Johann

- For now look at variety as a curve C
- There are morphisms and rational maps.

morphisms $\subset$ rational maps, i.e. rational maps is a weaker condition.

example : Morphisms: $\mathbb{A}^2 \to \mathbb{A}^2$, $(x,y) \mapsto (y^2, xy)$

Rational maps : $\mathbb{A}^2 \to \mathbb{A}^2$, $(x,y) \mapsto (\frac{1}{x}, y^2)$

- $f: V_1 \to V_2$ rational maps between projective varieties

$(x_1 : x_2 : \cdots : x_n) \mapsto (f_1 : \cdots : f_m)$

polynomials

So $p \in V_2$ is regular $\Leftrightarrow$ not all $f_i(x_1, \cdots, x_n) = 0$

- Coordinate ring & function fields

↳ let V be a variety over K. Then $K[V]$ coordinate ring are basically $\{V \to K \text{ morphisms}\}$ or $\{\text{polynomial functions on } V\}$.

↳ Example, coordinate ring for $V_1 : y^2 = x^3 + 1$ is $K[X,Y]/(y^2 - x^3 - 1) = K[V_1]$

↳ The function field of a variety is $\mathrm{Frac}(K[V])$.

Big theorem:

$$\boxed{\begin{array}{l} V_1, V_2 \text{ isomorphic} \Leftrightarrow K[V_1] = K[V_2] \\ V_1, V_2 \text{ birationally equivalent} \Leftrightarrow K(V_1) = K(V_2) \end{array}}$$

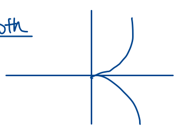
Example: $K[t^2, t^3] \subsetneq K[t]$ but $\mathrm{Frac}(K[t^2, t^3]) = K(t) = \mathrm{Frac}(K[t])$

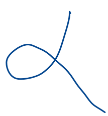
So, the line and $\prec$ are birationally equivalent but not isomorphic.

two rational func that compose to id two sided inverse

two morphisms two-sided inverse.

not smooth





interesting thm: If two coord rings not same, the but fraction field same, then what "indues" the "missing element" is where it's not smooth.

Preliminary Readings

Arithmetic of Elliptic curves by Silverman.

Chapter I. Algebraic Varieties

1.1. Affine Varieties

Note: K is a perfect field, (every alg extension of K is sep)

$\bar{K}$ a fixed alg closure.

$G_{\bar{K}/K}$ the Gal group of $\bar{K}/K$.

def Affine n-space, K-rational points

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{(x_1, \cdots x_n) ; x_i \in \bar{K}\}$$

$$\mathbb{A}^n(K) = \{(x_1, \cdots x_n) ; x_i \in K\}$$

$G_{\bar{K}/K}$ acts on $\mathbb{A}^n$, i.e. for $\sigma \in G_{\bar{K}/K}$, $P \in \mathbb{A}^n$,

$$P^\sigma = (x_1^\sigma, \cdots x_n^\sigma).$$

then $\mathbb{A}^n(K) = \{P \in \mathbb{A}^n \mid P^\sigma = P \quad \forall \sigma \in Gal_{\bar{K}/K}\}.$

def affine algebraic set

Let $\bar{K}[X] = \bar{K}[X_1, \cdots X_n]$, $I \subseteq \bar{K}[X]$ an ideal, then

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \quad \forall f \in I\}.$$

def Ideal of V

V an algebraic set, $I(V) = \{f \in \bar{K}[X] : f(P) = 0 \quad \forall P \in V\}.$

def. defined over

An algebraic set is "defined over K" if its ideal $I(V)$ can be gen. by polynomials in $K[X]$. Write V/K. If V is defined over K, then its set of K-rational points is:

$$V(K) = V \cap \mathbb{A}^n(K).$$

Remark

Hilbert Basis thm: all ideals of $K[X]$, $\bar{K}[X]$ are finitely generated.

Remark

V be an algebraic set. Consider $I(V/K)$

$$I(V/K) = \{f \in K[x] : f(P)=0 \ \forall P \in (V)\} = I(V) \cap K[X]$$

$I(V)$ defined this way except $f \in \bar{K}[x]$.

so, V is defined over $K \iff I(V) = I(V/K)\bar{K}[x]$

Note if $f(x) \in K[x]$, $P \in \mathbb{A}^n$, then $\forall \sigma \in G_{\bar{K}/K}$, $f(P^\sigma) = (f(P))^\sigma$

so $V(K) = \{P \in V \mid P^\sigma = P \ \forall \sigma \in Gal_{\bar{K}/K}\}$.

defn. Affine variety

An affine algebraic set V is called an affine variety if $I(V)$ is a prime ideal in $\bar{K}[x]$.

Note: If V is defined over K, it's not enough to check that $I(V/K)$ is prime in $K[x]$.

i.e. $(x_1^2 - 2x_2^2)$ is prime in $\mathbb{Q}[x_1, x_2]$. Not in $\bar{\mathbb{Q}}[x_1, x_2]$. So it's Not an affine variety.

def. Affine coordinate ring

V/K be a (affine) variety, (V is a variety defined over K).

The affine coordinate ring of V/K is:

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

V/K affine variety $\Rightarrow$ $K[V]$ is an ID.

def. function field.

$$K(V) = \operatorname{Frac}(K[V]).$$

def. $\bar{K}[V]$ and $\bar{K}(V)$

$$\bar{K}[V] = \frac{\bar{K}[x]}{I(V/K)} \qquad \bar{K}(V) = \operatorname{Frac}(\bar{K}[V])$$

Prop. $(f(P))^\sigma = f^\sigma(P^\sigma)$

let $f \in \bar{K}[V] = \frac{\bar{K}(X)}{I(V/K)}$ so f is well defined up to adding a polynomial that vanish on V.

we get a well defined function $f: V \to \bar{K}$. i.e. $f \in \bar{K}[V]$ then we get $f: V \to \bar{K}$ by evaluating f with coordinates.

$G_{\bar{K}/K}$ acts on $f \in \bar{K}[V]$ by acting on its coefficients.

so if V is defined over K. $G_{\bar{K}/K}$ takes $I(V)$ to itself.

so we get action $G_{\bar{K}/K}$ on $\bar{K}[V]$ & $\bar{K}(V)$. set of defining polynomials in $K[X]$.

(the action is well defined as the thing it's modded out stays fixed).

