# Elliptic Curves

## Lectures

### 1. Fermat's method infinite descent

- Let $\Delta$ be a right triangle with side lengths $a, b, c$. We say $\Delta$ is **rational** if side lengths are rational, and we say $\Delta$ is **primitive** if side lengths integers and $\gcd(a, b, c) = 1$.
- Every primitive triangle has side lengths $u^2 - v^2$, $2uv$, and $u^2 + v^2$ for some integers $u, v \in \mathbb{Z}$, $u > v > 0$.
- **Congruent number:** Let $D$ be a positive rational. $D$ is congruent number if there exists rational right-angled triangle with area $D$.

  (equivalently, there exists a rational solution to $y^2 = x^3 - D^2 x$ s.t. $y \neq 0$) (or to $Dy^2 = x^3 - x$) (or the elliptic curve has *positive* rank)
- 1 is not a congruent number. Equivalently, there are no integer solutions to $w^2 = uv(u+v)(u-v)$ where $w \neq 0$.
- In general, if $u, v, w \in \mathbb{Z}, w \neq 0$ such that $Dw^2 = uv(u-v)(u+v)$, then there exists right-angled triangle with area $D$ with side lengths:
$$\frac{u^2 - v^2}{w}, \quad \frac{2uv}{w}, \quad \text{and} \quad \frac{u^2 + v^2}{w}$$
- Let $K$ be a field with $\mathrm{char}(K) \neq 2$. Let $u, v \in K[t]$ be coprime polynomials. If $\alpha u + \beta v$ is a square for 4 distinct pairs $(\alpha, \beta) \in \mathbb{P}^1$, then $u, v \in K$.
- **Elliptic curve:** An elliptic curve $E/K$ is the projective closure of a plane affine curve $y^2 = f(x)$ where $f \in K[x]$ is a monic cubic polnomial with distinct roots in $\bar{K}$.

  or An elliptic curve $E/K$ is a smooth projective curve of genus 1 with a specified $K$-rational point $O_E$.
- **Weierstrass equation:** The equation $y^2 = f(x)$ is called Weierstrass equation.

  *Fact:* Let $L/K$ be field extension Then $E(L) = \{(x, y) \in L^2 : y^2 = f(x)\} \cup \{O_E\}$. $E(L)$ is an *abelian group.*

  Let $E/K$ be elliptic curve. Then $E(K(t)) = E(K)$.
- **Isomorphism:** Let $E$ and $E'$ be elliptic curves. Then $E$ and $E'$ are isomorphic if there exists a morphism $\phi : E \to E'$ and a morphism $\chi : E' \to E$ s.t. $\chi \circ \phi = \mathrm{id}_E$ and $\phi \circ \chi = \mathrm{id}_{E'}$.

  Some results on congruent numbers: Let $p$ be a prime number. Then:

  - If $p \equiv 3 \pmod 8$, then $p$ is not congruent, but $2p$ is congruent.
  - If $p \equiv 5 \pmod 8$, then $p$ is congruent.
  - If $p \equiv 7 \pmod 8$, then $p$ and $2p$ is congruent.

  List of congruent numbers: $5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, \ldots$.

## 2. Remarks on algebraic curves

- **Rational:** A plane algebraic curve $C = \{f(x, y) = 0\} \subset \mathbb{A}^2$ (where $f$ irreducible) is rational if it has a rational parameterisation

  I.e. there exists $\phi, \chi \in K(t)$ s.t.

  - The map $t \mapsto (\phi(t), \chi(t))$ is injective for all but finitely many points in $\mathbb{A}^1$.
  - $f(\phi(t), \chi(t)) = 0$

  Any non-singular plane conic is rational. (e.g. $x^2 + y^2 = 1$)
  Any singular plane curve is rational (**not** elliptic curves) (e.g. $y^2 = x^3$ or $y^2 = x^2(x+1)$).

- **Genus:** Let $C$ be smooth projective curve. Genus $g(C) \in \mathbb{Z}_{\geq 0}$ is invariant of $C$.

- A smooth projective curve $C \subset \mathbb{P}^2$ of degree $d$ has genus

$$g(C) = \frac{(d-1)(d-2)}{2}$$

  (so if $d = 1, 2$, then genus is 0)

  Let $C$ be smooth projective curve.

  - $C$ is **rational** $\iff g(C) = 0$.
  - $C$ is **elliptic curve** $\iff g(C) = 1$.

- **Order of vanishing:** Let $C$ algebraic curve, function field $K(C)$. $P \in C$ a smooth point. Write $\mathrm{ord}_p(f)$ as the **order of vanishing** of $f \in K(C)$ at $P$

  $\mathrm{ord}_p(f) : K(C)^* \to \mathbb{Z}$ is a discrete valuation

  - $\mathrm{ord}_p(f_1 f_2) = \mathrm{ord}_p(f_1) + \mathrm{ord}_p(f_2)$
  - $\mathrm{ord}_p(f_1 + f_2) \geq \min(\mathrm{ord}_p(f_1), \mathrm{ord}_p(f_2))$

  E.g. If $y^2 = x(x-1)(x-\lambda)$, then $\mathrm{ord}_P(x) = -2$ and $\mathrm{ord}_P(y) = -3$ where $P = (0:1:0)$.

- **Uniformiser:** An element $t \in K(C)^*$ is a uniformiser at $P$ if $\mathrm{ord}_p(t) = 1$.

- Let $C$ be an affine curve, defined by $C = \{g(x, y) = 0\} \in \mathbb{A}^2$ where $g \in K[X, Y]$ is irreducible. Express $g(x, y)$ as

$$g(x, y) = g_0 + g_1(x, y) + g_2(x, y) + g_3(x, y) + \dots$$

  where each $g_i$ is homogenoues of degree $i$.

  Suppose $P = (0, 0) \in C$ is a smooth point on $C$, so we have $g_0 = 0$ and $g_1 = \alpha x + \beta y$ where $\alpha, \beta$ not both zero. ($g_1$ is tangent to $C$ at $P$)

  Then, for any $\gamma, \delta \in K$, we have that $\gamma x + \delta y \in K(C)$ is a **uniformiser** at $P$ if and only if $\alpha\delta - \beta\gamma \neq 0$ (i.e. $\gamma x + \delta y$ not some multiple of $g_1$, so not tangent)

- **Divisor:** A formal sum of points on $C$. Can be expressed in the form:

$$\sum_{p \in C} n_p P \quad \text{with } n_p \in \mathbb{Z}$$

  and $n_p = 0$ for all but finitely many $p \in C$.

- **Degree of divisor:** $\deg(D) = \sum n_p$
- **Divisor of function:** If $f \in K(C)^*$, then

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

This is called a **principal divisor**.

- **Effective divisor:** Let $D$ be divisor. $D$ is **effective** if $n_p \geq 0$ for all $P$. Notation: $D \geq 0$
- **Riemann Roch space**: The Riemann Roch space of $D \in \mathrm{Div}(C)$ is

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

(i.e. the $K$-vector space of rational functions on $C$ with poles no worise than that specified by $D$)

*Remark:* $\mathcal{L}(D)$ is a finite-dimensional $\bar{K}$-vector space

- **Riemann Roch for genus 1:** Let $D = \sum n_p P$, $\mathrm{deg}D = \sum n_p$:

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

- Let $C \subset \mathbb{P}^2$ be a smooth plane cubic and $P \in C$ a point of inflection. Then one can change coordinates such that

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

where $P = (0 : 1 : 0)$ and $\lambda \neq 0, 1$. This is called **Legendre form**.

- **Degree of a morphism** Let $\phi : C_1 \to C_2$ be non-constant morphism of smooth projective curve. Let $\phi^* : K(C_2) \to K(C_1)$ be **pullback** given by $f \mapsto f \circ \phi$.

The **degree** of $\phi$ is $[K(C_1) : \phi^* K(C_2)]$ (we define $\phi$ is **separable** iff extension $K(C_1)/\phi^* K(C_2)$ is separable)

*Fact:* $\deg \phi = 1$ if and only if $\phi$ is an isomorphism. $\deg \phi = 0$ if and only if $\phi$ is a constant map.

- **Ramification index:** Let $P \in C_1$ and $Q \in C_2$ such that $\phi(P) = Q$. Let $t \in K(C_2)$ be a uniformizer at $Q$ (i.e. $\mathrm{ord}_Q(t) = 1$) Then the **ramification index** $e_\phi(P)$ is

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t) \qquad (\text{note } e_\phi(P) \geq 1)$$

This is independent of choice of $t$.

- Let $\phi : C_1 \to C_2$ be non-constant morphism of smooth projective curves. Then

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi) \quad \text{for all } Q \in C_2$$

If $\phi$ is separable, then $e_\phi(P) = 1$ for all but finitely many $P \in C_1$.

- $\phi$ is surjective
- $|\phi^{-1}(Q)| \leq \deg(\phi)$ with equalty for all but finitely many $Q \in C_2$.

- **Rational map:** Let $C$ be an algebraic curve. A rational map $\phi : C \to \mathbb{P}^n$ is given by

$$P \mapsto (f_0(P) : f_1(P) : \cdots : f_n(P))$$

where $f_0, f_1, \ldots, f_n \in K(C)$ are not all zero.

*Fact:* If $C$ is smooth, then $\phi$ is a morphism.

