Elliptic Curves

Dr T. Dokchitser
Typeset by Aaron Chan(akyc2@cam.ac.uk)

Last update: June 8, 2010

Chapter 1

Informal Introduction

Number Theory
—Diophantis equations: Algebraic NT, Arithmetic geometry, Birch-Swinnerton-Dyer Conjecture
—Primes: Analytic NT, Riemann Hypothesis

This course is a an introduction of arithmetic geometry

$$V : \begin{cases} f_1(x_1, \ldots, x_m) = 0 \\ \quad \vdots \\ f_n(x_1, \ldots, x_m) = 0 \end{cases}$$

System of polynomial equations with $\mathbb{Z}$-coefficient (algebraic variety over $\mathbb{Q}$)

Main question Describe:
$V(\mathbb{Q})$ =set of rational solutions ($x_i \in \mathbb{Q}$)
$V(\mathbb{Z})$ =set of integer solutions ($x_i \in \mathbb{Z}$)

Example: Is $V(\mathbb{Q})$ infinite (or empty)?
Exercise (Fermat's Last Theorem):
$x^n + y^n = z^n$ has no $\mathbb{Z}$-solutions with $xyz \neq 0, x, y, z \in \mathbb{Z}$ for $n > 2$
$\Leftrightarrow \quad V : x^n + y^n = 1$ has $V(\mathbb{Q}) \subseteq \{(\pm 1, 0), (0, \pm 1)\}$ for $n > 2$
Generally, simplest case is 1 equation in 2 variables

$C : f(x, y) = 0 \qquad \deg f = d$
Plane curve
If C is non-singular projective, then $C(\mathbb{C})$=compact Riemann surface of genus $g = \frac{(d-1)(d-2)}{2}$

When can $C(\mathbb{Q})$ be infinite?

$g = 0$: Either $C(\mathbb{Q}) = \emptyset$ or $C(\mathbb{Q})$ infinite. $\exists$ algorithm to determine which
$g = 1$: Unsolved problem (BSD conjecture)
$g \geq 2$: Falting's Theorem (= Mordell Conjecture) (very hard) $C(\mathbb{Q})$ always finite

$\underline{g = 0}$
C line, $ax + by = c$, $C(\mathbb{Q})$ infinite
or
C conic, $f(x, y) = 0$, $\deg f = 2$, (circle, parabola, hyperbola)

E.g.: $C : x^2 + y^2 = 1$
What is $C(\mathbb{Q})$?
Take $Q = (-1, 0)$ and line l_t through Q of slope $t \in \mathbb{Q}$

Claim: 2nd point of intersection P_t is in $C(\mathbb{Q})$

Proof

$$\begin{cases} x^2 + y^2 = 1 \\ y = t(x+1) \end{cases}$$

$\Leftrightarrow \quad x^2 + t^2(x+1)^2 - 1 = 0$ quadratic equation on x with $\mathbb{Q}$-coeff., 1st root $x = -1$ rational
$\Rightarrow$ 2nd root rational

Explicitly,

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

has roots

$$\begin{aligned} x &= -1 \qquad & y &= 0 \\ x &= \frac{1-t^2}{1+t^2} \qquad & y &= t\left(\frac{1-t^2}{1+t^2} + 1\right) = \frac{2t}{1+t^2} \end{aligned}$$

i.e.

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

Conversely, $P \in C(\mathbb{Q}) \Rightarrow$ line PQ has slope $\in \mathbb{Q}$
$\Rightarrow \quad P = P_t$ for some $t \in \mathbb{Q}$

$$\begin{array}{ccc} \mathbb{Q} \cup \{\infty\} & \leftarrow 1:1 \rightarrow & C(\mathbb{Q}) \\ t & \mapsto & \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \\ \frac{y}{x+1} & \leftarrow\!\shortmid & (x, y) \end{array}$$

(in fact, $C \cong \mathbb{P}^1_{\mathbb{Q}}$) □

Corollary
Every Pythagorean triples $a^2 + b^2 = c^2$, $a, b, c \in \mathbb{N}$, are of the form

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$$

(Put $t = m/n$)
Remark:

$C : f(x, y)$ any conic
Either $C(\mathbb{Q}) \neq \emptyset \Rightarrow C(\mathbb{Q})$ infinite, $C \cong \mathbb{P}^1_{\mathbb{Q}}$ (same proof)
or $C(\mathbb{Q}) = \emptyset$ can happen
E.g. $x^2 + y^2 = -1, C(\mathbb{R}) = \emptyset$
E.g.2 $x^2 + y^2 = 3$ no solution mod 3 ($C(\mathbb{Q}_3) = \emptyset$)

Theorem 1.0.1 (Hasse-Minkowski)
C conic, then

$$C(\mathbb{Q}) \neq \emptyset \Leftrightarrow C(\mathbb{R}) \neq \emptyset, C(\mathbb{Q}_p) \neq \emptyset \; \forall p$$

In fact, write $C : ax^2 + by^2 = c$ (easy), $a, b, c \in \mathbb{Z}$ Then enough to check $\mathbb{R}, \mathbb{Q}_p$ for $p|2abc$
Solves $g = 0$ completely

$g = 1$: Elliptic curves - can be represented as a plane cubic

$$E : y^2 = x^3 + Ax + B \quad (A, B \in \mathbb{Q})$$

use Riemann-Roch Theorem:
If $P, Q \in E(\mathbb{Q})$, then line PQ intersect E in third point $R \in E(\mathbb{Q})$

Theorem 1.0.2
Define operation $+$ as follows:
$P + Q = R' = R$ reflected in x-axis
This makes $E(\mathbb{Q})$ into an abelian group

This gives elliptic curves a very rich structure

Theorem 1.0.3 (Mordell-Weil)
$E(\mathbb{Q})$ is a finitely generated abelian group

Our course:

- Geometry of ECs, group law
- Structure of $E(\mathbb{C})$, $E(\mathbb{F}_q)$, $E(\mathbb{Q}_p)$
- Mordell-Weil Theorem
- State Birch-Swinnerton-Dyer Conjecture and related bits

Chapter 2

Curves

2.1 Background

k algebraically closed (e.g. $k = \mathbb{C}$)

Definition 2.1.1
Affine space $\mathbb{A}^n = \mathbb{A}^n_k = \{(a_1, \dots, a_n) | a_i \in k\}$
Projective space $\mathbb{P}^n = \mathbb{P}^n_k = \{(a_0 : a_1 : \cdots : a_n) | a_i \in k$, not all $0\} / \sim$
where $(a_0 : \cdots : a_n) \sim (\alpha a_0 : \cdots : \alpha a_n)$ $\forall \alpha \in k^\times$

$\mathbb{P}^n$ covered by $\mathbb{A}^n$'s:

$$\begin{array}{rcl} \mathbb{A}^n & \hookrightarrow & \mathbb{P}^n \\ (a_1, \dots, a_n) & \mapsto & [1 : a_1 : \cdots : a_n] \end{array}$$

This gives a copy of $\mathbb{A}^n$ in $\mathbb{P}^n$, say $\mathbb{A}^n_0$.
Similarly, get $\mathbb{A}^n_0, \mathbb{A}^n_1, \dots, \mathbb{A}^n_n \hookrightarrow \mathbb{P}^n$
by $(a_1, \dots, a_n) \mapsto [a_0 : \cdots : 1 : \cdots : a_n]$ (1 at j-th place)
If $P \in \mathbb{P}^n$, say $P = (a_0 : \cdots : a_j : \cdots : a_n)$ with not all $a_n = 0$, say $a_j \neq 0$, then
$P = (a_0 : \dots : a_n) = (\frac{a_0}{a_j} : \cdots : \frac{a_j}{a_j} : \cdots : \frac{a_n}{a_j}) \in \mathbb{A}^n_j$
So $\mathbb{P}^n = \mathbb{A}^n_0 \cup \cdots \cup \mathbb{A}^n_n$ (this is called affine charts)

Example 2.1.2
Projective line $\mathbb{P}^1$
$\mathbb{P}^1 = \{(x : 1)\} \cup \{(1 : 0)\} = \mathbb{A}^1_1 \cup \{\infty$ point at infinity$\}$
$= \{(0 : 1)\} \cup \{(1 : y)\} = \{0\} \cup \mathbb{A}^1_0$
Algebraic subsets are $\emptyset, \mathbb{P}^1$, finite subsets $\{b_1, \dots, b_k\}$ zero set of $f(x, y) = \prod (x - b_i y)$

Definition 2.1.3
An (affine) algebraic set $V \subseteq \mathbb{A}^n$ is the set of all solutions to a system of polynomial equations in $x_1, \dots, x_n$

$$V : \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \qquad \vdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

A (projective) algebraic set $V \subseteq \mathbb{P}^n$ is the set of all solutions to a system of homogeneous polynomial equations in $x_0, \dots, x_n$
Exercise: Equivalent to $V \cap \mathbb{A}^n_j$ affine algebraic set $\forall j$

Definition 2.1.4
A (projecitve) curve is an infinite algebraic set $C \subseteq \mathbb{P}^n$ s.t. $Y \subsetneq C$ algebraic $\Rightarrow Y$ finite
(irreducible projective variety of dimension 1)

E.g. $\mathbb{P}^1$ is a curve

A curve $C \subseteq \mathbb{P}^2$ is plane curve. These are given by $C : f(x,y,z) = 0$, $f \in k[x,y,z]$ homog. irred.

E.g. $xy - z^2 = 0$
$xy = 1$ in $z = 1$ chart
$x = z^2$ in $y = 1$ chart
$y = z^2$ in $x = 1$ chart

We often write e.g. $C : xy = 1 \subseteq \mathbb{P}^2$ meaning associated projective curve $xy = z^2$

Algebraic sets in $\mathbb{P}^2$ are $\emptyset, \mathbb{P}^2$ finite unions of points and plane curves

2.1.1 Rational functions

Definition 2.1.5
A rational function on $\mathbb{A}^n$ is $f \in k(x_1, \ldots, x_n) =: k(\mathbb{A}^n)$
A rational function on $\mathbb{P}^n$ is $f = 0$ or

$$f = \frac{g(x_0, \ldots, x_n)}{h(x_0, \ldots, x_n)}$$

where g, h homog. polynomials of the same degree.

They form a field $k(\mathbb{P}^n)$; and in fact, $k(\mathbb{P}^n) = k(\mathbb{A}^n_j)$ $\forall$ chart

Example $k(\mathbb{P}^1) \ni \frac{y}{x+y} \leftrightarrow \frac{1}{x+1} \in k(\mathbb{A}^1)$ via,
from left to right, $y \mapsto 1$, and from right to left, homogenize.

Definition 2.1.6
$C \subseteq \mathbb{P}^n$ curve, $f = g/h \in k(\mathbb{P}^n), h \neq 0$ on C
The restriction of f to C

$$f : C \setminus \{\text{finite set}\} \to k$$

(not defined where $h = 0$) is a rational function on C. They form a field $k(C)$

Example 2.1.7

- $C \subseteq \mathbb{P}^2$ plane curve $f(x,y) = 0$ Then $k(C) = ff(k[x,y]/(f))$
- $C = \mathbb{P}^1 \hookrightarrow \mathbb{P}^2$
  Then $k(C) = ff(k[x,y]/(y)) = ff(k[x]) = k(x)$
- $C : y^2 = x^3 + 1$. $k(C) = ff(k[x,y]/y^2 - x^3 - 1) \cong k(x, \sqrt{x^3+1})$

Fact: $k(C)$ is a finitely generated field of transcendence degree 1 over k; so $\forall f \in k(C) \setminus k$

$$k \overset{\text{transc.}}{\hookrightarrow} k(f) \cong k(t) \overset{\text{finite}}{\hookrightarrow} k(C)$$

Fact: (Not hard) Conversely, K f.g. field of tr.deg. 1 over $k \Rightarrow \exists C$ s.t. $k(C) \cong K$

Definition 2.1.8
$C \subseteq \mathbb{P}^n, D \subseteq \mathbb{P}^m$ curves. A rational map $\phi : C \dashrightarrow D$ is one given by rational functions

$$\phi(P) = (f_0(P) : \cdots : f_m(P))$$

where $f_i \in k(C)$, not all 0.
Note: This may not be defined on finitely many points.

Definition 2.1.9
We say ϕ is defined at $P \in C$ if $f_0 g, \ldots, f_m g$ defined at P for some $g \in k(C)^\times$
If ϕ is defined everywhere, ϕ is a morphism

A non-constant $\phi : C \to D$ induces

$$\begin{aligned} \phi^* : k(D) &\hookrightarrow k(C) \\ f &\mapsto \phi^*(f) := f \circ \phi \end{aligned}$$

injective (since fields) of finite index (tr.deg 1)

Definition 2.1.10
Degree of morphism is $\deg \phi = [k(C) : \phi^* k(D)]$

Conversely, any injection $k(D) \hookrightarrow k(C)$ comes from a unique rational map $C \to D$

Example 2.1.11
$C : x^2 + y^2 = 1$, $D : y = 0$, $\phi(x, y) := (x, 0)$
$k(C) \cong k(x, \sqrt{1 - x^2})$, $k(D) \cong k(x)$
So induces $\phi^* x = x$
$\deg \phi = [k(x, \sqrt{1 - x^2}) : k(x)] = 2$

Exercise: $\{$ Rational maps $C \to \mathbb{P}^1$ $\} = k(C)$

2.1.2 Smoothness

Definition 2.1.12
Affine curve C (defined by $f_1, \ldots, f_m$) is non-singular at $P = (a_1, \ldots, a_n) \in C$ if the matrix $A = \left(\frac{\partial f_i}{\partial x_j}(P)\right)_{i,j}$ has rank $n - 1$ (note the rank is always $\leq n - 1$)

Formal derivative

$$\frac{\partial(cx^i y^j \cdots)}{\partial x} := cix^{i-1} y^j \cdots + \text{linearity}$$

with usual rules, product rule, chain rule, etc.

Definition 2.1.13
Projective curve $C \subseteq \mathbb{P}^n$ is non-singular at P if $C \cap \mathbb{A}^n_j$ non-singular at P for some (equivalently, for any) chart containing P

Example 2.1.14
Plane curve $C : f(x, y) = 0$, f irreducible, singular at $P = (a, b) \quad \Leftrightarrow \quad \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$

We can think in terms of picture:

Example 2.1.15
$f = y^2 - x^3 = 0$
$\frac{\partial f}{\partial x} = -3x^2$
$\frac{\partial f}{\partial y} = 2y$
Both 0 at $(0,0)$ and not both 0 otherwise, so f has unique singular point $(0,0)$

Definition 2.1.16
C non-singular (or smooth) if it is non-singular at every point

Exercise: (char $k \neq 2$) Affine plane curve $y^2 = f(x)$ is non-singular $\Leftrightarrow$ $f(x)$ has non multiple roots

Fact: Non-singular $P \in C$ defines a discrete valuation ("order of vanishing at P")

$$\begin{aligned} v_p : k(C)^\times &\twoheadrightarrow \mathbb{Z} \\ f &\mapsto v_p(f) = \begin{cases} n > 0 & f \text{ has zero of order } n \text{ at } P \\ -n < 0 & f \text{ has pole of order } n \text{ at } P \\ 0 & f(P) \in k^\times \\ \infty & f \equiv 0 \end{cases} \end{aligned}$$

$$v_p(fg) = v_p(f) + v_p(g) \qquad v_p(f/g) = v_p(f) - v_p(g)$$
$$v_p(f \pm g) \geq \min(v_p(f), v_p(g))$$

Example 2.1.17
$C = \mathbb{P}^1, k(C) = k(X) \ni f = \frac{g}{h} = \frac{\prod (x-a_i)^{n_i}}{\prod (x-b_i)^{m_i}}$

$$v_{a_i} f = n_i, \quad v_{b_i} f = -m_i, \quad v_\infty f = \deg h - \deg g, \quad v_P f = 0 \text{ otherwise}$$

Definition 2.1.18
f is a uniformiser at P if $v_P f = 1$
One of coordinate functions $x_j - a_j$ is always a uniformiser at $P = (a_1, \ldots, a_n)$

Example 2.1.19
$C : x^2 + y^2 = 1, P = (a,b) \in C$
$P \neq (\pm 1, 0) \qquad x - a$ uniformiser
$P = (1,0) \qquad y$ uniformiser, $x - 1 = \frac{y^2}{x+1}$ (has valuation 2)

Lemma 2.1.20
If $\phi : C \to C'$ rational map, C non-singular, then ϕ is a morphism

Proof
$\phi = (f_0 : \cdots : f_n), \quad P \in C$
Say $v_P f_0 < v_P f_j, \ j \neq 0$
Then
$$\phi = \left(1 : \underbrace{\frac{f_1}{f_0} : \cdots : \frac{f_n}{f_0}}_{v_P \geq 0}\right)$$
defined at P $\square$

Corollary 2.1.21
If $\phi : C \to C'$ has degree 1, C, C' non-singular, then ϕ is an isomorphism

Proof
ϕ induces $\phi^* : k(C') \xrightarrow{\sim} k(C)$
$\exists\psi$ rational map $C' \to C$ s.t. $\phi\psi = \mathrm{id} = \psi\phi \Rightarrow \phi, \psi$ morphism by the lemma. □

Summary: There is an equivalence of categories

$$\begin{array}{ccc} \text{non-singular curves}/k & \to & \text{f.g. fields } K/k \text{ of tr.deg. } 1 \\ \text{(rational maps =) morphisms } \phi & \to & \text{fields inclusions} \\ C & \mapsto & k(C) \\ \left\{ \begin{array}{c} \text{discrete valuations on } K \\ v : K^\times \twoheadrightarrow \mathbb{Z} \text{ s.t.} \\ v(k^\times) = 0 \end{array} \right\} & \leftarrow\!\shortmid & K \end{array}$$

2.1.3 Divisor

All curves non-singular over $k = \overline{k}$

Definition 2.1.22
A divisor D on C is a formal finite linear combination of points

$$D = \sum_i n_i P_i \qquad n_i \in \mathbb{Z}, P_i \in C$$

$$\mathrm{Div}(C) = \{\text{divisors of } C\}$$

this is an abelian group.

$$\underline{\text{degree of divisor}} : \deg(D) = \sum_i n_i \in \mathbb{Z}$$

Divisor of degree zero forms $\mathrm{Div}^0 C$ a subgroup.

Non-constant $\phi : C \to C'$ induces homomorphisms

$$\begin{array}{rcll} \phi_* : \mathrm{Div}\, C & \to & \mathrm{Div}\, C' & \underline{\text{pushforward}} \\ (Q) & \mapsto & (P), P = \phi(Q) & \\ \phi^* : \mathrm{Div}\, C' & \to & \mathrm{Div}\, C & \underline{\text{pullback}} \\ (P) & \mapsto & \sum_{\phi(Q)=P} e_Q(Q) & \end{array}$$

where

$$e_Q = \underline{\text{ramification index}} := v_Q(\phi^* t_P) \geq 1$$

t_P is uniformiser at P

Fact: $\deg \phi^* P = \deg \phi$ always (in particular, ϕ surjective)

Example 2.1.23
(see picture)
$\phi^*(a) = (a, \sqrt{1-a}) + (a, -\sqrt{1-a}) \quad a \neq \pm 1$
$\phi^*(1) = 2(1, 0) \qquad (\phi^*(x-1) = x - 1$ has valuation 2)
$\phi^*(-1) = 2(-1, 0)$
We say that (1,0), (-1,0) are ramified (i.e. $e_Q > 1$)

Remark.

$$\begin{array}{c} k(C) \\ d \big\uparrow \\ k(C') \end{array} \qquad \begin{array}{ccc} Q_1 & Q_2 & \cdots \\ \diagdown & | & \diagup \\ & P & \end{array} \qquad \sum e_Q = d$$

(Note residue field $k = \overline{k} \implies f = 1$ always) Compare with algebraic number theory

$$\begin{array}{c} K \\ d \big\uparrow \\ \mathbb{Q} \end{array} \qquad \begin{array}{ccc} Q_1 & Q_2 & \cdots \\ \diagdown & | & \diagup \\ & \mathfrak{p} & \end{array} \qquad \sum e_i f_i = d$$

2.1.4 Frobenius map

If char $k = p$ then $a \mapsto a^p$ is a bijection (in fact, isomorphism) $k \to k$
$0 = x^p - b = (x - \sqrt[p]{b})^p$ has one solution in k
So

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

is a bijection on points
But $k(x^p) \hookrightarrow k(x)$ has index p, so $\deg\phi = p$.
Every point is ramified, $e_Q = p \ \ \forall Q \in \mathbb{P}^1$

Can do this for every curve:

Definition 2.1.24

$$C : \quad \begin{cases} f_1 = 0 \\ \vdots \\ f_m = 0 \end{cases} \qquad \subseteq \mathbb{P}^n \text{ curve}$$

$$C^{(p)} : \quad \begin{cases} f_1^{(p)} = 0 \\ \vdots \\ f_m^{(p)} = 0 \end{cases}$$

$f^{(p)} := f$ with all coefficients raised to p-th powers
The p-th power Frobenius map is:

$$\begin{aligned} \mathrm{Frob}_p : C &\to C^{(p)} \\ (x_0 : \cdots : x_n) &\mapsto (x_0^p : \cdots : x_n^p) \end{aligned}$$

Example 2.1.25
$C : y^2 = x^3 + Ax + B, A, B \in k$
$(y^2)^p = (x^3 + Ax + B)^p$
$(y^p)^2 = (x^p)^3 + A^p(x^p) + B^p \quad \Rightarrow \quad (x^p, y^p) \in C^{(p)}$

It is a bijection on points, $e_Q = p \quad \forall Q \in C$ (some uniformiser computation)

Alternatively, by definition of $e_Q : Q = a \in \mathbb{A}^1, P = a^p$,
$\phi^*(x - a^p) = x^p - a^p = (x - a)^p$ has valuation p at Q

So deg $\mathrm{Frob}_p = p$

Remark. $k \supseteq \mathbb{F}_p$
Say $f_i \in \mathbb{F}_p[x_1, \dots, x_n]$, i.e. C is defined over $\mathbb{F}_p$. Then

(1) $C = C^{(p)} \qquad (a \in \mathbb{F}_p \Leftrightarrow a^p = a)$

(2) $C(\mathbb{F}_p) := \{(a_1, \dots, a_n) \in C | a_i \in \mathbb{F}_p\}$
$=$ fixed points of $\mathrm{Frob}_p : C \to C$
$=$ fixed points of $(\mathrm{Frob}_p)^n$

This leads to Lefschetz trace formula, etale cohomology, Weil conjecture

Lemma 2.1.26
K f.g. field of tr.deg.1 over k, char $k = p$, $K' := K(\{\sqrt[p]{f}\}_{f \in K})$. Then

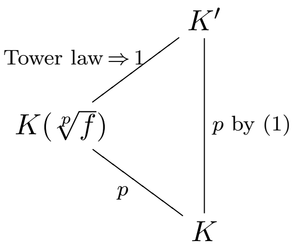
(1) $[K' : K] = p$

(2) $K' = K(\sqrt[p]{f})$ for any $f \in K$ with $\sqrt[p]{f} \notin K$

Proof

(1) $K = k(C), K' = k(C^{(1/p)}), C^{(1/p)} \xrightarrow{\mathrm{Frob}_p} C$ has degree p, $[K' : K] = p$

(2)



□

Definition 2.1.27
Finite field extension K'/K is <u>separable</u> if $\forall \alpha \in K'$ is a simple root of an irreducible polynomial $f(x) \in K[x]$
<u>Inseparable</u> otherwise.

Fact:

(1) char $K = 0 \quad \Rightarrow \quad$ every K'/K is separable

(2) char $K = p \quad \Rightarrow \quad K(\sqrt[p]{\alpha}), \alpha \in K, \sqrt[p]{\alpha} \notin K$ is inseparable.
Every F/K factors
$$K \underset{\text{separabe}}{\subseteq} K' \underset{\text{purely inseparable}}{\subseteq} F$$
<u>purely inseparable</u> means that the (inseparable) extension is obtained by successively adjoining p-th roots
<u>separable degree</u> $\deg_s F/K := [K' : K]$

(3) $F/M/K$ finite. Then $\deg_s F/K = \deg_s F/M \deg_s M/K$

(4) F/K separable $\Leftrightarrow$ $F = K(\alpha), \alpha$ root of some irred. polyn. $f(x) \in K[x]$ with $f'(\alpha) = 0 (\Leftrightarrow f' \not\equiv 0)$

For $\phi : C \to C'$ non-constant, we say ϕ is separable if $k(C)/\phi^* k(C')$ is.