Prop (Not proven)

$K[V]$, $K(V)$, are respectively the subsets of $\bar{K}[V]$ and $\bar{K}(V)$ fixed by $G_{\bar{K}/K}$.

denote $\sigma \in G_{\bar{K}/K}$ on f by $f \mapsto f^\sigma$ then $\forall P \in V$,

$$(f(P))^\sigma = f^\sigma(P^\sigma).$$

def. dim(V)

transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

i.e. $\dim(\mathbb{A}^n) = n$

$\dim(V) = n-1$ if $V \subset \mathbb{A}^n$ is given by a single polynomial eqn.

$$f(x_1, \cdots, x_n) = 0$$

def. (Smooth or nonsingular) (Jacobian criterion)

V be variety, $f_1, \cdots f_m \in \bar{K}[X]$ set of generator for V. $P \in V$.

V is nonsingular at P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$ has rank $n - \dim(V)$.

if V is nonsingular at every point $\Rightarrow$ V is nonsingular / smooth.

Prop. Condition for singular points on var defined over 1 polynomial.

let V be given by single nonconstant polynomial eqn.

$$f(x_1, \cdots, x_n) = 0.$$

Then we know $\dim(V) = n-1$. so $P \in V$ is nonsingular $\Leftrightarrow$ $\left(\frac{\partial f}{\partial x_i}\right)_{1 \le i \le n}$ has rank 1.

$\Leftrightarrow$ $\frac{\partial f}{\partial x_i}(P) \neq 0$ for any x_i.

So, $P \in V$ is a singular point iff

$$\frac{\partial f}{\partial x_1}(P) = \cdots = \frac{\partial f}{\partial x_n}(P) = 0$$

to find a singular point. As P satisfy $f(P)$, we would need to solve n+1 equations to find a singular point. so, generally speaking, a "randomly chosen" polynomial is expected to be nonsingular.

Prop (A different characterisation of smoothness)

let $P \in V$, define M_P, an ideal of $\bar{K}[V]$ by

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

M_P maximal $\Rightarrow$ $\bar{K}[V]/M_P$ is field. get iso

$$\bar{K}[V]/M_P \longrightarrow \bar{K}$$
$$f \longmapsto f(P)$$

$P \in V$ is nonsingular iff

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

def. Local ring of V at P.

unfamiliar but doesn't seem to be needed.

1.2. Projective Varieties

def. Projective n-space

$\mathbb{P}^n$. or $\mathbb{P}^n(K)$, is set of n+1-tuples

$$(x_0, \cdots, x_n) \in \mathbb{A}^{n+1}$$

s.t. $x \sim y$ iff $x = \lambda y$, $\lambda \in \bar{K}^*$.

homogenous coordinates

Set of rational points is $\mathbb{P}^n(K) = \{ [x_0 : \cdots : x_n] \in \mathbb{P}^n : \text{all } x_i \in K \}$.

Note : If $P=[x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$, doesn't mean each $x_i \in K$ but we do have some i with $x_i \neq 0$ yet $x_j/x_i \in K$ $\forall j$.

def. minimal field of definition.

$p = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\bar{K})$. The minimal field of definition

$K(P) = K(x_0/x_i, \cdots, x_n/x_i)$ for any i with $x_i \neq 0$.

Note: $G_{\bar{K}/K}$ acts on $\mathbb{P}^n$ by acting on the homogenous coordinates.

$[x_0 : \cdots : x_n]^\sigma = [x_0^\sigma : \cdots : x_n^\sigma]$ is well defined.

Prop. Projective space under Galois Action.

$\mathbb{P}^n(K) = \{ P \in \mathbb{P}^n : P^\sigma = P \ \forall \sigma \in G_{\bar{K}/K} \}$ &

$K(P)$ = fixed field of $\{ \sigma \in G_{\bar{K}/K} : P^\sigma = P \}$. note $P \in \bar{K}$

def. homogenous polynomial.

$f \in \bar{K}[x] = \bar{K}[x_0, \cdots x_n]$ is homogenous of degree d if

$f(\lambda x_0, \cdots, \lambda x_n) = \lambda^d f(x_0, \cdots, x_n)$ $\forall \lambda \in \bar{K}$. Closed under sum.? yes. as long as sceify degree d. Great example for gradeds rigs.

def. homogenous ideals

an ideal $I \subset K[\bar{x}]$ is homogenous if it's generated by homogenous polynomials.

def Projective algebraic set

let I be a homogenous ideal. We associate a subset of $\mathbb{P}^n$ to it.

$V_I = \{ P \in \mathbb{P}^n : f(P) = 0$ for all homogenous $f \in I \}$.

A projective algebraic set is any set of form V_I for a homogenous ideal I.

def. $I(V)$ where V is a projective algebraic set.

Ideal of $\bar{K}[x]$ generated by

$\{ f \in \bar{K}[x] : f$ is homogenous and $f(P) = 0$ $\forall P \in V \}$.

def. Projective algebraic set defined over K.

If $I(V)$ can be generated by hom. polynomials in $K[X]$.

If V/K then the set of K-rational points of V is

$$V(K) = V \cap \mathbb{P}^n(K).$$

also $V(K) = \{ P \in V \mid P^\sigma = P \quad \forall \sigma \in Gal\, \bar{K}/K \}$.

def. hyperplane in $\mathbb{P}^n$

$$a_0 x_0 + a_1 x_1 + \cdots + a_n x_n = 0 \quad \text{with} \quad a_i \in \bar{K} \quad \text{not all zero.}$$

note: $\mathbb{P}^n(\mathbb{Q})$ can be scaled by integers so find $x \in V/\mathbb{Q}$ implies find relatively prime solutions to the hom equations.

def. Projective variety

A proj. Alg. set is called a proj. variety if its homogenous ideal $I(V)$ is a prime ideal in $\bar{K}[x]$.

Note: relationship $\mathbb{A}^n$ and $\mathbb{P}^n$ i.e. $\mathbb{C}\mathbb{P}^n \setminus \mathbb{R}\mathbb{P}^n$ is a smooth manifold.

Remark: going from $\mathbb{A}^n$ to $\mathbb{P}^n$

$\phi_i : \mathbb{A}^n \longrightarrow \mathbb{P}^n$

$(y_1, \cdots, y_n) \longmapsto [y_1 : y_2 : \cdots : y_{i-1} : 1 : y_i : \cdots : y_n]$.