## 3. Weierstrass Equations

- **Elliptic curve:** An elliptic curve $E$ over $K$ is a smooth projective curve of genus 1 defined over $K$ with a specified $K$-rational point $O_E$.
- **Weierstrass form:** A Weierstrass equation, over a field $K$, is an equation of the form
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
with coefficients $a_1, a_2, a_3, a_4, a_6$ in $K$.
- **Weierstrass isomorphism:** Every elliptic curve $E$ is isomorphic over $K$ to a curve in Weierstrass form via an isomorphism, taking $O_E$ to $(0:1:0)$.
- If $D \in \mathrm{Div}(E)$ is defined over $K$ (i.e. fixed by $\mathrm{Gal}(\bar{K}/K)$, then $\mathcal{L}(D)$ has a basis in $K(E)$ (not just in $\bar{K}(E)$)
- **Points of inflection:** Let $C = \{F = 0\} \subset \mathbb{P}^2$ be algebraic curve. THe points of inflection are given by
$$\det\left(\frac{\partial^2 F}{\partial X_i \partial X_j}\right) = 0$$
(i.e. where the **Hessian determinant** of $F$ is zero)
- Let $E$ and $E'$ be elliptic curves over $K$ in Weierstrass form. Then $E \cong E'$ over $K$ iff the equations are related by a change of variables:
$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$
where $u, r, s, t \in K$, $u \neq 0$.
*Note:* This changes the discriminant by $u^{12}\Delta' = \Delta$.
- **Discriminant:** A Weierstrass equation for a curve $E$:
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
defines an elliptic curve if and only if the **discriminant** $\Delta(a_1, \ldots, a_6) \neq 0$ where $\Delta \in \mathbb{Z}[a_1, \ldots, a_6]$ is the polynomial
$$\begin{aligned} \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ \text{where} \quad b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$
If $\mathrm{char}K \neq 2, 3$, then can reduce to $E : y^2 = x^3 + ax + b$ defines elliptic curve, iff the **discriminant** $\Delta = -16(4a^3 + 27b^2)$ is non-zero, where
$$\begin{aligned} a &= -27c_4 \quad \text{where} \quad c_4 = b_2^2 - 24b_4 \\ b &= -54c_6 \quad \text{where} \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \end{aligned}$$
- If $\mathrm{char}K \neq 2, 3$, then $E : y^2 = x^3 + ax + b$ and $E : y^2 = x^3 + a'x + b'$ are isomorphic over $K$ iff there exists $u \in K^*$ s.t. $a' = u^4a$ and $b' = u^6b$.
- **$j$-invariant:** $j(E) = \dfrac{1728(4a^3)}{4a^3 + 27b^2}$
$E \cong E' \implies j(E) = j(E')$ and converse holds if $K = \bar{K}$

## 4. Group Law

- **Group law** Let $E$ be elliptic curve with specified point $O_K \in E(K)$. Set of points on $E$ form an *abelian group* $(E, \oplus)$.
  - Identity is specified point $O_E$
  - Group operation $P \oplus Q$ is as follows:
    - Let $S$ be 3rd point of intersection of line $PQ$ and curve $E$ (if $P = Q$, then let $S$ be intersection between $T_pE$ (tangent line at $P$) and $E$)
    - Let $R$ be 3rd point of intersection fo line $O_ES$ and curve $E$.
    - Then $P \oplus Q = R$
  - Inverse of $P$:
    - Let $S$ be 3rd point of intersection of the tangent line at $O_E$ with the curve $E$.
    - Let $Q$ be 3rd point of intersection of line $PS$ and $E$.
    - Then $P \oplus Q = O_E$
- **Linearly equivalent** $D_1, D_2 \in \mathrm{Div}(E)$ are linearly equivalent if $\exists f \in \bar{K}(E)^*$ s.t. $\mathrm{div}(f) = D_1 - D_2$. (written $D_1 \sim D_2$).
- **Picard group**: $\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim$

  $\mathrm{Div}^0(E)$ is the degree 0 divisors (i.e. $\mathrm{Div}^0(E) = \ker(\mathrm{Div}(E) \to \mathbb{Z})$)

  $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\sim$
- Let $\phi : E \to \mathrm{Pic}^0(E)$ be given by $P \mapsto [P - O_E]$. Then $\phi(P \oplus Q) = \phi(P) + \phi(Q)$ and $\phi$ is a bijection.

  *Remark:* $\phi$ identifies $(E, \oplus)$ with $(\mathrm{Pic}^0(E), +)$ which proves associaitvity!
- **Explicit formula:** Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $E$.
  - **Inverse:** The inverse of $P_1$ is $\ominus P_1 = (x_1, -(a_1x_1 + a_3 + y_1))$.
  - **Sum:**
    - **Case I:** $x_1 = x_2, y_1 \neq y_2$**:** $P_1 \oplus P_2 = O_E$.
    - **Case II:** $x_1 \neq x_2$**:** $P_1 \oplus P_2 = (x_3, y_3)$ where

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

      where

      $$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{and} \quad \nu = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}$$
    - **Case III:** $x_1 = x_2$**,** $y_1 = y_2$**:** So $P_1 = P_2$, where we instead use the tangent slope

      $$\lambda = \frac{3x_1^2 + 3a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \quad \text{and} \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$
- **Explicit formula** for the case $y^2 = x^3 + ax + b$:
  - **Inverse:** The inverse of $P_1$ is $\ominus P_1 = (x_1, -y_1)$

- **Sum:**
  - If $x_1 \neq x_2$, then $P_1 \oplus P_2 = (x_2, y_2)$ where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right) - x_1 - x_2$$
$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \left(\frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}\right)$$

  - If $x_1 = x_2$ and $y_1 = y_2$, Then $2P_1 = (x_3, y_3)$ where

$$x_3 = \frac{x^4 - 2ax^2 - 8bx + a^2}{(2y)^2} = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x$$
$$y_3 = \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{(2y)^3} = -\left(\frac{3x^2 + a}{2y}\right)(x_3 - x_1) - y_1$$

- $E(K)$ is an abelian group.
- Elliptic curves are **group varieties**. I.e. The inverse map $[-1] : E \to E$ given by $P \mapsto -P$ and the addition map $A : E \times E \to E$ given by $(P, Q) \mapsto P + Q$ are both morphisms of algebraic varieties.
- **$n$-torsion** Define $[n] : E \to E$ as the $n$-torsion map given by

$$P \mapsto P + P + \cdots + P \quad n \text{ times} \quad \text{for } n > 0.$$

  The **$n$-torsion subgroup** of $E$ is

$$E[n] = \ker([n] : E \to E) = \{P \in E : P + P + \ldots P = 0 \quad n \text{ times }\}$$

  E.g. If $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$, then $E[2] = \{O_E, (e_1, 0), (e_2, 0), (e_3, 0)\}$
- **3-torsion:** If $0 \neq P = (x, y) \in E(K)$, then

$$3P = O_E \iff 3x^4 + 6ax^2 + 12bx - a^2 = 0$$

## Elliptic curves over $\mathbb{C}$

- **Lattice:** Let $w_1, w_2$ be basis for $\mathbb{C}$ as $\mathbb{R}$ vector space. Then a lattice $\Lambda$ can be given as $\Lambda = \{aw_1 + bw_2 : a, b \in \mathbb{Z}\}$.
- **Weierstrass p-function:** Let $\Lambda$ be a lattice. Then the **Weierstrass p-function** is:

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

  This satisfies $\wp'(z)^2 = 4\wp(z) - g_2\wp(z) - g_3$ where $g_2$, $g_3 \in \mathbb{C}$ depend on the lattice:

  $$g_2 = 60 \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^4} \quad \text{and} \quad g_3 = 140 \sum_{0 \neq \lambda \in \Lambda} \frac{1}{\lambda^6}$$

  *Fact:* $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ where $E$ is the elliptic curve $y^2 = 4x^3 - g_2x - g_3$. This is isomorphic both as Riemann surfaces and abelian groups.
- **Uniformisation theorem:** Every elliptic curve over $\mathbb{C}$ is isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda$.

## Summary of results:

- For $K = \mathbb{C}$, then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ (isomorphic to complex torus)
- For $K = \mathbb{R}$, then

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

- For $K = \mathbb{F}_q$, then $E(\mathbb{F}_q)$ is *approximately* $q + 1$. We have Hasse's Theorem:

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

- For **local fields**, $[K : \mathbb{Q}_p] < \infty$, let $\mathcal{O}_K$ be the ring of integers. Then $E(K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

  E.g. If $K = \mathbb{Q}_p$, then $E(K)$ contains subgroup of finite index isomorphic to $(\mathbb{Z}_p, +)$. Note that $(\mathbb{Z}_p, +)$ is **not** finitely generated (contains all rationals without $p$ in denominator), so $E(K)$ is not finitely generated.
- For **number fields** $[K : \mathbb{Q}] < \infty$, we have that $E(K)$ is a **finitely generated abelian group** (Mordell-Weil Theorem)

## 5. Isogenies

- **Isogeny** Let $E_1, E_2$ be elliptic curves. An **isogeny** $\phi : E_1 \to E_2$ is a nonconstant morphism with $\phi(O_{E_1}) = O_{E_2}$. We say $E_1$ and $E_2$ are **isogenous**.
- Every morphism $\phi : C_1 \to C_2$ of curves is either *constant* or *surjective.*

  *Fact:* Two elliptic curves $E_1$ and $E_2$ are isogenuous over $\mathbb{F}_q$ if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.
- $\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\} \cup \{0\}$. This is a *group* under $(\phi + \psi)(P) = \phi(P) + \psi(P)$

  If $\phi : E_1 \to E_2$ is isogeny and $\psi : E_2 \to E_3$ is isogeny, then $\psi\phi$ is isogeny.
- Let $n \in \mathbb{Z}$ with $n \neq 0$. Then $[n] : E \to E$ is an isogeny.

  *Corollary:* $\mathrm{Hom}(E_1, E_2)$ is torision-free as a $\mathbb{Z}$-module.
- (**homomorphisms**): Let $\phi : E_1 \to E_2$ be isogeny. Then $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$.
- **Degree 2 isogeny:** Let $E, E'$ be two elliptic curves over $K$, defined by

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

  where $a, b \in K$ such that $b(a^2 - 4b) \neq 0$, and where $a' = -2a$ and $b' = a^2 - 4b$.