Corollary 2.1.28

(1) Every ϕ factors $C \xrightarrow{(\mathrm{Frob}_p)^n} C^{(p^n)} \xrightarrow{\phi_0} C'$ with ϕ_0 separable

(2) Every C admits separable $\phi : C \twoheadrightarrow \mathbb{P}^1$ (i.e. $k(C) \supseteq k(t)$ separable extension)

(3) If $\phi : C \twoheadrightarrow C'$ separable, only finitely many points are ramified ($\Rightarrow$ In general, If $\phi : C \twoheadrightarrow C'$ arbitrary, all but finitely many $P \in C'$ have exactly $\deg_s \phi$)

Proof

(1) Fact (2) + Lemma

(2) Let $f = t_p \in k(C)$ be a unit at (some) $P \in C$; check that $f : C \to \mathbb{P}^1$ is separable

(3) May assume $C' = \mathbb{P}^1$ by Fact (2).
Write $k(C) = k(t)(\alpha)$, α root of irred. polyn. $f \in k[t]$
Then {ramified points} $\subseteq$ {those where $f'(\alpha) = 0, l \neq 0$}

$\square$

2.1.5 Divisors of functions

Definition 2.1.29
For $f \in k(C)^\times$ define divisor of f

$$\begin{aligned}\mathrm{div}(f) = (f) &:= \sum_{P \in C} v_P(f) \cdot (P) \\ &= f^*((0)) - f^*((\infty))\end{aligned}$$

Remark. Has degree $\deg f - \deg f = 0$

Definition 2.1.30
$D, D' \in \mathrm{Div}(C)$ are linearly equivalent, write $D' \sim D$, if $D - D' = \mathrm{div}(f)$ for some $f \in k(C)^\times$
$D \sim 0$ are called principal divisors

Definition 2.1.31

$$\begin{aligned}\mathrm{Pic}^0(C) &:= \mathrm{Div}^0(C)/\sim \\ \mathrm{Pic}(C) &:= \mathrm{Div}(C)/\sim \;\cong \mathrm{Pic}^0(C) \times \mathbb{Z}\end{aligned}$$

In algebraic number theory

points	$\leftrightarrow$	prime ideals
Div(C)	$\leftrightarrow$	group of fractional ideals
Principal	$\leftrightarrow$	Principal ideals
Pic(C)	$\leftrightarrow$	Class group

Example 2.1.32
$C = \mathbb{P}^1$. For $P, Q \in \mathbb{A}^1 \subseteq \mathbb{P}^1$
$(P) \sim (Q)$ $\quad$ $[\ (P) - (Q) = \operatorname{div} \frac{x-P}{x-Q}\ ]$
$\Rightarrow \quad \mathrm{Pic}^0(\mathbb{P}^1) = \{0\}$ and deg define isomorphism $\mathrm{Pic}(\mathbb{P}^1) \cong \mathbb{Z}$

Conversely, if C is a curve on which $(P) \sim (Q)$ for some $P, Q \in C$ then $C \cong \mathbb{P}^1$
Proof: Take $f \in k(C)^\times$ s.t. $\operatorname{div}(f) = (P) - (Q)$. Then $f : C \to \mathbb{P}^1$ has only one pole at Q and so has degree $1 \Rightarrow C \cong \mathbb{P}^1$

2.1.6 Differentials

Definition 2.1.33
A (rational) differential on a non-singular curve C is a formal finite sum

$$\omega = \sum_i f_i \, dg_i, \quad f_i, g_i \in k(C)$$

subject to relations

$$\begin{aligned} d(g_1 g_2) &= g_1 dg_2 + g_2 dg_1 \\ d(g_1 + g_2) &= dg_1 + dg_2 \\ da &= 0 \ \forall a \in k \subseteq k(C) \end{aligned}$$

Example 2.1.34
(char $k \neq 2$) $C : x^2 + y^2 = 1$
we have, for example, $d(x^2 y) = x^2\, dy + 2xy\, dx$
Generally, any $f\, dg = f \cdot {g_x}' \cdot dx + f \cdot {g_y}' \cdot dy$
$\Rightarrow$ can express any w as $f_1\, dx + f_2\, dy$

Also $x^2 + y^2 = 1$
$\Rightarrow \quad 2x\, dx + 2y\, dy = 0$
$\Rightarrow \quad dy = -(x/y) dx$
$\Rightarrow \quad \forall \omega \ \ \exists! f \in k(C)$ s.t. $\omega = f\, dx$

$$\Rightarrow \qquad \{\text{differentials on } C\} = k(C) \cdot dx$$

Similarly, for any C, we have the 1-dimensional $k(C)$-vector space

$$\{\text{differentials on } C\} \quad = \quad k(C) \cdot df$$

For any f s.t. $K(C)/k(f)$ is separable, let ω be a differential on C. For $P \in C$, write

$$\omega = f \cdot dt_P, \qquad t_P \text{ uniformiser at } P$$

and define

$$\begin{aligned} v_P(\omega) &:= v_P(f) && \text{(independent of the choice of } t_P) \\ \operatorname{div}(\omega) &:= \sum_P v_P(\omega)\,(P) && \text{(finite sum)} \end{aligned}$$

Because any w, w' differ by a function,

$$\omega = f \cdot \omega' \quad \Rightarrow \quad \operatorname{div}(\omega) = \operatorname{div}(\omega') + \operatorname{div}(f) \sim \operatorname{div}(\omega')$$

So divisors of differential forms span a class $\mathbb{K} \in \mathrm{Pic}(C)$, the canonical class

ω regular at P if $v_P(w) \geq 0$
ω regular if all $v_P(w) \geq 0$ (i.e. $\operatorname{div}(w) \geq 0$)

2.1.7 Riemann-Roch

Definition 2.1.35
The <u>complete linear system</u> of a divisor D

$$\begin{array}{rcll} \mathcal{L}(D) & := & \{f \in k(C) \mid \operatorname{div}(f) + D \geq 0\} & k\text{-vector space} \\ & \leftrightarrow & \{D' \in \operatorname{Div}(C) \mid D' \geq 0 \text{ and } D \sim D'\} & \end{array}$$

(via $f \mapsto D' = D + \operatorname{div}(f)$)

Remark. $D \sim D' \Rightarrow \mathcal{L}(D) \cong \mathcal{L}(D')$

Example 2.1.36
$\mathcal{L}(0) = \{f \in k(C) \mid \operatorname{div}(f) \geq 0\}$ functions with no poles
$= k$ (f non-constant $\Rightarrow f : C \twoheadrightarrow \mathbb{P}^1$ hits ∞)

Example 2.1.37
$\mathcal{L}(3(P)) = \{f \in k(C) \mid \operatorname{div}(f) \geq -3(P)\}$ functions with pole of order ≤ 3 at P and no other poles

(Generally, "$\mathcal{L}(D)$ = functions with a pole at most at D")

<u>Exercise</u>:

(1) $\mathcal{L}(D) = 0$ when $\deg D < 0$ (equivalently, when $\deg D = 0$ and $D \nsim 0$)
(2) $\dim_k \mathcal{L}(D + P) \leq \dim_k \mathcal{L}(D) + 1$ ($\Rightarrow \dim_k \mathcal{L}(D) < \infty \ \forall D$)

Definition 2.1.38
The <u>genus of C</u> is

$$g(C) := \dim_k \mathcal{L}(\mathbb{K}) = \dim_k \mathcal{L}(\operatorname{div}(\omega)) \text{ for any } \omega \neq 0$$

<u>Fact</u> Non-constant $\phi : C \to C'$ induces pullback map on differential forms:

$$\omega = f dg \rightsquigarrow \phi^*\omega := (\phi^* f) d(\phi^* g)$$

and therefore

$$\phi^* : \mathcal{L}(\mathbb{K}_{C'}) \to \mathcal{L}(\mathbb{K}_C)$$

Not hard to see that ϕ^* injective $\Leftrightarrow \phi$ separable
and $\phi^* = 0 \Leftrightarrow \phi$ inseparable

Corollary 2.1.39
$g(C) \geq g(C')$ always (i.e. genus goes down under non-constant maps)

Remark. A non-singular plane curve $C \subseteq \mathbb{P}^2$, $C : f(x, y) = 0$ has genus

$$\begin{array}{rcll} g & = & \frac{(d-1)(d-2)}{2} & d = \deg f \\ & = & 0 & \text{for linear and conics} \\ & = & 1 & \text{for cubics} \\ & = & 3 & \text{for quartics} \end{array}$$

In particular, genus 2 curves (they exist) cannot embedded in $\mathbb{P}^2$

Theorem 2.1.40 (Riemann-Roch)
C non-singular curve. For every $D \in \operatorname{Div}(C)$

$$\dim \mathcal{L}(D) - \dim \mathcal{L}(\mathbb{K} - D) = \deg D - g + 1$$

Corollary 2.1.41

- $\deg \mathbb{K} = 2g - 2$ (Proof: Take $D = \mathbb{K}$)
- If $\deg D > 2g - 2$, then $\dim \mathcal{L}(D) = \deg D - g + 1$ (Proof: Since $\deg(\mathbb{K} - D) < 0$)

Lemma 2.1.42 (Classification of Curve of Genus 0)
A non-singular curve C has genus 0 $\Leftrightarrow$ $C \cong \mathbb{P}^1$

Proof

$\underline{\Leftarrow}$: $\mathbb{P}^1$ genus 0: uniformisers

$$\begin{aligned} t_a &= x - a, \quad a \in \mathbb{A}^1 \\ t_\infty &= \frac{1}{x} \end{aligned}$$

$$\begin{aligned} dx &= d(x-a) && \text{valuation 0 at } a \in \mathbb{A}^1 \\ dx &= d\left(\frac{1}{t_\infty}\right) = -\frac{1}{t_\infty^2} \cdot dt_\infty && \text{valuation } -2 \text{ at } \infty \end{aligned}$$

$\Rightarrow$ $\operatorname{div}(dx) = -2(\infty), \deg = -2 = 2g(\mathbb{P}^1) - 2$ (by Corollary)
$\Rightarrow$ $g(\mathbb{P}^1) = 0$

$\underline{\Rightarrow}$: Suppose a curve C has genus 0. Take $P \in C, D = (P)$
$\deg D > 2g - 2 = -2$ $\Rightarrow$ $\dim \mathcal{L}((P)) = 1 - 0 + 1 = 2$
$\Rightarrow$ $\mathcal{L}((P)) \supsetneq \mathcal{L}(0) = k$ $\Rightarrow$ $\exists f \in k(C)$ with a simple pole at P and no other poles
$\operatorname{div}(f) = -(P) + (Q)$ for some $Q \in C$
$\Rightarrow$ $f : C \xrightarrow{\sim} \mathbb{P}^1$ is an isom.

□

Corollary 2.1.43
k algebraically closed, every conic is isomorphic to $\mathbb{P}^1$

2.2 Cubics

Suppose char $k \neq 2, 3$, $C \subseteq \mathbb{P}^2$ non-singular of the form

$$\begin{aligned} C : y^2 &= x^3 + ax + b \qquad a, b \in k \\ &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \qquad \alpha_i \in k \end{aligned}$$

$C \cap \mathbb{A}^2$ non-singular $\Leftrightarrow$ α_i are distinct

(see picture for the 3 different cases)

Exercise: When α_i not distinct, C is singular, $k(C) \cong k(\mathbb{P}^1)$ (C has "geometric genus 0")

To get a morphism $\begin{array}{ccc} \mathbb{P}^1 & \to & C \\ t & \mapsto & P \end{array}$ of degree 1 (see picture)

Recall

$$\underset{(x:y:z)}{\mathbb{P}^2} = \underset{(x:y:1)}{\mathbb{A}^2_{z=1}} \cup \underset{(x:y:0)}{\mathbb{P}^1_{z=0}} \quad \leftarrow \text{line at } \infty$$

$$\begin{array}{ccc} C \subseteq \mathbb{P}^2 & : & y^2 z = x^3 + axz^2 + bz^3 \\ \underbrace{C \cap \mathbb{P}^1_{z=0}}_{\substack{\text{has unqiue pt.} \\ \mathcal{O} = (0:1:0) \\ \text{point at infinity}}} & : & 0 = x^3 + 0 + 0 \Rightarrow \begin{cases} x = 0 \\ z = 0 \\ y = 1 \end{cases} \end{array}$$

In the $y = 1$ chart
$C : z = x^3 + axz^2 + bz^3$
$\mathcal{O} = (0, 0)$ (see picture)
$g(x, z) = z - x^3 - axz^2 - bz^3$
$\frac{dg}{dz}\Big|_{(0,0)} = 1 \neq 0$
$\Rightarrow$ C non-singular at 0

So, $C \subseteq \mathbb{P}^2$ non-singular $\Leftrightarrow$ $C \cap \mathbb{A}^2_{z=1}$ non singular $\Leftrightarrow$ α_i distinct

Differentials:
e.g. $\text{div}(dx) = (P_1) + (P_2) + (P_3) - 3(0)$ (exercise: check)
this has degree $0 = 2g - 2$ (by Corollary of Riemann-Roch)
$\Rightarrow$ C has genus 1 ($= \frac{(3-1)(3-2)}{2}$ as expected)

$\text{div}(y) = (P_1) + (P_2) + (P_3) + \lambda(0)$ some λ
this has degree 0 $\Rightarrow \lambda = -3$
$\Rightarrow$ $\text{div}(\frac{dx}{y}) = 0$ since $w = \frac{dx}{y}$ has no zeroes, no poles
In fact, $\mathbb{K} = \langle \frac{dx}{y} \rangle$ as it is 1-dimensional over k by definition of genus.

Definition 2.2.1
An elliptic curve , $(E, \mathcal{O})$, is a non-singular projective curve E of genus 1 with a marked point $\mathcal{O}$

Example 2.2.2
(char $k \neq 2, 3$)

$$y^2 = x^3 + ax + b \qquad \mathcal{O} = (0 : 1 : 0)$$

is an elliptic curve in (simplified) Weierstrass form (if $\Delta_E = 16\Delta_{\text{RHS}} = -16(4a^3 + 27b^2) \neq 0$)

In any characteristic, have (generalised) Weierstrass form

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

(char $k \neq 2, 3 \Rightarrow$ complete the square in LHS, complete the cube in RHS, then we get simplified form)

Theorem 2.2.3
Every elliptic curve is isomorphic to one in Weierstrass form

Proof
$(E, \mathcal{O})$ elliptic curve.

$$\begin{array}{rcl}
\dim \mathcal{L}(n(0)) & = & n-1+1 \ = \ n \ \text{ for } n \geq 1 \\
\mathcal{L}(1(0)) & = & k \ = \ \langle 1 \rangle \text{ constant} \\
\mathcal{L}(2(0)) & = & \langle 1, x \rangle \ \text{ where } x \in k(C) \text{ with double pole at } 0 \\
\mathcal{L}(3(0)) & = & \langle 1, x, y \rangle \ \text{ where } y \in k(C) \text{with triple pole at } 0 \\
 & & \qquad\qquad \text{Note that } y \notin k(x) \quad \text{(elements of } k(x) \text{ has even order)} \\
\mathcal{L}(4(0)) & = & \langle 1, x, y, x^2 \rangle \\
\mathcal{L}(5(0)) & = & \langle 1, x, y, x^2, xy \rangle \\
\underbrace{\mathcal{L}(6(0))}_{\text{dim=6}} & \ni & \underbrace{1, x, y, x^2, xy, \qquad \overbrace{x^3, y^2}^{\text{pole of order 6 at } \mathcal{O}}}_{\text{7 functions}}
\end{array}$$

$\Rightarrow$ must have a linear relation, involving both x^3, y^2

$$\underbrace{\alpha y^2}_{\neq 0} + \underbrace{\beta x^3}_{\neq 0} + \cdots = 0$$

Rescaling x, y may make $\alpha = 1, \beta = -1$

$$\begin{array}{rc}
 & y^2 - x^3 + \cdots = 0 \\
y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 & \text{for some } a_i \in k
\end{array}$$

Let $C \subseteq \mathbb{P}^2_{x,y,z}$ by a curve given by this equation

$$\begin{array}{rcl}
k(C) = ff(\dfrac{k[x,y]}{y^2 + \cdots = x^3 + \cdots}) & \hookrightarrow & k(E) \\
x & \mapsto & x \\
y & \mapsto & y
\end{array}$$

$[k(x,y) : k(x)] = 2$
This defines a map $E \to C$
$x : E \to \mathbb{P}^1$ has $x^*((\infty)) = 2(\mathcal{O})$ (as $\mathcal{O} \mapsto \infty$), so this map has degree 2

$$\begin{array}{ccc}
k(x) & \xrightarrow{\quad 2 \quad} & k(E) \\
 {\scriptstyle 2} \searrow & & \nearrow {\scriptstyle \cong} \\
 & k(x,y) = k(C) &
\end{array}$$

the lower left map is non-trivial, $y \in k(x)$ and its degree ≤ 2 by equation $y^2 + \cdots = x^3 + \cdots$
$\Rightarrow$ $k(C) \hookrightarrow k(E)$ is isomorphism, i.e. $E \to C$ has degree 1

If C is singular, then $k(C) \cong k(\mathbb{P}^1)$, and then $E \cong \mathbb{P}^1$ #
So C is non-singular □

Corollary 2.2.4
Every elliptic curve admits a degree 2 map to $\mathbb{P}^1$, namely $E \xrightarrow{x} \mathbb{P}^1$
Such curves (of any genus) are called hyperelliptic

$g = 1$ $\Rightarrow$ hyperelliptic
$g = 2$ $\Rightarrow$ hyperelliptic (exercise)
$g = 3$ $\Rightarrow$ Either a plane quartic or hyperelliptic, but not both

Remark. If E, E' in Weierstrass form and $E \cong E'$ then

$$\begin{aligned}\mathcal{L}_E(2(\mathcal{O})) &\cong \mathcal{L}_{E'}(2(\mathcal{O}))\\ \mathcal{L}_E(3(\mathcal{O})) &\cong \mathcal{L}_{E'}(3(\mathcal{O}))\end{aligned}$$

(these are k-vector spaces), so

$$\begin{aligned}x_{E'} &= u^2x + r \qquad && u \in k^\times\\ y_{E'} &= u^3y + sx + t \qquad && r, s, t \in k\end{aligned}$$

i.e. Weierstrass form is unique up to such transformations

Suppose char $k \neq 2, 3$:
• Simplified Weierstrass form unique up to

$$\begin{aligned}x_{E'} &= u^2x \qquad && u \in k^\times\\ y_{E'} &= u^3y\end{aligned}$$

and

$$E : y^2 = x^3 + ax + b \quad \cong \quad E' : (y')^2 = (x')^3 + a'x' + b' \Leftrightarrow \begin{cases} a' = u^4a\\ b' = u^6b\end{cases}$$

$(\Delta_{E'} = -16(4a'^3 + 27b'^2) = u^{12}\Delta_E)$

Definition 2.2.5
<u>j-invariant</u> $j(E) := 1728\frac{(-4a)^3}{\Delta}$

Example 2.2.6
- $y^2 = x^3 + ax$ has $j = 1728$
- $y^2 = x^3 + b$ has $j = 0$

Proposition 2.2.7

(1) $E \cong E' \Leftrightarrow j(E) = j(E')$

(2) For any $j \in k$ $\exists E$ s.t. $j(E) = j$, hence

$$\{\text{elliptic curves (up to isom.)}/k\} \overset{\text{1:1 map}}{\underset{}{\overset{j(E)}{\longleftrightarrow}}} k$$

Proof

(1)

$$\begin{aligned}\begin{matrix}a' = u^4a\\ b' = u^6b\end{matrix} &\Leftrightarrow \sqrt[4]{\frac{a'}{a}} = \sqrt[6]{\frac{b'}{b}}\\ &\Leftrightarrow \left(\frac{b'}{b}\right)^2 = \left(\frac{a'}{a}\right)^3\\ &\Leftrightarrow \frac{4a^3 + 27b^2}{a^3} = \frac{4(a')^3 + 27(b')^2}{(a')^3}\\ &\Leftrightarrow j(E) = j(E')\end{aligned}$$

Do $d = 0, b = 0$ separately $(j = 0, 1728)$

(2) $y^2 + xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728}$ works for $j \neq 0, 1728$

$\square$

Corollary 2.2.8
The automorphism group $\mathrm{Aut}(E) = \{$ morphisms $\phi : E \to E$ s.t. $\phi(\mathcal{O}) = \mathcal{O}\}$ is

- $\mathbb{Z}/2\mathbb{Z}$ for $y^2 = x^3 + ax + b, a, b \neq 0$ $(j \neq 0, 1728)$
- $\mathbb{Z}/4\mathbb{Z}$ for $y^2 = x^3 + ax$ $(j = 1728)$
- $\mathbb{Z}/6\mathbb{Z}$ for $y^2 = x^3 + b$ $(j = 0)$

Proof

$$\begin{aligned}\mathrm{Aut}(E) &= \left\{ u \in k^\times \middle| \begin{array}{l} u^4 a = a \\ u^6 b = b \end{array} \right\} \\ &= \begin{cases} \{\pm 1\} & ab \neq 0 \\ \langle i \rangle & b = 0 \\ \langle \zeta_6 \rangle & a = 0 \end{cases}\end{aligned}$$

For most elliptic curves, $(x, y) \to (x, -y)$ is the only automorphism. $\square$

Remark. If char $k = 2, 3$

- Δ, j complicated polynomial, rational function of $a_1, \ldots, a_6$
- a_i change $a_i{}' = u^i a_i + \cdots$
- Proposition still holds
- $|\mathrm{Aut}(E)| \leq 24$

2.2.1 Group Law

Over $\mathbb{C}$: $E(\mathbb{C}) \cong \mathbb{C}/\text{lattice}$, group law = addition

Recall $\mathrm{Pic}^0(E) = \dfrac{\text{divisors of deg } 0}{\text{divisors of functions}}$, e.g. $\mathrm{Pic}^0\,\mathbb{P}^1 = \{0\}$
E elliptic curve

Theorem 2.2.9
The following map is a bijection

$$\begin{aligned} E &\to \mathrm{Pic}^0(E) \\ P &\mapsto (P) - (\mathcal{O}) \end{aligned}$$

Proof
Injective $\hookrightarrow$:
If $(P) - (\mathcal{O}) \sim (Q) - (\mathcal{O})$, then $(P) \sim (Q) \Rightarrow E \cong \mathbb{P}^1$ $\quad \#$ unless $P = Q$

Surjective $\twoheadrightarrow$:
Take $D \in \mathrm{Div}^0(E)$. By Riemann-Roch,
$\dim \mathcal{L}(\underbrace{D + (\mathcal{O})}_{\deg=1}) = 1$
$\Rightarrow \quad \exists f$ s.t. $\mathrm{div}(f) \geq \underbrace{-D - (\mathcal{O})}_{\deg=-1}$
$\Rightarrow \quad \mathrm{div}(f) = -D - (\mathcal{O}) + (P)$ for some $P \in E$
$\Rightarrow \quad D \sim (P) - (\mathcal{O})$ $\square$

Corollary 2.2.10
E has a structure of an abelian group

Proof
$\mathrm{Pic}^0(E)$ has structure of abelian group, apply theorem. $\square$

$E: \quad y^2 = x^3 + ax + b$

Identity $= \mathcal{O}$ because $(\mathcal{O}) - (\mathcal{O}) = 0 \in \mathrm{Pic}^0(E)$

Inverse of $P = (x_1, y_1)$ is $P' = (x_1, -y_1)$
$\mathrm{div}(x - x_1) = (P) + (P') - 2(\mathcal{O}) \Rightarrow (P) - (\mathcal{O}) \sim -[(P') - (\mathcal{O})]$

Addition $P = (x_1, y_1), Q = (x_2, y_2), P \neq -Q; P, Q \neq 0$
$P + Q + R = 0$ in $E \quad \Leftrightarrow \quad P + Q = (-R)$

Need function with

$$\begin{aligned} \mathrm{div}(f) &= (P) - (\mathcal{O}) + (Q) - (\mathcal{O}) + (R) - (\mathcal{O}) \\ &= (P) + (Q) + (R) - 3(\mathcal{O}) \end{aligned}$$

$(\Rightarrow \quad f \in \mathcal{L}(3\,\mathcal{O}) = \langle 1, x, y \rangle)$
So $f = \alpha y + \beta x + \gamma, \qquad \alpha \neq 0$
So $f = 0$ is an equation of a line passing through P and Q (tangent to P if $P = Q$) with $R =$ third point of intersection

Explicitly, solve

$$\begin{cases} y^2 = x^3 + ax + b & \text{elliptic curve} \\ y = \kappa(x - x_1) + y_1 & \text{line} \end{cases}$$

with

$$\kappa = \text{ slope } = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & P = Q \end{cases}$$

$(\kappa x + \cdots)^2 = x^3 + ax + b$
$x^3 - \kappa^2 x^2 + \cdots = 0$ and $\sum$roots $= \kappa^2$
$\Rightarrow \quad$ 3rd root x, y defining $R = (x, y)$ is

$$\begin{cases} x = \kappa^2 - x_1 - x_2 \\ y = \kappa(x - x_1) + y_1 \end{cases}$$

Hence,

$$(x_1, y_1) + (x_2, y_2) = (\kappa^2 - x_1 - x_2, -\kappa(x - x_1) - y_1)$$

Important: This shows (+some extra work when $P = \pm Q$ see Silverman Theorem III 3.6) that

$$\begin{aligned} \text{inverse} : E &\xrightarrow{i} E \\ \text{addition} : E \times E &\xrightarrow{\mu} E \end{aligned}$$

are morphisms, i.e. given by rational functions that are defined everywhere
That is, E is algebraic group (= group variety = group object in the category of varieties)

In particular, translation maps

$$\begin{aligned} \tau_Q : E &\to E \\ P &\mapsto P + Q \end{aligned}$$

are morphisms. (Proof: This is just composition $\mu \circ (\mathrm{id}, Q)$)

Corollary 2.2.11

$$\left\{ \begin{array}{c} \text{isomorphisms} \\ E \to E \text{ as a curve} \end{array} \right\} \cong \{\text{translations}\} \rtimes \mathrm{Aut}(E)$$
$$\cong E \rtimes \text{ finite groups}$$
$$\mathrm{Iso}(C,C) \cong \begin{cases} PGL_2(k) & g=0 \\ E \rtimes \text{finite group} & g=1 \\ \text{finite group} & g \geq 2 \end{cases}$$

Exercise: The only (affine or projective) curves that are algebraic groups are

- Additive group $\mathbb{G}_a = \mathbb{P}^1 \setminus \{\infty\} = (k, +)$
- Multiplicative group $\mathbb{G}_m = \mathbb{P}^1 \setminus \{0, \infty\} = (k^\times, \times)$
- Elliptic curves (the only projective algebraic groups in dimension 1)

Remark. genus(C)=g $\Rightarrow$ $\mathrm{Pic}^0(C)$ has a structure of a g-dimensional abelian variety (i.e. projective algebraic group, by definition) the Jacobian of C, denoted $\mathrm{Jac}(C)$

Fixing $P_0 \in C$, define the Abel-Jacobi map

$$\begin{array}{rcl} C & \to & \mathrm{Jac}(C) \\ P & \mapsto & (P) - (P_0) \end{array}$$

injective when $g > 0$, $\cong$ when $g = 1$. Every $D \in \mathrm{Pic}^0(C)$ is $\sim (P_1) + \cdots (P_g) - g(P_0)$, usually unique such.

2.2.2 Isogenies

Definition 2.2.12
An isogeny between elliptic curves is a morphism $\phi : E \to E'$ s.t. $\phi(\mathcal{O}) = \mathcal{O}$

Example 2.2.13

$$\begin{array}{rcl} [0] : E & \to & E \\ P & \mapsto & \mathcal{O} \end{array} \qquad \text{zero isogeny}$$

we let $\deg[0] := 0$, so $\deg(\phi \circ \psi) = \deg\phi \deg\psi$ for all isogenies

Example 2.2.14
Elements of $\mathrm{Aut}(E)$ are isogenies (of degree 1), e.g.

$$\begin{array}{rcl} [1] : E & \to & E \\ P & \mapsto & P \\ [-1] : E & \to & E \\ P & \mapsto & -P \end{array}$$

Example 2.2.15
Multiplication-by-m maps

$$\begin{array}{rcll} [m] : E & \to & E & \\ P & \mapsto & \underbrace{P + \cdots + P}_{m \text{ times}} & (m > 0) \\ P & \mapsto & \underbrace{(-P) + \cdots (-P)}_{m \text{ times}} & (m < 0) \end{array}$$

Example 2.2.16
([2] when char $k \neq 2, 3$)
$E: \; y^2 = x^3 + ax + b$

$$\begin{array}{rcll} [2] : E & \to & E & \\ P = (x, y) & \mapsto & P + P = (\kappa^2 - 2x, -\kappa(\kappa^2 - 2x - x) - y) & (\kappa = \dfrac{3x^2 + a}{2y}) \\ & & = \left(\underbrace{\dfrac{\frac{1}{2}(x^2 - a)^2 - 2bx}{x^3 + ax + b}}_{\psi(x)}, \cdots \right) & \end{array}$$

This has degree 4:

$$\begin{array}{ccc} E & \xrightarrow{[2]} & E \\ {\scriptstyle x,\deg=2}\downarrow & & \downarrow{\scriptstyle x,\deg=2} \\ \mathbb{P}^1 & \xrightarrow{\psi(x)} & \mathbb{P}^1 \end{array}$$

$\Rightarrow \quad \deg[2] = \deg(\psi : \mathbb{P}^1 \to \mathbb{P}^1) = \max(\deg(\text{numerator}), \deg(\text{denominator})) = 4$

E.g.: $[2]^*(\mathcal{O}) = (\mathcal{O}) + (T_1) + (T_2) + (T_3)$

Corollary 2.2.17
$[m] \neq [0] \quad 0 \neq m \in \mathbb{Z}$

Proof
In char $k \neq 2, 3$:
$[2] \neq [0]$
$[n] \neq [0]$ for n odd since $[n]T_1 = T_1$
$[mn] = [m] \circ [n]$ □

Theorem 2.2.18
An isogeny $\phi : E \to E'$ is a group homomorphism.

