}}/K)$, we modify the definition of $H^1(G,A)$ by insisting:

(1) The stabilizer of each $a \in A$ is an open subgroup of $G$.

(2) All cochains $G \to A$ are continuous where $A$ carries the discrete topology.

**Theorem** (Hilbert's Theorem 90)**.** *Let $L/K$ be a finite Galois extension. Then*

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

*Proof.* Let $G = \mathrm{Gal}(L/K)$. Let $(a_\sigma)_{\sigma \in G} \in Z^1(G, L^\times)$. Distinct automorphisms are linearly independent, so there exists $y \in L$ such that $x := \sum_{\tau \in G} a_\tau^{-1} \tau(y) \neq 0$. For $\sigma \in G$, $\sigma(x) = \sum_{\tau \in G} \sigma(a_\tau)^{-1} \sigma\tau(y) = a_\sigma \sum_{\tau \in G} a_{\sigma\tau}^{-1} \sigma\tau(y) = a_\sigma x$. Hence $a_\sigma = \frac{\sigma(x)}{x}$, so $(a_\sigma)_{\sigma \in G} \in B^1(G, L^\times)$, so $H^1(G, L^\times) = 0$. □

We have

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

where the direct limit is taken with respect to the inflation maps.

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

**Example.** Assume $\mathrm{char}\, K \nmid n$. There is a short exact sequence of $\mathrm{Gal}(K^{\mathrm{alg}}/K)$-modules:

$$0 \to \mu_n \to K^{\mathrm{alg}\times} \xrightarrow{n} K^{\mathrm{alg}\times} \to 0$$

This is gives a long exact sequence

$$K^\times \xrightarrow{n} K^\times \xrightarrow{\delta} H^1(\mathrm{Gal}(K^{\mathrm{alg}}/K), \mu_n) \to H^1(\mathrm{Gal}(K^{\mathrm{alg}}/K), K^{\mathrm{alg}\times}) = 0.$$

Hence $H^1(\mathrm{Gal}(K^{\mathrm{alg}}/K), \mu_n) \cong K^\times/(K^\times)^n$.

If $\mu_n \subseteq K$, then $\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(K^{\mathrm{alg}}/K), \mu_n) = H^1(\mathrm{Gal}(K^{\mathrm{alg}}/K), \mu_n) \cong K^\times/(K^\times)^n$.

And there is a bijection:

$$\left\{ \begin{matrix} \text{finite abelian extensions } L/K \\ \text{of exponent dividing } n \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{finite subgroups of} \\ \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(K^{\mathrm{alg}}/K), \mu_n) \end{matrix} \right\},$$
$$L \longmapsto \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$$

This gives another proof of Theorem 11.2.[1]

Notation: $H^1(K, -)$ means $H^1(\mathrm{Gal}(K^{\mathrm{alg}}/K), -)$.

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

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

[1] Remark by L.T.: To get the precise statement of Theorem 11.2 we probably need something like Pontryagin duality so that we have a canonical bijection between open subgroups of $\mathrm{Gal}(K^{\mathrm{alg}}/K)$ and finite subgroups of $\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(K^{\mathrm{alg}}/K), \mu_n)$...

This gives the long exact sequence:

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

So we get a short exact sequence:

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

Now take $K$ to be a number field. For each place $v$ of $K$ fix an embedding $K^{\text{alg}} \hookrightarrow K_v^{\text{alg}}$. Then $\text{Gal}(K_v^{\text{alg}}/K_v) \hookrightarrow \text{Gal}(K^{\text{alg}}/K)$. Then we get:

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

**Definition.** *The* $\phi$-Selmer group *is*

$$S^{(\phi)}(E/K) = \ker \searrow = \ker \Big( H^1(K, E[\phi]) \to \prod_v H^1(K_v, E) \Big).$$

*The* Tate-Shafarevich group *is*

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

We get a short exact sequence

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

Taking $\phi = [n]$ gives

$$0 \to \frac{E(K)}{nE(K)} \xrightarrow{\delta} S^{(n)}(E/K) \to \text{Ш}(E/K)[n] \to 0.$$