  Then, there is a degree 2 isogeny $\phi : E \to E'$ where

  $$(x, y) \mapsto \left( \left(\frac{y}{x}\right)^2 : \frac{y(x^2 - b)}{x^2} : 1 \right) \quad \text{and} \quad \phi(O_E) = O_{E'}$$
- Let $\phi : E_1 \to E_2$ be an isogeny. Then there exists a morphism $\xi : \mathbb{P}^1 \to \mathbb{P}^1$ making the following diagram commute:

  $$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "x_1"] & E_2 \arrow[d, "x_2"] \\ \mathbb{P}^1 \arrow[r, "\xi"] & \mathbb{P}^1 \end{tikzcd}$$

  where $x_i$ denote the $x$-coordinates on a Weierstrass equation for $E_i$.

  Moreover, if $\xi(t) = \frac{r(t)}{s(t)}$ where $r, s \in K[t]$ coprime, then $\deg(\phi) = \deg(\xi) = \max(\deg(r), \deg(s))$.
- $\deg[2] = 4$.
- **Quadratic form** Let $A$ abelian group. $q : A \to \mathbb{Z}$ is a **quadratic form** if
  - $q(nx) = n^2 q(x)$ for all $n \in \mathbb{Z}$, $x \in A$
  - $(x, y) \mapsto q(x + y) - q(x) - q(y)$ is $\mathbb{Z}$-bilinear.

  A map $q : A \to \mathbb{Z}$ is a quadratic form iff it satisfies the parallelogram law: $q(x + y) + q(x - y) = 2q(x) + 2q(y)$ for all $x, y \in A$.
- $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form.

- Let $P, Q \in E$, and let $P, Q, P+Q, P-Q \neq 0$, and let $x_1, x_2, x_3, x_4$ be the $x$-coordinates of these 4 points respectively. Then, 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 of degree $\leq 2$ in $x_2$ such that

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

  These polynomials can explicitly be given as

$$\begin{aligned} W_0 &= (x_1 - x_2)^2 \\ W_1 &= 2(x_1x_2 + a)(x_1 + x_2) + 4b \\ W_2 &= x_1^2x_2^2 - 2ax_1x_2 - 4b(x_1 + x_2) + a^2 \end{aligned}$$

- *Corollary:* $\deg(n\phi) = n^2\deg(\phi)$. In particular, $\deg[n] = n^2$.

## 6. Invariant differential

- **Invariant differential** Let $C$ algebraic curve. The **space of differentials** $\Omega_C$ is the $K(C)$-vector space generated by $df$ for $f \in K(C)$ subject to the relations
  - $d(f+g) = df + dg$
  - $d(fg) = fd(g) + gd(f)$
  - $da = 0$ for all $a \in K$

  Fact: $\Omega_C$ is 1-dimensional $K(C)$ vector space (for *curves* $C$)

  (In general, if $V$ is an algebraic variety of dimension $d$, then $\Omega_V$ is $d$-dimensional $K(V)$ vector space)

- **Order of differential:** Let $0 \neq w \in \Omega_C$. Let $P \in C$ be a smooth point and $t \in K(C)$ be a uniformiser at $P$. Then $w = fdt$ for some $f \in K(C)^*$.

  We define
  $$\text{ord}_P(w) := \text{ord}_P(f)$$
  which is independent of choice of uniformiser $t$.

- Let $f \in K(C)^*$ such that $\text{ord}_P(f) = n \neq 0$. If $\text{char}(K) \not| n$, then $\text{ord}_p(df) = n-1$.

- Let $C$ be smooth projective curve, and let $0 \neq w \in \Omega_C$ Then $\text{ord}_p(w) = 0$ for all but finitely many $P \in C$.

- **Divisor of differential:** Let $C$ be smooth projective curve, and let $0 \neq w \in \Omega_C$. We define the divisor of $w$:
  $$\text{div}(w) := \sum_{P \in C} \text{ord}_P(w) P \in \text{Div}(C)$$

- **Genus:** Define the genus as
  $$g(C) := \dim_K \{w \in \Omega_C : \text{div}(w) \geq 0\}$$

  The set $\{w \in \Omega_C : \text{div}(w) \geq 0\}$ is the **space of regular differentials**

  Riemann-Roch states that: If $0 \neq w \in \Omega_C$, then $\deg(\text{div}(w)) = 2g(C) - 2$.

- Assume $\text{char}(K) \neq 2$. Given elliptic curve $E : y^2 = f(x)$. THen $w = \frac{dx}{y}$ is a differential on $E$ with no zeros/poles. (i.e. $\text{ord}_P(w) = 0$ for all $P \in E$)

  In particular, the $K$-vector space of regular differentials on $E$ is spanned by $w$. $w$ is called the invariant differential.

- **Pullback differential:** Let $\phi : C_1 \to C_2$ be nonconstant morphism. Then $\phi^* : \Omega_{C_1} \to \Omega_{C_2}$ is given by
  $$fdg \mapsto (\phi^* f)\, d(\phi^* g) \qquad \text{(recall } \phi^*(f) = f \circ \phi)$$

- Let $P \in E$. Let $\tau_P : E \to E$ be the translation map given by $X \mapsto P + X$. Then if $w = \frac{dx}{y}$, then
  $$\tau_p^* w = w$$
  Thus, $w$ is called the **invariant differential**.

- Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, and let $w$ be invariant differential on $E_2$. Then

$$(\phi + \psi)^* w = \phi^* w + \psi^* w$$

- Let $\phi : C_1 \to C_2$ be a nonconstant morphism. Then

$$\phi \text{ separable} \quad \Longleftrightarrow \quad \phi^* : \Omega_{C_1} \to \Omega_{C_2} \text{ is non-zero}$$

- **N-torsion group:** If $\mathrm{char}(K) \not| n$, then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ (note: this is over algebraically closed field!)

  *Remark:* If $\mathrm{char}(K) = p$, then $[p]$ is inseperable. We have

$$E[p^r] \cong \begin{cases} \mathbb{Z}/p^r\mathbb{Z} & \text{for all } r \geq 1 \quad \text{(ordinary), or} \\ 0 & \text{for all } r \geq 1 \quad \text{(supersingular)} \end{cases}$$

# 7. Elliptic curves over finite fields

- Let $A$ be abelian group, and $q : A \to \mathbb{Z}$ a positive definite quadratic form. If $x, y \in A$, then
$$|q(x+y) - q(x) - q(y)| \leq 2\sqrt{q(x)q(y)}$$
- Let $\mathbb{F}_q$ be the unique finite field with $q$ elements, where $q = p^m$ for some prime $p$. THe extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is always *Galois*.

  $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is *cyclic* of order $r$, generated by the **Frobenius** map $x \mapsto x^q$.
- **Hasse's theorem** Let $E/\mathbb{F}_q$ be elliptic curve. Then
$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$$
  *Note:* $\#E(\mathbb{F}_q) = \#\ker(1-\phi) = \deg(1-\phi)$ where $\phi(x,y) = (x^q, y^q)$ is *Frobenius* map. (since $1 - \phi$ is separable)
- **Zeta functions**: For $k$ a number field
$$\zeta_K(s) = \sum_{\mathfrak{a} \in \mathcal{O}_K} \frac{1}{(N\mathfrak{a})^s} = \prod_{\mathfrak{p} \in \mathcal{O}_K} \left(1 - \frac{1}{(N\mathfrak{p})^s}\right)^{-1}$$
  where $N\mathfrak{a}$ is the norm of the ideal $\mathfrak{a}$.

  For $K$ a function field (i.e. $K = \mathbb{F}_q(C)$ where $C/\mathbb{F}_q$ a smooth projective curve)
$$\zeta_k(s) = \prod_{x \in |C|} \left(1 - \frac{1}{(Nx)^s}\right)^{-1}$$
  where $|C|$ is the closed points of $C$ (orbits for action $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ on $C(\bar{\mathbb{F}}_q)$. and $Nx = q^{\deg(x)}$ where $\deg(x)$ is the size of the orbit.

  We have that $\zeta_K(s) = F(q^{-s})$ for some $F \in \mathbb{Q}[[T]]$, where
$$F(T) = \prod_{x \in |C|} \left(1 - T^{\deg(x)}\right)^{-1} = \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n\right)$$
- **Zeta function of variety**: The zeta function of a variety $V$ is
$$Z_V(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#V(\mathbb{F}_{q^n})}{n} T^n\right)$$
  Let $E/\mathbb{F}_q$ elliptic curve, with $\#E(\mathbb{F}_q) = q + 1 - a$. Then
$$Z_E(T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$
- Let $\#E(\mathbb{F}_q) = q + 1 - a$. Then
$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - \alpha^n - \beta^n$$
  where $\alpha, \beta \in \mathbb{C}$ are roots of $X^2 - aX + q = 0$.

  If $\#E(\mathbb{F}_q) = q + 1 - a$, then
$$\begin{aligned}
&\#E(\mathbb{F}_{q^2}) = (q+1-a)(q+1+a), \\
&\#E(\mathbb{F}_{q^3}) = q^3 + 3aq - a^3 + 1 = (q+1-a)(1+a+a^2-q+aq+q^2), \\
&\#E(\mathbb{F}_{q^4}) = -a^4 + 4a^2q + (q^2-1)^2 = (q+1-a)(q+1+a)(1+a^2-2q+q^2)
\end{aligned}$$

- **Trace:** Define $\mathrm{tr} : \mathrm{End}(E) \to \mathbb{Z}$ given by

$$\phi \mapsto \langle \phi, 1 \rangle = \deg(\phi + 1) - \deg(\phi) - 1$$

  E.g. If $\phi : E \to E$ is $q$-power Frobenius, then $\mathrm{tr}(\phi) = \#E(\mathbb{F}_q) - q - 1$.

  *Fact:* For any $\phi \in \mathrm{End}(E)$, we have $\phi^2 - [\mathrm{tr}\phi]\phi + [\deg\phi] = 0$

- Let $\phi \in \mathrm{End}(E)$ with $n \in \mathbb{Z}$. Then $\mathrm{tr}(\phi) = 2n$ and $\deg(\phi) = n^2$ if and only if $\phi = [n]$.