H_i : the hyperplane in $\mathbb{P}^n$ given by $x_i = 0$

$$H_i = \{ P = [x_0 : \cdots : x_n] \in \mathbb{P}^n, \ x_i = 0 \}.$$

U_i : the complement of H_i

$$U_i = \{ P = [x_0 : \cdots : x_n] \in \mathbb{P}^n, \ x_i \neq 0 \} = \mathbb{P}^n \setminus H_i$$

there is a natural bijection (Atlas map).

$\phi_i^{-1} : U_i \longrightarrow \mathbb{A}^n$

$$[x_0 : \cdots : x_n] \longrightarrow \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \cdots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \cdots \frac{x_n}{x_i} \right)$$

Prop. dehomogenization and homogenisation

let V be a projective algebraic set with homogenous ideals $I(V) \subset \bar{K}[X]$.

then $V \cap \mathbb{A}^n$ ($\phi_i^{-1}(V \cap U_i)$ for some fixed i), is an affine alg set

with ideal $I(V \cap \mathbb{A}^n) \subset \bar{K}[Y]$ given by

$$I(V \cap \mathbb{A}^n) = \{ f(Y_1, \cdots, Y_{i-1}, 1, Y_{i+1}, \cdots Y_n) : \underbrace{f(X_0, \cdots, X_n)}_{f\text{'s domain is } \mathbb{A}^{n+1}.} \in I(V) \}$$

Since $U_0, \cdots U_n$ cover $\mathbb{P}^n$, each projective varieties is covered by subsets $V \cap U_0, \cdots V \cap U_n$

each is an affine variety via some ϕ_i^{-1}. The process of

replacing $f(X_0, \cdots, X_n)$ by $f(y_1, \cdots y_{i-1}, 1, y_{i+1}, \cdots y_n)$ is called dehomogenization w.r.t. X_i

We can reverse this. For $f(Y) \in \bar{K}[Y]$, define f not need to be homogenous but f^* is hom.

$$f^*(X_0, \cdots X_n) = X_i^d \, f\left(\frac{X_0}{X_i}, \cdots \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \cdots \frac{X_n}{X_i}\right)$$

(The homogenization). so make non hom into hom equations.

where $d = \deg(f)$ is smallest integer s.t. $f^* = X_i^d f$ is a polynomial.

def. Projective closure.

Projective closure is defined for affine sets. You homogenize it to be in $\mathbb{P}^n$.

let $V \subset \mathbb{A}^n$ be an affine algebraic set with ideal $I(V)$. Consider $V \subset \mathbb{P}^n$ as

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n$$

the projective closure of V, write $\bar{V}$, is the projective algebraic set whose

homogenous ideal $I(\bar{V})$ is generated by

$$\{ f^*(X) \mid f \in I(V) \}.$$

Def. Point at infinity

$\bar{V} \setminus V$

Prop. Some properties about projective variety vs affine variety.

a) let V be an affine variety. Then $\bar{V}$ is a projective variety, $V = \bar{V} \cap \mathbb{A}^n$.

b) let V be a projective variety. Then $V \cap \mathbb{A}^n$ is an affine variety and

either $V \cap \mathbb{A}^n = \emptyset$ or $V = \overline{V \cap \mathbb{A}^n}$

c) If an affine (resp. projective) variety V is defined over K, then $\bar{V}$ (resp $V \cap \mathbb{A}^n$) is also defined over K.

defn. The dimension of a projective variety

V/K be a projective variety, pick $\mathbb{A}^n \subset \mathbb{P}^n$, s.t. $V \cap \mathbb{A}^n \neq \emptyset$, then $\dim(V) = \dim(V \cap \mathbb{A}^n)$

defn function field.

function field of V is $K(V)$ is the function field of $V \cap \mathbb{A}^n$. Similarly with $\bar{K}(V)$.
diffirent choices of $\mathbb{A}^n$ still give different $K(V)$ that are canonically isomorphic.

def nonsingular / smooth

V a projective variety, $p \in V$, choose $\mathbb{A}^n \subset \mathbb{P}^n$, s.t. $p \in \mathbb{A}^n$, Then V is nonsingular (smooth) at P if $V \cap \mathbb{A}^n$ is nonsingular at P.

Remark. function field of $\mathbb{P}^n$, and a projective variety V.

Function field of $\mathbb{P}^n$: subfield of $\bar{K}(x_0, \cdots x_n)$ consisting of rational functions

$F(x) = f(x)/g(x)$, where $f(x)$, $g(x)$ are homogenous polynomial of same degree.

Function field of V, a projective variety is the field of rational functions

$F(x) = f(x)/g(x)$ s.t.

a) f and g are hom of same degree.

b) $g \notin I(V)$

c) $f_1/g_1 \sim f_2/g_2 \Leftrightarrow f_1 g_2 - f_2 g_1 \in I(V)$.

notation: in $\mathbb{A}^n$ use $(x_1, \cdots x_n)$

in $\mathbb{P}^n$ use $[x_0 : \cdots : x_n]$

1.3 Maps between varieties.

def Rational map

let $V_1, V_2 \subset \mathbb{P}^n$ be projective varieties. A rational map from V_1 to V_2 is a map of the form

$$\phi : V_1 \longrightarrow V_2 \qquad \phi = [f_0 : \cdots : f_n]$$

where $f_i \in \bar{K}(V_1)$ are functions s.t. for P s.t. all $f_0(P), \cdots f_n(P)$ are defined,

$$\phi(P) = [f_0(P) : \cdots f_n(P)] \in V_2$$

i.e. it's possible to have a $p \in V_1$ s.t not all f_i are defined.
Note: it's possible a rational map $\phi : V_1 \to V_2$ is not a well defined function at every point of V_1.
It's possible to evaluate $\phi(P)$, $p \in V_1$, if f_i not regular & replace each f_i by $g f_i$. $g \in \bar{K}(V_1)$.