Rearranging the proof of the weak Mordell Weil Theorem gives:

**Theorem 15.3.** *$S^{(n)}(E/K)$ is finite.*

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

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

By extending our field we may thus assume $E[n] \subseteq E(K)$ (and hence $\mu_n \subseteq K$). So $E[n] \cong \mu_n \times \mu_n$ as Galois modules. Then $H^1(K, E[n]) \cong H^1(K, \mu_n) \times H^1(K, \mu_n) \cong K^\times/(K^\times)^n \times K^\times/(K^\times)^n$.

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

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

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

There is a commutative diagram with exact rows

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

The map $E(K_v^{\mathrm{ur}}) \xrightarrow{\times n} E(K_v^{\mathrm{ur}})$ is surjective for $v \notin S$. So $E(K_v^{\mathrm{ur}}) \xrightarrow{\delta_v} H^1(K_v^{\mathrm{ur}}, E[n])$ is the zero map. Then $\mathrm{Im}(\delta_v) \subseteq \ker(\downarrow)$. Then

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

We know that $K(S, n)$ is finite by Lemma 11.4. Hence $S^{(n)}(E/K)$ is finite. □

# 16 Descent by Cyclic Isogeny

Let $E, E'$ be elliptic curves over a number field $K$ and $\phi : E \to E'$ an isogeny of degree $n$. Suppose $E'[\widehat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$ is cyclic and generated by $T \in E'(K)$. Then $E[\phi] \cong \mu_n$ as $\mathrm{Gal}(K^{\mathrm{alg}}/K)$-modules via $S \mapsto e_\phi(S,T)$. There is a short exact sequence of $\mathrm{Gal}(K^{\mathrm{alg}}/K)$-modules

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

This gives a long exact sequence

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

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

*Proof.* Let $Q \in \phi^{-1}P$. Then $\delta(P)$ is represented by the cocycle $\sigma \mapsto \sigma Q - Q \in E[\phi]$. And $E[\phi] \cong \mu_n$ via $S \mapsto e_\phi(S,T)$. Then $e_\phi(\sigma Q - Q, T) = \frac{g(X+\sigma Q - Q)}{g(X)}$ for any $X \in E \setminus \{\text{zeros, poles of } g\}$. Take $X = Q$, so $e_\phi(\sigma Q - Q, T) = \frac{g(\sigma Q)}{g(Q)} = \frac{\sigma(g(Q))}{g(Q)} = \frac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}}$. So $\delta(P)$ is represented by the cocycle $\sigma \mapsto \frac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}}$. But $H^1(K,\mu_n) \cong K^\times/(K^\times)^n$ where $x \in K^\times$ corresponds to $\sigma \mapsto \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}}$. Therefore

$$\alpha(P) = f(P) \bmod (K^\times)^n.$$

$\square$

## 16.1 Descent by 2-Isogeny

Let

$$E : y^2 = x(x^2 + ax + b)$$
$$E' : y^2 = x(x^2 + a'x + b')$$

where $b(a^2-4b)\neq 0$ and $a'=-2a$, $b'=a^2-4b$. Consider the isogenies:

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

The kernels are:

$$\begin{aligned} E[\phi] &= \{O_E, T\} \quad T=(0,0)\in E(K), \\ E'[\widehat{\phi}] &= \{O_{E'}, T'\} \quad T'=(0,0)\in E'(K). \end{aligned}$$

**Proposition 16.2.** *There is a group homomorphism*

$$\begin{aligned} E'(K) &\longrightarrow K^\times/(K^\times)^2 \\ (x,y) &\longmapsto \begin{cases} x \bmod (K^\times)^2 & \text{if } x\neq 0, \\ b' \bmod (K^\times)^2 & \text{if } x=0 \end{cases} \end{aligned}$$

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

*Proof.* Either apply the theorem with $f=x\in K(E')$, $g=\frac{x}{y}\in K(E)$, or use direct calculation (see Example Sheet 4). □

We get maps

$$\begin{aligned} \alpha_E &: \frac{E(K)}{\widehat{\phi}E'(K)} \hookrightarrow K^\times/(K^\times)^2 \\ \alpha_{E'} &: \frac{E'(K)}{\phi E(K)} \hookrightarrow K^\times/(K^\times)^2 \end{aligned}$$

**Lemma 16.3.** $2^{\operatorname{rank} E(K)} = \frac{\#\operatorname{Im}(\alpha_E)\cdot\#\operatorname{Im}(\alpha_{E'})}{4}$.