Proof
$\phi = [0]$ is a homomorphism, so assume ϕ is non-constant

Then recall: ϕ induces

$$\begin{array}{rcl} \phi_* : \mathrm{Div}(E) & \to & \mathrm{Div}(E') \\ (Q) & \mapsto & (\phi(Q)) \\ \phi^* : \mathrm{Div}(E') & \to & \mathrm{Div}(E) \\ (P) & \mapsto & \sum\limits_{\phi(Q)=P} e_Q(Q) \end{array}$$

<u>Fact</u>: (For all curves) Both map principal divisors to principal divisors:

$$\begin{array}{rcl} \phi^*(\mathrm{div}(f)) & = & \mathrm{div}(\phi^* f) \\ \phi_*(\mathrm{div}(f)) & = & \mathrm{div}(N(f)), \quad N(f) := \mathrm{Norm}_{k(E)/\phi^* k(E_2)}(f) \end{array}$$

Now $P + Q = R$ on $E \quad \Rightarrow \quad (P) - (\mathcal{O}) + (Q) - (\mathcal{O}) \sim (R) - (\mathcal{O})$
$\Rightarrow$ (by fact above) $(\phi(P)) - (\mathcal{O}) + (\phi(Q)) - (\mathcal{O}) \sim (\phi(R)) - (\mathcal{O})$
$\Rightarrow \quad \phi(P) + \phi(Q) = \phi(R) \quad$ in E' □

Corollary 2.2.19

(1)

$$\mathrm{Hom}(E_1, E_2) := \{ \text{ isogenies } E_1 \to E_2\}$$

is a torsion-free abelian group (will see later that $\cong \mathbb{Z}^r$, some $r \leq 4$)

(2) $\mathrm{End}(E) := \mathrm{Hom}(E, E)$ is a (not necessarily commutative) integral domain of characteristic 0, $\mathrm{Aut}(E) = \mathrm{End}(E)^\times$ its units

Proof

(1) $\phi + \psi :=$ composition $\begin{array}{ccccccc} E & \xrightarrow{\Delta} & E \times E & \xrightarrow{(\phi,\psi)} & E \times E & \xrightarrow{\mu} & E \\ P & \mapsto & (P, P) & \mapsto & (\phi(P), \psi(P)) & & \end{array}$

$\phi + \psi$ =morphism

Homomorphisms between abelian groups are abelian groups:

$$m\phi = 0 \Rightarrow [m] \circ \phi = [0] \Rightarrow [m] = [0] \text{ or } \phi = 0$$

(2) $\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathrm{End}(E) \\ m & \mapsto & [m] \end{array}$ injective ring hom $\Rightarrow$ char. 0

$\phi\psi = [0] \Rightarrow \phi = [0]$ or $\psi = [0]$

□

Most of the time $\mathrm{End}(E) = \mathbb{Z}$ (only $[m]$'s)

Definition 2.2.20
We say E has <u>complex multiplication</u> if $\mathrm{End}(E) \supsetneq \mathbb{Z}$ (this is very special)

Example 2.2.21
$E: \ y^2 = x^3 + x$ over $\mathbb{C}$ has $\mathrm{End}(E) \cong \mathbb{Z}[i]$

$$\begin{array}{rcl} [1] : (x, y) & \mapsto & (x, y) \\ [i] : (x, y) & \mapsto & (-x, iy) \end{array}$$

$[i]^2 = [-1] \Rightarrow \quad \mathrm{End}(E) \supseteq \mathbb{Z}[i]$
(for $\subseteq$, we will get from $\mathbb{C}$)

Example 2.2.22
$E: \ y^2 + y = x^3$ over $\overline{\mathbb{F}_2}$ has $\mathrm{End}(E) \cong \mathbb{Z} + \mathbb{Z}\, i + \mathbb{Z}\, j + \mathbb{Z}\, \frac{1+i+j+k}{2}$
where $i^2 = j^2 = k^2 = 1, ij = k, jk = i, ki = j$

$$[i]: \begin{array}{ccc} x & \mapsto & x+1 \\ y & \mapsto & y+x+\zeta \end{array} \qquad [j]: \begin{array}{ccc} x & \mapsto & x+\zeta^2 \\ y & \mapsto & y+\zeta x+\zeta \end{array} \qquad [k]: \begin{array}{ccc} x & \mapsto & x+\zeta \\ y & \mapsto & y+\zeta^2 x+\zeta \end{array}$$

$$[-1]: \begin{array}{ccc} x & \mapsto & x \\ y & \mapsto & y+1 \end{array}$$

$\mathrm{Frob}_2 : (x \mapsto x^2, y \mapsto y^2) = [j] + [k], (\mathrm{Frob}_c)^2 = [-2] \quad \Rightarrow \quad [2]$ inseparable

2.2.3 Invariant Differential

Definition 2.2.23
A differential $w \neq 0$ on E is an invariant differential if $\mathrm{div}(\omega) = 0$

Recall: $g(C) = \dim \mathcal{L}(\mathbb{K}) = 1$
$\Rightarrow \ \exists \omega$ with no poles, $\deg \mathbb{K} = 2g - 2 = 0$
$\Rightarrow$ has no zeroes either
$\Rightarrow$ such ω exist up to $\omega \mapsto \alpha\omega$ $(\alpha \in k^\times)$

Example 2.2.24
$E: \ y^2 = x^3 + ax + b \qquad \omega = \frac{dx}{y}$
For E in generalised Weierstrass form, $\omega = \frac{dx}{2y+a_1x+a_3}$

Theorem 2.2.25

(1) $\tau_P^*\omega = \omega \quad \forall P \in E$ and ω invariant differential on E (invariant differential invariant under translation)
(2) $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega \ \ \forall \phi, \psi : E \to E'$ isogenies, ω on E'
(3) $(\phi\chi)^*\omega = \chi^*(\phi^*\omega)$

Proof
Omitted (see Silvermann III 5.1, 5.2)
Idea: (1) uses brute force, (2) can get from formal groups (see later), (3) is easy given (1),(2) □

Remark. Recall: for $\phi : E \to E'$, non-zero isogeny
$\phi^*\omega \neq 0 \ \Leftrightarrow \ \phi^* : \mathcal{L}(\mathbb{K}_{E'}) \to \mathcal{L}(\mathbb{K}_E) \ \Leftrightarrow \ \phi$ separable
So, in particular,

$$\begin{array}{rcl} \mathrm{End}(E) & \to & k \\ \phi & \mapsto & \alpha = \dfrac{\phi^*\omega}{\omega} \qquad (\alpha \in k \text{ s.t. } \phi^*\omega = \alpha\omega) \end{array}$$

is a ring homomorphism, kernel = inseparable isogenies (but kernel=0 in char k=0)

Corollary 2.2.26
char $k = 0 \quad \Rightarrow \quad \mathrm{End}(E)$ is commutative

Corollary 2.2.27
$[m]^*\omega = m\omega$

(Check $m = 0, 1$. Then done by induction, using $(\phi + \psi)^*\omega$)

Corollary 2.2.28
For $m \neq 0$, $[m]$ separable $\quad \Leftrightarrow \quad$ char $k \nmid m$

Example 2.2.29
$E: \ y^2 = x^3 + x$ (over $\mathbb{C}$)

$$\begin{array}{rrcll} & [i]:(x,y) & \mapsto & (-x, iy) & \\ \Rightarrow & [i]^*\dfrac{dx}{y} & = & \dfrac{d(-x)}{iy} & = \ i\dfrac{dx}{y} \\ \Rightarrow & \mathrm{End}(E) & \hookrightarrow & \mathbb{C} & \\ & \bigcup\vert & & \bigcup\vert & \\ & \mathbb{Z}[i] & = & \mathbb{Z}[i] & \end{array}$$

<u>Exercise</u>: Describe $\mathrm{End}(E) = \mathbb{Z}\langle 1, i, j, \frac{1+i+j+k}{2}\rangle \to \overline{\mathbb{F}_2}$ for $E: \ y^2 + y = x^3$ over $\overline{\mathbb{F}_2}$

2.2.4 Galois Theory for Isogenies

If $\phi : E_1 \to E_2$ non-zero isogeny, then $\ker\phi = \phi^{-1}(\mathcal{O})$ is a finite subgroup

Example 2.2.30
$E: \ y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$
$\ker[2] = \{\mathcal{O}, T_1, T_2, T_3\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
Conversely, every finite subgroup $\Phi \subseteq E$ arises like this:

Theorem 2.2.31
$\phi : E_1 \to E_2$ separable isogeny, $\deg\phi = n \neq 0$

(1) ϕ is unramified, i.e. $|\phi^{-1}(P)| = n \ \ \forall P \in E_2$

(2) $K_1 = k(E_1)/\phi^* k(E_2) = K_2$ is Galois of degree n, and

$$\begin{array}{rcl} \ker(\phi^*) & \cong & \mathrm{Gal}(K_1/K_2) \\ f & \mapsto & \tau_P^* \end{array}$$

(this implies $\mathrm{Gal}(K_1/K_2)$ abelian)

(3) If $\psi : E_1 \to E_3$ another isogeny (may be inseparable) and $\ker\psi \supseteq \ker\phi$ then $\exists!\chi$ s.t. $\psi = \chi \circ \phi$

$$\begin{array}{ccc} E_1 & \xrightarrow{\phi} & E_2 \\ & \searrow^{\psi} & \downarrow {\scriptstyle \exists!\chi} \\ & & E_3 \end{array}$$

(4) Conversely, given any finite subgroup $\Phi \in E_1$, $\exists$ separable $\phi : E_1 \to$ some elliptic curve (denoted E_1/Φ) s.t. $\ker\phi = \Phi$

Proof

(1) By separability, $\exists\widetilde{P} \in E_2$ with n preimages $\widetilde{Q_1}, \dots, \widetilde{Q_n}$ by separability
If $\phi(Q) = P$ arbitrary, then

$$\underbrace{Q + (\widetilde{Q_1} - \widetilde{Q_1})}_{T_1}, \underbrace{Q + (\widetilde{Q_2} - \widetilde{Q_1})}_{T_2}, \dots, \underbrace{Q + (\widetilde{Q_n} - \widetilde{Q_1})}_{T_n}$$

are n direct preimages of P

(2) $\Phi := \ker\phi = \{T_1, \dots, T_n\}$ and

Claim: $\tau_{T_i}^* : k(E_2) \hookrightarrow k(E_1)$ preserves $\phi^*(k(E_2))$

Proof of Claim:

$\tau_{T_i}^*(\phi^* f) = \phi^* f(\cdot + T_i) = f(\phi(\cdot + T_i)) = f(\phi(\cdot) + \phi(T_i)) = f(\phi(\cdot) + \mathcal{O}) = f(\phi(\cdot)) = \phi^* f$ ■

$\Rightarrow \quad |\operatorname{Aut}(K_1/K_2)| \geq n$ ($\tau_{T_i}^* \in \operatorname{Aut}(K_1/K_2)\ \forall i$)
also $[K_1 : K_2] = n$, so by Galois theory, K_1/K_2 Galois and $|\operatorname{Gal}| = n$

(3) $K_3 = \psi^* k(E_3) \hookrightarrow K_1$
K_3 is fixed by $\{\tau_P^* | P \in \ker\psi\} \supseteq \{\tau_P^* | P \in \ker\phi\} = \operatorname{Gal}(K_1/K_2)$
$\Rightarrow \quad K_3 \subseteq K_2 \quad \Rightarrow \quad \exists!\chi : E_2 \to E_3$ inducing this inclusion
and $\psi = \chi \circ \phi$, $\chi(\mathcal{O}) = \psi(\mathcal{O}) = \mathcal{O}$
$\Rightarrow \quad \chi$ isogeny

(4) $\tau_P^* : k(E/\Phi) \hookrightarrow K_1 = k(E_1)$, where $P \in \Phi$
Let $K := K_1^\Phi$. By Galois theory, K_1/K is Galois of degree $|\Phi|$
In particular, tr.deg$K = 1 \Rightarrow K = k(C)$ for some (unique up to isom) non-singular curve C, get non-constant map

$$\phi : E_1 \to C \qquad \text{(this map is unramified, same argument as in (1))}$$

Recall $g(C) \leq g(E_1) = 1$
If $g(C) = 1 \Rightarrow$ done (define $\mathcal{O}_C = \phi(\mathcal{O}_{E_1})$)
If $g(C) = 0, C \cong \mathbb{P}^1$, check the following:

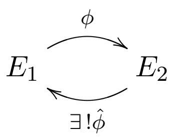
$$\operatorname{div}(\phi^* dx) = \sum_{\phi(Q)=\infty} e_Q(Q)$$

(Note dx has divisor $-2(\infty)$) all $a_Q < 0$, and this divisor has degree < 0 #

□

2.2.5 Dual Isogeny

Definition 2.2.32



We say E_1, E_2 are <u>isogeneous</u> if $\exists$ isogeny $\phi \neq 0 : E_1 \to E_2$

Proposition 2.2.33
$\phi : E_1 \to E_2$ isogeny of degree $m \neq 0$
Then $\exists!\,\hat{\phi} : E_2 \to E_1$ (the <u>dual</u> isogeny) s.t. $\hat{\phi}\phi = [m]$
(This proposition implies being isogeneous is an equivalence relation)

Proof
<u>Uniqueness:</u>
If $\hat{\phi}\phi = \psi\phi = [m] \Rightarrow (\hat{\phi} - \psi)\phi = [0] \Rightarrow$ (by $\phi \neq 0$) $\hat{\phi} = \psi$

<u>Existence</u>:
Suffice to show for ϕ separable and Frob_q

(1) <u>ϕ separable</u>: This implies $\#\ker\phi = m$, hence, $\forall P \in \ker\phi, mP = \mathcal{O} \Rightarrow \ker\phi \subseteq \ker[m]$
$\Rightarrow \quad$ done by previous Theorem 2.2.31(3).

(2) $\phi = \mathrm{Frob}_p, \quad p = \mathrm{char} k > 0, m = \deg \mathrm{Frob}_p = p$
w invariant differential on E
$[p]^* w = pw = 0 \Rightarrow [p]$ inseparable $\Rightarrow [p] = \mathrm{Frob}_p \circ \psi$ for some ψ

□

Theorem 2.2.34

(1) $\widehat{\phi}\phi = [m]$ on E_1, $\phi\widehat{\phi} = [m]$ on E_2
(2) $\widehat{\chi \circ \phi} = \widehat{\phi} \circ \widehat{\chi} \;\; \forall \chi : E_2 \to E_3$
(3) $\widehat{\phi + \psi} = \widehat{\phi} + \widehat{\psi} \;\; \forall \psi : E_1 \to E_2$
(4) $\widehat{[m]} = [m]$ and $\deg[m] = m^2 \;\; \forall m \in \mathbb{Z}$
(5) $\deg \widehat{\phi} = \deg \phi$
(6) $\widehat{\widehat{\phi}} = \phi$

Proof
May assume all isogenies $\neq [0]$

(1) $\widehat{\phi}\phi = [m]$ by definition
$\phi\widehat{\phi}\phi = \phi[m] = [m] \circ \phi \Rightarrow \phi\widehat{\phi} = [m]$ (as $\phi \neq 0$)

(2) $\chi\phi\widehat{\phi}\widehat{\chi} = \chi[\deg \phi]\widehat{\chi} = [\deg \phi][\deg \chi] = [\deg(\chi\phi)] = \chi\phi\widehat{\chi\phi}$
$\Rightarrow \quad \widehat{\phi}\widehat{\chi} = \widehat{\chi\phi}$

(3) Omitted (Silverman III 6.2)

(4) By induction: Clearly true for $m = -1, 0, 1$
$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$ by (3)
$= [m] + [1] = [m+1] = [\deg[m]] = [m]\widehat{[m]} = [m^2]$
$\Rightarrow \quad \deg[m] = m^2$

(5) $\widehat{\phi}\phi = [m]$ Take degrees

(6) $\widehat{\phi}\phi = [\deg \phi] = [\deg \widehat{\phi}] = \widehat{\widehat{\phi}}\widehat{\phi}$
$\Rightarrow \quad \phi = \widehat{\widehat{\phi}}$

□

Definition 2.2.35
A an abelian group. A quadratic form is a function $d : A \to \mathbb{R}$ s.t.

(1) $d(-x) = dx \;\; \forall x \in A$
(2) The pairing

$$\begin{aligned} \langle \; , \; \rangle : A \times A &\to \mathbb{R} \\ (\phi, \psi) &\mapsto d(\phi + \psi) - d\phi - d\psi \end{aligned}$$

is $\mathbb{Z}$-bilinear

Say d is positive-definite if $d(x) \geq 0$, and $d(x) = 0 \Leftrightarrow x = 0$

Corollary 2.2.36
$\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive definite quadratic form

Proof
All clear except bilinearity. Using $[\cdot] : \mathbb{Z} \hookrightarrow \mathrm{End}(E_1)$:

$$\begin{aligned} \langle \phi, \psi \rangle &= [\deg(\phi + \psi)] - [\deg \phi] - [\deg \psi] \\ &= (\widehat{\phi + \psi}) \cdot (\phi + \psi) - \phi\widehat{\phi} - \psi\widehat{\psi} \\ &= \widehat{\phi}\psi + \widehat{\psi}\phi \qquad \text{bilinear} \end{aligned}$$

□

2.2.6 Torsion

Definition 2.2.37
The <u>m-torsion group</u> (or group of m-torsion points)

$$E[m] := \ker[m] = \{P | mP = 0\} \qquad (m \geq 1)$$

Corollary 2.2.38
If char $k \nmid m$ then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

Proof
$[m]$ separable $\Rightarrow |E[m]| = m^2$ (because $\deg[m] = m^2$)

$$\left.\begin{array}{l} |E[m]| = m^2 \\ |E[d]| = d^2 \ \forall d | m \end{array}\right\} \Rightarrow E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

(Exercise: check this) □

Remark. $E[m] \cong E[p_1^{n_1}] \times \cdots E[p_k^{n_k}]$ if $m = p_1^{n_1} \cdots p_k^{n_k}$ prime decomposition

2.2.7 Tate module

l prime, $l \nmid$ char k

$$\cdots \xrightarrow{[l]} E[l^3] \xrightarrow{[l]} E[l^2] \xrightarrow{[l]} E[l] \overset{[l]}{\twoheadrightarrow} 0$$
$$E[l^n] = \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$$

Definition 2.2.39
The <u>l-adic Tate module</u> is

$$\begin{aligned} T_l E &:= \varprojlim_{n \geq 1} E[l^n] \\ &= \{(P_n)_{n \geq 1} | P_n \in E[l^n], [l]P_n = P_{n-1}\} \quad \text{(by defn)} \\ &= \mathbb{Z}_l \oplus \mathbb{Z}_l \quad \text{as an abelian group or } \mathbb{Z}_l\text{-module} \end{aligned}$$

Recall: The <u>l-adic integer</u> $\mathbb{Z}_l := \{(\cdots, a_2, a_1) | a_n \in \mathbb{Z}/l^n\mathbb{Z}, a_{n+1} \equiv a_n \mod l^n\}$
This a ring (component-wise) and $\supseteq \mathbb{Z} = \{(\cdots, a, a) | a \in \mathbb{Z}\}$

An isogeny $\phi : E_1 \to E_2$ induces linear maps

$$E_1[l^n] \to E_2[l^n]$$

so a $\mathbb{Z}_l$-linear map $\phi_l : T_l E_1 \to T_l E_2$ (think this as element of $M_2(\mathbb{Z}_l)$)

Theorem 2.2.40
E_1, E_2 elliptic curves. Then

$$\underbrace{\mathrm{Hom}(E_1,E_2)}_{\text{torsion free}\,\mathbb{Z}\text{-modules}} \otimes \mathbb{Z}_l \quad \hookrightarrow \quad \mathrm{Hom}(T_lE_1, T_lE_2)$$

Proof
Let $H = \mathrm{Hom}(E_1,E_2)$ torsion-free abelian group.
Now suppose $\phi \in H \otimes \mathbb{Z}_l$ s.t. $\phi_l = 0$

$$\phi = a_1\psi_i + \cdots a_t\psi_t \quad a_i \in \mathbb{Z}_l, \psi_i \in H$$

$M := \langle \psi_1, \ldots, \psi_t \rangle$. Use the following Lemma 2.2.41, replace ψ_i by a basis of M^{div}, may assume $M = M^{\mathrm{div}}$

$$\phi = a_1\psi_1 + \cdots a_t\psi_t \qquad \phi_l = 0$$

for all $n \neq 1$,
Since $(a_1 \mod l^n) \in \mathbb{Z}$ s.t. its class in $\mathbb{Z}/l^n\mathbb{Z}$ is the same as that of a_1

$$[a_1 \mod l^n]\psi_1 + \cdots [a_t \mod l^n]\psi_t \text{ kills } E[l^n]$$

$\Rightarrow$ factoring isogenies theorem

$$\begin{aligned} &= l^n \times (\text{some elts of } M^{\mathrm{div}} = M) \\ &= [l^nb_1]\psi_1 + \cdots + [l^nb_t]\psi_t \quad \text{for some } b_i \in \mathbb{Z} \end{aligned}$$

ψ_i basis of $M \Rightarrow a_i = l^nb_i \equiv 0 \mod l^n$
True for all $n \Rightarrow$ all $a_i = 0 \Rightarrow \phi = 0$ □

Lemma 2.2.41
If $M \subseteq H = \mathrm{Hom}(E_1,E_2)$ finitely generated subgroup, then

$$M^{\mathrm{div}} = \{\phi \in H | m\phi \in M \text{ for some } m \geq 1\}$$

is finitely generated

Proof
Note $M \otimes \mathbb{R}$ is a finite dimensional vector space, degree as quadratic form

$$\begin{aligned} M^{\mathrm{div}} &\hookrightarrow M \otimes \mathbb{R} \\ \text{open nbhd of 0:} \quad U = \{\phi \in M \otimes \mathbb{R} \,|\, \deg\phi < 1\} &\hookrightarrow M \otimes \mathbb{R} \end{aligned}$$

$M^{\mathrm{div}} \cap U = \{0\}$ (deg ≥ 1 for non-zero isogenies)
$\Rightarrow$ M^{div} discrete $\Rightarrow$ finitely generated □

Corollary 2.2.42

$$\begin{aligned} \mathrm{rk}_{\mathbb{Z}}\,\mathrm{Hom}(E_1,E_2) &\leq \mathrm{rk}_{\mathbb{Z}_l}\,\mathrm{Hom}(\mathbb{Z}_l^2, \mathbb{Z}_l^2) = 4 \\ \mathrm{rk}_{\mathbb{Z}}\,\mathrm{End}(E) &\leq 4 \end{aligned}$$

Easy algebra:
Any integral domain R of char 0 which has $\mathrm{rk}_{\mathbb{Z}} \leq 4$ and has a positive-definite quadratic form

$$d : R \to \mathbb{Z}$$
$$\text{s.t. } d(ab) = d(a)d(b)$$

then

(1) $R \cong \mathbb{Z} \qquad (d(x) = x^2)$ or

(2) $R \cong \mathcal{O}_K$ order in imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D}) \qquad (d(x) = |x|^2)$

(3) R rank 4 order in a quaternion algebra $\qquad (d(x) = a^2 + b^2 + c^2 + d^2)$

Corollary 2.2.43
End(E) is one of the 4 cases above, in character 0 (commutative) either (1) or (2)

2.3 Elliptic Curves over $\mathbb{C}$

2.3.1 Aside

A non-singular projective curve C over $\mathbb{C}$ with its usual complex topology is a compact (i.e. $\mathbb{P}^n_{\mathbb{C}}$ compact) complex manifold (i.e. non-singular) of dimension 1 (i.e. curve)
$\Rightarrow$ a complex Riemann surface.
Conversely, by Riemann Existence Theorem:
Every complex Riemann surface X comes from a C over $\mathbb{C}$

$$\begin{array}{ccc} C & \longrightarrow & X \\ \text{rational function} & & \text{meromorphic function} \\ \mathbb{C}(C) & = & \mathbb{C}(X) \end{array}$$

(This is an equivalence of categories)
(Note: This is very hard, the main step is to prove $\mathbb{C}(X) \neq \mathbb{C}$)

Universal curve $\widetilde{X}$ has a complex structure (easy),

$$X = \widetilde{X}/\pi_1(X)$$

($\pi_1(X)$ is a discrete group acting freely, the fundamental group)

Complex Uniformization Theorem (also hard). As a $\mathbb{C}$-manifold,

$$\begin{array}{ll} \widetilde{X} = \mathbb{C} \cup \{\infty\} = \mathbb{P}^1_{\mathbb{C}} & \text{if } g(X) = 0 \\ \widetilde{X} = \mathbb{C} & \text{if } g(X) = 1 \\ \widetilde{X} = \{z : |z| < 1\} & \text{if } g(X) \geq 2 \end{array}$$

If $g = 1$, then $\mathrm{Aut}_{\mathbb{C}-\mathrm{inf}} \mathbb{C} = \{z \mapsto az + b | a, b \in \mathbb{C}\}$
fixed-point free ones $= \{z \mapsto z + w | w \in \mathbb{C}\}$
$\pi_1(X) = \cong \mathbb{Z} \oplus \mathbb{Z} \Rightarrow X \cong \mathbb{C}/\Lambda$ (Λ lattice)
$\Rightarrow \{\mathbb{C}/\Lambda\} =$ elliptic curves over $\mathbb{C}$

Our Goal: Do this explicitly

2.3.2 Theory

Recall function on $\mathbb{C}$ is meromorphic $\Leftrightarrow \forall a \in \mathbb{C}$ it has Laurent expansion at a:

$$f(z) = \sum_{n=n_0}^{\infty} c_n (z-a)^n \qquad c_{n_0} \neq 0 \text{ unless } f \equiv 0$$

Notation:

$$\begin{aligned} \operatorname{ord}_a f &:= n_0 \in \mathbb{Z} \quad \text{for order of vanishing at } a \text{ (discrete valuation)} \\ \operatorname{res}_a f &:= c_{-1} \quad \text{residue at } a \end{aligned}$$

Definition 2.3.1
A lattice $\Lambda \subseteq \mathbb{C}$ is a discrete subgroup of rank 2

$$\Lambda = \mathbb{Z}\, w_1 + \mathbb{Z}\, w_2$$

(Note: Basis w_1,w_2 not unique, up to $GL_2(\mathbb{Z})$) We use π to denote the fundamental domain of Λ (i.e. the parallelogram spanned by w_1 an w_2)

An elliptic function (w.r.t to Λ) is a meromorphic function s.t.

$$f(z+w) = f(z) \qquad\qquad \forall z \in \mathbb{C}, w \in \Lambda$$

(These are precisely meromorphic functions on $X = \mathbb{C}/\Lambda$, they form a field $\mathbb{C}(X) \supseteq \mathbb{C}$)

Lemma 2.3.2
$f \not\equiv 0$ elliptic function

(1) f analytic (all $\operatorname{ord}_a f \geq 0$) $\Rightarrow$ f constant

(2) $\sum_{w \in \mathbb{C}/\Lambda} \operatorname{res}_w f = 0$

(3) $\sum_{w \in \mathbb{C}/\Lambda} \operatorname{ord}_w f = 0$

(4) $\sum_{w \in \mathbb{C}/\Lambda} \operatorname{ord}_w f \cdot w \in \Lambda$ (i.e. =0 in $\mathbb{C}/\Lambda$)

(Note: (2),(3),(4) are finite sums (π compact), well-defined)

Proof

(1) f analytic $\Rightarrow$ bounded on π $\Rightarrow$ bounded on $\mathbb{C}$ $\Rightarrow$ constant by Liouville's Theorem

(2) $\sum \text{res} = \frac{1}{2\pi i} \int_{\partial \pi} f(z) dz = \int + \int + \int + \int = 0$
(f elliptic)

(3) $\sum \text{ord} = \frac{1}{2\pi i} \int_{\partial \pi} \frac{f'}{f} dz = 0$ as above

(4) Use $z \frac{f'}{f}$ (Exercise)

□

Notation: $\mathcal{L}(n(0)) = \{\text{elliptic functions w.r.t. } \Lambda \text{ s.t. } f \text{ analytic for } z \notin \Lambda, \operatorname{ord}_z f \geq -n \text{ for } z \in \Lambda\}$

Lemma 2.3.2(1) $\Rightarrow$ $\mathcal{L}(0) = \mathbb{C}$ constants
Lemma 2.3.2(2) $\Rightarrow$ $\mathcal{L}(1(0)) = \mathbb{C}$ (by LHS=$\operatorname{res}_0 f$, RHS=0 $\Rightarrow$ analytic at 0 as well)