Remark. Galois Action with Rational maps

If V_1, V_2 are defined over K, then $G_{\bar{K}/K}$ acts on ϕ in an obvious way

$$\phi^\sigma(P) = [f_0^\sigma(P), \cdots, f_1^\sigma(P)].$$

also $\phi(P)^\sigma = \phi^\sigma(P^\sigma)$ $\forall \sigma \in G_{\bar{K}/K}$, $P \in V_1$.

def. A rational map defined over K.

if $\exists \lambda \in \bar{K}^*$ s.t. $\lambda f_0, \cdots, \lambda f_n \in K(V_1)$.

also, ϕ is defined over $K \Leftrightarrow \phi = \phi^\sigma$ $\forall \sigma \in Gal\,\bar{K}/K$.

def. regular, morphism

A rational map

$$\phi : [f_0 : \cdots : f_n] : V_1 \longrightarrow V_2$$

is regular at $P \in V_1$ if there is a function $g \in \bar{K}(V_1)$ s.t.

i) each gf_i is regular at P_i

ii) $\exists$ some i s.t. $(gf_i)(P) \neq 0$.

If such g exists, set $\phi(P) = [(gf_0)(P) : \cdots : (gf_n)(P)]$

Note: might have to take different g at different points.

A morphism is a rational map regular at every point.

Alternative definition

A rational map $\phi : V_1 \to V_2$ is a map of the form

$$\phi = [\phi_0(X) : \cdots : \phi_n(X)]$$

where

i) $\phi_i(X) \in \bar{K}[X] = \bar{K}[x_0, \cdots x_n]$ are
- homogenous poly
- not all in $I(V_1)$
- same degree

ii) for every $f \in I(V_2)$

$$f(\phi_0(X), \cdots \phi_n(X)) \in I(V_1)$$

Furthermore, ϕ is regular at point $P \in V_1$, if $\exists$ hom polynomials $\psi_0, \cdots, \psi_n \in \bar{K}[X]$ s.t.

i) $\psi_0, \cdots, \psi_n$ all have same degree

ii) $\phi_i \psi_j \equiv \psi_j \phi_i \mod I(V_1) \quad \forall\ 0 \le i, j \le n.$

iii) $\psi_i(P) \neq 0$ for some i

If this happens, we set $\phi(P) = [\psi_0(P), \cdots \psi_n(P)]$.

<u>Morphism</u> a rational map that is everywhere regular.

<u>def isomorphic</u>

$V_1 \cong V_2$ if there are both morphisms $\phi: V_1 \to V_2$, $\psi: V_2 \to V_1$ s.t. $\psi \circ \phi$ and $\phi \circ \psi$ are identity maps on V_1, V_2.

Say V_1/K and V_2/K are isomorphic over K if ϕ, ψ can be defined over K.

possible to have $\phi \circ \psi$, $\psi \circ \phi$ both id, ϕ a morphism but ψ not.

<u>Remark</u> for $\phi: \mathbb{P}^m \to \mathbb{P}^n$

ϕ is an morphism $\Leftrightarrow$ ϕ_i have no common zeros in $\mathbb{P}^m$.

as $I(\mathbb{P}^m) = 0$, no way to alter the ϕ_i's.

Chapter II. Algebraic Curves

def. curve.

Projective variety of dimension one.

def

Zero at P, pole at P, regulat at P, singular point

defined by $\mathrm{Ord}_P(V)$

II.2. Maps between curves.

Prop 2.1

let C be a curve, let $V \subset \mathbb{P}^N$ be a variety, let $P \in C$ be a smooth point, let $\phi : C \to V$ be a rational map. Then ϕ is regular at P.

In particular, if C is smooth, ϕ is a morphism.

Thm 2.3 let $\phi : C_1 \to C_2$ be a morphism of curves, then ϕ is either constant or surjective.

Note: Everything else are covered in class.

Lecture 1

Books : 1) Silverman , The arithmetic of elliptic curves ☆ Read Chap 1 & 2 TODO

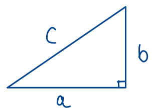
2) Cassels , Lectures on elliptic curves

3) Silverman & Tate , Rational points on elliptic curves.

4) Milne , Elliptic curves.

§1. Fermat's method of infinite descent

$\triangle$:



$a^2+b^2=c^2$

$\text{area}(\triangle)=\frac{1}{2}ab.$

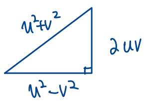
Def. rational, primitive triangles

$\triangle$ is rational if $a, b, c \in \mathbb{Q}$

$\triangle$ is primitive if $a, b, c \in \mathbb{Z}$ and are coprime.

Lemma 1.1 Parametrisation for primitive triangles

Every primitive triangle is of the form



for some integer $u > v > 0$.

Proof: a and b can't both be odd. can't both be even.

So w.l.o.g. a odd, b even, c odd.

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

coprime positive integers.

By unique factorisation in $\mathbb{Z}$, get

$$\Rightarrow \frac{c+a}{2}=u^2, \quad \frac{c-a}{2}=v^2 \quad \text{for some } u, v \in \mathbb{Z}$$

Set $a=u^2-v^2$, $c=u^2+v^2$, $b=2uv$ $\blacksquare$

Defn. Congruent number

$D \in \mathbb{Q}_{>0}$ is a congruent number if $\exists$ rational right angle $\triangle$ s.t. $\text{area}(\triangle) = D$.

N.B. suffices to consider $D \in \mathbb{Z}_{>0}$ and square free.

e.g. $D = 5, 6$ are congruent numbers.

exercise $3 \cdot 4 \cdot 5$ $\triangle$

$5 \cdot d^2 = (u^2 - v^2) uv = (u+v)(u-v) \cdot u \cdot v$?

$= (5+4)(5-4)(5 \cdot 4) = 5 \cdot (4 \cdot 9) \Rightarrow u, v = 4, 5$

$\Rightarrow 9, 40, 41 \Rightarrow$ area $180 = 5 \cdot 6^2$

$\Rightarrow 9/6, 40/6, 41/6$.

7 is congruent number $(24/5, 35/12, 337/60)$

Lemma 1.2 Equivalent condition for being congruent number.

$D \in \mathbb{Q}_{>0}$ is congruent $\Leftrightarrow$ $Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}$, $y \neq 0$.

Proof D congruent $\Leftrightarrow$ $Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}$, $w \neq 0$.

Put $x = \frac{u}{v}$, $y = \frac{w}{v^2}$ $\quad Dw^2 = uv(u^2 - v^2) \Rightarrow D\left(\frac{w}{v^2}\right)^2 = \frac{u}{v} \cdot \frac{v}{v}\left(\frac{u^2}{v^2} - 1\right)$

$Dy^2 = x(x^2 - 1)$

$\blacksquare$

Fermat showed that 1 is not a congruent number.