# 8. Formal groups

- ***I*-adic topology** Let $R$ ring, $I \subset R$ an ideal. The **$I$-adic topology** is the topology on $R$ with basis $\{r + I^n : r \in R, n \geq 1\}$.
- **Cauchy** A sequence $(x_n)$ in $R$ is Cauchy if $\forall k$, $\exists N$ s.t. $\forall m, n \geq N$, $x_m - x_n \in I^k$.
- **Complete**: $R$ is **complete** if
  - $\bigcap_{n \geq 0} I^n = \{0\}$
  - Every Cauchy sequence converges

  Note: If $x \in I$, then $1 - x$ is unit

  *Examples:*

  - The $p$-adic integers $\mathbb{Z}_p$ is completion of $\mathbb{Z}$ w.r.t the ideal $p\mathbb{Z}$.
  - The power series in $t$, $\mathbb{Z}[[t]]$ is completion of $\mathbb{Z}[t]$ w.r.t the ideal $(t)$.
- **Hensel's Lemma:** Let $R$ be integral domain, and complete w.r.t ideal $I \subset R$. Let $F \in R[X]$ and $s \geq 1$.

  Supose $a \in R$ satisifes

  - $F(a) \equiv 0 \pmod{I^s}$
  - $F'(a) \in R^*$

  Then, there exists a unique $b \in R$ s.t.

  - $F(b) = 0$
  - $b \equiv a \pmod{I^s}$

  *Setup:* Consider the elliptic curve $E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. Usually we take affine piece where $Z \neq 0$, **but intead** we now take affine piece where $Y \neq 0$. Let $t = -X/Y$ and $w = -Z/Y$. Define

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

  Thus $E : w = f(t, w)$

  Applying Hensel's Lemma with $R = \mathbb{Z}[a_1, \ldots, a_6][[t]]$, $I = (t)$, and $F(X) = X - f(t, X)$ with $s = 3$, $a = 0$, we get there exists a unique $w(t) \in \mathbb{Z}[a_1, \ldots, a_6][[t]]$ such that

  - $w(t) = f(t, w(t))$, and
  - $w(t) \equiv 0 \pmod{t^3}$

  The function $w(t)$ can be given as $w(t) = \lim_{n \to \infty} w_n(t)$ where

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

The approximations are:

$$
\begin{aligned}
w_0(t) &= 0 \\
w_1(t) &= t^3 \\
w_2(t) &= t^3(1 + a_1t + a_2t^2 + a_3t^3 + a_4t^4 + a_6t^6) \\
w_3(t) &= t^3(1 + a_1t + (a_1^2 + a_2)t^2 + (2a_1a_2 + a_3)t^3 + (a_2^2 + 3a_1a_3 + a_4)t^4 + \dots) \\
&\ \ \vdots \\
w(t) &= t^3(1 + A_1t + A_2t^2 + A_3t^3 + \dots) = \sum_{n=2}^{\infty} A_{n-2}t^{n+1}
\end{aligned}
$$

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

- Let $R$ be integral domain, complete w.r.t. ideal $I$, and $a_1, \dots, a_6 \in R$, and $K = \mathrm{Frac}(R)$. THen $\hat{E}(I) = \{(t, w) \in E(K) : t, w \in I\}$ is a subgroup of $E(K)$.

  *Remark:* By uniqueness in Hensel's Lemma (using $s = 1$), we have

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

- By Hensel's lemma, there exists $i(t) \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ with $i(0) = 0$ such that

  $$[-1](t, w(t)) = (i(t), w(i(t)))$$

  where
  $$i(X) = -X - a_1X^2 - a_2X^3 - (a_1^3 + a_3)X^4 + \dots$$

  Also by Hensel's lemma, there exists $F(t_1, t_2) \in \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$ with $F(0, 0) = 0$ such that
  $$(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2)))$$

  where

  $$
  \begin{aligned}
  F(X, Y) = X + Y - a_1XY &- a_2(X^2Y + XY^2) \\
  &+ (2a_3X^3Y + (a_1a_2 - 3a_3)X^2Y^2 + 2a_3XY^3) + \dots
  \end{aligned}
  $$

- **Formal group:** Let $R$ be a ring. A formal group over $R$ is a power series $F(X, Y) \in R[[X, Y]]$ satisfying:

  1. $F(X, Y) = F(Y, X)$
  2. $F(X, 0) = X$ and $F(0, Y) = Y$. (one implies the other)
  3. $F(F(X, Y), Z) = F(X, F(Y, Z))$

  Furthermore, one automatically gets that there exists a unique $i(T) = -T + \cdots \in R[[T]]$ such that $F(T, i(T)) = 0$.

  *Construction of inverse:* We define a sequence of power series $(g_n(T))_{n=1}^{\infty}$. Let $g_1(T) = -T$. For $n \geq 2$, set

  $$g_n(T) = g_{n-1}(T) - bT^n \quad \text{where } b \text{ is such that } F(T, g_{n-1}(T)) = -bT^n \pmod{T^{n+1}}$$

  Then take the limit $g(T) = \lim_{n\to\infty} g_n(T)$. The **inverse** is $i(T) = g(T)$

  *Examples:*

- **Additive formal group:** $\hat{\mathbb{G}}_a$. Power series is $F(X,Y) = X + Y$ (with inverse $i(X) = -X$)
- **Multiplicative formal group:** $\hat{\mathbb{G}}_m$. Power series is $F(X,Y) = X + Y + XY$ (with inverse $i(X) = -X(1 - X + X^2 - X^3 + X^4 - X^5 + \dots))$
- $F(X,Y) = \frac{X+Y}{1-XY} = X + Y + (XY^2 + X^2Y) + (X^2Y^3 + Y^3X^2) + \dots$
- **Sum on $\hat{E}(I)$:** $F(X,Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + (2a_3X^3Y + (a_1a_2 - 3a_3)X^2Y^2 + 2a_3XY^3) + \dots$

- **Morphism of formal groups:** Let $\mathcal{F}$ and $\mathcal{G}$ be formal groups over $R$ given by power series $F$ and $G$.

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

- Let $R$ be ring with $\mathrm{char}(R) = 0$. Then every formal group $\mathcal{F}$ over $R$ is isomorphic to $\hat{G}_a$ over $R \otimes \mathbb{Q}$ (i.e. $R$ with denominators)

  More precisely

  - There is unique power series
  $$\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots$$
  with $a_i \in R$ such that $\log(F(X,Y)) = \log(X) + \log(Y)$.
  - There is 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 $\exp(\log(T)) = \log(\exp(T)) = T$.

  *Note:* Let $F_1(X,Y) = \frac{\partial F}{\partial X}(X,Y)$. Define log by using
  $$p(T) = F_1(0,T)^{-1} = 1 + a_2T + a_3T^2 + a_4T^3 + \dots$$

- **Multiplicative Inverse:** Let $f \in R[[T]]$ be given as
  $$f = \sum_{n=0}^{\infty} a_nT^n$$
  Then $f$ has a multiplicative inverse $g$ in $R[[T]]$ ($fg = 1$) if and only if $a_0$ is a unit in $R$. If so, then $g$ is
  $$g = \sum_{n=0}^{\infty} b_nT^n \qquad \text{where} \quad b_0 = \frac{1}{a_0} \quad \text{and} \quad b_n = -\frac{1}{a_0}\sum_{i=1}^{n} a_ib_{n-i} \quad \text{for } n \geq 1$$

- **Composition Inverse:** Let $f = aT + \cdots \in R[[T]]$ with $a \in R^\times$. THen there exists unique $g = a^{-1}T + \cdots \in R[[T]]$ such that $f(g(t)) = g(f(T)) = T$ (i.e. power series has inverse)

  *Construction:* Let $g_1(T) = a^{-1}T$. Set

  $$g_n(T) = g_{n-1}(T) - \frac{b}{a}T^n \quad \text{where } b \text{ is such that } \; f(g_{n-1}(T)) = T + bT^n \pmod{T^{n+1}}$$

  Then take the limit $g(T) = \lim_{n\to\infty} g_n(T)$.

- **Ideal into group:** Let $R$ be ring complete w.r.t. ideal $I$. Let $\mathcal{F}$ be a formal group given by $F \in R[[X,Y]]$. For $x, y \in I$, define

  $$x \oplus_{\mathcal{F}} y = F(x,y) \in I$$

  This turns $I$ into a group!. $\mathcal{F}(I) := (I, \oplus_{\mathcal{F}})$ is an **abelian group**.

  *Examples:*

  - **Additive group:** $\hat{\mathbb{G}}_a(I) = (I, +)$.
  - **Multiplicative group:** $\hat{\mathbb{G}}_m(I) = (1 + I, \times)$.

- **Multiplication-by-$m$:** Let $\mathcal{F}$ be a formal group with power series $F \in R[[X,Y]]$. For any $n \in \mathbb{Z}$, we define the map $[n]$ recursively as:

  $$[0](T) = 0, \quad \text{and} \quad [n](T) = F([n-1]T, T)$$

- Let $\mathcal{F}$ be a formal group over $R$ and $n \in \mathbb{Z}$. Suppose $n \in R^\times$ (where $n = 1 + 1 + \ldots 1$ $n$ times). Then

  - $[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.
  - IF $R$ complete w.r.t. ideal $I$, then $[n] : \mathcal{F}(I) \to \mathcal{F}(I)$ is an isomorphism. In particularm $\mathcal{F}(I)$ has no $n$-torsion.