Definition 2.3.3
Eisenstein series of weight $2k$

$$G_{2k} = G_{2k}(\Lambda) := \sum_{\substack{w\in\Lambda \\ w\neq 0}} w^{-2k} \qquad k \geq 2$$

(Exercise: $\sum_{0\neq w\in\Lambda} \frac{1}{|w|^\alpha} < \infty \Leftrightarrow \alpha > 2$)

Example 2.3.4
$\Lambda = \mathbb{Z} + \sqrt{2}i\,\mathbb{Z}$
$G_4 = 2.23661\ldots$
$G_6 = 1.89217\ldots$

Theorem 2.3.5

$$\mathcal{L}(2(0)) = \langle 1, \wp(z)\rangle$$

where $\wp(z)$ unique elliptic function (Weierstrass $\wp$-function) s.t.

$$\wp(z) = \frac{1}{z^2} + O(z) \qquad \text{at } z = 0$$

($O(z)$ means, at $z = 0$, Laurent series has $c_{-1} = 0, c_0 = 0$)

Proof
Uniqueness:
$\dim \mathcal{L}(2(0)) \leq 2$, clear:
$\wp_1 - \wp_2 \in \mathcal{L}(0) \Rightarrow$ constant, zero at $z = 0$, as cannot have pole of order 1 by previous lemma $\Rightarrow 0$

Existence:
Define the Weierstrass $\wp$-function as follows

$$\wp(z) := \wp(z;\Lambda) = \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{(z-w)^2} - \frac{1}{w^2}$$

If $|w| > 2|z|$

$$\left|\frac{1}{(z-w)^2} - \frac{1}{w^2}\right| = \left|\frac{z(2w-z)}{w^2(w-z)^2}\right| \leq \frac{10\cdot|z|}{|w|^3}$$

note $\sum_{|w|\geq 2|z|} \leq 10\cdot|z| \left(\sum \frac{1}{|w|^3}\right) < \infty$
So this converges uniformly on compact $\subseteq \mathbb{C}\setminus\Lambda$
$\Rightarrow$ analytic on $\mathbb{C}\setminus\Lambda$, double pole at $w \in \Lambda$

$\wp(z)$ elliptic:
$\wp(z)$ clearly even; in particular $\wp(\frac{w}{2}) = \wp(-\frac{w}{2})$ for $w \in \Lambda$

$$\wp'(z) = -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3}$$

this clearly is elliptic

$$\Rightarrow \qquad \wp(z+w) - \wp(z) = c(w) \quad \text{constant } (w \in \Lambda)$$

$z = -\frac{w}{2} \Rightarrow c(w) = 0 \Rightarrow \wp(z)$ elliptic □

Remark. For $|z| < |w|$

$$\begin{aligned} \frac{1}{(z-w)^2} - \frac{1}{w^2} &= w^{-2}\left(\frac{1}{\left(1-\frac{z}{w}\right)^2} - 1\right) \\ &= \sum_{k=1}^{\infty} \frac{n+1}{w^{n+2}} z^n \end{aligned}$$

Sum over $w \in \Lambda$, interchange order

$$\Rightarrow \qquad \wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty}(2k+1)G_{2k+2}z^{2k}$$

Theorem 2.3.6
Writing

$$\begin{aligned} g_2 &= g_2(\Lambda) &:=& \; 60G_4(\Lambda) \\ g_3 &= g_3(\Lambda) &:=& \; 140G_6(\Lambda) \end{aligned}$$

We get

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

Proof

$$\begin{aligned} \wp(z) &= \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + \cdots \\ \wp(z)^3 &= \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + \cdots \\ \wp'(z)^2 &= \frac{1}{4z^6} - 24G_4\frac{1}{z^2} - 80G_6 + \cdots \end{aligned}$$

LHS − RHS in Theorem is elliptic, holomorphic (i.e. analytic, i.e. no poles as all negative power of z cancel)
LHS − RHS $\equiv 0$ by Lemma 2.3.2 (1) □

Remark. (see picture)
$\wp(z)$ even, $\wp'(z)$ odd $\Rightarrow \wp'(T_i) = \wp'(-T_i) \Rightarrow \wp'(T_i) = 0$
$\frac{d}{dz}(\frac{1}{z^2}) = \frac{-2}{z^3} \Rightarrow -3(\mathcal{O})$

$$\operatorname{div}\wp'(z) = -3(\mathcal{O}) + (T_1) + (T_2) + (T_3)$$

and $\forall\, a \in C$

$$\begin{aligned} \operatorname{div}(\wp(z) - a) &= -2(\mathcal{O}) + (w) + (-w) \quad \text{for some } w \in \mathbb{C}/\Lambda \\ \text{and} \quad \operatorname{div}(\wp(z) - \wp(T_i)) &= -2(\mathcal{O}) + 2(T_i) \end{aligned}$$

in particular, $\wp(T_i)$ distinct

Theorem 2.3.7
$\Lambda \subseteq \mathbb{C}$ lattice, $X = \mathbb{C}/\Lambda$. Then

$$\mathbb{C}(X) = \mathbb{C}(\wp(z), \wp'(z))$$

Proof
Take $f \in \mathbb{C}(X)$. May assume f is even

$$\text{general } f = \underbrace{\frac{1}{2}(f(z) + f(-z))}_{\text{even elliptic}} + \underbrace{\frac{1}{2}(f(z) - f(-z))}_{\text{odd elliptic}} \quad \Rightarrow \quad \text{odd} = \wp' \times \text{even}$$

Now $\mathrm{div}(f) = n_1[(z_1) + (-z_1)] + \cdots + n_k[(z_k) + (-z_k)]$ for some $n_k \in \mathbb{Z}, z_k \in \mathbb{C}/\Lambda$
(check T_i carefully using f' odd)

Define

$$\widetilde{f} := \prod_i [\wp(z) - \wp(z_i)]^{n_i}$$

$\Rightarrow \quad \mathrm{div}(f) = \mathrm{div}(\widetilde{f}) + ?(0)$
both deg $\mathrm{div}(f)$, div $(\widetilde{f})$ =0 $\Rightarrow$ $\frac{\widetilde{f}}{f}$ has no zero or poles
$\Rightarrow$ holomorphic elliptic $\Rightarrow$ constant □

Write

$$E_\Lambda: \quad y^2 = 4x^3 - g_2 x - g_3$$

where $g_2 = g_2(\Lambda)$, $g_3 = g_3(\Lambda)$
$E_\Lambda \cong y^2 = (x - \wp(T_1))(x - \wp(T_2))(x - \wp(T_3))$
In particular, this is non-singular
Actually, $(\wp(z) : \wp'(z) : 1) \in \mathbb{P}^2$ and $\Lambda \mapsto (0:1:0) = \mathcal{O}$

Theorem 2.3.8
ϕ as follows is an analytic isomorphism of complex Lie groups

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\to E_\Lambda \\ z &\mapsto (\wp(z), \wp'(z)) \end{aligned}$$

Proof
Surjectivity:
$\mathcal{O}, (\alpha_i, 0)$ (where α_i is root of RHS) in the image
Take $(x, y) \in E_\Lambda$ where $y \neq 0, \infty$

$$\mathrm{div}(\wp(z) - x) = -2(\mathcal{O}) + (w_1) + (-w_1) \quad \text{for some } w_1 \in \mathbb{C}/\Lambda$$

$\Rightarrow \quad \wp(w_1) = x$

$$(\wp'(w))^2 = f(\wp(w)) = f(x) = y^2$$

$\Rightarrow \quad y = \wp'(w_1)$ or $y = -\wp'(w1) = \wp'(-w_1)$
$\Rightarrow$ either w_1 or $-w_1$ maps to (x, y)

Injectivity: Check T_i; otherwise follows from the proof of surjectivity

locally analytic isom:
$\frac{dx}{y}$ differential on E with no zeros/poles

$$\phi^* \frac{dx}{y} = \frac{d\wp(z)}{\wp'(z)} = \frac{\wp'(z) dz}{\wp'(z)} = dz$$

$\Rightarrow \quad \phi^*$ isomorphism on cotangent spaces

ϕ^{-1} group homomorphism
If $P_1 + P_2 + P_3 = \mathcal{O}$ on E_Λ
Take $f \in \mathbb{C}(E_\Lambda)$ s.t.

$$\mathrm{div}(f) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O})$$

say $\phi : z_i \mapsto P_i$. Then

$$\mathrm{div}(\phi^* f) = (z_1) + (z_2) + (z_3) - 3(\mathcal{O})$$

(Note: $\phi^* f = f(\wp(z), \wp'(z))$ which is meromorphic)

previous Lemma 2.3.2 (4) $\Rightarrow z_1 + z_2 + z_3 = 0 \mod \Lambda$ □

Corollary 2.3.9
A divisor $D = \sum_{z_i \, \mathbb{C}/\Lambda} n_i(z_i)$ is a divisor of some elliptic function
$\Leftrightarrow \quad \sum n_i = 0$ and $\sum n_i z_i = 0 \mod \Lambda$

Proof
True on E_Λ □

2.3.3 Constructing Λ from E, and $\phi^{(-1)} : E \to \mathbb{C}/\Lambda$

(see picture)

If $\phi(z_0) = P_0$, then

$$z_0 = \int_0^{z_0} dz = \int_0^{z_0} \frac{d\wp(z)}{\wp'(z)} = \int_{\mathcal{O}}^{P_0} \frac{dx}{y} = \underbrace{\int_\infty^{x(P_0)} \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}}}_{\underline{\text{elliptic integral}}}$$

$(x(P_0) = x$-coordinate of $P_0)$

$$\Rightarrow \qquad P \mapsto \int_\infty^{x(P)} \frac{dx}{\sqrt{4f(x)}} \text{ is } \phi^{-1} : E \to \mathbb{C}$$

$\int_{\mathcal{O}}^{P_0} \frac{dx}{y}$ depends on the choice of a path from $\mathcal{O}$ to P (see picture)

The integral is well-defined up to $\mathbb{Z}$-multiples of $\int_{\gamma_1} \frac{dx}{y}, \; \int_{\gamma_2} \frac{dx}{y}$ with γ_1, γ_2 basis of $H_1(E, \mathbb{Z}) = \Lambda$ (see picture)

The lattice Λ is recovered as $\mathbb{Z} \cdot \int_{\gamma_1} \frac{dx}{y} + \mathbb{Z} \cdot \int_{\gamma_2} \frac{dx}{y} \subseteq \mathbb{C}$

Choose (picture)

$\Rightarrow \quad \int_{\gamma_1} = w_1, \int_{\gamma_2} w_2$

Example 2.3.10
$E: \quad y^2 = x(x-1)(x-3)$. Two well-defined choices of $\sqrt{x(x-1)(x-3)}$ on $\mathbb{C}$ with $(0,1)$ and $(3,\infty)$ removed, call them "$+\sqrt{\cdot}$" and "$-\sqrt{\cdot}$"

$E =$ $\cup$ $=$ $\cup$

$=$

Deform it $\Rightarrow$

$$\begin{aligned} w_1 &= \not{2}\int_0^1 \frac{dx}{\sqrt{\not{4}x(x-1)(x-3)}} = 0.620131\ldots \\ w_2 &= \not{2}\int_1^3 \frac{dx}{\sqrt{\not{4}x(x-1)(x-3)}} = 2.20335\ldots \cdot i \end{aligned}$$

This proves this E comes from a Λ (!!)
(namely, this $\Lambda = \mathbb{Z}\, w_1 + \mathbb{Z}\, w_2$)

2.3.4 Conclusion

Let $E: \quad y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

- If $\alpha_i \in \mathbb{R}$, E comes from a lattice $\Lambda = \mathbb{Z}\, w_1 + \mathbb{Z}\, w_2$, $w_1 \in \mathbb{R}, w_2 \in i \cdot \mathbb{R}$
- If $\alpha_1 \in \mathbb{R}, \alpha_2 = \overline{\alpha_3}$ similar argument $\Rightarrow$ E comes from $\Lambda = \mathbb{Z}\, w_1 + \mathbb{Z}\, w_2$, $w_1 \in \mathbb{R}$, $w_2 = \frac{1}{2}w_1 + i \cdot \mathbb{R}$
- If $\alpha_i \in \mathbb{C}$ arbitrary distinct, can show that $\int_{\gamma_1}, \int_{\gamma_2}$ are still linear independent over $\mathbb{R}$, so they form a lattice Λ (and $\mathbb{C}/\Lambda = E$ by construction)

Corollary 2.3.11
$\deg[m] = m^2$ and $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ all $m \geq 1$

Proof
$E \cong \mathbb{C}/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ as abelian group
$E[m] \cong (\frac{1}{m}\mathbb{Z}/\mathbb{Z})^2 \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ $\square$

2.3.5 Homotheties and Isogenies

What are isogenies $E = \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' = E'$?

- If $\alpha \in \mathbb{C}$ s.t. $\alpha\Lambda \leq \Lambda'$ then

  $$\begin{array}{rcl} \mathbb{C}/\Lambda & \to & \mathbb{C}/\Lambda' \\ z & \mapsto & \alpha z \end{array}$$

  well-defined holomorphic $E \to E'$, $\mathcal{O} \mapsto \mathcal{O}$, given by

  $$\phi_\alpha : (\wp_\Lambda(z), \wp'_\Lambda(z)) \mapsto (\wp_{\Lambda'}(\alpha z), \wp'_{\Lambda'}(\alpha z))$$

  But $z \mapsto \wp_{\Lambda'}(\alpha z)$ is elliptic w.r.t. Λ for $w \in \Lambda$

  $$\wp_{\Lambda'}(\alpha(z+w)) = \wp_{\Lambda'}(\alpha z + \underbrace{\alpha w}_{\in \Lambda'}) = \wp_{\Lambda'}(\alpha z) \quad \text{similar for } \wp'_{\Lambda'}(\alpha z)$$

  $$\Rightarrow \quad \wp_{\Lambda'}(\alpha z), \wp'_{\Lambda'}(\alpha z) \; in \, \mathbb{C}(E) = \mathbb{C}(\wp_\Lambda(z), \wp'_\Lambda(z))$$

  i.e. ϕ_α is a rational map

- Conversely, $\phi : E \to E'$ holomorphic, $\phi(\mathcal{O}) = \mathcal{O}$; e.g. ϕ isogeny.
  $\phi : \mathbb{C} \to \mathbb{C}/\Lambda'$, lifts to the universal cover

  $$\widetilde{\phi} : \mathbb{C} \to \mathbb{C} \quad , \quad \widetilde{\phi}(\Lambda) \subseteq \Lambda'$$

  For $w \in \Lambda$,

  $$z \mapsto \widetilde{\phi}(z+w) - \widetilde{\phi}(z) \qquad \mathbb{C} \to \Lambda' \quad \text{holomorphic}$$

  is constant (dependent on w). So $\widetilde{\phi}'(z)$ is elliptic holomorphic $\Rightarrow \widetilde{\phi}' =$ constant α, i.e.

  $$\widetilde{\phi}(z) = \alpha z + \not{\beta}$$

Corollary 2.3.12

$$\begin{array}{rcl} \{\text{isogenies } \phi : E \to E'\} & = & \{\alpha \in \mathbb{C} \,|\, \alpha\Lambda \subseteq \Lambda'\} \\ \phi & \mapsto & \alpha = \dfrac{\phi^* dz}{dz} = \dfrac{\phi^*(dx/y)}{dx/y} \\ \phi & \leftarrow\!\shortmid & \alpha \quad \text{as above} \end{array}$$

Corollary 2.3.13
$\mathrm{rk}_{\mathbb{Z}}(LHS) \leq 4$ (confirming previous result)

We proved:

Theorem 2.3.14
These categories are equivalent:

- Elliptic curves over $\mathbb{C}$, maps: isogenies
- Elliptic curves over $\mathbb{C}$, maps: analytic maps taking $\mathcal{O}$ to $\mathcal{O}$
- Lattices $\Lambda \subseteq \mathbb{C}$, maps $\{\alpha \in \mathbb{C} \,|\, \alpha\Lambda \subseteq \Lambda'\}$

Corollary 2.3.15
$E \cong E' \Leftrightarrow \Lambda = \alpha\Lambda'$ for some $\alpha \in \mathbb{C}^\times$ (note lattices are homothetic), i.e.

$$\frac{\text{Elliptic curves}}{\cong} = \frac{\text{Lattices}}{\text{homothety}}$$

2.3.6 Curves with Complex Multiplication

Remark. Every $\mathbb{Z}\,w_1 + \mathbb{Z}\,w_2$ is homothetic to $\Lambda = \mathbb{Z} + \mathbb{Z}\,\tau$ for some $\tau \in \mathbb{H} = \{z \in \mathbb{C}\,|\mathrm{Im}(z) > 0\}$

Exercise: τ unique up to $SL_2(\mathbb{Z})$-action

Suppose,

$$\begin{aligned} E &= \mathbb{C}\,/\Lambda \text{ has CM, i.e.} \\ R &= \mathrm{End}(E) = \{\alpha \in \mathbb{C}\,|\alpha\Lambda \subseteq \Lambda\} \supsetneqq \mathbb{Z} \end{aligned}$$

We say that E has complex multiplication (CM) by R

$\alpha \in R$, $\alpha \cdot 1 = \alpha \in \Lambda, \alpha \cdot \tau \in \Lambda$
$\Rightarrow \quad \alpha = a + b\tau, \quad \alpha\tau = c + d\tau$ for some $a, b, c, d \in \mathbb{Z}$
$\Rightarrow \quad b\tau^2 + (a - d)\tau - c = 0$ (quadratic equation for τ over $\mathbb{Q}$)
$\Rightarrow \quad \tau \in K = \mathbb{Q}(\sqrt{-D})$, some $D \in \mathbb{Z}_{>0}$; imaginary quadratic field

$R \subseteq \mathbb{Z} + \mathbb{Z}\,\tau$ rank 2 subring $\Rightarrow$ order in K
(Exercise: $R = \mathbb{Z} + f \cdot \mathcal{O}_K$ for some $f \geq 1$, the conductor of R)

Λ an R-module $\subseteq K \Rightarrow$ fractional ideal of R

Conversely, for each order $R \subseteq K$ (any R, any K) e.g. $\Lambda = R$ has CM by R

Generally,

$$\left\{ \begin{array}{c} \text{elliptic curves} \\ \text{with CM by } R \end{array} \right\} \Big/ \text{isom.} = \left\{ \begin{array}{c} \text{fractional ideal} \\ \text{of } R \end{array} \right\} \Big/ \sim \;=\; \text{Class group of } R$$

($I_1 \sim \alpha I_2$ for $\alpha \in K^\times$)
(note the above are finite groups)

Example 2.3.16
$R = \mathbb{Z}[i], K = \mathbb{Q}(i)$
$E : \mathbb{C}\,/\,\mathbb{Z} + \mathbb{Z}\,i \qquad y^2 = x^3 + x$

Example 2.3.17
$R = \mathbb{Z}[\zeta_3], K = \mathbb{Q}(\sqrt{-3})$
$E : \mathbb{C}\,/\,\mathbb{Z} + \mathbb{Z}\,\zeta_3 \qquad y^2 = x^3 + 1$

Example 2.3.18
$R = \mathbb{Z}[\sqrt{-5}], K = \mathbb{Q}(\sqrt{-5})$ (has class number 2)
$E : \mathbb{C}\,/\,\mathbb{Z} + \mathbb{Z}\,\sqrt{-5} \qquad j = 632000 + 282880\sqrt{5}$
$E : \mathbb{C}\,/\,\mathbb{Z} + \mathbb{Z}\,\frac{1+\sqrt{-5}}{2} \qquad j = 632000 - 282880\sqrt{5}$
Beyond Syllabus Fact: j-invariants of elliptic curves with CM by $\mathcal{O}_K$ generate maximal unramified abelian extension, i.e. the Hilbert class field, of K, e.g.:

$$\mathbb{Q}(\sqrt{-5}) \xrightarrow{\text{unramified}} \mathbb{Q}(\sqrt{-5}, \sqrt{5})$$

The study of these is called Theory of CM.

Exercise: If $E \sim E'$ isogenies then E has CM $\Leftrightarrow$ E' has CM; with the same K
Conversely, any 2 elliptic curves with CM by subrings ($\neq \mathbb{Z}$) of $K = \mathbb{Q}(\sqrt{-D})$ with the same D are isogeneous

Exercise: $\mathrm{End}(E) = \mathbb{Z}[\alpha]$, complex conjugation = taking dual isogeny, degree = $|\cdot|^2$

Chapter 3

Arithmetic

3.1 Elliptic Curves over Perfect Field

Ground field K, always perfect

Definition 3.1.1
K is perfect if every finite extension of K is separable $\quad (\Leftrightarrow \overline{K}^{\mathrm{Gal}(\overline{K}/K)} = K)$

Example 3.1.2
Perfect field: char K=0 $K = \overline{K}$
$K = \mathbb{F}_{p^n}$
Non-perfect field: $K = \mathbb{F}_p(X)$

Definition 3.1.3
A curve $C \subseteq \mathbb{P}^n_{\overline{K}}$ is defined over K (written C/K) if it can be give by

$$C : \begin{cases} f_1 = 0 \\ \quad\vdots \\ f_m = 0 \end{cases} \qquad f_i \in K[x_0, \ldots, x_n] \text{ homog. polynomials}$$

The set of K-rational points $C(K)$= $\{(a_0, \ldots, a_n) \in C | a_i \in K\}$

Exercise: $C: \ x^2 + y^2 = -1 \subseteq \mathbb{P}^2_{\mathbb{C}}$ defined over $\mathbb{Q}: C(\mathbb{Q}) = \emptyset$

Definition 3.1.4
K-rational functions: $K(C) = \{\frac{f}{g} \in \overline{K}(C) | f, g \in K(x_0, \ldots, x_n)\}$
K-rational maps: $C_1 \to C_2$ = those defined by K-rational functions

Fact: {non-singular curves over K} $\to$ { f.g. extensions L of K of tr.deg. 1 s.t. $L \cap \overline{K} = K$} (exercise: why $L \cap \overline{K}$) $C \mapsto K(C)$ this is an equivalence of categories

Definition 3.1.5
K-rational divisors

$$\mathrm{Div}_K(C) = (\underbrace{\mathrm{Div}(C)}_{\text{over } \overline{K}})^{\mathrm{Gal}(\overline{K}/K)} \qquad \text{Galois invariants}$$

Clearly $f \in K(C)^\times \ \Rightarrow \ \mathrm{div}(f) \in \mathrm{Div}_K(C)$
(and conversely, the lemma below)

Example 3.1.6
$y^2 = x^3 + 1$ over $\mathbb{Q}$
$\mathrm{div}(x) = (0,1) + (0,-1) - 2(\mathcal{O})$
$\mathrm{div}(y) = (-1,0) + (-\zeta,0) + (-\zeta^2,0) - 3(\mathcal{O})$

Lemma 3.1.7
$D \in \mathrm{Div}_K(C) \Rightarrow \mathcal{L}(D)$ has a basis of functions in $K(C)$

Proof
General fact about vector space with $\mathrm{Gal}(\overline{K}/K)$-action (Silverman III, 5.8.1) □

Definition 3.1.8
An <u>elliptic curve</u> is a pair $(E, \mathcal{O})$, E/K genus 1, $\mathcal{O} \in E(K)$

Example 3.1.9
(Selmer) $C: \ 3x^3 + 4y^3 = 5$ has genus 1, $C(\mathbb{Q}) = \emptyset$, NOT an elliptic curve over $\mathbb{Q}$

- Riemann-Roch + Lemma $\Rightarrow$

$$E \cong y^2 + a_1xy + a_3y = x^3 + \cdots$$

  with $a_i \in K$, unique up to

$$\begin{array}{lll} x & \mapsto & u^2x + r \qquad u, r, s, t \in K \\ y & \mapsto & u^3y + sx + t \qquad u \neq 0 \end{array}$$

- Addition: $E \times E \to E$, inverse: $E \to E$ both defined over K. In particular $(P+Q)^\sigma = P^\sigma + Q^\sigma \ \forall \sigma \in \mathrm{Gal}(\overline{K}/K)$
  Thus $E(K)$ abelian group (main object of study)

Definition 3.1.10

$$\begin{array}{rcl} \mathrm{Hom}_K(E_1, E_2) & = & \underline{K\text{-rational isogenies}} \\ & = & K\text{-morphism s.t. } \mathcal{O} \mapsto \mathcal{O} \\ & = & \mathrm{Hom}(E_1, E_2)^{\mathrm{Gal}(\overline{K}/K)} \\ \mathrm{End}_K(E) & = & \mathrm{Hom}_K(E, E) \overset{\text{subring}}{\subseteq} \mathrm{End}(E) \text{ over } \overline{K} \end{array}$$

Example 3.1.11
$E: y^2 = x^3 + x$ over $\mathbb{Q}$
$\mathrm{End}_{\mathbb{Q}(i)}(E) \cong \mathbb{Z}[i]$
$[i] : (x, y) \mapsto (ix, -y)$
$\mathrm{End}_{\mathbb{Q}}(E) = \mathbb{Z}$
$\dfrac{\phi^* dx/y}{dx/y} \notin \mathbb{Q}$ for $\phi \in \mathbb{Z}[i] \setminus \mathbb{Z}$
$\Rightarrow$ cannot be defined over $\mathbb{Q}$
i.e. E has CM over $\mathbb{Q}(i)$ but not over $\mathbb{Q}$

3.1.1 Torsion and Weil Pairing

E/K, $m \geq 1$, char $K \nmid m$
Recall: <u>m-torsion subgroup</u> $E[m] = \{P \in E(\overline{K}) | mP = \mathcal{O}\} \cong \mathbb{Z}/m\mathbb{Z} + \mathbb{Z}/m\mathbb{Z}$ as abelian group

If $mP = \mathcal{O}$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$ then
$m(P^\sigma) = (mP)^\sigma = \mathcal{O}^\sigma = \mathcal{O} \Rightarrow P^\sigma \in E[m]$
$\Rightarrow$ $E[m]$ is $\mathrm{Gal}(\overline{K}/K)$-module with linear action, i.e. we have representation:

$$\overline{\rho_m} : \mathrm{Gal}\,\overline{K}/K \to \mathrm{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}) (= GL_2(\mathbb{F}_l) \text{ if prime } m = l)$$

Example 3.1.12
$E/\mathbb{Q}: \quad y^2 = (x-1)(x^2+1) \quad , m = 2$

$$E[2] = \{\mathcal{O}, (1,0), (i,0), (-i,0)\} \quad \cong \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$$

$$\begin{array}{cccc} \overline{\rho_2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2 \hookrightarrow & S_3 = GL_2(\mathbb{F}_2) \\ \mathrm{id} & \longmapsto & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \text{complex conjugation} & \longmapsto & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array}$$

Example 3.1.13
$E/\mathbb{Q}: \quad y^2 = x^3 - 2$

$$\overline{\rho_2} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}) \cong S_3 = GL_2(\mathbb{F}_2)$$

Remark. Important Theorem (Serre): E/K non-CM, K number field $\Rightarrow$ $\overline{\rho_l}$ surjective $\mathrm{Gal}(\overline{K}/K) \twoheadrightarrow GL_2(\mathbb{F}_l)$ for almost all l

Notation: $\mu_m = m$-th roots of unity in $\overline{K}$ ($\cong \mathbb{Z}/m\mathbb{Z}$ abelian group)

$\bigwedge^2 E[m] \cong \mu_m$ as a Galois module:

Theorem 3.1.14
E/K. There is a bilinear, alternating, non-degenerate, Galois-equivalent pairing

$$e_m : E[m] \times E[m] \to \mu_m \qquad \underline{\text{Weil pairing}}$$

which is adjoint w.r.t. isogenies

$S, T \in E[m]$
bilinear: $e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T)$ and $e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2)$
alternating: $e_m(T, T) = 1 \quad (\Rightarrow e_m(S, T) = e_m(T, S)^{-1})$
non-degenerate: if $e_m(S, T) = 1 \ \forall S \in E[m]$ then $T = \mathcal{O}$
Galois: $e_m(S^\sigma, T^\sigma) = e_m(S, T)^\sigma \ \forall \sigma \in \mathrm{Gal}(\overline{K}/K)$
adjoint: $\phi : E_1 \to E_2$, $\hat{\phi} : E_2 \to E_1$, $S \in E_1[m], T \in E_2[m]$, then $e_m(S, \hat{\phi}(T)) = e_m(\phi(S), T)$

Over $\mathbb{C}$: $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2$

$$e_m(\frac{a}{m}w_1 + \frac{k}{m}w_2, \frac{c}{m}w_1 + \frac{d}{m}w_2) = \exp(2\pi i \frac{ad - bc}{m}) \ \forall a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$$

Proof
Construction:
Say $D_1 = \sum_i a_i(P_i)$, $D_2 = \sum_j b_j(Q_j)$ are disjoint if $P_i \neq Q_j$ (written $D_1 \cap D_2 = \emptyset$)
If $f \in \overline{K}(E)^\times, D = \sum_i a_i(P_i)$ with $\mathrm{div}(f) \cap D = \emptyset$
then define

$$f(D) := \prod_i f(P_i)^{a_i} \quad \in \overline{K}^\times$$

Exercise: (Weil reciprocity) If $\operatorname{div}(f) \cap \operatorname{div} g = \emptyset$, then $f(\operatorname{div}(g)) = g(\operatorname{div}(f))$ (Hint: do $\mathbb{P}^1$ first)

Note:

$$\begin{array}{rcl} E[m] & = & \{D \in \operatorname{Pic}^0(E) | mD \sim 0\} \\ T & \mapsto & (T) - (\mathcal{O}) \\ \sum a_i P_i & \leftarrow & D = \sum a_i(P_i) \end{array}$$

We define e_m on the RHS:
Choose $D_S = \sum a_i(P_i)$, $D_T = \sum b_j(Q_j)$

$$\begin{array}{rcl} mD_S & = & \operatorname{div}(f_S) \\ mD_T & = & \operatorname{div}(f_T) \\ D_S \cap D_T & = & \emptyset \quad \text{(easy using Riemann-Roch)} \end{array}$$

So now we can define:

$$e_m(S,T) := \frac{f_S(D_T)}{f_T(D_S)}$$

Note: $e_m(S,T)^m = \dfrac{f_S(mD_T)}{f_T(mD_S)} = \dfrac{f_S(\operatorname{div}(f_T))}{f_T(\operatorname{div}(f_S))} = 1$
$\Rightarrow \; e_m(S,T) \in \mu_m$

Exercise: e_m is well-defined
Properties: Computation □

3.1.2 Characteristic polynomials of endomorphisms

$E/K, \phi \in \operatorname{End}_K(E), m = \deg \phi$

Lemma 3.1.15
$\exists a_\phi \in \mathbb{Z}$ s.t. the characteristic polynomial

$$f_\phi(T) := T^2 - a_\phi T + m$$

has $f_\phi(\phi) = 0$

Proof
$\deg \phi = \phi\widehat{\phi} = m$
$\deg(1-\phi) = (1-\phi)(1-\widehat{\phi}) = 1 - (\phi + \widehat{\phi}) + m \;\Rightarrow\; \phi + \widehat{\phi} \in \mathbb{Z} \subseteq \operatorname{End}_K(E)$
Let $a_\phi := \phi + \widehat{\phi} \in \mathbb{Z}$
$\Rightarrow \quad f_\phi(T) = T^2 - (\phi + \widehat{\phi})T + \phi\widehat{\phi}$
$\Rightarrow \quad f_\phi(\phi) = 0$ □

Lemma 3.1.16
$f_\phi(T) = (T-\alpha)(T-\overline{\alpha})$ with $\alpha \in \mathbb{C}, |\alpha| = \sqrt{m}$

Proof
Need $\Delta_{f_\phi} = a_\phi^2 - 4m \le 0$
$f(\frac{b}{c}) = \frac{1}{c^2}\deg(c\phi - b) \ge 0 \;\; \forall \frac{b}{c} \in \mathbb{Q}$
$\Rightarrow \quad f(x) \ge 0 \;\; \forall x \in \mathbb{R} \quad \Rightarrow \quad \Delta \le 0$ □

Lemma 3.1.17
$\phi : E \to E$ induces $\phi_l : T_l E \to T_l E$ ($l \neq \text{char } K$)
and

$$\det(\phi_l - TI) = f_\phi(T)$$

i.e. characteristic polynomial of ϕ_l is in $\mathbb{Z}[T]$ (not just $\mathbb{Z}_l[T]$) and is independent of l

Proof
Want: $\det \phi_l = \deg \phi \ \forall \phi \in \text{End}_K(E)$ (so then constant term of $T^2 + a_\phi T + c$ is clear)
Then also

$$\begin{aligned} a_\phi &= 1 - \deg(1-\phi) + \deg \phi \\ \phi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\in M_2(\mathbb{Z}_l) \\ \text{tr } \phi_l &= 1 - \det(1-\phi_l) + \det(\phi_l) \end{aligned}$$

Then linear term of the characteristic polynomial are done too.

To prove $\deg \phi_l = \deg \phi$. Write $E[l^n] = \mathbb{Z}/l^n\mathbb{Z} \cdot v_1 + \mathbb{Z}/l^n\mathbb{Z} \cdot v_2$, $\phi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $e = e_{l^n}$ for the Weil pairing

$$\begin{aligned} e(v_1, v_2)^{\deg \phi} &= e(\deg \phi \cdot v_1, v_2) = e(\widehat{\phi}\phi \cdot v_1, v_2) \\ &= e(\phi v_1, \phi v_2) = e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det \phi_l} \end{aligned}$$

e non-degenerate $\Rightarrow \deg \phi \equiv \det \phi_l \mod l^n$
True for all $n \geq 1 \Rightarrow \deg \phi = \deg \phi_l$ ☐

3.2 Elliptic Curves over Finite Fields

$K = \mathbb{F}_q$ finite, $q = p^d$
$\mathbb{P}^n(K) = \{(a_0 : \ldots : a_n) \in K^{n+1} \setminus \{0\}\}/K^\times$ finite set, size $\frac{q^{n+1}-1}{q-1}$
C/K curve $\Rightarrow C(K)$ finite
E/K elliptic curve $\Rightarrow E(K)$ finite abelian group

Example 3.2.1
$E: \ y^2 = x^3 + 1$ over $K = \mathbb{F}_5$
$|E(\mathbb{F}_5)| = 6, \quad E(\mathbb{F}_5) = \{\mathcal{O}, (0, \pm 1), (2, \pm 3), (4, 0)\} \cong \mathbb{Z}/6\mathbb{Z}$
$|E(\mathbb{F}_{25})| = 36$
$|E(\mathbb{F}_{125})| = 126$, etc.

Definition 3.2.2
Zeta-function of a curve C/K (or a variety)

$$\begin{aligned} Z_{C/\mathbb{F}_q}(T) &:= \exp\left(\sum_{n=1}^{\infty} \frac{\#C(\mathbb{F}_{q^n})}{n} T^n\right) \\ &= 1 + \#C(\mathbb{F}_q)T + \cdots \end{aligned}$$

Example 3.2.3
$C = \mathbb{P}^1$

$\# \mathbb{P}^1(\mathbb{F}_{q^n}) = 1 + q^n$ (since $\{\infty\} \cup K$), so

$$\begin{aligned} Z_{\mathbb{P}^1/\mathbb{F}_{q^n}}(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{T^n}{n} + \sum_{n=1}^{\infty} \frac{q^n T^n}{n}\right) \\ &= \exp(-\log(1-T) - \log(1-qT)) \\ &= \frac{1}{(1-T)(1-qT)} \end{aligned}$$

Theorem 3.2.4 (Hasse)
For an elliptic $E/\mathbb{F}_q$

$$\begin{aligned} Z_{E/\mathbb{F}_q}(T) &= \frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-qT)} \quad \text{with } |\alpha| = \sqrt{q}, \alpha \in \mathbb{C} \\ &= \frac{1 - aT + qT^2}{(1-T)(1-qT)} \quad \text{with } a = q + 1 - \#E(\mathbb{F}_q) \end{aligned}$$

and $T^2 - aT + q = f_{\mathrm{Frob}_q}(T) =$ characteristic polynomial of Frob_q on $T_l E$ for $l \nmid q$

Corollary 3.2.5
$\#E(\mathbb{F}_q)$ determines $\#E(\mathbb{F}_{q^n})\ \ \forall n \geq 1$

Corollary 3.2.6 (Hasse-Weil Inequality)
$\#E(\mathbb{F}_{q^n}) = 1 - \alpha^n - \overline{\alpha}^n + q^n\ \ \forall n \geq 1$
In particular,

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

Remark. (Weil:) This is true for all curves, numerator = inverse characteristic polynomial of Frob_q on $T_l(\mathrm{Jac}(C))$ of degree $2g(C)$
"Weil conjectures": Has analogue for all varieties, but this is much harder (Dwork, Deligne, Grothendeck)
$T_l \rightsquigarrow$ étale cohomology

Corollary 3.2.7
$\psi : E \to E'$ isogeny over K, then $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$

Proof
ψ induces $T_l E \to T_l E'$, isomorphism of $\mathrm{Gal}(\overline{K}/K)$-modules when $l \nmid \deg \psi$
$\Rightarrow \quad \mathrm{Frob}_q \in \mathrm{Gal}(\overline{K}/K)$ has same characteristic polynomial on both ☐

Remark. Converse also holds (Silverman Chapter V)
Generally for abelian varieties over $\mathbb{F}_q$

$$\mathrm{Hom}(A, A') \otimes \mathbb{Z}_l \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{Gal}(\overline{K})/K}(T_l A, T_l A')$$

this is the "Tate's Theorem on endomorphisms"
(Faltings:) Also true over number field, but much harder

Can think of $T_l E$ as something that replaces a complex lattice

Proof of Hasse's Theorem 3.2.4
Let $\phi = \mathrm{Frob}_q : E \to E^{(q)} = E$ (Recall $E^{(q)}$ is the E with coefficient in $\mathbb{F}_q = \{a \in \overline{\mathbb{F}_q} | a^q = a\}$)
$\Rightarrow \quad \phi \in \mathrm{End}(E)$
Write $f_\phi(T) = 1 - aT + qT^2 = (1-\alpha T)(1-\overline{\alpha}T)$

$E(\mathbb{F}_q) =$ fixed points of $\phi : E \to E = \ker(1-\phi)$
$1-\phi$ is separable, because $(1-\phi)^* w = w - 0 \neq 0$

$$\begin{aligned} \Rightarrow \quad |\ker(1-\phi)| &= \deg(1-\phi) \\ &= (1-\phi)(1-\widehat{\phi}) \\ &= 1-a+q \\ &= 1-\alpha-\overline{\alpha}+q \end{aligned}$$

Similarly

$$\begin{aligned} |E(\mathbb{F}_{q^n})| &= \deg(1-\phi^n) \\ &= (1-\alpha^n)(1-\overline{\alpha}^n) \quad \alpha, \overline{\alpha} \text{ eigenvalues on } T_l E \\ &= 1-\alpha^n-\overline{\alpha}^n+q^n \end{aligned}$$

Put these in $Z(T)$ and we are done □

Example 3.2.8
$E: \ y^2 = x^3+1$ over $\mathbb{F}_5$
$\phi = \mathrm{Frob}_p$ satisfies $T^2 - aT + q = 0$
$a = 5+1-\#E(\mathbb{F}_5) = 0$
$\Rightarrow \quad f_\phi(T) = 1+5T^2$, $Z_{E/\mathbb{F}_q}(T) = \frac{1+5T^2}{(1-T)(1-5T)}$ $(\alpha, \overline{\alpha} = \sqrt{-5}, -\sqrt{-5})$

$$\begin{aligned} \#E(\mathbb{F}_{5^n}) &= 1-(\sqrt{-5})^n-(-\sqrt{-5})^n+5^n \\ &= 6 \quad \text{if } n=1 \\ &= 36 \quad \text{if } n=2 \\ &= 126 \quad \text{if } n=3 \end{aligned}$$

3.2.1 Reduction mod p

$K = \mathbb{Q}$, p prime, p-adic valuation:

$$\begin{aligned} v = v_p : \mathbb{Q}^\times &\to \mathbb{Z} \\ p^n \frac{a}{b} &\mapsto n \end{aligned}$$

with $(ab, p) = 1$
$\mathcal{O} = \{\frac{a}{b} \in \mathbb{Q} \,|\, p \nmid b\}$
$\mathcal{O}$ mod $p = k = \mathbb{F}_p$ residue field

Generally K field, valuation $v : K^\times \to \mathbb{Z}$
$\mathcal{O} = \{x \in K | v(x) \geq 0\}$ integer ring
$p \rightsquigarrow \pi$ uniformiser, $v(\pi) = 1$
$k = \mathcal{O}/\pi$ residue field

Definition 3.2.9
E/K elliptic curve. A Weierstrass equation

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

is integral at p if all $a_i \in \mathcal{O}$ ($\exists$ rescale $a_i \mapsto p^i$ enough times)
Then $\Delta \in \mathcal{O}, v(\Delta) \geq 0$

A minimal model at p is an integral model with $v(\Delta)$ minimal among integer models
THe reduced curve:

$$\widetilde{E}/K: \ y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6}, \quad \overline{a_i} = a_i \mod p$$

for any minimal model

Easy: minimal model is unique up to $\begin{array}{lll} x & \mapsto & u^2x+r \\ y & \mapsto & u^3y+sx+t \end{array}$; $u,r,s,t \in \mathcal{O}, u \in \mathcal{O}^\times$; induces $\cong$ on reduced curves. When char $k = p \neq 2,3$, may take $y^2 = x^3+ax+b$, $\begin{array}{lll} x & \mapsto & u^2x \\ y & \mapsto & u^3y \end{array}$ as usual.

Example 3.2.10
$y^2 = x^3 - 3\cdot 5^5 x - 3\cdot 5^6$ integral, not minimal at $p=5$, $\Delta = -2^4\cdot 3^3 \cdot 5^{13}$
$x \mapsto 5^2 x$
$y \mapsto 5^3 y$
$a_i \mapsto 5^{-i} a_i$
$\Delta \mapsto 5^{-12}\cdot\Delta$
$\rightsquigarrow$ $y^2 = x^3 - 3x - 3$ integral, $\Delta = -2^4 \cdot 3^3 \cdot 5$ minimal at 5 ($v(\Delta)$ can only change by multiples of 12)
Reduced curve: $\widetilde{E}:\ y^2 = x^3+2x+2 = (x-1)^2(x+2)$ over $\mathbb{F}_5$
Singular ($\Delta \mod p = 0$)

Exercise:
For $p \neq 2,3$ and $j(E) \in \mathcal{O}$ integral model $y^2 = x^3+ax+b$, $a,b \in \mathcal{O}$, is minimal $\Leftrightarrow v(\Delta) < 12$
($p=2,3:$ $\Leftarrow$ still true, but $\Rightarrow$ false, classification is more complicated, need "Tate's algorithm")

Remark. If $K = \mathbb{Q}$ (or number field with class number 1) may choose $a_i \in \mathbb{Z}$ (or $a_i \in \mathcal{O}_K$ resp.) minimal at all primes, global minimal model

3.2.2 Reduction types

Take minimal model ($p \neq 2$), $y^2 = x^3+ax^2+bx+c =: f(x)$, $a,b,c \in \mathcal{O}$
Roots of $\overline{f} = f \mod p$

- Good reduction, $\Delta \not\equiv 0 \mod p$:
  Distinct roots, $\widetilde{E}$ elliptic curve (i.e. non-singular)
- Bad reduction, $\Delta \equiv 0 \mod p$:
  - Multiplicative reduction
    Double root $\widetilde{E}:\ y^2 = x^2(x+\eta)$, this has 2 cases:
    (1) split: $\sqrt{\eta} \in k^\times$
    (2) non-split: $\sqrt{\eta} \notin k^\times$
  - Additive reduction
    Triple root, equivalently, $16a^2 - 28b \not\equiv 0 \mod p$; $\widetilde{E}: y^2 = x^3$

Definition 3.2.11
$\widetilde{E}_{ns}(k) := \widetilde{E}(k) \setminus \{$ singular point if there is one$\}$

In all cases, this is an abelian group with identity $0 = (0:1:0)$
Group law $P+Q+R = 0 \Leftrightarrow P,Q,R$ on a line

Reduction type	$\widetilde{E}_{ns}(k)$ isomorphic to (via $(x,y)\mapsto y/x$)
Additive	$\mathbb{P}^1\setminus\{0\} = \mathbb{G}_a$ additive group
Split multiplicative	$\mathbb{P}^1\setminus\{\pm\sqrt{\eta}\} = \mathbb{G}_m$ multiplicative group
Non-split multiplicative	$k(\sqrt{\eta})^\times/k^\times$ abelian group of order p^n+1

$y^2 = x^3 + \eta x^2$ "looks like" $y^2 - \eta x^2 = 0$ (near (0,0)), so "looks like" $(y-\sqrt{\eta}x)(y+\sqrt{\eta}x) = 0$
$\pm\sqrt{\eta}$ slopes of the two tangent lines (asymtopes)

Proposition 3.2.12
K'/K finite extension, $v' : (K')^\times \twoheadrightarrow \mathbb{Z}$ s.t. $v'|_{K^\times} = ev$ ($e \geq 1$ ramification index)

(1) E good or multiplicative reduction over $K \Rightarrow$ minimal model stays minimal, reduction type stays the same (non-split may become split)

(2) E addictive over $K \Rightarrow \exists K'$ s.t. E/K' either good, $v(j_E) \geq 0$ or multiplicative, $v(j_E) < 0$
We say E/K has potentially good (resp. potentially multiplicative) reduction

Good and multiplicative reduction are called semistable reduction type
Additive also called unstable

Proof
($p \neq 2$)

(1) Clear from the equation

(2) Adjoin roots of $f(x)$ to K, put E in Legendre form (c.f. Example Sheet 2):

$$y^2 = x(x-1)(x-\lambda), \quad \lambda \in \mathcal{O}$$

integral model $j = \dfrac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2}$
$\lambda \not\equiv 0, 1 \mod v' \Rightarrow \widetilde{E}$ elliptic; $v(j) \geq 0$
$\lambda \equiv 0, 1 \mod v' \Rightarrow \widetilde{E}$ has double root; $v(j) < 0$

□

3.2.3 Reduction on Points

$\mathbb{P}^n(K) \ni (x_0 : \cdots : x_n) = (\alpha x_0 : \cdots \alpha x_n)$ choose $\alpha \in K^\times$ s.t. $\alpha x_i \in \mathcal{O}$ for some $x_j \in \mathcal{O}^\times$
$\mapsto (\overline{\alpha x_0} : \cdots : \overline{\alpha x_n}) \in \mathbb{P}^n(k)$ (via mod p)

Clearly independent of the choice of α
For E/K elliptic curve, get

$$\begin{aligned} \text{mod } p : E(K) &\rightarrow \widetilde{E}(k) \\ (x,y) &\mapsto \begin{cases} (\overline{x}, \overline{y}) & \text{if } x, y \in \mathcal{O} \\ (0:1:0) = 0 & \text{if } x, y \notin \mathcal{O} \end{cases} \end{aligned}$$

Definition 3.2.13
$E_0(K) = \{P \in E(K) | P \text{ reduces to a point in } \widetilde{E}_{ns}\}$
subgroup of $E(K)$ as $P + Q + R = 0 \Rightarrow P, Q, R$ on a line
$\Rightarrow \overline{P}, \overline{Q}, \overline{R}$ on a line
$\Rightarrow \overline{P} + \overline{Q} + \overline{R} = 0$ in $E_0(K)$
and $E_0(K) \rightarrow \widetilde{E}_{ns}(k)$ is a group homomorphism

Definition 3.2.14
$E_1(K)$ = kernel of above homomorphism
$= \{P \in E(K) | P \text{ reduces to } (0:1:0)\}$
$= \{P = (x,y) \in E(K) | v_p(x) \geq 1, v_p(y) \geq 1\}$ subgroup, so get exact sequence:

$$0 \rightarrow E_1(K) \rightarrow E_0(K) \xrightarrow[\text{}]{\substack{\text{group hom} \\ \text{mod } p}} \widetilde{E}_{ns}(k)$$

Example 3.2.15
$E/\mathbb{Q}: \quad y^2 = x(x+2)(x-3) \quad \Delta = 2^6 3^2 5^2, p = 3$
$\downarrow$
$\widetilde{E}/\mathbb{F}_3: \quad y^2 = x^2(x-1) = x^3 + 2x^2 \quad$ singular ($\sqrt{2} \notin \mathbb{F}_3$ non-split multiplicative reduction)

$\widetilde{E}_{ns}(\mathbb{F}_3) \cong \mathbb{F}_9^\times / \mathbb{F}_3^\times \cong \mathbb{Z}/4\mathbb{Z} = \{\mathcal{O}, (2,1), (1,0), (2,2)\}$
(see picture)
$\mathcal{O} \xrightarrow{\text{mod } 3} \mathcal{O}$
$T_1 = (-2, 0) \mapsto (1, 0)$
$T_2 = (0, 0) \mapsto (0, 0)$ (singular)
$T_3 = (3, 0) \mapsto (0, 0)$ (singular)
$P = (-1, -2) \mapsto (2, 1)$
$2P = (\frac{49}{16}, -\frac{63}{64}) \mapsto (1, 0)$
$2P + T_1 = (-\frac{2}{82}, \frac{280}{729}) \mapsto \mathcal{O}$

$$\begin{array}{rcl} E(\mathbb{Q}) & = & \overbrace{\mathbb{Z}/2}^{T_1} \times \overbrace{\mathbb{Z}/2}^{T_2} \times \overbrace{\mathbb{Z}}^{P} \\ & & \bigcup | \text{ index } 2 \\ E_0(\mathbb{Q}) & = & \underbrace{\mathbb{Z}/2}_{T_1} \times \underbrace{\mathbb{Z}}_{P} \\ & & \bigcup | \text{ index } 4 \quad (\text{in this case, } E_0/E_1 \leftrightarrow \widetilde{E}_{ns}(\mathbb{F}_3)) \\ E_1(\mathbb{Q}) & = & \underbrace{\mathbb{Z}}_{2P+T_1} \end{array}$$

3.3 Elliptic Curves over Local Fields

3.3.1 Completeness and Hensel

$K, v : K^\times \twoheadrightarrow \mathbb{Z}$, $\mathcal{O}, k, \pi$ as above $\rightsquigarrow$ topology on K given by a norm

$$|x| = \left(\frac{1}{\#k}\right)^{v(x)} \qquad x \in K, |0| = 0$$

Properties:

$$\begin{array}{rcl} |xy| & = & |x| \cdot |y| \\ |x+y| & \leq & \max(|x|, |y|) \leq |x| + |y| \quad \text{strong triangle inequality} \\ |x| = 0 & \Leftrightarrow & x = 0 \end{array}$$

$|\cdot|$ is called a non-Archimedean absolute value

Definition 3.3.1
We say $x_n (\in K) \to x (\in K)$ if $|x_n - x| \to 0$
$\Leftrightarrow \quad v(x_n - x) \to \infty$
$\Leftrightarrow \quad x_n \equiv x \mod$ larger and larger powers of π as $n \to \infty$

Definition 3.3.2
The completion $\widehat{K}$ of K (wrt v or $|\cdot|$)
= the completion in topological sense
= {Cauchy sequences x_n, $x_n \in K, |x_n - x_m| \to 0$ as $n, m \to \infty$}/{ sequence $x_n \to 0$}
= field, contains K; $v : \widehat{K} \twoheadrightarrow \mathbb{Z}$ extending one on K with ring of integer $\widehat{\mathcal{O}}$, and same π, k

Definition 3.3.3
K complete $\Leftrightarrow K = \widehat{K} \Leftrightarrow$ every Cauchy sequence converges
(Alternatively: $\widehat{\mathcal{O}} := \varprojlim_{n \geq 1}(\mathcal{O}/\pi^n), \widehat{K} := ff(\widehat{\mathcal{O}})$)

Example 3.3.4
$K = \mathbb{Q}, v = v_p$
$\widehat{\mathcal{O}} = \mathbb{Z}_p = \left\{ \sum_{n=0}^{\infty} a_n p^n | a_n \in \{0, \dots, p-1\} \right\} \supseteq \mathbb{Z}$
$\widehat{K} = \mathbb{Q}_p = \left\{ \sum_{n=n_0}^{\infty} a_n p^n | n_0 \in \mathbb{Z}, a_n \in \{0, \dots, p-1\} \right\}$

Theorem 3.3.5 (Hensel's Lemma)
K complete wrt $v : K^\times \to \mathbb{Z}$, $f(x) \in \mathcal{O}[x], \overline{f} = f \mod \pi \in k[x]$
If $\widetilde{\alpha} \in k$ is s.t. $\overline{f}(\widetilde{\alpha}) = 0, \overline{f}'(\widetilde{\alpha}) \neq 0$
then $\exists! \alpha \in \mathcal{O}$ s.t. $\overline{\alpha} = \widetilde{\alpha}, f(\alpha) = 0$
("simple root lift from k to K")

Proof
Lift $\widetilde{\alpha} \in k$ to any $\alpha_1 \in \mathcal{O}$, let $\alpha_{n+1} = \alpha_n - \dfrac{f(\alpha_n)}{f'(\alpha_n)}$
Check α_n Cauchy so $\alpha_n \to \alpha$ and $f(\alpha) = 0$
(see Newton's method picture) □

3.3.2 Analysis of $E(K)$ for K complete, E/K elliptic curve

Case I: E vs. E_0

Theorem 3.3.6 (Kodaira-Néron)
Write $n = v(\Delta_{\min})$.
Then $E(K)/E_0(K)$ (Néron component group) is finite and

$$\frac{E(K)}{E_0(K)} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & E \text{ has split multi. reduction} \\ \{1\} & E \text{ has non-split multi. reduction and } n \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} & E \text{ has non-split multi. reduction and } n \text{ even} \\ \text{Group of order} \leq 4 & E \text{ has additive reduction} \end{cases}$$

The first 3 cases are called reduction type I_n

Remark. Tate's algorithm $\Rightarrow$ more precise description.
Reduction types $II, III, IV, I_n^o, I_n^*, IV^*, III^*, II^*$

Proof
See exercises □

Case II: E_0 vs. E_1

Theorem 3.3.7
K complete, $0 \to E_1(K) \to E_0(K) \to \widetilde{E}_{ns}(k) \to 0$ is exact
i.e. $E_0(K) \twoheadrightarrow \widetilde{E}_{ns}(k)$

Proof
$E: \ g(x,y) = 0$ integral ($g(x,y) = y^2 + a_1xy + a_3y - x^3 - \cdots$)
Take $\widetilde{P} = (\widetilde{x}, \widetilde{y}) \in \widetilde{E}_{ns}(k) \setminus \{0\}$ non-singular
$\Rightarrow \quad \frac{\partial \widetilde{g}}{\partial x}\big|_{\widetilde{P}} \neq 0$ or $\frac{\partial \widetilde{g}}{\partial y}\big|_{\widetilde{P}} \neq 0$