Thm 1.3. 1 is not a congruent number

There is no solution to $w^2 = uv(u+v)(u-v)$, $\left.\begin{matrix} w, u, v \in \mathbb{Z} \\ w \neq 0 \end{matrix}\right\} (*)$

Proof w.l.o.g. can assume u, v coprime. $u > 0$, $w \geq 0$.

If $v < 0$, replace (u, v, w) by $(-v, u, w)$

$uv(u+v)(u-v)$
$(-v)(u)(-v+u)(-v-u)$
$= uv(u+v)(u-v)$

if u, v have same parity, i.e. $u \equiv v \pmod 2$, they must be both odd, then

Replace (u,v,w) by $\left(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2}\right)$ get $\left(\frac{w}{2}\right)^2 = \left(\frac{u+v}{2}\right)\left(\frac{u-v}{2}\right) u\cdot v$

$\Rightarrow w^2 = (u+v)(u-v)\,u\cdot v.$

Then, $u, v, u+v, u-v$ are pairwise coprime positive integers (since 3 are, the other must be) with product a square.

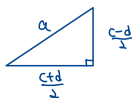
Recall : $w^2 = uv(u+v)(u-v)$, unique factorisation in $\mathbb{Z}$ implies

$\Rightarrow u=a^2, \quad v=b^2, \quad u+v=c^2, \quad u-v=d^2,$ for some $a,b,c,d \in \mathbb{Z}_{>0}$.

Since $u \not\equiv v \bmod 2$, c and d are odd, so

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

So we get



this is a primitive triangle. (Check coprime!)

to check coprime, $\left(\frac{c+d}{2}, \frac{c-d}{2}\right)$ are o.w. (c,d) are not.

Now, for a, $\frac{c+d}{2}$, if not $p\mid a$, $p \mid \frac{c+d}{2}$, then $p \mid \frac{c-d}{2}$, $p\mid u$, $p \mid v$. ※.

area $= \frac{1}{2}\left(\frac{c+d}{2}\right)\left(\frac{c-d}{2}\right) = \frac{1}{8}(c+d)(c-d) = \frac{1}{4}v = \left(b/2\right)^2$

let $w_1 = b/2$

lemma 1.1 $\Rightarrow$ $w_1^2 = u_1v_1(u_1+v_1)(u_1-v_1)$ for some $u_1, v_1 \in \mathbb{Z}$.

So we have a new solution to $(*)$.

But $4w_1^2 = b^2 = v$ and $v \mid w^2$ $\Rightarrow$ $w_1 \leq \frac{1}{2}w$

So by Fermat's method of infinite descent, there are no solutions to $(*)$. ∎

Proof scheme :

↳ W.T.S. $\nexists\ u,v,w \in \mathbb{Z}$, $w \neq 0$ and $w^2 = uv(u+v)(u-v)$

↳ Can assume :
- u, v coprime
- $w > 0$
- $u, v > 0$
- u, v diff parity

↳ so $u, v, u+v, u-v$ coprime and $u=a^2$, $v=b^2$, $u+v=c^2$, $u-v=d^2$.

↳ $\boxed{\left(\frac{c+d}{2}\right), \left(\frac{c-d}{2}\right), \ a \ \text{is a primitive } \Delta. \text{ area } (b/2)^2}$ this is key

↳ letting $w_1 = b/2$, $w_1^2 = u_1 v_1 (u_1+v_1)(u_1-v_1)$ get soln for $(*)$

↳ yet $w_1 \leq 1/2\, w$

A variant of infinite descent for polynomials

Convention in §1, K is a field with char $K \neq 2$, algebraic closure $\overline{K}$

Lemma 1.4 Infinite descent polynomial version

let $u, v \in K[t]$ be coprime.

4 distinct α, β pairs

If $\alpha u + \beta v$ is a square for 4 distinct $(\alpha:\beta) \in \mathbb{P}^1$, then $u, v \in K$.

Proof W.l.o.g. $K = \overline{K}$

changing coordinates on $\mathbb{P}^1$, we may assume ratios (α, β) are

$(1:0), (0:1), (1:-1), (1:-\lambda)$? How are change of coords performed?

for some $\lambda \in K \setminus \{0,1\}$.

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

a, b polynomials.

where $\mu = \sqrt{\lambda}$ ← using integral closure.

Unique factorisation in $K[t]$ implies that

$a+b$, $a-b$, $a+\mu b$, $a-\mu b$ are squares. ← get $a, b \in K[t]$ s.t. 4 lin. comb gives then squares. But half degree.

But $\max(\deg(a), \deg(b)) \leq \frac{1}{2}\max(\deg(u), \deg(v))$ Recall we replaced by linear combinations

So by Fermat's method of infinite descent, $u, v \in K$. as before, so we might change deg but not the max degree.

■

$\boxed{\begin{array}{l} \text{Scheme: } \cdot\ (1:0)\ (0:1)\ (1:-1)\ (1:-\lambda) \\ \quad\ \cdot \text{ compare max } \deg a, \deg b, \deg u, v. \end{array}}$

Defn 1.5 Elliptic curves and E(L)

i) An Elliptic curve E/K is the projective closure ? of the plane affine ? curve $y^2 = f(x)$] - a wierstrauss equation.

Where $f(x) \in K[x]$ is a monic cubic polynomial with distinct roots in $\overline{K}$.

ii) for L/K, any field extension, define

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

point at infinity

Fact $E(L)$ is naturally an abelian group. In this course, we study $E(K)$ for K = finite field, local field, number field

$[K:\mathbb{Q}_p] < \infty$ $\quad$ $[K:\mathbb{Q}] < \infty$

Remark: Lemma 1.2 & thm 1.3 implies

point at infinity

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

Scheme: · WLOG $\bar{K}=K$
· $y^2 = x(x-1)(x-\lambda)$
· write $x=\frac{u}{v}$. then use lemma.
· $u,v \in K$.

Lecture 2

Cor 1.6. let E/K be an elliptic curve, then $E(K(t)) = E(K)$. $\{E(K(t)) = (x,y) \in K(t)\times K(t) \mid y^2 = f(x)\}$

Proof. w.l.o.g. $K=\bar{K}$. $K = \bar{K}\cap K(t)$. So, if $\exists$ soln in $E(K(t))$, there would exist $E(\bar{K}(t)) = E(\bar{K})$. so no poly soln in $\bar{K}(t) \Rightarrow$ no poly soln in $K(t)$.