*Proof.* If $A\xrightarrow{f}B\xrightarrow{g}C$ homomorphisms of abelian groups, then there is an exact sequence

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

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

$$0\to\underbrace{E(K)[\phi]}_{\cong\mathbb{Z}/2\mathbb{Z}}\to E(K)[2]\xrightarrow{\phi}\underbrace{E'(K)[\widehat{\phi}]}_{\cong\mathbb{Z}/2\mathbb{Z}}\to\underbrace{\frac{E'(K)}{\phi E(K)}}_{\cong\operatorname{Im}(\alpha_{E'})}\xrightarrow{\widehat{\phi}}\frac{E(K)}{2E(K)}\to\underbrace{\frac{E(K)}{\widehat{\phi}E'(K)}}_{\cong\operatorname{Im}(\alpha_E)}\to 0$$

Counting orders gives

$$\frac{\#\big(E(K)/2E(K)\big)}{\#E(K)[2]}=\frac{\#\operatorname{Im}(\alpha_E)\#\operatorname{Im}(\alpha_{E'})}{4}.$$

By the Mordell-Weil Theorem, $E(K) \cong \Delta \times \mathbb{Z}^r$ where $r$ is the rank and $\Delta$ is a finite group. Then

$$\begin{aligned} E(K)/2E(K) &= \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r, \\ E(K)[2] &= \Delta[2]. \end{aligned}$$

Since $\Delta$ is finite, $\Delta[2]$ and $\Delta/2\Delta$ have the same order, so $\frac{\#(E(K)/2E(K))}{\#E(K)[2]} = 2^r$. $\square$

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

*Proof.* We must show that if $x, y \in K$ with $y^2 = x(x^2 + ax + b)$ and $v_\mathfrak{p}(b) = 0$, then $v_\mathfrak{p}(x) \equiv 0 \bmod 2$.

- Case $v_\mathfrak{p}(x) < 0$: then $v_\mathfrak{p}(x)$ is even by Lemma 9.1.
- Case $v_\mathfrak{p}(x) > 0$: then $v_\mathfrak{p}(x^2 + ax + b) = 0$, so $v_\mathfrak{p}(x) = v_\mathfrak{p}(y^2) = 2v_\mathfrak{p}(y)$ is even. $\square$

**Lemma 16.5.** *If $b_1 b_2 = b$, then $b_1(K^\times)^2 \in \mathrm{Im}(\alpha_E)$ iff*

$$w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4 \qquad (*)$$

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

*Proof.* If $b_1 \in (K^\times)^2$ or $b_2 \in (K^\times)^2$, then both conditions are satisfied. So we may assume $b_1, b_2 \notin (K^\times)^2$. Then

$$\begin{aligned} b_1(K^\times)^2 &\in \mathrm{Im}(\alpha_E) \\ &\iff \exists (x,y) \in E(K) \text{ such that } x = b_1 t^2 \text{ for some } t \in K^\times \\ &\implies y^2 = b_1 t^2((b_1 t^2)^2 + a b_1 t^2 + b) \\ &\implies \left(\frac{y}{b_1 t}\right)^2 = b_1 t^4 + a t^2 + \frac{b}{b_1} \end{aligned}$$

So $(*)$ has a solution $u = t, v = 1, w = \frac{y}{b_1 t}$. Conversely, if $(u, v, w)$ is a solution to $(*)$, then $uv \neq 0$ and $\left(b_1\left(\frac{u}{v}\right)^2, b_1 \frac{uw}{v^3}\right) \in E(K)$. $\square$

Take $K = \mathbb{Q}$.