If $\frac{\partial \widetilde{g}}{\partial y}\big|_{\widetilde{P}} \neq 0$, lift $\widetilde{x}$ to any $x \in \mathcal{O}$, solve $g(x,y) = 0$ (as equation of y) by Hensel.
If $\frac{\partial \widetilde{g}}{\partial x}\big|_{\widetilde{P}} \neq 0$, lift $\widetilde{y}$ to $y \in \mathcal{O}$, solve $g(x,y) = 0$ (as equation of x) by Hensel □

Case III: E_1

K complete, $\mathcal{O}$, $\mathfrak{m} = \pi\,\mathcal{O}, \mathcal{O}\,/\,\mathfrak{m} = k$

Proposition 3.3.8
The following map is a bijection

$$\begin{array}{rcll} E_1(K) & \leftrightarrow & \mathfrak{m} & \\ (x,y) & \mapsto & \dfrac{x}{y} & \quad \text{(uniformiser at } \mathcal{O}) \\ \mathcal{O} & \mapsto & 0 & \end{array}$$

Proof
(char $k \neq 2,3$)
$E: \ y^2 = x^3 + ax + b \ \ (\mathbb{A}^2_{Z=1}) \subseteq Y^2Z = X^3 + aXZ^2 + bZ^3 \ \ (\mathbb{P}^2)$
$z = w^3 + awz^2 + bz^3 \ \ (\mathbb{A}^2_{Y\neq 0}) \subseteq Y^2Z = X^3 + aXZ^2 + bZ^3 \ \ (\mathbb{P}^2)$

$$(x,y) \xrightarrow{\text{homogenise}} (x:y:1) = (\frac{x}{y} : 1 : \frac{1}{y}) \mapsto (\underbrace{\frac{x}{y}}_{w}, \underbrace{\frac{1}{y}}_{z})$$

(see pictures)

For each $w \in \mathfrak{m}$ (i.e. $w \equiv 0 \mod \pi$), equation $z = w^3 + awz^2 + bz^3$ has a unique solution, $z(w)$ by Hensel's Lemma ($\frac{\partial}{\partial z}\big|_{(0,0)} = 1 \neq 0$)
$\Rightarrow \quad E_1(K) \ni (w, z(w)) \leftrightarrow w \in \mathfrak{m}$ is a bijection □

Remark. Do Hensel's explicitly $\Rightarrow$ $z(w)$ some explicit power series

$$z(w) = w^3 + aw^7 + bw^9 + 2a^2a^{11} + 5abw^{13} + \cdots \quad \in \mathbb{Z}[a,b][[w]]$$

universal. On $Y = 1$ chart

$$\begin{array}{rcl} y(w) & = & \dfrac{1}{z(w)} = \dfrac{1}{w^3} - aw - bw^3 - a^2w^5 - 3abw^7 + \cdots \\ x(w) & = & \dfrac{w}{z(w)} = \dfrac{1}{w^2} - aw^2 - bw^4 - a^2w^6 + \cdots \end{array}$$

$$\Rightarrow \quad \begin{array}{rcc} E_1(K) & \leftarrow (1:1) \rightarrow & \mathfrak{m} \\ (x,y) & \longmapsto & \frac{x}{y} \\ (x(w), y(w)) & \longleftarrow & w \end{array}$$

3.4 Formal Group

Addition $E_1(K) \times E_1(K) \to E_1(K)$
becomes $\mathcal{F} : \mathfrak{m} \times \mathfrak{m} \to \mathfrak{m}$

$$\begin{array}{lll} w_1 & \mapsto & (\overbrace{x(w_1)}^{x_1}, \overbrace{y(w_1)}^{y_1}) \\ w_2 & \mapsto & (\underbrace{x(w_2)}_{x_2}, \underbrace{y(w_2)}_{y_2}) \end{array} \longmapsto \begin{array}{rcl} \kappa & = & \frac{y_2-y_1}{x_2-x_1} \\ x_3 & = & \kappa^2 - x_1 - x_2 \\ y_3 & = & -\kappa(x_3 - x_1) + y_1 (\in K((w_1, w_2))) \end{array} \longmapsto w_3 = \frac{x_3}{y_3}$$

$$\begin{aligned} w_3 &= w_1 + w_2 + 2aw_1w_2(w_1^3 + w_1^2w_2 + w_1w_2^2 + w_2^3) \\ &\quad -3bw_1w_2(w_1^5 + 3w_1^4w_2 + 5w_1^3w_2^2 + 5w_1^2w_2^3 + 3w_1w_2^4 + w_2^5) \\ &\quad + \cdots \\ &=: \mathcal{F}(w_1, w_2) \in K[[w_1, w_2]] \end{aligned}$$

(in fact, $\mathcal{F}(w_1, w_2) \in \mathbb{Z}[a, b][[w_1, w_2]]$ universal for $y^2 = x^3 + ax + b$)

Remark. $\begin{array}{lll} x & \mapsto & x(w) \\ y & \mapsto & y(w) \end{array}$ is the embedding $K(E) \hookrightarrow$ completion of $K(E)$ wrt $v_0 : K(E)^\times \to \mathbb{Z} \cong K[[w]]$

This defines a "kind of addition on $\mathfrak{m}$"

$$w_1, w_2 \in \mathfrak{m} \rightsquigarrow \mathcal{F}(w_1, w_2) \in \mathfrak{m} \quad \text{(converges)}$$

Properties of μ (associative, commutative, etc.)
$\Rightarrow$ $\mathcal{F}$ is a formal group over $\mathcal{O}$

Definition 3.4.1
A (one parameter, commutative) formal group over a ring R is $\mathcal{F} \in R[[X, Y]]$ s.t.

(1) $\mathcal{F}(X, Y) = X + Y +$(terms of deg ≥ 2)
(2) (associative) $\mathcal{F}(X, \mathcal{F}(Y, Z)) = \mathcal{F}(\mathcal{F}(X, Y), Z)$
(3) (commutative) $\mathcal{F}(X, Y) = \mathcal{F}(Y, X)$
(4) (inverse) $\exists! i(T) \in R[[T]]$ s.t. $\mathcal{F}(T, i(T)) = 0 = \mathcal{F}(i(T), T)$
(5) (identity) $\mathcal{F}(X, 0) = X, \mathcal{F}(0, Y) = Y$

"Group law without elements"

Definition 3.4.2
A homomorphism of formal groups $\mathcal{F} \to \mathcal{G}$ is $f \in TR[[T]]$ s.t.

$$f(\mathcal{F}(X, Y)) = \mathcal{G}(f(X), f(Y))$$

$\mathcal{F}$ and $\mathcal{G}$ are isomorphic if $\exists$ hom. $f : \mathcal{F} \to \mathcal{G}$ and $g : \mathcal{G} \to \mathcal{F}$ s.t. $f(g(T)) = T$
(Exercise: $\Rightarrow$ $g(f(T)) = T$)

Remark. If $R = \mathcal{O}$ complete, $\mathfrak{m} \subseteq R$ maximal ideal, then

$$\begin{array}{rcl} \mathcal{F} : \mathfrak{m} \times \mathfrak{m} & \to & \mathfrak{m} \\ a, b & \mapsto & a \oplus_{\mathcal{F}} b = \mathcal{F}(a, b) \quad \text{(converges in } \mathfrak{m}) \end{array}$$

makes $(\mathfrak{m}, \oplus_{\mathcal{F}})$ into an abelian group, also denoted $\mathcal{F}(\mathfrak{m})$

Hom. $f : \mathcal{F} \to \mathcal{G}$ induces $\begin{array}{rcl} (\mathfrak{m}, \oplus_{\mathcal{F}}) & \to & (\mathfrak{m}, \oplus_{\mathcal{G}}) \\ a & \mapsto & \end{array}$

Example 3.4.3
Formal addition group: $\widehat{\mathbb{G}_a}(X,Y) = X + Y$
($\rightsquigarrow (\mathfrak{m}, +)$)

Example 3.4.4
Formal multiplicative group: $\widehat{\mathbb{G}_m}(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$
($\rightsquigarrow (1+\mathfrak{m}, \times)$)

Example 3.4.5
Formal group law on $E : y^2 = x^3 + ax + b$, $a, b \in \mathcal{O}$

$$\widehat{E} := \mathcal{F}(X,Y) = X + Y - 2aXY(\cdots) + \cdots$$

$\rightsquigarrow (\mathfrak{m}, \oplus_{\mathcal{F}}) = E_1(K)$

<u>Exercise</u>: Find $i(T)$ in all 3 cases

Example 3.4.6
$\mathcal{F}$ any formal group, denote $\mathcal{F}(X,Y)$ by $X \oplus_{\mathcal{F}} Y$

$$\begin{aligned}
[0](T) &:= 0 \\
[1](T) &:= T \\
[-1](T) &:= i(T) \\
[m](T) &:= \underbrace{T \oplus_{\mathcal{F}} T \cdots \oplus_{\mathcal{F}} T}_{m \text{ times}} \quad \text{(similarly for } m < 0\text{)}
\end{aligned}$$

are homomorphisms $\mathcal{F} \to \mathcal{F}$

<u>E.g.</u>: On $\widehat{E}$

$$[2](T) = 2T - 2aT^5 - 54bT^7 - 140a^2T^9 + O(T'')$$

Example 3.4.7
R field of char. 0

$$\widehat{\mathbb{G}_a} \underset{\log(1+T)}{\overset{\exp(T)-1}{\rightleftarrows}} \widehat{\mathbb{G}_m} \quad \text{isomorphism (check)}$$

Example 3.4.8
$\phi = (\phi_x(x,y), \phi_y(x,y)) : E_1 \to E_2$ isogeny over K
induces $\widehat{E_1} \to \widehat{E_2}$ over K

$$\frac{\phi_y(x(T), y(T))}{\phi_x(x(T), y(T))} \in TK[[T]]$$

3.5 Structure of formal groups

3.5.1 Filtration

$R = \mathcal{O}$ complete, $\mathfrak{m}$ maximal ideal, $\mathcal{F}$ formal group over R, $k = R/\mathfrak{m}$

$$\mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots \quad \text{sets}$$

$$x, y \in \mathfrak{m}^n \;\Rightarrow\; x \oplus_{\mathcal{F}} y = \underbrace{x + y}_{\in \mathfrak{m}^n} + (\text{something} \in \mathfrak{m}^{n+1}) \in \mathfrak{m}^n$$

$$\mathcal{F}(\mathfrak{m}) \supseteq \mathcal{F}(\mathfrak{m}^2) \supseteq \cdots \quad \text{subgroups}$$

$$\begin{array}{rcl} \mathcal{F}(\mathfrak{m}^n)/\,\mathcal{F}(\mathfrak{m}^{n+1}) & \cong & (\mathfrak{m}^n\,/\,\mathfrak{m}^{n+1}, +) \;\cong\; (k,+) \\ x & \leftrightarrow & x \end{array}$$

So "$\mathcal{F}$ (like $\widehat{\mathbb{G}_a}$) is built up from pieces that look like k"

3.5.2 Invertible Homomorphism

(Work over any R)

Theorem 3.5.1
A homomorphism $f(T) = a_1T + a_2T^2 + \cdots : \mathcal{F} \to \mathcal{F}$ is an isomorphism $\Leftrightarrow a_1 \in R^\times$

Proof
$\underline{\Rightarrow}$:
$f(g(T)) = T, g(T) = b_1T + b_2T^2 + \cdots$
$f(g(T)) = a_1b_1T + \cdots = T$
$\Rightarrow \quad a_1b_1 = 1$
$\Rightarrow \quad a_1 \in R^\times$

$\underline{\Leftarrow}$:
Assume $a_1^{-1} \in R$, let $g_1(T) = a_1^{-1}T$
Want: Construct inductively unique $g_n(T) = g_{n-1}(T) + \lambda_nT^n$
s.t. $f(g_n(T)) \equiv T \mod T^{n+1}$
$\Rightarrow \quad g := \lim g_n \in TR[[T]]$ is unique g s.t. $f(g(T)) = T$

$$\begin{array}{rcl} f(g_n(T)) & = & f(g_{n-1}(T) + \lambda_nT^n) \\ & \equiv & f(g_{n-1}(T)) + a_1\lambda_nT^n \mod T^{n+1} \\ & \equiv & \underbrace{T + bT^n}_{\substack{\text{by induction,} \\ \text{for some } b\in R}} + a_1\lambda_nT^n \mod T^{n+1} \end{array}$$

Now let $b + a_1\lambda_n = 0$ i.e. $\lambda := \frac{-b}{a_1} \Rightarrow$ unique g_n with $f(g_n(T)) \equiv T \mod T^{n+1}$ as required □

Corollary 3.5.2
$R = \mathcal{O}$ complte, $E_1(K)$ has no elts of order m, i.e. no m-torsion, for char $k \nmid m$ (such m are in $\mathcal{O}^\times$)

In general, we have

Corollary 3.5.3
$[m] : \mathcal{F} \to \mathcal{F}$ isom $\Leftrightarrow m \in R^\times$

Proof
$[m](T) = mT + \cdots$ (by induction, true $\forall\, m \in \mathbb{Z}$) □

3.5.3 The Invariant Differential

R ring, $\mathcal{F}\,/R$ formal group

Definition 3.5.4
A <u>differential form</u> ω=expression

$$f(X)dX \quad , \quad f \in R[[X]]$$

for a power series g in X

$$\omega \circ g := f(g(X))g'(X)dX$$

Definition 3.5.5
ω is an <u>invariant differential</u> of $\mathcal{F}/R$

$$\omega \circ \mathcal{F}(X,Y) = \omega$$

as a function of X.
i.e. if

$$f(\mathcal{F}(X,Y)) \cdot \underbrace{\mathcal{F}_1'(X,Y)}_{\text{derivative 1st var.}} dX = f(X)dX$$

ω is <u>normalised</u> if $\omega = (1 + \cdots)dX$ (equivalently, $f(0) = 1$)

Example 3.5.6
$\omega = dX$ on $\widehat{\mathbb{G}_a}$
$\omega = (1+X)^{-1}dX$ on $\widehat{\mathbb{G}_m}$
$\omega_{\widehat{E}} = \frac{x'(w)dw}{y(w)}$; $E: \quad y^2 = x^3 + ax + b$

Proposition 3.5.7
Any $\mathcal{F}/R$ has a unique normalised invariant differential, namely

$$\omega_{\mathcal{F}} := \mathcal{F}_1'(0,Y)^{-1}dY$$

Every invariant differential on $\mathcal{F}$ is of form $a\omega_{\mathcal{F}}$ some $a \in R$

Proof

$$\begin{aligned} & \mathcal{F}(X,\mathcal{F}(Y,Z)) &=& \mathcal{F}(\mathcal{F}(X,Y),Z) \\ \overset{\partial/\partial X}{\Rightarrow} & \mathcal{F}_1'(X,\mathcal{F}(Y,Z)) &=& \mathcal{F}_1'(\mathcal{F}(X,Y),Z) \cdot \mathcal{F}_1'(X,Y) \\ \overset{\text{Put } X=0}{\Rightarrow} & \mathcal{F}_1'(0,\mathcal{F}(Y,Z)) &=& \mathcal{F}_1'(Y,Z) \cdot \mathcal{F}_1'(0,Y) \end{aligned}$$

$\Rightarrow \quad \omega_{\mathcal{F}}$ invariant
$\mathcal{F}_1'(0,Y) = 1 + \cdots \quad \Rightarrow \quad$ normalised

Conversely, $f(X)dX$ invariant
$\Rightarrow \quad$ (by defn) $f(\mathcal{F}(X,Y))\mathcal{F}_1'(X,Y) = f(X)$
$\Rightarrow \quad$ (put $X = 0$) $f(Y) \cdot \mathcal{F}_1'(0,Y) = f(0)$
$\Rightarrow \quad f(Y)dY = f(0) \cdot \omega_{\mathcal{F}}$ $\square$

Corollary 3.5.8
$f : \mathcal{F} \to \mathcal{G}$ homomorphism, $f(T) = a_f T + \cdots$, (i.e. $a_f = f'(0)$) then

$$\omega_{\mathcal{G}} \circ f = a_f \cdot \omega_{\mathcal{F}}$$

Proof

$$\begin{aligned} \omega_{\mathcal{G}} \circ f(\mathcal{F}(X,Y)) &= \omega_{\mathcal{G}}(\mathcal{G}(f(X), f(Y))) \quad (f \text{ hom.}) \\ &= \omega_{\mathcal{G}} \circ f \quad (\omega_{\mathcal{G}} \text{ invariant}) \end{aligned}$$

$\omega_{\mathcal{F}}$ unique $\quad \Rightarrow \quad \omega_{\mathcal{G}} \circ f = \text{constant} \times \omega_{\mathcal{F}}$
constant $= a_f$ $\square$

Corollary 3.5.9
$f, g : \mathcal{F} \to \mathcal{G}$ hom. Then

$$\omega_{\mathcal{G}} \circ (\underbrace{f \oplus g}_{\text{addition form}}) = \omega_{\mathcal{G}} \circ f + \omega_{\mathcal{G}} \circ g$$

(as both equal $(a_f + a_g)\omega_{\mathcal{F}}$) (This was left unproved in Theorem 2.2.25 for isogenies of elliptic curves)

<u>Exercise</u>: p prime, $\mathcal{F}/R$ formal group

$$[p](T) = pf(T) + g(T^p) \quad \text{for some } f, g \in TR[[T]]$$

3.5.4 $\log_{\mathcal{F}}$ and $\exp_{\mathcal{F}}$

•$R = K$ field of characteristic 0, $\mathcal{F}/R$, $\omega_{\mathcal{F}} = (1 + a_1 T + \cdots)dT$

Definition 3.5.10

$$\log_{\mathcal{F}}(T) = \text{“}\int \omega_{\mathcal{F}}\text{”} = T + \frac{a_1}{2}T^2 + \frac{a_2}{3}T^3 + \cdots \in R[[T]]$$

Proposition 3.5.11
$\log_{\mathcal{F}} : \mathcal{F} \to \widehat{\mathbb{G}}_a$ isomorphism of formal groups

Proof
Integrate $\omega_{\mathcal{F}}(\mathcal{F}(X, Y)) = \omega_{\mathcal{F}}(X)$ to X:

$$\log_{\mathcal{F}}(\mathcal{F}(X, Y)) = \log_{\mathcal{F}}(X) + C(Y)$$

where $C(Y) \in R[[Y]]$ const. of integration
$X = 0 \quad \Rightarrow \quad C(Y) = \log_{\mathcal{F}}(Y) \quad \Rightarrow \quad \log_{\mathcal{F}}$ hom. to $\widehat{\mathbb{G}}_a$
Starts with $1 \cdot T + \cdots \quad \Rightarrow \quad$ isom (its inverse called $\exp_{\mathcal{F}}$) □

•K complete wrt $v : K^\times \to \mathbb{Z}$, char K=0, $R = \mathcal{O}$, $\mathfrak{m}$
Now $\log_{\mathcal{F}}, \exp_{\mathcal{F}}$ not necessarily defined over $\mathcal{O}$ (denominators!)
Analyse denominators carefully $\Rightarrow$ still ok on $\mathfrak{m}^n$ for n large enough

Theorem 3.5.12

(1) $\log_{\mathcal{F}} : \mathcal{F}(\mathfrak{m}^r) \xrightarrow{\sim} \widehat{\mathbb{G}}_{\mathrm{a}}(\mathfrak{m}^r)$ for $r > \frac{v(p)}{p-1}$

(2) If $x \in \mathcal{F}(\mathfrak{m})$ has exact order p^n then $p^{n-1}v(x) \leq \frac{v(p)}{p-1}$

Proof
See Silverman, IV 6.4, 61 □

Example 3.5.13
$K = \mathbb{Q}_p$, $\mathcal{F}/\mathbb{Z}_p$
p odd $\quad \Rightarrow \quad \mathcal{F}(p\,\mathbb{Z}_p) \cong (\mathbb{Z}_p, +) \quad (1 > \frac{v(p)}{p-1} = \frac{1}{p-1})$
$p = 2 \quad \Rightarrow \quad \mathcal{F}(4\,\mathbb{Z}_2) \cong (\mathbb{Z}_2, +)$

Example 3.5.14
Set $\mathcal{F} = \widehat{\mathbb{G}}_{\mathrm{m}}$ in the above example, we get:

$$\begin{aligned} (1 + p\,\mathbb{Z}_p, \times) &\cong (\mathbb{Z}_p, +) \quad p \text{ odd} \\ (1 + 4\,\mathbb{Z}_2, \times) &\cong (\mathbb{Z}_2, +) \end{aligned}$$

3.5.5 Consequences for all elliptic curves

WARNING: If E has minimal model $y^2 + a_1xy + a_3y = \cdots$ (may be necessary if char $k = 2$ or 3) then formulae for $x(w), y(w), \mathcal{F}_E(X,Y)$,

$$\omega_{\mathcal{F}} = \frac{x'(w)dw}{2y(w) + a_1x(w) + a_3}$$

more complicated than for $y^2 = x^3 + ax + b$

E/K complete, $K/\mathbb{Q}_p$ finite extension, $v, \mathcal{O}, \mathfrak{m}, k$

Theorem 3.5.15
$E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}, +)$ (even topologically)

Proof

$$E(K) \overset{\text{finite quot.}}{\supseteq} E_0(K) \overset{\text{fin.}\hookrightarrow \widetilde{E}_{ns}(k)}{\supseteq} E_1(K) = \widehat{E}(\mathfrak{m}) \supseteq \widehat{E}(\mathfrak{m}^2) \supseteq \cdots \supseteq \widehat{E}(\mathfrak{m}^r) \cong (\mathcal{O}, +)$$

the containment on the RHS of the qual sign are all finite index, all quotient $\cong (\mathfrak{m}/\mathfrak{m}^2) \cong (k, +)$ $\square$

Corollary 3.5.16
$E(K)/mE(K)$ is finite for any $m > 1$

Proof
r large enough, as before

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widehat{E}(\mathfrak{m}^r) & \longrightarrow & E(K) & \longrightarrow & A & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle [m]} & & \downarrow{\scriptstyle [m]} & & \downarrow{\scriptstyle [m]} & & \\
0 & \longrightarrow & \widehat{E}(\mathfrak{m}^r) & \longrightarrow & E(K) & \longrightarrow & A & \longrightarrow & 0
\end{array}$$

(Note $\widehat{E}(\mathfrak{m}^r) \cong (\mathcal{O}, +)$)
Kernel-cokernel exact sequence:

$$\begin{array}{l}
0 \longrightarrow \mathcal{O}[m] \longrightarrow E(K)[m] \longrightarrow A[m] \\
\qquad \longrightarrow \mathcal{O}/m\,\mathcal{O} \longrightarrow E(K)/mE(K) \longrightarrow A/mA \longrightarrow 0
\end{array}$$

(Top rows are kernels, bottom row are cokernels)
$\mathcal{O}/m\,\mathcal{O}$ finite group of order $(\#k)^{v(m)}$, A/mA finite
$\Rightarrow \quad E(K)/mE(K)$ finite $\square$

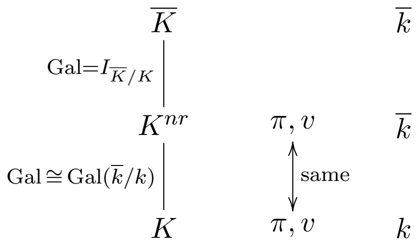
3.6 Néron-Ogg-Shafarevich Criteria

K complete, $p=$ char k, $[K : \mathbb{Q}_p] < \infty$

Definition 3.6.1

$$\begin{aligned}
K^{nr} &= \text{maximal unramified extension of } K \\
&= \bigcup_{(n,p)=1} K(\mu_n) \quad \text{complete, residue field } \overline{k} \\
I_{\overline{K}/K} &= \mathrm{Gal}(\overline{K}/K^{nr}) \quad \text{inertia group} \\
&= \ker\left(\begin{array}{ccc} \mathrm{Gal}(\overline{K}/K) & \to & \mathrm{Gal}(\overline{k}/k) \\ \sigma & \mapsto & \widetilde{\sigma} \end{array} \right)
\end{aligned}$$

(Also, I_K, I_v)



A Gal$(\overline{K}/K)$-module M is <u>unramified</u> if $M^{I_v} = M$
i.e. $\sigma(m) = m \ \ \forall m \in M, \sigma \in I_{\overline{K}/K}$
(i.e. Gal$(\overline{K}/K)$ acts on M through Gal$(\overline{k}/k)$ quotient)

Example 3.6.2
E/K elliptic curve, $M = E[m]$
$F = K(E[m]) = K($ coordinates of all m-torsion points$)$ (this is finite Galois over K)

Then $E[m]$ unramified $\Leftrightarrow$ I_v acts trivially on $E[m]$
$\Leftrightarrow$ I_v acts trivially on $F = K(E[m])$
$\Leftrightarrow$ $F \subseteq K^{nr}$
$\Leftrightarrow$ F/K unramified (in the sense $v_F|_{K^\times} = v_K$)

Example 3.6.3
$E/\mathbb{Q}_p:\ \ y^2 = x^3 - 77$, $M = E[2]$
$F = \mathbb{Q}_p(\text{roots of } x^3 - 77) = \mathbb{Q}_p(\zeta_3, \sqrt[3]{77})$ (this is unramified for $p \neq 3, 7, 11$)
(note: bad primes for $E/\mathbb{Q}$ are $2, 3, 7, 11$)

Theorem 3.6.4
E/K has good reduction, p=char $k \nmid m$. Then

1. mod $p : E(K)[m] \hookrightarrow \widetilde{E}(k)$ is injective
2. $E[m]$ is unramified

Proof

(1) Good reduction $\Rightarrow$ $E = E_0$, $\widetilde{E}_{ns} = \widetilde{E}$
and ker(mod p)=$E_1 = \widehat{E}$ has no torsion (recall, Corollary 3.5.2 $[m] : \widehat{E} \xrightarrow{\sim} \widehat{E}$ for $p \nmid m$)

(2) Let $F = K(E[m])$, $P \in E[m]$, $\sigma \in I_v$
$Q := \sigma(P) \Rightarrow \widetilde{Q} = \widetilde{\sigma}(\widetilde{P})$
$\widetilde{\sigma} = 1$ as $\sigma \in I_v$
$\Rightarrow$ (by (1)) $Q = P$, so $E[m]^{I_v} = E[m]$

$\square$

Remark. In particular, for number field K, $E(K)[m] \hookrightarrow \widetilde{E}(k)$, this help us to determine an upper bound for $E(\mathbb{Q})_{tors}$

Theorem 3.6.5 (Criterion of Néron-Ogg-Shafarevich)
E/K, $l \neq p$
E/K has good reduction $\Leftrightarrow$ $T_l E$ unramified

Remark. This relates two seemingly unrelated things: reduction is a geometric property, and $T_l E$ is purely representation theory

Proof

$\underline{\Rightarrow}$:

By Theorem 3.6.4 (2), all $E[l^n]^{I_v} = E[l^m]$, since $T_l E = \varprojlim E[l^n]$

$\Rightarrow \quad T_l E$ unramified as well

$\underline{\Leftarrow}$:

If $F := K(E[l^n])$ unramified extension over K

so E/K has good reduction $\Leftrightarrow$ E/F does (Exercise)

To find such n, choose n large enough s.t. $l^n > 4, l^n > v(\Delta_E)$

$\Rightarrow \quad l^n > [E(F) : E_0(F)]$ (Kodaira-Néron)

$\Rightarrow \quad E[l^n] \cap E_0[F]$ not cyclic ($E[l^n]$, all defined over F, $\cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$)

$\Rightarrow \quad \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z} \subseteq E_0(F)$

$\Rightarrow \quad$ (as $l \neq p$, $\widehat{E}$ has no l-torsion point) $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z} \subseteq \widetilde{E}_{ns}(k_F)$

But, if E/F has bad reduction,

$$\widetilde{E}_{ns}(k_F) \cong \underbrace{k_F^\times \quad , \quad k_F(\sqrt{\eta})^\times / k_F^\times}_{\text{cyclic}} \quad , \quad \underbrace{k_F^+}_{\text{order = power of } p}$$