## 9. Elliptic Curves over Local Fields

*Setup:* $K$ is field, complete w.r.t. discrete valuation $v : K^\times \to \mathbb{Z}$.
Valuation ring is $\mathcal{O}_K = \{x \in K^\times : v(x) \geq 0\} \cup \{0\}$.
The unit group $\mathcal{O}_K^\times = \{x \in K^\times : v(x) = 0\}$
Maximal ideal is $\pi\mathcal{O}_K$, where $\pi \in K$ is chosen such that $v(\pi) = 1$.
Residue field is $k = \mathcal{O}_K/\pi\mathcal{O}_K$.
*Example:* $K = \mathbb{Q}_p,\ \mathcal{O}_K = \mathbb{Z}_p,\ \pi\mathcal{O}_K = p\mathbb{Z}_p,\ k = \mathbb{F}_p$

- **Integral:** A Weierstrass equation for $E$ with coefficients $a_1, \ldots, a_6 \in K$ is **integral** if $a_1, \ldots a_6 \in \mathcal{O}_k$.

  *Note:* Substituting $a_i = u^i a_i'$ proves that integral Weierstrass equations always exist for any EC.

- **Minimal:** Let $\Delta$ be discriminant of elliptic curve. Equation is minimal if $v(\Delta)$ minimal among all integral Weierstrass equations for $E$

  *Fact:* If $E$ integral then $\Delta \in \mathcal{O}_k$ and thus $v(\Delta) \geq 0$. Thus, by well-ordering, minimal Weierstrass equations always exist. If $\mathrm{char}(k) \neq 2, 3$ then there exist minimal Weierstrass equations of the form $y^2 = x^3 + ax + b$.

  *Fact:* If $\mathrm{char}(k) \neq 2, 3$, then $y^2 = x^3 + ax + b$ is minimal if and only if $v_p(a) < 4$ or $v_p(b) < 6$.

- Let $E/K$ have integral Weierstrass equation: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Let $0 \neq P \in E(K)$, say $P = (x, y)$. Then either $x, y \in \mathcal{O}_K$, or $v(x) = -2s$ and $v(y) = -3s$ for some $s \geq 1$

  We define:

  $$\begin{aligned} E_r(K) := \hat{E}(\pi^r\mathcal{O}_K) &= \{(t, w) \in E(K) : t, w \in \pi^r\mathcal{O}_K\} \\ &= \{(x, y) \in E(K) : v(x) \leq -2r \text{ and } v(y) \leq -3r\} \cup \{0\} \end{aligned}$$

  Obtain a sequence of subgroups:

  $$\cdots \subset E_4(K) \subset E_3(K) \subset E_2(K) \subset E_1(K)$$

  More generally, for any formal group $\mathcal{F}$ over $\mathcal{O}_K$:

  $$\cdots \subset \mathcal{F}(\pi^4\mathcal{O}_K) \subset \mathcal{F}(\pi^3\mathcal{O}_K) \subset \mathcal{F}(\pi^2\mathcal{O}_K) \subset \mathcal{F}(\pi\mathcal{O}_K)$$

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

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

  is an *isomorphism* with inverse $\exp : \hat{\mathbb{G}}_a(\pi^r\mathcal{O}_K) \to \mathcal{F}(\pi^r\mathcal{O}_K)$ .

- For $r \geq 1$,

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

  If $|k| < \infty$, then $\mathcal{F}(\pi\mathcal{O}_K)$ contains a subgroup of finite index $\cong (\mathcal{O}_K, +)$

- **Reduction mod $\pi$:** Reduction mod $\pi$ is the natural quotient map $\mathcal{O}_k \to \mathcal{O}_K/\pi\mathcal{O}_K = k$ given by $x \mapsto \tilde{x}$

- **Reduction of curve:** The **reduction** $\tilde{E}/k$ of $E/k$ is defined to be the reduction of a minimal Weierstrass equation. Let $E/K$ have minimal Weierstrass equation

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

We then reduce each coefficient modulo $\pi$ to obtain a (possibly singular) curve over $k$:

$$\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$$

- Let $E/K$ elliptic curve. The reduction mod $\pi$, of two minimal Weierstrass equations for $E$ define *isomorphic* curves over $k$.

  $E$ has **good reduction** if $\tilde{E}$ is non-singular (and thus elliptic curve), otherwise has **bad reduction**.

  *Fact:* $E$ has good reduction at $p$ if and only if $v(\Delta) = 0$ for minimal $v(\Delta)$.

- Let $E/K$ be an elliptic curve with integral Weierstrass equation. Let discriminant tbe $\Delta$. Then

$$\begin{aligned} v(\Delta) = 0 &\quad\Longrightarrow\quad \textbf{good}\text{ reduction} \\ 0 < v(\Delta) < 12 &\quad\Longrightarrow\quad \textbf{bad}\text{ reduction} \\ v(\Delta) \geq 12 &\quad\Longrightarrow\quad \text{equation may not be minimal} \end{aligned}$$

  If $\Gamma k \neq 2, 3$, ...

- **Reduction map:** Let $E/K$ be elliptic curve over $K$. Let $P \in E$ with homogenous projective coordinates $P = (x : y : z) \in \mathbb{P}^2(K)$. Choose representative such that $\min(v(x), v(y), v(z)) = 0$ (i.e. all $x, y, z \in \mathcal{O}_K$ and $\gcd(x, y, z) = 1$).

  Then we define the reduction map

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

  Restricting the above map to the curve $E(K)$ gives

$$\begin{aligned} E(K) &\longrightarrow \tilde{E}(k) \\ P &\mapsto \tilde{P} \end{aligned}$$

- Let $E(K)$ be given by minimal Weierstrass equation. Then if $P = (x, y) \in E(K)$, then
  - If $x, y \in \mathcal{O}_K$, then $\tilde{P} = (\tilde{x}, \tilde{y})$.
  - Otherwise, $\tilde{P} = (0 : 1 : 0) = O_E$.

- Let $E/k$ elliptic curve. We define

$$\tilde{E}_{\text{ns}} = \begin{cases} \tilde{E} & \text{if } E \text{ has good reduction} \\ \tilde{E}\backslash\{\text{singular point}\} & \text{if } E \text{ has bad reduction} \end{cases}$$

  $\tilde{E}_{\text{ns}}$ is a group.

  If bad reduction, then $\tilde{E}_{\text{ns}}$ is isomorphic to either $\mathbb{G}_a$ (if cusp) or $\mathbb{G}_m$ (if node).

- Define $E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\}$ (i.e. all points on $E(K)$ which don't get reduced to the singular point. Good reduction implies $E_0(K) = E(K)$)
- $E_0(K)$ is a subgroup of $E(K)$ and reduction mod $\pi$ is a surjective group homomorphism $E_0(K) \longrightarrow \tilde{E}_{\mathrm{ns}}(k)$
- We have the following **filtration**:

$$\begin{array}{ccccccccccccc}
 & & & & \hat{E}(\pi^3\mathcal{O}_K) & & \hat{E}(\pi^2\mathcal{O}_K) & & \hat{E}(\pi\mathcal{O}_K) & & & & \\
 & & & & \| & & \| & & \| & & & & \\
E_r(K) & \subset & \dots & \subset & E_3(K) & \subset & E_2(K) & \subset & E_1(K) & \subset & E_0(K) & \subset & E(K) \\
 & & & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow & \\
 & & & (k,+) & & (k,+) & & (k,+) & & \hat{E}_{\mathrm{ns}}(k) & & c_K(E) &
\end{array}$$

- If $|k| < \infty$, then $\mathbb{P}^n(k)$ is compact (w.r.t $\pi$-adic topology)
- If $|k| < \infty$, then $E_0(k) \subset E(K)$ has finite index.
- **Tamagawa number:** Define the **Tamagawa** number $c_K(E) = [E(K) : E_0(K)] < \infty$. Note that good reduction implies $c_K(E) = 1$.

  *Fact:* $c_k(E) = v(\Delta)$ or $c_k(E) \leq 4$.
- If $[K : \mathbb{Q}_p] < \infty$, then $E(k)$ contains a subgroup $E_r(K)$ of finite index with $E_r(K) \cong (\mathcal{O}_k, +)$

  *Corollary:* $E(K)_{\text{torsion}}$ injects into $\dfrac{E(K)}{E_r(K)}$ and therefore $E(K)_{\text{torsion}}$ is finite!.

- **Unramified extension:** Let $[K : \mathbb{Q}_p] < \infty$ be local field, and let $L/K$ be a finite extension. Let $L$ and $K$ have residue fields $\ell$ and $k$. Let $f$ be the residue degree $f = [\ell : k]$, and let $[L : K] = ef$.

  $L/K$ is **unramified** if $e = 1$ (i.e. $[L : K] = [\ell : k]$ and $\mathrm{Gal}(L/K) = \mathrm{Gal}(\ell/k)$)

$$\begin{array}{ccc}
K & \xrightarrow{V_K} & \mathbb{Z} \\
\cap & & \downarrow{\scriptstyle \times e} \\
L & \xrightarrow{V_L} & \mathbb{Z}
\end{array}$$

- For each integer $m \geq 1$
  - $k$ has unique extension of degree $m$ (say $k_m$)
  - $K$ has unique unramified extension of degree m (say $K_m$)

  *Note:* Can be found by adjoining the $(p^m - 1)$-th roots of unity to $\mathbb{Q}_p$
- **Maximal unramified extension:** $K^{\text{ur}} = \bigcup_{m \geq 1} K_m$ (inside $\bar{K}$)

  *Notation:* Let $P \in E(K)$. Then $[n]^{-1}P = \{Q \in E(\bar{K}) : nQ = P\}$. We define the field extension $K(\{P_1, \dots, P_2\}) = K(x_1, \dots, x_r, y_1, \dots, y_r)$ where $P_i = (x_i, y_i)$.
- Let $[K : \mathbb{Q}_p] < \infty$, $E/K$ elliptic curve with good reduction, and $p \not| n$. If $P \in E(K)$ then $K([n]^{-1}P)/K$ is unramified.