By change of coordinates, we may assume

$$E: y^2 = x(x-1)(x-\lambda) \quad \text{for some } \lambda \in K\setminus\{0,1\}.$$ Since it is monic cubic with distinct roots.

Suppose $(x,y) \in E(K(t))$.

write $x = \frac{u}{v}$, $u,v = K[t]$, u,v coprime (note that $k(t) = \mathrm{Frac}(K[t])$)

then $y^2 = \frac{u}{v}\left(\frac{u}{v}-1\right)\left(\frac{u}{v}-\lambda\right) \Rightarrow (vy)^2 = uv(u-v)(u-\lambda v)$. Substitute $w=vy$.

so $w^2 = uv(u-v)(u-\lambda v)$ for some $w \in K[t]$

By unique factorisation of $K[t]$, we get $u, v, u-v, u-\lambda v$ are all squares.

lemma 1.4 $\Rightarrow u,v \in K$, so $x,y\in K$.

§ 2. Some Remarks on Algebraic Curves (work over $\bar{K}=K$)

Def 2.1 Rational Plane curve, rational parametrisation

A plane curve $C=\{f(x,y)=0\} \subset \mathbb{A}^2$ is rational if it has a rational parametrisation.
irreducible

i.e. $\exists\, \phi,\psi$ s.t.

i) $\mathbb{A}^1 \longrightarrow \mathbb{A}^2$ is injective on $\mathbb{A}\setminus\{\text{finite set}\}$.

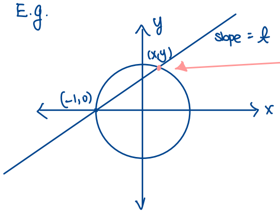
$t \longmapsto (\phi(t), \psi(t))$

Example 2.2:

parameters are embedded smoothly.

a) any nonsingular plane conic is rational.

E.g.



want rational parametrisation for this point

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

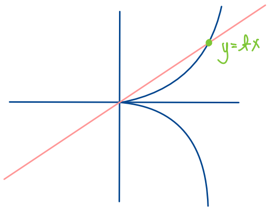
$x^2 - 1 + t^2(x+1)^2 = 0 \Rightarrow (x+1)\left(x-1+t^2(x+1)\right) = 0 \Rightarrow x \neq -1$ then

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

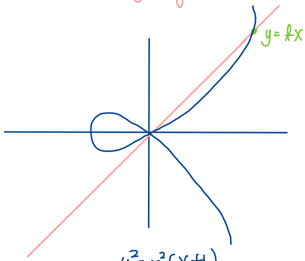
$$\Rightarrow (x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

b) any singular plane cubic is rational.

Bezout's theorem: no more than 1 singularity for irred plane curve.



$y^2=x^3$



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

Parametrisation:

$(x,y)=(\_\_\_\_,\ \_\_\_)$

$$\begin{cases} y=tx \\ (tx)^2=x^3 \end{cases} \qquad \begin{cases} y=tx \\ (tx)^2=x^2(x+1) \end{cases}$$

$\Rightarrow \quad (x,y)=(t^2,t^3)$ if $x\neq0$, get $t^2=x+1$, so $(x,y)=(t^2-1,\ t(t^2-1))$

Note: above are curves but not ECs.

c) Corollary 1.6 $\Rightarrow$ Elliptic curves are not rational. $(E(K(t))=E(K))$ (implies if $x,y\in K(t)\times K(t)$ s.t. $y^2=f(x)$ then $x,y\in K$. So there is no parametrisation, i.e. write things w.r.t. t).

Remark 2.3 The genus

The genus $g(C)\in\mathbb{Z}_{\geq0}$ is an invariant of smooth projective curve C.

i) if $K=\mathbb{C}$, $g(C)$ = genus of Riemann surface. ???

ii) A smooth plane curve $C\subset\mathbb{P}^2$ of degree d has $g(C)=\frac{(d-1)(d-2)}{2}$

Do they coincide? when $\mathbb{C}$ is regarded as $\mathbb{R}\times\mathbb{R}$?

Prop 2.4 Still assuming $K=\bar{K}$

Define this!

Let C be a smooth projective curve.

i) C is rational (see def 2.1) $\Leftrightarrow$ $g(C)=0$

ii) C is an elliptic curve (see def 1.5) $\Leftrightarrow$ $g(C)=1$

Johann: If we work over $\mathbb{C}$, genus is the top invariant that count # of holes.

i.e. genus 0 → genus 1 → genus 2 →

for projective line, is a genus 0 curve. It's a circle.

$\mathbb{CP}^1$ is a circle taken in $\mathbb{R}$, ($\mathbb{RP}^1$) and sphere when taken in $\mathbb{C}$ ($\mathbb{CP}^1$) so it's a genus 0 line.

genus measures "complexity". All conics genus 0. $x^2+y^2=1$, is a circle. in $\mathbb{C}$ it's $\cong \mathbb{CP}^1$. in ellipse, hyperbola, same

Proof i) omitted extensive proof that needed A.G.

ii) "$\Rightarrow$" Ex sheet + Rem 2.3

"$\Leftarrow$" later.

def Order of vanishing

K(variables)/(the curve defined by vars)

C an algebraic curve, with function field $K(C)$, $P \in C$ a smooth point.

Write $\mathrm{ord}_P(f)$ = order of vanishing of $f \in K(C)$ at P. (negative if f has a pole).

defn of rationals. get rational param. have map from $\mathbb{A}^1 \to$ obj of interest

Fact. $\mathrm{ord}_P(\cdot)$ is a discrete valuation.

$\mathrm{Ord}_P : K(C)^* \longrightarrow \mathbb{Z}$ is a discrete valuation.

that is: $\begin{cases} \mathrm{ord}_P(f_1 f_2) = \mathrm{ord}_P(f_1) + \mathrm{ord}_P(f_2) \\ \mathrm{ord}_P(f_1+f_2) \geq \max\{\mathrm{ord}_P(f_1), \mathrm{ord}_P(f_2)\}. \end{cases}$

i.e. finitely many point have higher multiplicity. same as " birational to affine line ". has same function field as affine line so rational.

Defn Uniformizer

$t \in K(C)^*$ is a uniformizer if $\mathrm{ord}_P(t) = 1$.

Example 2.5

$C = \{g=0\} \subset \mathbb{A}^2$, $g \in K[X,Y]$ irreducible.