**Examples.**

(1) $E : y^2 = x^3 - x$, so $a = 0, b = -1$. Then $\mathrm{Im}(\alpha_E) = \langle -1 \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. We have $E' : y^2 = x^3 + 4x$, $\mathrm{Im}(\alpha_{E'}) \subseteq \langle -1, 2 \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. We get the equations:

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

The first and last equation are insolvable over $\mathbb{R}$, the second has solution $(u,v,w) = (1,1,2)$.

Hence $\mathrm{Im}(\alpha_{E'}) = \langle 2 \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Therefore $2^{\operatorname{rank} E(\mathbb{Q})} = \frac{2\cdot 2}{4} = 1$, so $\operatorname{rank} E(\mathbb{Q}) = 0$, so 1 is not a congruent number as we have already seen in Theorem 1.3.

(2) $E : y^2 = x^3 + px$ where $p$ is a prime, $p \equiv 5 \bmod 8$. For $b_1 = -1$ we get $w^2 = -u^4 - pv^4$ which is insolvable over $\mathbb{R}$, hence $\mathrm{Im}(\alpha_E) = \langle p \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

$E' : y^2 = x^3 - 4px$. Then $\mathrm{Im}(\alpha_{E'}) \subseteq \langle -1, 2, p \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

N.B. $\alpha_{E'}(T') = (-4p)(\mathbb{Q}^\times)^2 = (-p)(\mathbb{Q}^\times)^2$. We get

$$b_1 = 2 \quad \to \quad w^2 = 2u^4 - 2pv^4 \tag{1}$$
$$b_1 = -2 \quad \to \quad w^2 = -2u^4 + 2pv^4 \tag{2}$$
$$b_1 = p \quad \to \quad w^2 = pu^4 - 4v^4 \tag{3}$$

We continue it below.

We have the exact sequence

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

Consider the equation

$$w^2 = b_1 u^4 + a' u^2 v^2 + (b'/b_1) v^4. \tag{$*$}$$

Then:

$$\mathrm{Im}(\alpha_{E'}) = \{b_1 (\mathbb{Q}^\times)^2 \mid (*) \text{ is soluble over } \mathbb{Q}\},$$
$$S^{(\phi)}(E/\mathbb{Q}) = \{b_1 (\mathbb{Q}^\times)^2 \mid (*) \text{ is soluble over } \mathbb{Q}_p \text{ for all primes } p \text{ and over } \mathbb{R}\}.$$

Fact (use Exercise 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 soluble over $\mathbb{Q}_p$.

Continuation of Example (2) above: Suppose (1) is soluble, WLOG $u, v, w \in \mathbb{Z}$ with $\gcd(u,v) = 1$. If $p \mid u$, then $p \mid w$ and then $p \mid v$, so we get $p \nmid u$. So $w^2 \equiv 2u^4 \not\equiv 0 \bmod p$, so $\left(\frac{2}{p}\right) = 1$, contradicting $p \equiv 5 \bmod 8$. Likewise (2) is insoluble over $\mathbb{Q}$ since $\left(\frac{-2}{p}\right) = -1$. The same arguments show that (1) and (2) are insoluble over $\mathbb{Q}_p$.

Therefore $\operatorname{rank} E(\mathbb{Q}) = \begin{cases} 0 & \text{if (3) is insoluble over } \mathbb{Q}, \\ 1 & \text{if (3) is soluble over } \mathbb{Q}. \end{cases}$

- (3) is soluble over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right) = 1$, so by $-1 \in (\mathbb{Z}_p^\times)^2$ by Hensel's Lemma.
- (3) is soluble over $\mathbb{Q}_2$ since $p - 4 \equiv 1 \bmod 8$, so $p - 4 \in (\mathbb{Z}_2^\times)^2$.
- (3) is soluble over $\mathbb{R}$, since $\sqrt{p} \in \mathbb{R}$.