## 10. Elliptic Curves over Number Fields (Torsion Subgroup)

*Notation:* $K$ is number field, $[K:\mathbb{Q}] < \infty$. $E/K$ is elliptic curve.
$\mathfrak{p}$ is a prime of $K$ (i.e. of $\mathcal{O}_K$). $K_\mathfrak{p}$ is the $p$-**adic completion** of $K$.
$k_\mathfrak{p}$ is the residue field $\mathcal{O}_K/\mathfrak{p}$
*Example:* $K = \mathbb{Q}$, $\mathcal{O}_K = \mathbb{Z}$, $\mathfrak{p} = p\mathbb{Z}$, $K_\mathfrak{p} = \mathbb{Q}_p$, $k_\mathfrak{p} = \mathbb{F}_p \sim \mathbb{Z}/p\mathbb{Z}$.

- **Good reduction:** $\mathfrak{p}$ is a prime of good reduction for $E/K$, if $E/K_\mathfrak{p}$ has good reduction.
- $E/K$ has only finitely many primes of bad reduction. Indeed, any primes of bad reduction must divide $\Delta$.

  *Remark:* If $K$ has class number 1 (e.g. $K = \mathbb{Q}$), then can always find Weierstrass equation for $E$ with $a_1, \dots, a_6 \in \mathcal{O}_K$ minimal at all primes $\mathfrak{p}$.
- $E(K)_{\text{torsion}}$ is finite.
- Let $p$ be a prime with good reduction, with $p \not| n$, THen reduction mod $p$ gives an injection $E(K)[n] \hookrightarrow \tilde{E}(k_P)[n]$
- Let $E/\mathbb{Q}$ be elliptic curve. Let $p$ be a prime for which $E$ has *good* reduction (e.g. any $p \not| \Delta$ will have good reduction) We have

  $$\#E(\mathbb{Q})_{\text{tors}} \,|\, \#\tilde{E}(\mathbb{F}_p) \cdot p^a \quad \text{for some } a \geq 0$$

  Furthermore, if working in $K = \mathbb{Q}_p$, then $e = 1$, and thus

  $$\#E(\mathbb{Q})_{\text{tors}} \,|\, \#\tilde{E}(\mathbb{F}_p) \quad \text{if } p \text{ odd}$$
  $$\#E(\mathbb{Q})_{\text{tors}} \,|\, 2 \cdot \#\tilde{E}(\mathbb{F}_p) \quad \text{if } p = 2$$

- Let $E : y^2 = f(x)$ be an elliptic curve over $\mathbb{F}_p$. Let $\left(\frac{f(x)}{p}\right)$ be the Legendre symbol for $f(x)$ mod $p$. In other words

  $$\left(\frac{f(x)}{p}\right) = \begin{cases} 1 & \text{if } f(x) \text{ is a square mod } p \text{, and } p \not| f(x) \\ -1 & \text{if } f(x) \text{ is not a square mod } p \\ 0 & \text{if } p \text{ divides } f(x) \end{cases}$$

  Then we have
  $$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_P} \left( \left(\frac{f(x)}{p}\right) + 1 \right)$$

- Let $E/\mathbb{Q}$ be given by Weierstrass equation $a_1, \dots, a_6 \in \mathbb{Z}$. Suppose $0 \neq T = (x, y) \in E(\mathbb{Q})_{\text{tors}}$. THen
  - $4x, 8y \in \mathbb{Z}$
  - If $2|a_1$ or $2T \neq 0$, then $x, y \in \mathbb{Z}$
- **Nagell–Lutz** Let $E/\mathbb{Q}$ be given with equation $y^2 = x^3 + ax + b$ 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 $y^2 | (4a^3 + 27b^2)$
- **(Mazur):** Let $E/\mathbb{Q}$ elliptic curve. Then

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

  Furthermore, all 15 possibilities occur infinitely often over $\mathbb{Q}$.

## 11. Kummer theory

*Setup:* Fix $n > 1$. Let $K$ be field, char$K \nmid n$. Denote $\mu_n$ as the multiplicative group of $n$th roots of unity (in $K$). Assuming $\mu_n \subset K$

- Let $\Delta \subset K^\times/(K^\times)^n$ be a finite subgroup. Define $\sqrt[n]{\Delta} = \{\sqrt[n]{a} : a \in K^\times, a \cdot (K^\times)^n \in \Delta\}$ Let $L = K(\sqrt[n]{\Delta})$. Then $L/K$ is Galois and $\mathrm{Gal}(L/K) \cong \mathrm{Hom}(\Delta, \mu_n)$.

- **Kummer pairing:** Define the map $\langle\ ,\ \rangle : \mathrm{Gal}(L/K) \times \Delta \to \mu_n$ given by

$$(\sigma, x) \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$$

  *Fact:* This map is well-defined and bilinear.

- We have the two group isomorphisms:

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Hom}(\Delta, \mu_n) \qquad \sigma \mapsto (x \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}})$$
$$\Delta \longrightarrow \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \qquad x \mapsto (\sigma \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}})$$

- **Exponent:** Let $G$ be a finite group. the **exponent** of $G$ is the lowest common multiple of the orders of the elements of $G$. Note that the exponent divides $|G|$.

  *Fact:* $\mathrm{Gal}(K(\sqrt[n]{\Delta})/K)$ is an abelian group of exponent dividing $n$.

- There is a bijection

$$\left\{\begin{array}{l}\text{finite subgroups}\\ \Delta \subset K^\times/(K^\times)^n\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{finite abelian extensions}\\ L/K \text{ of exponent dividing } n\end{array}\right\}$$

$$\Delta \longmapsto K(\sqrt[n]{\Delta})$$
$$\frac{(L^*)^n \cap K^*}{(K^*)^n} \longleftarrow L$$

- Let $K$ number field, $\mu_n \subset K$. Let $S$ be a finite set of primes of $K$. There are only finitely many extensions $L/K$ such that
  - $L/K$ is abelian of exponent dividing $n$.
  - $L/K$ is unramified at all primes $\mathfrak{p} \notin S$

- Let

$$K(S, n) := \{x \in K^\times/(K^\times)^n : v_{\mathfrak{p}}(x) \equiv 0 \pmod{n}\ \forall \mathfrak{p} \notin S\}$$

  Then $K(S, n)$ is finite.

- If $K = \mathbb{Q}$, then

$$|\mathbb{Q}(S, 2)| = 2^{|S|+1}$$

## 12. Elliptic curves over number fields (Mordell-Weil)

- Let $E/K$ elliptic curve, with $L/K$ a finite Galois extension. Then the map

$$\frac{E(K)}{nE(K)} \longrightarrow \frac{E(L)}{nE(L)}$$

has finite kernel.

- **Weak Mordell Weil:** Let $K$ number field, $E/K$ elliptic curve. Let $n \geq 2$ integer. Then

$$\left|\frac{E(K)}{nE(K)}\right| < \infty$$

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

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

Specifically, fix an integer $n \geq 2$. Let $P_1, P_2, \ldots, P_m$ be set of coset representatives for $E(K)/nE(K)$. Then

$$\Sigma = \{P \in E(K) : \hat{h}(P) \leq \max_{1 \leq i \leq m} \hat{h}(P_i)\}$$

generates $E(K)$.

This proves $E(K) \cong E(K)_{\text{tors}} \times \mathbb{Z}^r$ where $r$ is the rank of the curve.

*(Curve with rank at least 28 are known. Conjectured that rank is unbounded. Conjectured that average rank is* $1/2$*, current upper bound is 1.5)*

## 13. Heights

- **Height of a point:** Let $K = \mathbb{Q}$. Let $P \in \mathbb{P}^n(\mathbb{Q})$ be $P = (a_0 : a_1 : \cdots : a_n)$ where $a_i \in \mathbb{Z}$ and $\gcd(a_0, a_1, \ldots, a_n) = 1$ The **height** of $P$ is

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

  *Height of rational:* Equivalently, if $x = \frac{u}{v} \in \mathbb{Q}$, with $u, v \in \mathbb{Z}$ coprime, then height of $x$ is $H(x) = \max(|u|, |v|)$

- Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be coprime homogenuous polynomials of degree $d$. Let $F : \mathbb{P}^1 \to \mathbb{P}^1$ be $(x_1 : x_2) \to (f_1(x_1, x_2), f_2(x_1, x_2))$ Then there exists $c_1, c_2 > 0$ s.t.

$$c_1 H(P)^d \le H(F(P)) \le c_2 H(P)^d \quad \text{for all } P \in \mathbb{P}^1(\mathbb{Q})$$

- **Logarithmic height:** The logarithmic height is a function $h : E(\mathbb{Q}) \to \mathbb{R}_{\ge 0}$ defined by $h(P) = \log(H(P))$ (and $h(O_E) = 0$).

- Let $E, E'$ be elliptic curves over $\mathbb{Q}$. Let $\phi : E \to E'$ be isogeny over $\mathbb{Q}$. There exists $c > 0$ such that

$$|h(\phi(P)) - \deg(\phi) h(P)| \le c \quad \text{for all } P \in E(\mathbb{Q})$$

  *Note:* $c$ depends on $E, E'$ and $\phi$, but **not** on $P$.

  *Example:* If $\phi = [2] : E \to E$, then there exists $c > 0$ such that

$$|h(2P) - 4h(P)| < c \quad \text{for all } P \in E(\mathbb{Q})$$

- **Canonical height:** For $P \in E(\mathbb{Q})$, we define

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

  This converges for all $P \in E(\mathbb{Q})$ and does not depend on Weierstrass equation.

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

- For any $B > 0$

$$\#\{P \in E(\mathbb{Q}) : \hat{h}(P) < B\} < \infty$$

- Let $\phi : E \to E'$ be isogeny over $\mathbb{Q}$. Then

$$\hat{h}(\phi P) = (\deg \phi) \hat{h}(P) \quad \text{for all } P \in E(\mathbb{Q})$$

- Let $E/\mathbb{Q}$ be elliptic curve. There exists $c > 0$ such that

$$H(P + Q) \cdot H(P - Q) \le c \cdot H(P)^2 \cdot H(Q)^2 \quad \text{for all } P, Q \in E(\mathbb{Q})$$

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

- Let $P \in E(\mathbb{Q})$. Then $P$ is a torsion point if and only if $\hat{h}(P) = 0$.