□

Corollary 3.6.6

E/K has potentially good reduction (recall, this is equivalent to $v(j) \geq 0$)

$\Leftrightarrow$ E/F has good reduction over some finite F/K

$\Leftrightarrow$ $T_l E^{I_{\overline{F}/F}} = T_l E$ some finite $\overline{F}/K$

$\Leftrightarrow$ $I_{\overline{K}/K}$ acts on $T_l E$ through a finite quotient (i.e. image of $I_{\overline{K}/K} \to \mathrm{Aut}(T_l E)$ is finite)

<u>Exercise</u>:

E/K has potentially good reduction. Then,

(1) if $p \neq 2$, then $E/K(E[4])$ has good reduction

(2) if $p \neq 3$, then $E/K(E[3])$ has good reduction

(3) $I_{\overline{K}/K}$ acts on $T_l E$ through a group of order divides 24 (and 24 may occur when $p = 2$)

3.7 Elliptic curves over number fields

K number field, E/K elliptic curve

Main result:

Theorem 3.7.1 (Mordell-Weil)

E/K elliptic curve over number field

Then $E(K)$ is a finitely generated abelian group

(Asked by Poincaré (1908), proved by Mordell over $\mathbb{Q}$ (1922), then proved by Weil for Jacobians over number fields (1929), Lang-Néron proved for abelian varieties over finite generated fields)

Thus,

$$E(K) \cong \mathbb{Z}^r \oplus T$$

where T is (finite) <u>torsion</u> subgroup

r is the <u>Mordell-Weil rank</u> (or <u>arithmetic rank for E/K</u>)

Proof in 4 steps:

- Torsion is finite

- Existence of a height function on $E(K)$
  (e.g. $\Rightarrow$ $E(K) \not\cong \mathbb{Q}, \mathbb{R}, \ldots$)
- Weak Mordell-Weil Theorem: $E(K)/mE(K)$ is finite
  (e.g. $\Rightarrow$ $E(K) \not\cong \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots$ sum for infinitely many times)
- The above 3 $\Rightarrow$ $E(K)$ finitely generated

3.7.1 Torsion

<u>Notation</u>:

$$E(K)_{tors} = \bigcup_{m \geq 1} E(K)[m]$$

all points of finite order, subgroup (this is the T in Mordell-Weil)

Theorem 3.7.2
$E(K)_{tors}$ is finite

Proof
$\mathfrak{p} \subseteq \mathcal{O}_K$ any prime, $K \subseteq K_\mathfrak{p}$ completion
For n large, $\widehat{E}(\mathfrak{m}_{K_\mathfrak{p}}^n) \cong (\mathcal{O}_\mathfrak{p}, +)$ torsion-free
$\Rightarrow \quad E(K_\mathfrak{p})_{tors} \hookrightarrow E(K_\mathfrak{p})/(\mathcal{O}_\mathfrak{p}, +)$
But $E(K)_{tors} \hookrightarrow E(K_\mathfrak{p})_{tors}$ and $E(K_\mathfrak{p})/(\mathcal{O}_\mathfrak{p}, +)$ finite (Theorem 3.5.15) □

Theorem 3.7.3 (Cassels)
$E/\mathbb{Q}$ elliptic curve in Weierstrass form with $a_i \in \mathbb{Z}$
If $P = (x, y) \in E(\mathbb{Q})_{tors}$
$\Rightarrow$ either $x, y \in \mathbb{Z}$ or $x \in \frac{1}{4}\mathbb{Z}, y \in \frac{1}{8}\mathbb{Z}$

Proof
May assume E in global minimal model (proves stronger statement)
If p |denominator of x or y
then $P \in E_1(\mathbb{Q}) = \widehat{E}(p\mathbb{Z}_p)$
But $\widehat{E}(p\mathbb{Z}_p) \cong (p\mathbb{Z}_p, +)$ has no torsion for p odd, and
$\widehat{E}(4\mathbb{Z}_2) \cong (4\mathbb{Z}_2, +)$ for $p = 2$ $\quad (\Rightarrow \quad P \in \widehat{E}(2\mathbb{Z}_2) \setminus \widehat{E}(4\mathbb{Z}_2))$

□

Example 3.7.4
Equation $y^2 = (x-5)x(x+5)$ has infinitely many solutions
Proof: $(-\frac{5}{9}, \frac{100}{27}) \in E(\mathbb{Q})$ must have infinite order □

Torsion is generally well-understood:

Theorem 3.7.5 (Nagell-Lutz)
$E/\mathbb{Q}: \quad y^2 = x^3 + ax + b \quad a, b \in \mathbb{Z}$
If $\mathcal{O} \neq P(x, y) \in E(\mathbb{Q})_{tors}$, then

(1) $x, y \in \mathbb{Z}$

(2) either $2P = \mathcal{O}$ or $y | 4a^3 + 27b^2$

Proof
See Silverman VIII 7.2 □

Theorem 3.7.6 (Mazur)

$$E/\mathbb{Q} \text{ has } E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & n \in \{1, \ldots, 10, 12\} \\ \text{or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & n \leq 4 \end{cases}$$

Proof
Very hard (easy when $j(E) \in \mathbb{Z}$, in example sheet) $\square$

Over number fields $[K:\mathbb{Q}] = d$, $|E(K)_{tors}| \leq C(d)$ (Merel)
$\mathbb{Z}/l\,\mathbb{Z} \subseteq E(K)_{tors} \Rightarrow l \leq (3^{d/2}+1)^2$ (Uesterl)

3.7.2 Heights over $\mathbb{Q}$

Definition 3.7.7
For $\alpha = \frac{p}{q} \in \mathbb{Q}$, define $H_{\mathbb{Q}}(\alpha) = H(\alpha) := \max(|p|, |q|)$, called the height of α
$h_{\mathbb{Q}}(\alpha) = h(\alpha) := \log H(\alpha)$ is logarithmic height

Example 3.7.8
$H(\frac{2}{3})$ small. $H(\frac{20001}{30001})$ large
So the height is not measuring the size of number, but its arithmetic complexity

Properties:

- $h(\alpha) \geq 0$. Equality $\Leftrightarrow \alpha = \pm 1$ or 0
- $\{\alpha | h(\alpha) < c\}$ is finite
- $h(\alpha^d) = dh(\alpha)$, $H(\alpha^d) = H(\alpha)^d$
- Generally, if $f(x) = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0} \in \mathbb{Q}(x)$ is of degree d
  (degree of $\mathbb{Q}(x)$ is $\max(m, n)$)
  then $h(f(\alpha)) = dh(\alpha) + O(1)$, i.e.

$$dh(\alpha) - c \leq h(f(\alpha)) \leq dh(\alpha) + c \quad \text{for some } c \text{ independent of } \alpha$$

  Proof
  $\alpha = \frac{p}{q}$. Say $n \geq m$ (otherwise $f \leftrightarrow \frac{1}{f}$), so

$$f(\frac{p}{q}) = \frac{a_n p^n + \cdots a_0 q^n}{(b_m p^m + \cdots + b_0 q^m)q^{n-m}} =: \frac{A(p,q)}{B(p,q)}$$

  has $H(\alpha) \leq (n+1)\max_{i,j}(|a_i|, |b_j|)\max(|p|, |q|)^n \leq cH(\alpha)^{\deg f}$, hence the required upper bound

  For the lower bound, A, B coprime $\Rightarrow$ use Euclidean algorithm:

$$\begin{aligned} A(p,q)r(p,q) + B(p,q)s(p,q) &= p^N d_1 \\ A(p,q)r'(p,q) + B(p,q)s'(p,q) &= q^N d_2 \end{aligned}$$

  with $A, B, r, r', s, s' \in \mathbb{Z}[p,q]$ homogeneous, $d_1, d_2, \in \mathbb{Z}$
  $\Rightarrow$ Cancellation in $A(p,q)/B(p,q)$ is bounded by d_1, d_2
  Triangle inequality $\Rightarrow$ lower bound for $\max(|A|, |B|)$ $\square$

3.7.3 Heights over number fields

If K is a number field. Σ_K set of places (i.e. normalized absolute values) on K

- $|\cdot|_{\mathfrak{p}} := \left|\frac{1}{\#k_{\mathfrak{p}}}\right|^{v_{\mathfrak{p}}(\cdot)}$ for each prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ (finite places)
- $|\cdot|_\sigma := |\sigma(\alpha)|$ (usual real absolute value) for each $\sigma : K \hookrightarrow \mathbb{R}$ (real places)
- $|\cdot|_\sigma = |\sigma(\alpha)|^2$ for each pair $\sigma \neq \overline{\sigma}$ $K \hookrightarrow \mathbb{C}$ (complex places)

Definition 3.7.9
For $\alpha \in K$

$$\begin{aligned} H_K(\alpha) &:= \prod_{v \in \Sigma_K} \max(1, |\alpha|_v) \quad \in \mathbb{R}_{\geq 1} \\ h_K(\alpha) &:= \log H_K(\alpha) \quad \in \mathbb{R}_{\geq 0} \end{aligned}$$

Example 3.7.10
$K = \mathbb{Q}$

$$\begin{aligned} H_K(\frac{2}{3}) &= \max\left\{\left|\frac{2}{3}\right|, 1\right\} \cdot \max\left\{\left|\frac{2}{3}\right|_2, 1\right\} \cdot \max\left\{\left|\frac{2}{3}\right|_3, 1\right\} \cdot 1 \\ &= \max\left\{\frac{|\text{numerator}|}{|\text{denominator}|}, 1\right\} \cdot |\text{denominator}| = \max\{|\text{numer.}|, |\text{denom.}|\} \\ &= \text{same } H \text{ as before} \end{aligned}$$

Example 3.7.11
$K = \mathbb{Q}(\sqrt{5}), \alpha = \frac{1+\sqrt{5}}{2}$

$$\begin{aligned} H_K(\alpha) &= \max\left\{\left|\frac{1+\sqrt{5}}{2}\right|, 1\right\} \cdot \max\left\{\frac{1-\sqrt{5}}{2}, 1\right\} \cdot 1 \\ &= \frac{1+\sqrt{5}}{2} = 1.61\ldots \end{aligned}$$

Remark. For $P = [\alpha : \beta] \in \mathbb{P}^1(K) = K \cup \{\infty\}$, can let

$$H_K(P) = \prod_{v \in \Sigma_K} \max(|\alpha|_v, |\beta|_v)$$

(Analogous for $\mathbb{P}^n(K)$)
Well-defined: $H_K([\alpha : \beta]) = H_K([c\alpha : c\beta])$ as $\prod_v |c|_v = 1$
as this is product formula in number fields:

$$\prod_{v \in \Sigma_K} |c|_v = \prod_{v \in \Sigma_{\mathbb{Q}}} |N_{K/\mathbb{Q}}(c)|_v = 1$$

Remark. H_K, h_K depend on the choice of K, e.g., In $\mathbb{Q}$: $\quad H(\frac{1}{5}) = 5$
In $\mathbb{Q}(i)$: $\quad H_K(\frac{1}{5}) = H_K(\frac{1}{(2+i)(2-i)}) = 5^2 = H_{\mathbb{Q}}(\frac{1}{5})^{[\mathbb{Q}(i):\mathbb{Q}]}$
In $\mathbb{Q}(\sqrt{5})$: $H_K(\frac{1}{5}) = H_K(\frac{1}{(\sqrt{5})^2}) = 5^2 = H_{\mathbb{Q}}(\frac{1}{5})^{[\mathbb{Q}(\sqrt{5}):\mathbb{Q}]}$
Generally, $\alpha \in K \subseteq F$
$H_F(\alpha) = H_K(N_{F/K}(\alpha)) = H_K(\alpha^{[F:K]}) = H_K(\alpha)^{[F:K]}$ so,

Definition 3.7.12
The absolute height

$$H(\alpha) := H_K(\alpha)^{1/[K:\mathbb{Q}]} \quad , \quad h(\alpha) := \frac{1}{[K:\mathbb{Q}]} h_K(\alpha)$$

is independent of $K \ni \alpha$ (i.e. is defined on $\overline{\mathbb{Q}}$)

Properties:

(1) $\{\alpha \in K | h(\alpha) < c\}$ is finite
(2) $h(f(\alpha)) = \deg f \cdot h(\alpha) + O(1)$ for $f \in K(X)$
(3) $h(\alpha) \geq 0$, equality $\Leftrightarrow$ α root of unity or 0

Proof

$\Leftarrow$: All $|\alpha|_v$ are 1 if $\alpha = 0$ or root of unity

$\Rightarrow$: *Proof I*: $\alpha \in \mathcal{O}_K$, $|\sigma(\alpha)| \leq 1\ \forall \sigma : K \hookrightarrow \mathbb{C} \Rightarrow$ a root of unity or 0

Proof II: $h(\alpha) = 0 \Rightarrow \{\alpha^n | n \in \mathbb{Z}\}$ have bounded height
$\Rightarrow$ finite set $\Rightarrow$ two powers are equal $\Rightarrow$ $\alpha = 0$ or root of unity $\square$

3.7.4 Heights of points on elliptic curves

Definition 3.7.13
E/K, $P = (a, b) \in E(\overline{K})$, $h(P) := h(a)$
height relative to $x : E \to \mathbb{P}^1$

Properties:

Lemma 3.7.14

(1) $h(mP) = m^2 h(P) + O(1)$ (the error depends on E/K and m but not P)
"x-coordinate of mP has $\approx m^2$ digits"

(2) $\{P \in E(K) | h(P) < c\}$ finite

(3) Parallelogram law: $h(P+Q) + h(P-Q) = 2h(P) + 2h(Q) + O(1)$ (error depends on E/K not on P, Q)

Proof

(1)

$$\begin{array}{ccc} E & \xrightarrow{[m]} & E \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^1 \end{array}$$

$[m] = (\phi(x), \psi(x, y))$ and $\deg \phi = m^2$
$\Rightarrow \quad h(mP) = h(\phi(x(P))) = \deg \phi \cdot h(x(P)) + O(1) = m^2 h(P) + O(1)$

(2) Finite many x-coordinate; ≤ 2 choices for y-coordinates for each

(3) Computation with addition law (see Silvermann III 6.2)

□

3.7.5 Canonical Height

Theorem 3.7.15 (Néron-Tate)
There is a unique function $\widehat{h} : E(\overline{K}) \to \mathbb{R}$ s.t.

(1) $\widehat{h}(P) = h(P) + O(1)$

(2) $\widehat{h}(mP) = m^2 \widehat{h}(P) \ \ \forall P \in E(\overline{K})$

Proof
Uniqueness:
Let $\widehat{h}, \widehat{h}'$ be two such $\Rightarrow |\widehat{h}(P) - \widehat{h}'(P)| \leq 2C \ \ \forall P$
$\Rightarrow \quad |\widehat{h}(2^n P) - \widehat{h}'(2^n P)| \leq 2C \ \ \forall$
$\Rightarrow \quad 4^n |\widehat{h}(P) - \widehat{h}'(P)| \leq 2C \ \ \forall P$
$\Rightarrow \quad$ as $n \to \infty$, $\widehat{h} = \widehat{h}'$

Existence:

$$\widehat{h}(P) := \lim_{n \to \infty} \frac{1}{4^n} h(2^n P) \qquad \text{exists}$$

$a_n := \frac{1}{4^n} h(2^n P)$ check
$|a_n - a_m| \leq \sum_{i=m-n}^{n-1} 4^{-i} C$ as $m \geq n$ both $\to \infty$ get an Cauchy sequence $\Rightarrow$ converge
Finally, $P \mapsto \frac{1}{m^2} \widehat{h}(mP)$ equals $\widehat{h}$ by uniqueness argument □

Lemma 3.7.16 (Properties of Canonical Height)

(1) $\widehat{h} = h + O(1)$

(2) $\widehat{h}(mP) = m^2\widehat{h}(P)$

(3) $\{P \in E(K) | \widehat{h}(P) < C\}$ finite

(4) Parallelogram Law: $\widehat{h}(P+Q) + \widehat{h}(P-Q) = 2\widehat{h}(P) + 2\widehat{h}(Q)$

(5) $\widehat{h}(P) \geq 0$, and $\widehat{h}(P) = 0 \Leftrightarrow P \in E(\overline{K})_{tors}$

Proof

(1) by definition

(2) by definition

(3) True for $h \Rightarrow$ by (1), true for $\widehat{h}$

(4) Replace P, Q by $2^nP, 2^nQ$, divide by 4^n, let $n \to \infty$

(5) $\underline{\geq 0}$: $\widehat{h} := \lim_{n\to\infty} \underbrace{\frac{1}{4^n} h(\cdots)}_{\geq 0}$

$\underline{\Leftarrow}$: $(1+m)P = P$
$\Rightarrow \quad (m+1)\widehat{h}(P) = \widehat{h}(P)$
$\Rightarrow \quad \widehat{h}(P) = 0$

$\underline{\Rightarrow}$: $\{P, 2P, 3P, \ldots\}$ all have height $0 \Rightarrow$ finite set

□

Theorem 3.7.17 (Néron-Tate Pairing)

$$\begin{array}{rcl} E(\overline{K}) \times E(\overline{K}) & \to & \mathbb{R} \\ (P,Q) & \mapsto & \langle P, Q\rangle = \widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q) \end{array}$$

is bilinear, i.e. $\widehat{h}$ is a quadratic form

Proof

Formal consequences of the parallelgoram law and $\widehat{h}(P) = \widehat{h}(-P)$

Property (4) for $P+R, Q$
$-$ Property (4) for $P-R, Q$
$+$ Property (4) for $P+Q, R$
$-2\times$ Property (4) for $R+Q, R-Q$
$\Rightarrow \quad \langle P+R, Q\rangle = \langle P, Q\rangle + \langle R, Q\rangle$ □

Remark. $\langle\ ,\ \rangle$ can be used to get a lower bound on the Mordell-Weil rank

Example 3.7.18

$E/\mathbb{Q}$, say $P_1 = (2,3), P_2 = (\frac{1}{4}, \frac{1}{8}) \in E(\mathbb{Q})$
say the height pairing matrix is:

$$\begin{pmatrix} \langle P_1, P_1\rangle & \langle P_1, P_2\rangle \\ \langle P_2, P_1\rangle & \langle P_2, P_2\rangle \end{pmatrix} = \begin{pmatrix} 5.3 & 3.1 \\ 3.1 & 4.0 \end{pmatrix}$$

has determinant $\neq 0$
$\Rightarrow \quad P_1, P_2 \in E(\mathbb{Q})$ are linear independent over $\mathbb{Z}$
$\Rightarrow \quad \operatorname{rk}_{\mathbb{Z}} E(\mathbb{Q}) \geq 2$

Remark. Theorem + Property (3) $\Rightarrow$ (see Silverman III 9.5) $\widehat{h}$ positive definite quadratic form on $E(K)\otimes\mathbb{R}$ (a finite dimensional $\mathbb{R}$ vector space as tensor over $\mathbb{Z}$ with $\mathbb{R}$ kills the torsion) once we know $E(K)$ is finitely generated

Definition 3.7.19
The regulator of $E(K) = \mathbb{Z}P_1 \oplus \mathbb{Z}P_2 \oplus \cdots \oplus \mathbb{Z}P_r \oplus$(finite) is

$$\det\left(\langle P_i, P_j\rangle_{1\le i,j\le r}\right) = R \in \mathbb{R}_{>0}$$

Independent of choice of a basis

3.7.6 Descent

Theorem 3.7.20 (Descent Theorem)
K number field E/K elliptic curve
If $E(K)/mE(K)$ is finite for some $m \geq 2$
Then $E(K)$ is finitely generated

Proof
Let $P_1,\ldots,P_n \in E(K)$ be representatives for $E(K)/mE(K)$,

$$M = \max_i \widehat{h}(P_i)$$

Claim: $E(K)$ is generated by $S = \{R \in E(K) \text{ of height } \widehat{h}(R) \leq M\}$

Proof of Claim:
(note S is a finite set)
If not, let $P \in E(K)$ be a point of smallest height not in span(S)
Write $P = mQ + P_j$

$$\begin{aligned} \Rightarrow \quad m^2\widehat{h}(Q) &= \widehat{h}(mQ) = \widehat{h}(P - P_j) \\ &\leq 2\underbrace{\widehat{h}(P)}_{>M} + 2\underbrace{\widehat{h}(P_j)}_{\leq M} \\ &< 4\widehat{h}(P) \\ &\leq m^2\widehat{h}(P) \qquad (\text{as } m \geq 2) \end{aligned}$$

$\Rightarrow \quad \widehat{h}(Q) < \widehat{h}(P)$
$\Rightarrow \quad Q \in \mathrm{Span}(S)$
$\Rightarrow \quad P \in \mathrm{Span}(S) \qquad \# \qquad \blacksquare$

$\square$

Remark. All bounds and constants in $O(1)$'s can be made explicit. So *if* one knows how to find generator for $E(K)/mE(K)$ for some $m \geq 2$, get generators for $E(K)$ (but no such algorithm has been known)

3.8 Group Cohomology

Motivation:

$$0 \to E[m] \to E(\overline{K}) \overset{[m]}{\twoheadrightarrow} E(\overline{K}) \to 0$$

Note for the multiplication by m map $E(\overline{K}) \twoheadrightarrow E(\overline{K})$, every point has m^2 preimages, over algebraically closed field $\Rightarrow \quad E(\overline{K})/mE(\overline{K}) = 0$

Take $\mathrm{Gal}(\overline{K}/K)$-invariants $\Rightarrow$ exact sequence:

$$0 \to E(K)[m] \to E(K) \xrightarrow{[m]} E(K)$$

Failure to be exact on the right is measured by

$$\mathrm{coker}([m] : E(K) \to E(K)) = \frac{E(K)}{mE(K)}$$

In general, say G is a group

Definition 3.8.1
A (left) G-module is an abelian group M with an action of G given by a group homomorphism

$$\begin{array}{rcl} G & \to & \mathrm{Aut}(M) \\ g & \mapsto & (m \mapsto m^g) \end{array}$$

group hom. $\Leftrightarrow \left\{ \begin{array}{l} m^1 = m \ \ \forall m \\ m^{gh} = (m^h)^g \ \forall m \end{array} \right.$ e.g.: $\sigma, \tau \in \mathrm{Gal}(\overline{K}/K), P \in E(\overline{K}) \Rightarrow P^{\tau\sigma} = (P^\sigma)^\tau$

G-invariants

$$M^G := \{m \in M | m^g = m \ \ \forall g \in G\}$$

The functor

$$\begin{array}{rcl} G\text{-modules} & \to & G\text{-module} \\ M & \mapsto & M^G \end{array}$$

is left-exact but not right-exact, i.e. $0 \to A \to B \xrightarrow{\psi} C \to 0$ ses of G-modules $\Rightarrow$
$0 \to A^G \to B^G \xrightarrow{\psi} C^G$ exact (easy to check)

Why $B^G \not\twoheadrightarrow C^G$ in general?
Take $c \in C^G$, $B \twoheadrightarrow C \Rightarrow \exists b$ s.t. $\psi(b) = c$

$$\begin{array}{rcl} \xi : G & \to & B \\ g & \mapsto & b^g - b \end{array}$$

$(\xi = 0 \Leftrightarrow b^g = b \, \forall g)$
The map ξ lands in $A \subseteq B$, since:

$$\psi(b^g - b) = \psi(b)^g - \psi(b) = 0 \Rightarrow b^g - b \in \ker \psi = \mathrm{Im}(A \hookrightarrow B)$$

and satisfies

$$\xi(gh) = b^{gh} - b = (b^h)^g - b^g + b^g - b = \xi(h)^g + \xi(g)$$

ξ is called the crossed homomorphism $G \to A$ or 1-cocylce

Choosing another preimage $b' \in \psi^{-1}(c)$ (so $b' = b + a$ some $a \in A$) changes

$$\xi \to \xi' = \xi + \underbrace{(\text{map } g \mapsto a^g - a)}_{\text{1-coboundary}}$$

Definition 3.8.2
M a G-module

$$\begin{aligned} H^0(G,M) &:= M^G \quad \text{0th cohomology group} \\ H^1(G,M) &:= \frac{\text{1-cocycles}}{\text{1-coboundary}} \quad \text{1st cohomology group} \\ &= \frac{\{\xi : G \to M | \xi(gh) = \xi(g) + \xi(h)^g\}}{\{\text{maps of form } g \mapsto m^g - m \text{ some } m \in M\}} \end{aligned}$$

$\phi : M \to N$ map of G-modules indcues $H^1(G,M) \to H^1(G,N)$ *by composing $G \xrightarrow{\xi} M \xrightarrow{\phi} N$
If G acts trivially on M ($m^g = m \; \forall g, m$), then

$$H^1(G,M) = \frac{\{\xi | \xi(gh) = \xi(g) + \xi(h)\}}{\{0\}} = \mathrm{Hom}(G,M)$$

We constructed a map $\delta : C^G \to H^1(G,A)$ with

$$\ker \delta = \{c \in C^G | \xi : g \mapsto b^g - b = 0, b \in \psi^{-1}(c)\} = \psi(B^G)$$

Generally, we have:

Proposition 3.8.3
ses of G-modules $0 \to A \to B \to C \to 0$ induces a long exact sequence of abelian groups:

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G,A) \longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \longrightarrow \cdots$$

(the sequence continues to $H^2(G,A)$ etc. note that $H^2(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times)$ Brauer group, important in class field theory and central simple algebras)

Proof
Define maps, checked. Exactness at C^G, checked. Exactness elsewhere, not hard ☐

3.8.1 Galois Cohomology

$G_K = \mathrm{Gal}(\overline{K}/K)$ with K perfect

Definition 3.8.4
A G_K-module M is <u>continuous</u> if $\forall m \in M$, $\mathrm{Stab}_{G_K} m < G_K$ is $\mathrm{Gal}(\overline{K}/L_m)$ for some L_m/K finite extension

(this actuallly means $G_K \times M \to M$ is continuous if M is given discrete topology and G_K profinite topology - $\mathrm{Gal}(\overline{K}/L)$'s fundamental system of open nbhds of id)

Example 3.8.5
$\overline{K}, \overline{K}^\times, E(\overline{K})$

Definition 3.8.6
For continuous G_K-modules, define

- $H^0(G_K, M) := M^G$ as before

- $H^1(G_K, M) := \dfrac{\left\{\begin{array}{c}\text{cts 1-cocycles } \xi : G \to M \text{ s.t.} \\ \forall m \in M \ \ \xi^{-1}(m) = \mathrm{Gal}(\overline{K}/L) \text{ some } L/K \text{ finite}\end{array}\right\}}{\{\text{1-coboundaries}\}}$
(1-coboundaries are continuous automorphism)
- same long exact sequence as before

Theorem 3.8.7
If $\mu_m \subseteq K$ then

$$\begin{array}{rcl} K^\times/(K^\times)^m & \cong & H^1(G_K, \mu_m) \ \ (= \mathrm{Hom}_{\mathrm{cont.}}(G_K, \mu_m)) \\ b & \overset{\delta}{\mapsto} & (\sigma \ \mapsto \ \dfrac{(\sqrt[m]{b})^\sigma}{\sqrt[m]{b}}) \end{array}$$

This is the Kummer map

Proof
$0 \to \mu_m \to \overline{K}^\times \xrightarrow{x \mapsto x^m} \overline{K}^\times \to 0$ induces
$0 \to \mu_m \to K^\times \to K^\times \overset{\delta}{\to} H^1(G_K, \mu_m) \to H^1(G_K, \overline{K}^\times)$, extract:

$$0 \to K^\times/K^{\times m} \overset{\delta}{\hookrightarrow} H^1(G_K, \mu_m) \to H^1(G_K, \overline{K}^\times)$$

for some δ as claimed by definition of connecting homomorphism

To prove δ surjective, either (1) prove $H^1(G_K, \overline{K}^\times) = 0$ “Hilbert ’90 Theorem” (this theorem proves for even when $\mu_m \nsubseteq K$)
or (2) Take $\xi \in H^1(G_K, \mu_m) = \mathrm{Hom}_{\mathrm{cont}}(G_K, \mathbb{Z}/m\mathbb{Z})$,
$\ker \xi = G_L, L/K$ finite Galois by continuity,

$$\xi : \mathrm{Gal}(L/K) \hookrightarrow \mathbb{Z}/m\mathbb{Z}$$

By Kummer theory, any such L is $K(\sqrt[m]{b})$, some $b \in K^\times$ (as $\mu_m \subseteq K$) □

3.9 Weak Mordell-Weil a lá Mordell

K number field, E/K, our goal is to show $E(K)/2E(K)$ finite (Weak Mordell-Weil). The plan for achieving the goal is as follows:

$E/K: \ \ y^2 = (x - t_1)(x - t_2)(x - t_3), \quad t_i \in K$
Q1: Why may assume $E[2] \subseteq E(K)$

Define the Kummer map

$$\begin{array}{rcll} \kappa : E(K) & \to & (K^\times/K^{\times 2}) \times (K^\times/K^{\times 2}) \times (K^\times/K^{\times 2}) & \\ P & \mapsto & (\kappa_1(P), \kappa_2(P), \kappa_3(P)) & \\ E[2] \not\ni (x, y) & \mapsto & (x - t_1, x - t_2, x - t_3) & \text{(NB: Product of 3 is } 1 \in K^\times/K^{\times 2}) \\ \mathcal{O} & \mapsto & (1, 1, 1) & \\ (t_1, 0) & \mapsto & ((t_1 - t_2)(t_1 - t_3), t_1 - t_2, t_1 - t_3) & \text{(similarly for } (t_2, 0), (t_3, 0)) \end{array}$$

This is a group homomorphism with kerel $2E(K)$, so,
Q2: Why?

$$E(K)/2E(K) \ \hookrightarrow \ (K^\times/K^{\times 2}) \times (K^\times/K^{\times 2})$$

(say $\kappa = (\kappa_1, \kappa_2)$)
The image is trivial at primes $p \nmid 2\Delta_E$, so
$p \nmid 2$ prime of good reduction $\Rightarrow v_p(\kappa_i(P)) \equiv 0 \mod 2$, and so
Q3: Why?