So we see that (3) is soluble in $\mathbb{Q}_q$ for all primes $q$ and also $q = \infty$. Over $\mathbb{Q}$?

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

Conjecture: $\operatorname{rank} E(\mathbb{Q}) = 1$ for all primes $p$ with $p \equiv 5 \bmod 8$.

Example 3 (Lind): $E : y^2 = x^3 + 17x$. Then $\operatorname{Im}(\alpha_E) = \langle 17 \rangle \subseteq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. $E'$ is defined by $y^2 = x^3 - 68x$. Then:

$$b_1 = 2 \to w^2 = 2u^4 - 38v^4$$

Replace $w$ by $2w$ and divide by 2 to get

$$C : 2w^2 = u^4 - 17v^4$$

Notation: $C(K) = \{(u, v, w) \in K^3 \setminus \{0\} \text{ satisfying the equation}\}/\sim$ where $(u, v, w) \sim (\lambda u, \lambda v, \lambda^2 w)$ for all $\lambda \in K^\times$, (i.e. consider the equation in a weighed projective space).

Then:

- $C(\mathbb{Q}_2) \neq \emptyset$ since $17 \in (\mathbb{Q}_2^\times)^4$.
- $C(\mathbb{Q}_{17}) \neq \emptyset$ since $2 \in (\mathbb{Q}_{17}^\times)^2$.
- $C(\mathbb{R}) \neq \emptyset$ since $\sqrt{2} \in \mathbb{R}$.

But we claim that $C(\mathbb{Q}) = \emptyset$. Suppose $(u, v, w) \in C(\mathbb{Q})$, wlog $u, v, w \in \mathbb{Z}$ and $\gcd(u, v) = 1$, $w > 0$. Note that $17 \nmid w$. So if $p \mid w$, then $p \neq 17$ and $\left(\frac{17}{p}\right) = 1$, so $\left(\frac{p}{17}\right) = 1$ by Quadratic Reciprocity if $p \neq 2$. If $p = 2$, then also $\left(\frac{2}{17}\right) = 1$. Therefore $\left(\frac{w}{17}\right) = 1$. But $2w^2 \equiv u^4 \bmod 17$, so $2 \in (\mathbb{F}_{17}^\times)^4 = \{\pm 1, \pm 4\}$, a contradiction. Hence $C(\mathbb{Q}) = \emptyset$.

So $C$ is a counterexample to the Hasse principle. It represents a nontrivial element of $Ш(E/\mathbb{Q})$.

# 17 The Birch Swinnerton-Dyer Conjecture

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

**Definition.**

$$L(E,s) := \prod_p L_p(E,s)$$

*where*

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1} & \textit{if } E \textit{ has good reduction at } p, \\ (1 \pm p^{-s})^{-1} & \textit{if } E \textit{ has multiplicative reduction,} \\ 1 & \textit{if } E \textit{ has additive reduction.} \end{cases}$$

By Hasse's Theorem, we have $|a_p| \leq 2\sqrt{p}$. This implies that $L(E,s)$ converges for $\operatorname{Re} s > \frac{3}{2}$.

**Theorem** (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 $L(E,2-s)$.*

**Weak BSD:** $\operatorname{ord}_{s=1} L(E,s) = \operatorname{rank} E(\mathbb{Q})$ ($= r$ say).

**Strong BSD:**

$$\lim_{s \to 1} \frac{1}{(s-1)^r} L(E,s) = \frac{\Omega_E \operatorname{Reg} E(\mathbb{Q}) \# Ш(E/\mathbb{Q}) \prod_p c_p(E)}{(\# E(\mathbb{Q})_{\text{tors}})^2}$$

where

- $c_p(E)$ is the Tamagawa number of $E/\mathbb{Q}_p$, i.e. $[E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$.
- $\operatorname{Reg} E(\mathbb{Q}) = \det([P_i, P_j])$ where $P_1, \ldots, P_r$ form a basis for $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ and $[P,Q] = \widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q)$.
- $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y + a_1 x + a_3}$ using a globally minimal Weierstraß minimal equation.