- **Absolute values:** Let $M_{\mathbb{Q}}$ denote the set of standard absolute values on $\mathbb{Q}$, which consists of:
  - One archimedean absolute value $|x|_\infty = \max(-x, x)$.
  - For each prime $p \in \mathbb{Z}$, one nonarchimedean ($p$-adic) absolute value $|x|_p = p^{-v_p(x)}$.
- **Height:** For an arbitrary number field $K$, let $P = (a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n(K)$, and define the **height**

$$H_K(P) := \prod_{v \in M_K} \max\{|a_0|_v, |a_1|_v, \ldots, |a_n|_v\}^{[K_v:\mathbb{Q}_v]}$$

  where $M_K$ denotes the set of standard absolute values on $K$ (i.e. the absolute values in $K$ whose restriction to $\mathbb{Q}$ is in $M_{\mathbb{Q}}$)

  Note the absolute values are normalised such that

$$\prod_{v \in M_K} |x|_v^{[K_v:\mathbb{Q}_v]} = 1$$

## 14. Dual isogenies and the Weil pairing

- Let $\Phi \in E(\bar{K})$ be a finite $\mathrm{Gal}(\bar{K}/K)$-stable subgroup (i.e. for all $T \in \Phi$, then $T^\sigma \in \Phi$ for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$).

  Then there exists an elliptic curve $E'/K$ and a separable isogeny $\phi : E \to E'$ defined over $K$ with kernel $\Phi$ such that for every isogeny $\phi : E \to E'$ with $\Phi \subset \ker(\phi)$ factors uniquely via $\phi$.

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

- **Dual isogeny:** Let $\phi : E \to E'$ be an isogeny of degree $n$. Then there exists unique isogeny $\hat{\phi} : E' \to E$ s.t. $\hat{\phi} \circ \phi = [n]$. $\hat{\phi}$ is called the **dual isogeny** of $\phi$.

  – Elliptic curves being **isogenous** is equivalence relation.
  – $\deg(\hat{\phi}) = \deg(\phi)$ and $\hat{[n]} = [n]$
  – $\hat{\hat{\phi}} = \phi$
  – If $\psi : E \to E'$ isogeny and $\phi : E' \to E''$ isogeny, then $\widehat{\phi\psi} = \hat{\psi}\hat{\phi}$
  – If $\phi \in \mathrm{End}(E)$, then $\mathrm{tr}(\phi) = \phi + \hat{\phi}$

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

- **sum:** Define sum : $\mathrm{Div}(E) \to E$ as $\sum n_p(P) \mapsto \sum n_p P$ (sum using group law)

  *Remark:* Given the isomorphism $\phi : E \to \mathrm{Pic}^0(E)$ given by $P \mapsto [P - O_E]$, we have

$$\mathrm{sum} D \mapsto [D] \quad \text{for all } D \in \mathrm{Div}^0(E)$$

- Let $D \in \mathrm{Div}(E)$. Then $D \sim 0$ if and only if $\deg(D) = 0$ and $\mathrm{sum}D = 0$. (i.e. $D$ is principal iff both the sum and degree are 0)

- **Weil pairing:** Let $\phi : E \to E'$ be isogeny of degree $n$, with $\mathrm{char}(K) \nmid n$. Let $E[\phi]$ be the kernel of $\phi$. The **Weil pairing**:

$$e_\phi : E[\phi] \times E'[\hat{\phi}] \to \mu_n = \{x \in K : x^n = 1\}$$

  *Definition of map*: Let $S \in E[\phi], T \in E'[\hat{\phi}]$. As $\phi$ has degree $n$, this implies $nT = 0$.

  – Choose $f \in \bar{K}(E')$ such that $\mathrm{div}(f) = n(T) - n(0)$.
  – Choose $g \in \bar{K}(E)$ such that $\mathrm{div}(g) = \phi^*(T) - \phi^*(0)$
  – Thus $\phi^* f = cg^n$. Can assume wlog $\phi^* f = g^n$.

  We define

$$e_{\phi(}S, T) = \zeta = \frac{g(X+S)}{g(X)} \quad \text{for any } X \in E$$

- $e_\phi$ is bilinear and non-degenerate (i.e. if $e_\phi(S,T) = 1$ for all $S \in E[\phi]$, then $T = O_{E'}$)

- 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 $\sigma \in \mathrm{Gal}(\bar{K}/K)$

- Taking $\phi = [n] : E \to E$ gives a pairing:

$$e_n : E[n] : E[n] \to \mu_n$$

- If $E[n] \subset E(K)$, then $\mu_n \subset K$ (can find $S, T \in E[n]$ such that $e_n(S, T)$ is *primitive* $n$-th root of unity)
  - $e_n$ is **alternating**. I.e. $e_n(T, T) = 1$ for all $T \in E[n]$.
  - $e_n(S, T) = e_n(T, S)^{-1}$.

## 15. Galois cohomology

*Setup:* $G$ a group. $A$ is a $G$-module (i.e. an abelian group $A$ with a left group action $G \times A \to A$ s.t. we have identity, compatibility, and $g \cdot (a+b) = g \cdot a + g \cdot b$)

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

$$\begin{array}{rl} \textbf{Cochain:} & C_1(G,A) = \{\text{maps } G \to A\} \\ & \cup \\ \textbf{Cocycle:} & Z^1(G,A) = \{(a_\sigma)_{\sigma \in G} : a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\} \\ & \cup \\ \textbf{Coboundary:} & B^1(G,A) = \{(\sigma b - b)_{\sigma \in G} : b \in A\} \end{array}$$

$$H^1(G,A) = \frac{Z'(G,A)}{B'(G,A)} = \frac{\text{cocycles}}{\text{coboundaries}}$$

*Remark:* If $G$ acts trivially, then $Z^1(G,A) = \{\textit{homogeneous} \text{ maps} G \to A\}$ and $B^1(G,A) = \{(0)\}$ (the zero map). Thus $H^1(G,A) = \mathrm{Hom}(G,A)$

*Examples:* If $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R} = \{\mathrm{id}, \mathrm{conj}\}$ and $A = \mathbb{C}$, then

  - $C_1(G,A) = \{\text{maps } G \to A\} \cong \mathbb{C} \times \mathbb{C}$.
  - $Z^1(G,A) = \{(0, ix) : x \in \mathbb{R}\}$
  - $B^1(G,A) = \{(0, ix) : x \in \mathbb{R}\}$
  - $H^1(G,A)$ is trivial.

- A short exact sequence of $G$-modules:

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

gives rise to long exact sequence of abelian groups:

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

*Definition of $\delta$:* :

  - Let $c \in C^G$. THere exists $b \in B$ s.t. $\psi(b) = c$.
  - Note $\psi(\sigma b - b) = 0$. For all $\sigma \in G$, there exists $a_\sigma \in A$ s.t. $\psi(a_\sigma) = \sigma b - b$.
  - Can show $(a_\sigma)_{\sigma \in G} \in Z'(G,A)$.
  - Define $\delta(C) =$ class of $(a_\sigma)_{\sigma \in G}$ in $H'(G,A)$

- Let $A$ be a $G$-module, $H \lhd G$ a normal subgroup. THen there is an **inflation** and **restriction** exact sequence:

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

- **Hilbert's Theorem 90:** Let $L/K$ be finite Galois extension. THen $H^1(\mathrm{Gal}(L/K), L^\times) = 0$ (i.e. $Z^1 \subset B^1$).

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

  *Corollary 2:* $H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^*/(K^*)^n$. If $\mu_n \in K$, then $\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^*/(K^*)^n$

*Setup:* Let $\phi : E \to E'$ be isogeny of elliptic curves over $K$. Notation: $H'(K, \_)$ means $H'(\mathrm{Gal}(\bar{K}/K), \_)$.

There is short exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules:

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

Get long exact sequence

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

Get short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \frac{E'(K)}{\phi E(K)} \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\phi]) \arrow[r] \arrow[d, "\mathrm{res}_V"'] \arrow[dr, "\alpha"] & H'(K, E)[\phi_*] \arrow[r] \arrow[d, "\mathrm{res}_V"'] & 0 \\
0 \arrow[r] & \prod_V \frac{E'(K_V)}{\phi(E(K_V))} \arrow[r, "\delta_v"] & \prod_V H^1(K_V, E[\phi]) \arrow[r] & \prod_v H'(K_v, E)[\phi_*] \arrow[r] & 0
\end{tikzcd}$$

- **Selmer group:** THe $\phi$-Selmer group is

$$S^{(\phi)}(E/K) = \ker \alpha \qquad \text{(the diagonal map above)}$$

or alternatively

$$\begin{aligned} S^{(\phi)}(E/K) &= \mathrm{Ker}\left( H^1(K, E[\phi]) \to \prod_V H^1(K_V, E) \right) \\ &= \{\alpha \in H^1(K, E[\phi]) : \mathrm{res}_v(\alpha) \in \mathrm{im}(\delta_v)\ \forall v\} \end{aligned}$$

- **Tate-Shaferavich group:** $Ш(E/K) = \ker\left(H'(K, E) \to \prod_V H'(K_v, E)\right)$

  Get short exact sequence:

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

- **Place:** Let $K$ be number field. A **place** of $K$ is an equivalence class of absolute values on $K$. Three types: *Trivial*, *archimedan*, and *non-Archimedean.*
- $S^{(n)}(E/K)$ is finite.
- Let $S$ be finite set of places. THe subgroup of $H^1(K, A)$ unramified outside $S$ is

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

*Conjecture:* $Ш(E/k)$ is finite.