Then proves $E(K)/2E(K)$ finite
Q4: Why?

Example 3.9.1

$$\begin{array}{rcl} \mathbb{Q}^\times/\mathbb{Q}^{\times 2} & \overset{1:1}{\leftrightarrow} & \text{square-free integers} \\ 5 & \mapsto & 5 \\ 5\cdot\left(\frac{7}{8}\right)^2 & \mapsto & 5 \\ -\frac{2}{3} & \mapsto & -6 \end{array}$$

i.e. $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is a $\mathbb{F}_2$-vector space with basis $-1, 2, 3, 5, 7, \ldots$

3.9.1 Example of 2-descent

$E/\mathbb{Q} \;\; y^2 = x(x+3)(x-6)$
Goal: Determine the structure of $E(\mathbb{Q})$

Step 1: Determine torsion subgroup

- $\Delta = 2^6 3^8$ minimal at all primes as $v_p(\Delta) < 12 \;\; \forall p$
- $\{T_1 = (0,0), T_2 = (-3,0), T_3 = (6,0), \mathcal{O}\} = E[2] \subseteq E(\mathbb{Q}) \Rightarrow \#E(\mathbb{Q})_{tors} \geq 4$

$$\left.\begin{array}{rcl} \#\widetilde{E}(\mathbb{F}_5) & = & 8 \\ \#\widetilde{E}(\mathbb{F}_7) & = & 12 \end{array}\right\} \Rightarrow \#E(\mathbb{Q})_{tors} \leq 4 \text{ (by Theorem 3.6.4)}$$

$\Rightarrow \;\; \#E(\mathbb{Q})_{tors} = 4$

Step 2: Exploit structure using Kummer map
A search for points of small height ($H \leq 2$, i.e. points with x-coordinates $\in \{0, \pm1, \pm2, \pm\frac{1}{2}\}$) yields $P = (-2, 4) \in E(\mathbb{Q})$

Kummer map:	x	$x+3$	$x-6$
$\mathcal{O}$	1	1	1
$T_1 = (0,0)$	-2	3	-6
$T_2 = (-3,0)$	-3	3	~~-9~~, -1
$T_3 = (6,0)$	6	1	6
$P = (-2,4)$	-2	1	-2
$P + T_1 = (9,18)$	1	3	3
$P + T_2 = (24,-108)$	6	3	2
$P + T_3 = (-\frac{3}{4}, -\frac{27}{8})$	-3	1	-3
$2P = (\frac{121}{16}, -\frac{715}{64})$	1	1	$1^{(*)}$

$(*)$: Kernel of the Kummer map is precisely $2E(\mathbb{Q})$, see later

v_p(all entries)=0 for $p \nmid 2\Delta_E = 2^7 3^8$
$\Rightarrow$ all entries $\in \{\pm1, \pm2, \pm3, \pm6\}$ 8 choices
$\Rightarrow$ $E(\mathbb{Q})/2E(\mathbb{Q})$ has order $\leq 8^2 = 64 = 2^6$, hence finite

So Descent Theorem 3.7.20 $\Rightarrow$ $E(\mathbb{Q})$ finitely generated abelian group

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad \text{for some } r \geq 1 \ \ (r \neq 0 \text{ because of } P = (-2,4))$$

This has

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong (\mathbb{Z}/2\mathbb{Z})^{r+2} \qquad \text{order } \leq 2^6$$

$\Rightarrow$ $r \leq 4$. We now bound r further by local analysis.

<u>Over $\mathbb{R}$</u>:
$x + 3 \geq 0 \ \forall (x,y) \in E(\mathbb{Q})$ (can be easily seen by draw a picture)
i.e. the second entry of Kummer map is always ≥ 0

In other words, consider

$$\begin{array}{ccc}
E(\mathbb{Q})/2E(\mathbb{Q}) & \xhookrightarrow{\kappa_{E/\mathbb{Q}}} & \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \\
\downarrow & & \downarrow \\
E(\mathbb{R})/2E(\mathbb{R}) & \xhookrightarrow{\kappa_{E/\mathbb{R}}} & \mathbb{R}^\times/\mathbb{R}^{\times 2} \times \mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\} \times \{\pm 1\}
\end{array}$$

$$E(\mathbb{R})/2E(\mathbb{R}) = \frac{\mathbb{Z}/2\mathbb{Z} \times S^1}{\{1\} \times S^1} = \mathbb{Z}/2\mathbb{Z}$$

$\kappa_{E/\mathbb{Q}}(\mathcal{O}) = (1,1) \qquad \kappa_{E/\mathbb{Q}}(0,0) = (-1,1)$
(This shows that twice of a point always lies on a component of graph)
$\Rightarrow$ $\mathrm{Im}(\kappa_{E/\mathbb{Q}}) \subseteq \{$ anything $\} \times \{$ positive $\}$ because $\mathrm{Im}(\kappa_{E/\mathbb{R}})$ is.

Over $\mathbb{Q}_2$:
Compute $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^m$ some $m \geq 1$
$E: \ \ y^2 = x^3 - 3x^2 - 18x$
$\widetilde{E}/\mathbb{F}_2: \ \ (y+x)^2 = x^3$ (additive reduction at 2)
$\widetilde{E}(\mathbb{F}_2) = \{\mathcal{O}, (1,0), (0,0)\}$, (0,0) singular, others non-singular
$\Rightarrow$ $\widetilde{E}_{ns}(\mathbb{F}_2) = \{\mathcal{O}, (1,0)\} \cong (\mathbb{F}_2, +)$ $(\widehat{\mathbb{G}}_a(\mathbb{F}_2))$

The Néron component group: $E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2) \cong \mathbb{Z}/2\mathbb{Z}$ generated by $(0,0) \in E(\mathbb{Q}_2)$ (as $\widetilde{(0,0)}$ singular)

(Tate's algorithm; or directly as in Exercise 52 prove:
if $\widetilde{Q} = (0,0) = \widetilde{Q'}$, then $\widetilde{Q+Q'} \in \widetilde{E}_{ns}(\mathbb{F}_2)$)

<u>3 steps:</u>
Step 1:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E_0(\mathbb{Q}_2) & \longrightarrow & E(\mathbb{Q}_2) & \longrightarrow & E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2) & \longrightarrow & 0 \\
 & & \downarrow [2] & & \downarrow [2] & & \downarrow [2] & & \\
0 & \longrightarrow & E_0(\mathbb{Q}_2) & \longrightarrow & E(\mathbb{Q}_2) & \longrightarrow & E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2) & \longrightarrow & 0
\end{array}$$

Kernel-cokernel exact sequence:

$$0 \longrightarrow E_0(\mathbb{Q}_2)[2] \longrightarrow E(\mathbb{Q}_2)[2] \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \frac{E_0(\mathbb{Q}_2)}{2E_0(\mathbb{Q}_2)} \longrightarrow \frac{E(\mathbb{Q}_2)}{2E(\mathbb{Q}_2)} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow \underset{\langle(-3,0)\rangle}{\mathbb{Z}/2\mathbb{Z}} \longrightarrow \underset{\langle((0,0),(-3,0))\rangle}{\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}} \twoheadrightarrow \underset{\langle(0,0)\rangle}{\mathbb{Z}/2\mathbb{Z}} \xrightarrow{\text{zero}} A \hookrightarrow B \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

Exactness at $\langle(0,0)\rangle$ and A $\quad\Rightarrow$

$$0 \to \frac{E_0}{2E_0} \to \frac{E}{2E} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

Step 2:

$$0 \to E_1(\mathbb{Q}_2) \to E_0(\mathbb{Q}_2) \to \widetilde{E}_{ns}(\mathbb{F}_2) \to 0$$

$\widetilde{E}_{ns}(\mathbb{F}_2) \cong \mathbb{Z}/2\mathbb{Z}$ gen. by $(1,0)$ (the image of $(-3,0)$ under reduction map)
Kernel-cokernel exact sequence for [2] again:

$$0 \longrightarrow E_1(\mathbb{Q}_2)[2] \longrightarrow E_0(\mathbb{Q}_2)[2] \longrightarrow \widetilde{E}_{ns}(\mathbb{F}_2)[2] \longrightarrow \frac{E_1(\mathbb{Q}_2)}{2E_1(\mathbb{Q}_2)} \longrightarrow \frac{E_0(\mathbb{Q}_2)}{2E_0(\mathbb{Q}_2)} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

$$0 \longrightarrow 0 \longrightarrow \frac{\mathbb{Z}/2\mathbb{Z}}{\langle(-3,0)\rangle} \xrightarrow{\cong} \frac{\mathbb{Z}/2\mathbb{Z}}{\langle(\overline{1},\overline{0})\rangle} \xrightarrow{\text{zero}} C \hookrightarrow D \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

and get

$$0 \to \frac{E_1}{2E_1} \to \frac{E_0}{2E_0} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

Step 3:
$E_1(\mathbb{Q}_2) \cong \widehat{E}(2\mathbb{Z}_2)$ formal group,

$$\begin{array}{ccccccc} 0 \longrightarrow & \widehat{E}(4\mathbb{Z}_2) & \longrightarrow & \widehat{E}(2\mathbb{Z}_2) & \longrightarrow & \frac{\widehat{E}(2\mathbb{Z}_2)}{\widehat{E}(4\mathbb{Z}_2)} & \longrightarrow 0 \\ & \downarrow \cong & & & & \downarrow \cong & \\ & (\mathbb{Z}_2,+) & & & & \frac{2\mathbb{Z}_2}{4\mathbb{Z}_2} \cong \mathbb{Z}/2\mathbb{Z} & \end{array}$$

$\left(\frac{\widehat{E}(2\mathbb{Z}_2)}{\widehat{E}(4\mathbb{Z}_2)} \cong \frac{2\mathbb{Z}_2}{4\mathbb{Z}_2}\right.$ as, from section 3.5.1, $\mathcal{F}(\mathfrak{m}^n)/\mathcal{F}(\mathfrak{m}^{n+1}) \cong (\mathfrak{m}^n/\mathfrak{m}^{n+1},+) \cong (k,+))$
The last $\mathbb{Z}/2\mathbb{Z}$ is generated by $P+T_3$ (any point with v_2(x-coord)=-2)

Kernel-cokernel exact sequence for [2] $\Rightarrow$:

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}_2/2\mathbb{Z}_2 \longrightarrow \frac{\widehat{E}(2\mathbb{Z}_2)}{2\widehat{E}(2\mathbb{Z}_2)} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

So we get

$$E_1/2E_1 \cong \mathbb{Z}/2\mathbb{Z}$$

Combine all 3 steps $\Rightarrow$

$$\frac{E(\mathbb{Q}_2)}{2E(\mathbb{Q}_2)} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

generated by $(T_1, T_2, P+T_3) = ((0,0),(-3,0),(-\frac{3}{4},-\frac{27}{8}))$

Because $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \cong (\mathbb{Z}/2\mathbb{Z})^3$ with representatives $\{\pm1,\pm2,\pm3,\pm6\}$

$$\begin{array}{ccc} E(\mathbb{Q})/2E(\mathbb{Q}) & \hookrightarrow & \{\pm1,\pm2,\pm3,\pm6\} \times \{\pm1,\pm2,\pm3,\pm6\} \\ \downarrow & & \| \\ E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) & \hookrightarrow & (\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}) \times (\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}) \end{array}$$

the image of $\kappa_{E/\mathbb{Q}}$ has size at most $|E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)| = 8 \Rightarrow r \leq 1 \Rightarrow r = 1$

We proved:
$E/\mathbb{Q}:\ y^2 = x(x+3)(x-6)$ has $E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}/2$

3.9.2 Proof of (Weak) Mordell-Weil Theorem

Theorem 3.9.2 (Weak Mordell-Weil Theorem)
K number field, E/K elliptic curve, $m \geq 2$, then,

$$E(K)/mE(K) \qquad \text{finite}$$

Corollary 3.9.3 (Mordell-Weil Theorem)
$E(K)$ is finitely generated

Proof
Weak Mordell-Weil + Descent Theorem □

Proof of Weak Mordell-Weil Theorem
Each of the step in this proof is to answer each question stated at the start of the section, in the plan for proving Weak Mordell-Weil

Step 1
$F := K(E[m])$. If we show $E(F)/mE(F)$ is finite, then $E(F)$ finitely generated
$\Rightarrow \quad E(K) \hookrightarrow E(F) \quad \Rightarrow \quad E(K)$ also f.g.

Thus, replacing K by F, may assume $E[m] \subseteq E(K)$ $\quad$ ($\Rightarrow \mu_m \subseteq K$ Exercise)

Step 2
Take $G_K = \mathrm{Gal}(\overline{K}/K)$-cohomology of

$$0 \to E[m] \to E(\overline{K}) \xrightarrow{[m]} E(\overline{K}) \to 0$$

Get

$$0 \to E[m] \to E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta} H^1(G_K, E[m]) \to H^1(G_K, E(\overline{K})) \xrightarrow{[m]} H^1(G_K, E(\overline{K})) \to \cdots$$

Extract

$$0 \to \frac{E(K)}{mE(K)} \xrightarrow{\delta} H^1(G_K, E[m]) \to H^1(G_K, E(\overline{K}))[m] \to 0$$

Kummer sequence for elliptic curve

$\delta(P) = (\sigma \mapsto Q^\sigma - Q)$ for any $Q \in E(\overline{K})$ s.t. $mQ = P$

Now,

$$\overbrace{H^1(\, G_K, \underbrace{E[m]}_{\mathbb{Z}/m \times \mathbb{Z}/m}\,)}^{\mathrm{Hom}_{cont}} = H^1(\, G_K, \underbrace{\mu_m}_{\mathbb{Z}/m}) \times H^1(\, G_K, \underbrace{\mu_m}_{\mathbb{Z}/m}) \cong K^\times/K^{\times m} \times K^\times/K^{\times m} \qquad (3.9.1)$$

The first equality is due to Weil pairing, explicitly:
Let $E[m] = \mathbb{Z}/m\mathbb{Z}T_1 \oplus \mathbb{Z}/m\mathbb{Z}T_2$, have two Weil pairings:

$$\begin{array}{rcl} E[m] & \to & \mu_m \\ \alpha_1 : T & \mapsto & e_m(T, T_1) \\ \alpha_2 : T & \mapsto & e_m(T, T_2) \end{array}$$

and

$$(\alpha_1, \alpha_2) : E[m] \xrightarrow{\sim} \mu_m \times \mu_m$$

becuase e_m bilinear, non-degenerate.

The isomorphism in the ses (3.9.1) is due to Kummer map in Theorem 3.8.7, and we now construct:

$$\kappa = (\kappa_1, \kappa_2) : E(K)/mE(K) \hookrightarrow K^\times/K^{\times m} \times K^\times/K^{\times m} \tag{3.9.2}$$

which is a group homomorphism, given by $\kappa_i = H^1(\alpha_i) \circ \delta$

(Exercise: For $m = 2$, use definition of e_m (relies on function f s.t. $\mathrm{div}(f) = 2(T) - 2(\mathcal{O})$ e.g. $f = x - x_T$) to show $\kappa = (x - x(T_1), x - x(T_2))$ for $m = 2$)

Step 3
Let $p \nmid m\Delta_E$ be a prime of good reduction, K_p completion, valuation v_p, residue field k (finite) K_p^{nr} maximal unramified extension, same valuation, residue field $\overline{k}$

Claim: $E(K_p^{nr})/mE(K_p^{nr}) = 0$

Proof of Claim:
(Note: $E = E_0, \widetilde{E} = \widetilde{E}_{ns}$, good reduction at P)

$$0 \to E_1(K_p^{nr}) \to E(K_p^{nr}) \to \widetilde{E}(\overline{k}) \to 0$$

Kernel-cokernel exact sequence for $[m]$ $\Rightarrow$

$$\cdots \to \underbrace{\frac{E_1(K_p^{nr})}{mE_1(K_p^{nr})}}_{=0} \to \frac{E(K_p^{nr})}{mE(K_p^{nr})} \to \underbrace{\frac{\widetilde{E}(\overline{k})}{m\widetilde{E}(\overline{k})}}_{=0} \to 0$$

exact sequence.
First cancelling due to: $p \nmid m \Rightarrow [m]$ isom of formal groups
Second cancelling due to: $\widetilde{E}$ elliptic curve over algebraically closed field $\Rightarrow [m]$ surjective
$\Rightarrow$ the middle group is zero; proves the claim ■

Now consider the following commute diagram

$$\begin{array}{ccc} E(K)/mE(K) & \overset{\kappa}{\hookrightarrow} & K^\times/K^{\times m} \times K^\times/K^{\times m} \\ \downarrow & & \downarrow \\ \cancel{E(K_p^{nr})/mE(K_p^{nr})}=0 & \hookrightarrow & (K_p^{nr})^\times/(K_p^{nr})^{\times m} \times (K_p^{nr})^\times/(K_p^{nr})^{\times m} \end{array}$$

$\Rightarrow$ $\mathrm{Im}(\kappa_i)$ are elements of $K^\times$ which are in $(K_p^{nr})^{\times m}$
In particular, they have v_p, which is same on K and K_p^{nr}, multiple of m

We proved $v_p(\kappa_i(P)) \equiv 0 \mod m \quad \forall p \nmid m\Delta_E$

Step 4
Let $\mathfrak{p}, \dots, \mathfrak{p}_n$ be prime divisors of $m\Delta_E$

Claim: $H_{\mathfrak{p}_1,\dots,\mathfrak{p}_n} = \{\alpha \in K^\times/K^{\times m} | v_\mathfrak{p}(\alpha) \equiv 0 \mod m \,\forall \mathfrak{p} \neq \mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ is finite

Proof of Claim:
Enough to show

$$H_{\mathfrak{p}_1,\dots,\mathfrak{p}_{n-1}} = \ker(H_{\mathfrak{p}_1,\dots,\mathfrak{p}_n} \xrightarrow{v_{\mathfrak{p}_n}} \mathbb{Z}/m\mathbb{Z})$$

is finite. Inductively, need that

$$H_\emptyset = \{\alpha \in K^\times/K^{\times m} | v_\mathfrak{p} \equiv 0 \mod m \forall \mathfrak{p}\}$$

For $\alpha \in H_\emptyset$,

$$\underbrace{(\alpha)}_{\text{ideal}\subseteq\mathcal{O}_K} = \prod_{\mathfrak{p}} \mathfrak{p}^{mn_\mathfrak{p}} = \left(\prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}\right)^m =: I_\alpha^m$$

So enough to show

$$U = \ker\begin{pmatrix} H_\emptyset & \to & \text{class gp of } \mathcal{O}_K \\ \alpha & \mapsto & I_\alpha \end{pmatrix}$$

is finite. (note the class group is finite)

For $\alpha \in U, I_\alpha = (x_\alpha)$ principal (as it is in the principal ideal class)
$\Rightarrow \quad (\alpha) = (x_\alpha^m) \quad \Rightarrow \quad \frac{\alpha}{x_\alpha^m} \in \mathcal{O}_K^\times$

If $\frac{\alpha}{x_\alpha^m} = u^m \in (\mathcal{O}_K^\times)^m$
$\Rightarrow \quad \alpha = (ux_\alpha)^m \in K^{\times m}$ (i.e. trivial element in U). So

$$\begin{array}{rcl} U & \hookrightarrow & \mathcal{O}_K^\times / \mathcal{O}_K^{\times\, m} \\ \alpha & \mapsto & \dfrac{\alpha}{x_\alpha^m} \end{array}$$

Note $\mathcal{O}_K^\times / \mathcal{O}_K^{\times\, m}$ is finite, since $\mathcal{O}_K^\times$ is finite generated (by Dirichlet Unit Theorem, c.f. Algebraic Number Theory course) ■

Given claim $\quad\Rightarrow\quad E(K)/mE(K) \hookrightarrow H_{\mathfrak{p}_1,\ldots,\mathfrak{p}_n} \times H_{\mathfrak{p}_1,\ldots,\mathfrak{p}_n}$
$\Rightarrow$ DONE □

Remark. Same strategy works for many finitely generated field (e.g. $\mathbb{Q}(t_1, t_2), \mathbb{F}_q(t), \ldots$)

Remark. To actually find $E(K)/mE(K)$ is hard:
There may be classes in $H^1(G_K, E[m])$ that are in the image of $E(K_v)/mE(K_v)$ for all places v, but not the image of $E(K)/mE(K)$
The "Local-Global Principle" (Hasse Principle) may fail for elliptic curve.

Example 3.9.4
$y^2 = x(x+3)(x-6)$ over $\mathbb{Q}$, $m = 2$
Here the local-global principle works

If the local-global principle does work, can find $E(K)/mE(K)$ and therefore can find $E(K)$

Remark. In practice, $m = 2$ (may be $m = 3$, just)
A general $E/\mathbb{Q}$ would have, e.g. for $m = 3$, $\mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q}) \cong GL_2(\mathbb{F}_3)$
And $\mathbb{Q}(E[3])$ is too large to compute its class group, unit group in practice.

Index

$(m, \oplus_{\mathcal{F}})$, 52
$\mathbb{G}_a$, 21
$\mathbb{G}_m$, 21

Abel-Jacobi map, 21
absolute value
  non-Archimedian, 49
algebraic group, 20
arithmetic rank, *see* Mordell-Weil rank
automorphism group, 19

canonical class, $\mathbb{K}$, 13
coboundary
  1, 67
cocycle
  1, 67
cohomology group, 67
compact manifold of dim 1, 30
complete, 49
complete linear system, $\mathcal{L}(D)$, 13, 31
Completion $\widehat{K}$, 49
complex multiplication, 23
  by $R = \mathrm{End}(E)$, 38
Complex Uniformization Theorem, 30
conductor, 38
continuous G_K module, 68
Criterion of Néron-Ogg-Shafarevich, 59
crossed homomorphism, 67
curve
  universal, 30
Curve C defined over perfect field K, 39

differential
  rational, 13
differential form, 55
  invariant, 55
  normalised, 55
divisor
  $\mathrm{Div}^0(C)$, 8
  disjoint, 41
  divisor degree, 8
  group, 8
  of differential, 13
  on curve, 8
divisor of function, 11

$\widehat{E}$, 52
$E_{ns}(k)$, 46
Eisenstein series, $G_{2k}(\Lambda)$, 32
elliptic curve, 16
  over K, 40
elliptic function, 31
elliptic integral, 35

$\mathcal{F}(\mathfrak{m})$, 52
f_ϕ, 42
formal group, 52
fractional ideal, 38
Frobenius map, 9
fundamental group $\pi_1(X)$, 30

G-invariant, 66
G-module, 66
genus of curve, 14

$\mathbb{H}$, Upper Half Plane, 38
Hasse Theorem, 44
Hasse-Weil Inequality, 44
height, 61
  absolute, 63
  logarithmic, 61
  relative, 63
Hensel's Lemma, 49
$\mathrm{Hom}_K(E_1, E_2)$, 40
homomorphism
  of formal groups, 52
hyperelliptic, 17

imaginary quadratic field K, 38
  order in K, 38
inertia group, 58
inseparable
  extension, 10
  purely inseparable, 10
invariant differential, 24
isogeneous, 26
isogeny, 21
  dual, 26
  zero isogeny, 21

j-invariant, 18
Jacobian, $\mathrm{Jac}(C)$, 21

K-rational divisorrs, 39

K-rational functions, 39
K-rational isogenies, 40
K-rational maps, 39
K-rational points, 39
K^{nr}, 58
Kummer map, 68
Kummer sequence, 72

l-adic integer, 28
l-adic Tate module, 28
Laurent expansion
    of meromorphic function, 31
Legendre form, 47
Limit in K, 49
linear equivalent, 11

m-torsion subgroup, 40
Mazur Theorem, 61
meromorphic function, 31
minimal model, 45
    global, 46
Mordell-Weil
    rank, 60
    Theorem, 60
morphism, 6
    degree, 6
multiplication-by-m map, $[m]$, 22

Néron component group, 50
Néron-Tate Pairing, 65
Néron-Tate Theorem, 64
Nagell-Lutz Theorem, 61
non-singular
    at P, 6
    curve, 7

order of vanishing at a, $\mathrm{ord}_a f$, 31

perfect field, 39
Picard group, Pic^0 and Pic, 11
places, 62
    complex, 62
    finite, 62
    real, 62
point at infinity, 16
principal divisor, 11

quadratic form, 27
    positive-definite, 27

ramification index, 8
ramified, 8
rational map, 6
    defined at P, 6
rational points
    set of, $C(K)$, 39
reduced curve, 45
Reduction
    Bad
        Additive, 46
        Multiplicative, 46
    Good, 46
    potentially good, 46
    potentially multiplicative, 46
    type, semistable, 46
    type, unstable, 46
reduction type, 50
regular
    differential, 13
regulator, 65
residue at a, $\mathrm{res}_a f$, 31
Riemann Existence Theorem, 30
Riemann-Roch Theorem, 14

separable
    extension, 10
    morphism, 11
    separable degree, 10
smooth curve, 7
strong triangle inequality, 49

torsion group, 28
torsion points, *see* torsion group
translation maps, 20

uniformiser, 7
unramified module, 58

valuation, 7
    of differentials, 13

Weierstrass $\wp$-function, 32
Weierstrass equation
    integral, 45
Weierstrass form
    generalised, 16
    simplified, 16
Weil pairing, 41
Weil reciprocity, 42

Zeta-function, 43