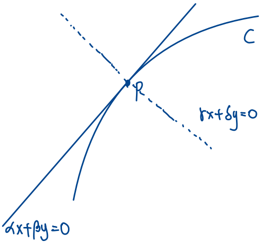
$K(C) = \mathrm{Frac}\, \dfrac{K[X,Y]}{(g)}$ (g) prime, $K[X,Y]/(g)$ ID, so we can take field of fractions.

then we can write $g = g_0 + g_1(x,y) + g_2(x,y) + \cdots$ g_i homogenous of degree i.

example of uniformizers:

Suppose $P=(0,0) \in C$ is a smooth point.

i.e. $g_0 = 0$ and $g_1(x,y) = \alpha x + \beta y$ (smooth implies both nonzero) o.w. take derivative at either get 0.



let $\gamma, \delta \in K$.

Fact: $\gamma x + \delta y \in K(C)$ is a uniformizer for P $\iff$ $\alpha\delta - \beta\gamma \neq 0$ i.e. any line works as a uniformizer except that it can't be tangent.

Example 2.6

$\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2$. $\lambda \neq 0, 1$.

this is an affine curve and we want to take projective closure.

Substituting $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ gives us

$\{(\frac{Y}{Z})^2 = (\frac{X}{Z})(\frac{X}{Z}-1)(\frac{X}{Z}-\lambda)\}$

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

So taking projective closure implies substituting all variable one a new one.

$P = (0:1:0)$ is an extra point we get (point at infty)

Aim: compute $\text{ord}_P(X)$, $\text{ord}_P(Y)$

Put $t = \frac{X}{Y}$, $w = \frac{Z}{Y}$

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

Start with 2 coords, proj closure $\Rightarrow$ 3 coord $\Rightarrow$ new point $\Rightarrow$ divide at two non-zero parts.

So, P is the point $(t, w) = (0, 0)$

It's smooth with tangent line $w = 0$

i.e. Smooth with $\text{ord}_P(t) = \text{ord}_P(t-w) = \text{ord}_P(t-\lambda w) = 1$

$(*) \Rightarrow \text{ord}_P(w) = 3$

$\text{Ord}_P(x) = \text{ord}_P(\frac{X}{Z}) = \text{Ord}_P(t/w) = \text{ord}_P(t) - \text{ord}_P(w) = 1-3 = -2.$

$\text{Ord}_P(y) = \text{ord}_P(\frac{Y}{Z}) = \text{ord}_P(1/w) = \text{ord}_P(1) - \text{ord}_P(w) = -3$

i.e. poles at infinity exist for ECs.

computation idea

- homogenize
- dehomogenize in a way that new point is not vanished
- get tangent line
- use ratios to compute.

Riemann - Roch Theorem

let C be a smooth proj curve.

defn divisor

A divisor is a formal sum of points on C.

Say $D = \sum_{P \in C} n_P P$ with $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$.

$\deg(D) = \sum_{P \in C} n_P$.

D is called <u>effective</u> (write $D \geq 0$) if $n_P \geq 0$ $\forall P$.

If $f \in K(C)^*$ then $\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$

<u>def Riemann-Roch space</u>

The Riemann-Roch space for $D \in \mathrm{Div}(C)$ is

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

i.e. the K-vector space for rational functions on C with "poles no worse than specified by D" As D defines a number of # of poles you can have for each point.

Johann

- For now look at variety as a curve C
- There are morphisms and rational maps.

morphisms $\subset$ rational maps, i.e. rational maps is a weaker condition.

example : { Morphisms: $\mathbb{A}^2 \to \mathbb{A}^2$, $(x,y) \mapsto (y^2, xy)$ } { Rational maps : $\mathbb{A}^2 \to \mathbb{A}^2$, $(x,y) \mapsto (\frac{1}{x}, y^2)$ }

- $f: V_1 \to V_2$ rational maps between projective varieties

$(x_1 : x_2 : \cdots : x_n) \mapsto (f_1 : \cdots : f_m)$ polynomials

So $p \in V_2$ is regular $\Leftrightarrow$ not all $f_i(x_1, \cdots, x_n) = 0$

- Coordinate ring & function fields

↳ let V be a variety over K. Then $K[V]$ coordinate ring are basically $\{V \to K$ morphisms$\}$ or $\{$polynomial functions on $V\}$.

↳ Example, coordinate ring for $V_1: y^2 = x^3 + 1$ is $K[x,y]/(y^2 - x^3 - 1) = K[V_1]$

↳ The function field of a variety is $\mathrm{Frac}(K[V])$.

Big theorem:

$$\boxed{\begin{array}{l} V_1, V_2 \text{ isomorphic } \Leftrightarrow K[V_1] = K[V_2] \\ V_1, V_2 \text{ birationally equivalent } \Leftrightarrow K(V_1) = K(V_2) \end{array}}$$

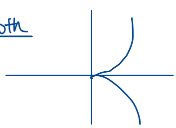
Example: $K[t^2, t^3] \subsetneq K[t]$ but $\mathrm{Frac}(K[t^2, t^3]) = K(t) = \mathrm{Frac}(K[t])$

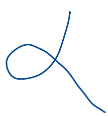
So, the line and $\prec$ are birationally equivalent but not isomorphic.

birationally: two rational func that compose to id two sided inverse

isomorphic: two morphisms two-sided inverse.

not smooth





interesting thm: If two coord rings not same, but fraction field same, then what "indues" the "missing element" is where it's not smooth.

Lecture 3.

C smooth projective curve.

Recall Riemann Roch space for $D \in \mathrm{Div}(C)$ is

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

Thm. The Riemann - Roch for genus 1:

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

Consider example 2.6: $\{ y^2 = x(x-1)(x-\lambda) \} \subset \mathbb{A}^2$. $\lambda \neq 0, 1$.

$E: y^2 = f(x)$, & P is point at infinity, So have $\mathrm{ord}_P(x) = -2$, $\mathrm{ord}_P(y) = -3$, then

$\mathcal{L}(2.P) = \langle 1, x \rangle$ $\quad$ $2.P,\ 3.P \in \mathrm{Div}(C)$

$\mathcal{L}(3.P) = \langle 1, x, y \rangle$ $\quad$ $2.P$ is pole at P at most 2, so $x \in \mathcal{L}(2.P)$

similarly $x, y \in \mathcal{L}(3.P)$

Now, assume $K = \bar{K}$ and char $K \neq 2$.