# 16. Descent by cyclic isogeny

*Setup:* Let $E, E'$ be elliptic curves over a number field $K$. Let $\phi : E \to E'$ be an isogeny of degree $n$.
Define the map $\alpha$ by the long exact sequence

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

- Let $f \in K(E')$ and $g \in K(E)$ with $\text{div}(f) = n(T) - n(0)$ and $\phi^* f = g^n$. THen $\alpha(P) = f(P) \bmod (K^*)^n$ for all $P \in E'(K) \backslash \{0, T\}$

- **Setup of 2-isogeny:** Let $E$ and $E'$ be elliptic curves:

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

  such that $b \neq 0$ and $a^2 - 4b \neq 0$, and $a' = -2a$ and $b' = a^2 - 4b$. There then is a 2-isogeny $\phi : E \to E'$ which maps:

$$(x, y) \mapsto \left( \left( \frac{y}{x} \right)^2, \ \frac{y(x^2 - b)}{x^2} \right)$$

  and its dual isogeny $\hat{\phi} : E' \to E$ which maps

$$(x, y) \mapsto \left( \frac{1}{4} \left( \frac{y}{x} \right)^2, \ \frac{y(x^2 - b')}{8x^2} \right)$$

  with kernels

$$E[\phi] = \{0_E, T\} \qquad T = (0, 0) \in E(K)$$
$$E'[\hat{\phi}] = \{0_{E'}, T'\} \qquad T' = (0, 0) \in E'(K)$$

- There is a group homomorphism:

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

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

  *Remark:* This gives two injective group homomorphisms:

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

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

- We have
$$2^{\text{rank } E(K)} = \frac{|\text{Im}(\alpha_E)| \cdot |\text{Im}(\alpha_{E'})|}{4}$$

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

  *Notation:* $K(S,n) = \{x \in K^\times/(K^\times)^n : \text{ord}_v(x) \equiv 0 \pmod n \text{ for all } v \in M_K - S\}$

  *Example:* Let $S$ be finite set of primes. Then $\mathbb{Q}(S,2)$ is simply a finite set of squarefree integers containing only primes from $S$. E.g. if $S = \{2,3,5\}$, then $\mathbb{Q}(S,2) = \langle -1, 2, 3, 5\rangle = \{1, -1, 2, -2, 3, -3, 5, -5, 6, -6, 10, -10, 15, -15, 30, -30\}$ (as cosets in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$)

- If $b_1 b_2 = b$, then
$$b_1(K^*)^2 \in \text{Im}(\alpha_E) \iff \begin{array}{l} w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4 \\ \text{is soluble for } u, v, w \in K \text{ not all zero} \end{array}$$

  *Fact:* If $a, b_1, b_2 \in \mathbb{Z}$ and $p \nmid 2b(a^2 - 4b)$, then $w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$ has solution over $\mathbb{Q}_p$

- Calculating the **rank** of $E : y^2 = x(x^2 + ax + b)$:
  - Setup the 2-isogeny by defining $E' : y^2 = x(x^2 + a'x + b)$ where $a' = -2a$ and $b' = a^2 - 4b$.
  - We aim to calculate $\text{Im}(\alpha_E)$ and $\text{Im}(\alpha_{E'})$.
  - Obtain bounds on the size by using that $\text{Im}(\alpha_E) \subset \langle -1, p_{b_1}, p_{b_2}, \ldots, p_{b_k}\rangle$ where $p_{b_i}$ are the primes dividing $b'$.

    Similarly, use that $\text{Im}(\alpha_{E'}) \subset \langle -1, p_{b'_1}, p_{b'_2}, \ldots, p_{b'_k}\rangle$ where $p_{b'_i}$ are the primes dividing $b'$.
  - For each $b_1$ dividing $b$, determine if $b_1$ is in $\text{Im}(\alpha_E)$ by determining if there exist $u, v, w \in K$ not all zero such that
$$w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4$$

    *Tips*:
    * If $b_1, b_2, a \leq 0$, then no solutions over $\mathbb{R}$, hence no solutions in $\mathbb{Q}$.
    * Can multiply through to assume integer solutions with $\gcd(u, v) = 1$.
    * Use quadratic reciprocity.
    * Use that $\text{Im}(\alpha_E)$ is a group to eliminate checking every possible subset of $\langle -1, p_{b_1}, \ldots, p_{b_k}\rangle$.
  - Finally, use
$$\text{rank } E(K) = \log_2 |\text{Im}(\alpha_E)| + \log_2 |\text{Im}(\alpha_{E'})| - 2$$
    to compute the rank, given $\text{Im}(\alpha_E)$ and $\text{Im}(\alpha_{E'})$.

## Birch Swinnerton-Dyer conjecture

- Let $E/\mathbb{Q}$ be elliptic curve. Define the associated L-fuction $L(E,s) = \prod_p L_p(E,s)$ where

$$L_p(E,s) = \begin{cases} (1-a_p p^{-s} + p^{1-2s})^{-1} & \text{if good reduction} \\ (1-p^{-s})^{-1} & \text{if split mult reduction} \\ (1+p^{-s})^{-1} & \text{if nonsplit mult reduction} \\ 1 & \text{if additive reduction} \end{cases}$$

  where $\#\tilde{E}(\mathbb{F}_p) = p+1-a_p$, By Hasse's bound, we know $L(E,s)$ converges for $\mathrm{Re}(s) > 3/2$.

- **Analytic continuation:** $L(E,s)$ is the L-functio of a weight 2 modular form and hence has an analytic continuation to all of $\mathbb{C}$

- **Weak BSD:** $\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank} E(\mathbb{Q})$

- **Strong BSD:**

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

  where

  - $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)] =$ Tamagawa number of $E/\mathbb{Q}_p$ .
  - Let $P_1, \dots, P_r$ generate the non-torsion part of $E(\mathbb{Q})$. So $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{torsion}} = \langle P_1, \dots, P_r \rangle$. Then the regulator of $E(\mathbb{Q})$ is

$$\mathrm{Reg} E(\mathbb{Q}) = \det([P_i, P_j])_{i,j=1,\dots,r} = \begin{vmatrix} [P_1,P_1] & [P_1,P_2] & \dots & [P_1,P_r] \\ [P_2,P_1] & [P_2,P_2] & \dots & [P_2,P_r] \\ \vdots & \vdots & \ddots & \vdots \\ [P_r,P_1] & [P_r,P_2] & \dots & [P_r,P_r] \end{vmatrix}$$

    where $[P,Q] = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$
  - $\Omega_E$ is the integral

$$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{|2y + a_1 x + a_3|}$$

    where $a_i$ are coefficients of globally minimal Weierstrass equation for $E$.

- **Kolyvagin:** If $\mathrm{ord}_{s=1} L(E,s) = 0$ or 1 (i.e. analytic rank is 0 or 1), then weak BSD is true and $|\text{Ш}(E/\mathbb{Q})| < \infty$

## Misc

**Automorphism group:** Let $E/k$ be elliptic curve. Then $\mathrm{Aut}(E)$ is finite, and its order is

- 2 if $j(E) \notin \{0, 1728\}$
- 4 if $j(E) = 0$ and char $k \notin \{2, 3\}$
- 6 if $j(E) = 1728$ and char $k \notin \{2, 3\}$
- 12 if $j(E) = 0 = 1728$ and char $k = 3$
- 24 if $j(E) = 0 = 1728$ and char $k = 2$

In the last two cases, $E$ is always supersingular

**Endomophisms:** An endomorphism of $E$ is an isogeny from $E$ to $E$. Denoted, $\mathrm{End}(E)$, it forms a ring

- Multiplication by n: $[n] : E \to E$ given by $X \mapsto X + X + \cdots + X$ $n$ times.
- (For finite fields) Frobenius endomorphism: $\phi : E \to E$ given by $(x, y) \mapsto (x^q, y^q)$
- Translation: $\tau_P : E \to E$ given by $X \mapsto P + X$

Some Geometric Notions

- **Coordinate ring:** Let $V$ be a variety over $K$. The **coordinate ring** of $V/K$ is defined by

$$K[V] = \frac{K[X]}{I(V/K)}$$

  Elements of $K[V]$ are the polynomial functions on $V$.

  $K(V)$ is an integral domain. It's quotient field is denoted by $K(V)$.

- **Maximal ideal:** Let $V$ be variety, and $P$ a point on $V$. The **maximal ideal** at $P$ is

$$M_P = \{f \in K[V] : f(P) = 0\}$$

- **Local ring:** Let $V$ be variety, and $P$ a point on $V$. The local ring of $V$ at $P$ is

$$K[V]_P = \{F \in K(V) : F = \frac{f}{g} \text{ for some } f, g \in K[V] \text{ with } g(P) \neq 0\}$$

  I.e. $K[V]_P$ is the set of regular function at $P$ (functions defined at $P$).

- **Rational map:** Let $V_1, V_2 \subset \mathbb{P}^n$ projective varieties. A rational map from $V_1$ to $V_2$ is a map of the form

$$\phi : V_1 \to V_2 \qquad \phi = [f_0, \ldots, f_n]$$

  where $f_0, \ldots, f_n \in \bar{K}(V_1)$ are s.t., fr every point $P \in V_1$ at which $f_0, \ldots, f_n$ are all defined: $\phi(P) = [f_0(P), \ldots, f_n(P)] \in V_2$.

  *Note:* A rational map $\phi : V_1 \to V_2$ may **not** necessarily be well-defined at every point of $V_1$.

- **Regular:** A rational map $\phi = [f_0, \ldots, f_n] : V_1 \to V_2$ is **regular** at $P \in V_1$ if there is a function $g \in \bar{K}(V_1)$ such that
  - For each $i$, $gf_i$ is regular at $P$.
  - There exists an $i$ for which $gf_i(P) \neq 0$

  *Note:* We may have to take different $g$'s for different points.

- **Morphism:** A rational map that is regular at every point.

## Curves

- Let $C$ be a curve, and $P \in C$ a smooth point. THen $K[C]_P$ is a discrete valuation ring.

- **Order of vanishing:** Let $C$ be a curve with function field $K(C)$. Let $P \in C$ be a smooth point. THe function $\mathrm{ord}_P(f) : K(C) \to \mathbb{Z} \cup \infty$ is the **order of vanishing** of $f \in K(C)$ at $P$.

  Defined as

$$\mathrm{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in M_p^d\}$$