Prop 2.7 Change curves to Legendre form

let $C \subset \mathbb{P}^2$ be a smooth plane curve and $p \in C$ a point of inflection.

Then we may change coordinates s.t.

$C: Y^2 Z = X(X-Z)(X-\lambda Z)$ for some $\lambda \neq 0, 1$, and make $P = (0:1:0)$

Proof:

Note Points of inflection on a plane curve $C = \{ F(x_1, x_2, x_3) = 0 \} \subset \mathbb{P}^2$ is given by

$$F = \underbrace{\det \left(\frac{\partial^2 F}{\partial x_j \partial x_j} \right)}_{\text{Hessian}} = 0$$

tangent to C at P.

Proof

We first change coordinates s.t. $P=(0:1:0)$ & $T_PC=\{Z=0\}$ $C=\{F(X,Y,Z)=0\}\subset\mathbb{P}^2$.

$P\in C$ is a point of inflection $\Rightarrow$ $F(t,1,0)=\text{const}\cdot t^3$. deg 0, 1, 2 terms disappear as tangent @ P with multiplicity 3.

i.e. F has no terms of $X^2Y,\ XY^2,\ Y^3$.

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

linear combination

Y^2Z: coefficient $\neq 0$ o.w. $p\in C$ is singular (Because taking derivative w.r.t. y, all vanish except Y^2Z.

X^3: $\neq 0$ o.w. $\{Z=0\}\subset C$ (contradiction to the curve irreducible. We don't want it to vanish, o.w. it'll be singular).

We are free to rescale X,Y,Z and F.

w.l.o.g. C is defined by

$$Y^2Z+a_1XYZ+a_3YZ^2=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$$ $\leftarrow$ Wierstrauss equation.

substituting $Y\leftarrow Y-\frac{1}{2}a_1X-\frac{1}{2}a_3Z$, (completing square) we may assume that $a_1=a_3=0$

Now we may write $Y^2Z=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$

so $C: Y^2Z=Z^3\cdot f(X/Z)$ for some monic cubic poly f.

C smooth $\Rightarrow$ distinct roots $\Rightarrow$ w.l.o.g. roots are $0, 1, \lambda$.

so write $C: Y^2Z=X(X-Z)(X-\lambda Z)$ $\leftarrow$ Legendre form

■

The degree of a morphism

let $\phi: C_1\to C_2$ be a nonconstant morphism of smooth projective curves.

then $\phi^*: K(C_2)\hookrightarrow K(C_1)$ get field extension $K(C_1)$ / $\cancel{\phi^*}K(C_2)$ so we can think as subfield.

$f\mapsto f\circ\phi$

injective as it's an ideal of a field so kernel must be 0.

don't write ϕ^* for convenience.

defn degree of morphism ϕ & separable

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

(ii) ϕ is separable if $K(C_1)/\phi^*K(C_2)$ is a separable field extension.

(this happens automatically in field of char 0)

Now, suppose $P \in C_1$, $Q \in C_2$, $\phi: P \to Q$.

let $t \in K(C_2)$ be a uniformizer of Q.

def $e_\phi(P)$

$e_\phi(P) = \mathrm{ord}_P(\phi^* t)$ (always ≥ 1, indep of t).

Theorem 2.8. Formula relating $e_\phi(P)$ and $\deg \phi$.

let $\phi: C_1 \to C_2$ be a nonconstant morphism of smooth projective curves, then

$$\sum_{P \in \phi^{-1}Q} e_\phi(P) = \deg \phi. \quad \forall Q \in C_2$$

Moreover, if ϕ is separable, then

$e_\phi(P) = 1$ for all but finitely many $P \in C_1$.

In particular,

i) ϕ is surjective (on $\bar{K}$ points)

ii) $\# \phi^{-1}(Q) \leq \deg \phi$.

iii) If ϕ is separable, then equality holds on (ii) for all but finitely many $Q \in C_2$.

Separable $\Rightarrow$ $\forall Q$, $\#(\phi^{-1}Q) = \deg \phi$. "almost everywhere".

Remark 2.9.

let C be an algebraic curve, A rational map is given by

$C \dashrightarrow \mathbb{P}^n$ Dotted arrow so no confusion with morphisms.

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

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

Fact If C is smooth then ϕ is a morphism.

§ 3. Weierstrauss equations

(In §3, K is a perfect field. so Galois group of field extensions. denote algebraic closure $\bar{K}$.)

Defn Elliptic curves (Adult version)

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

Non-example:

$\{x^3+pY^3+p^2Z^3=0\} \subset \mathbb{CP}^2$ is not an elliptic curve over $\mathbb{Q}$.
since it has no $\mathbb{Q}$-rational point.

Theorem 3.1 (How new defn related to old one)

Every elliptic curve E is isomorphic over K to a curve in Weierstrass form via an isomorphism taking O_E to $(0:1:0)$ (therefore, can represent all Elliptic Curve by Weierstrass form)

Remark Prop 2.7 treated the special case E is a smooth plane cubic and O_E is a point of inflection.

Fact If $D \in \mathrm{Div}(E)$ is defined over K, (much weaker condition than "all points defined over K) (i.e. it is fixed by $\mathrm{Gal}(\bar{K}/K)$) then $\mathcal{L}(D)$ has a basis in $K(E)$. (not just in $\bar{K}(E)$.

Proof of thm 3.1

We have $\mathcal{L}(2\cdot O_E) \subset \mathcal{L}(3\cdot O_E)$ with dimensions 2 and 3 respectively.
Pick basis $1, x$ for $\mathcal{L}(2\cdot O_E)$ and $1, x, y$ for $\mathcal{L}(3\cdot O_E)$. Note this implies $\mathrm{ord}_{O_E}(x)=2$ and $\mathrm{ord}_{O_E}(y)=3$.
The seven elements $\{\overset{0}{1}, \overset{2}{x}, \overset{3}{y}, \overset{4}{x^2}, \overset{5}{xy}, \overset{6}{y^2}, \overset{6}{x^3}\}$ in the 6-diml vec space $\mathcal{L}(6\cdot O_E)$ must satisfy a dependence relation.
Leaving out x^3 or y^2 gives a basis for $\mathcal{L}(6\cdot O_E)$ since each term has a different order of pole at O_E. (see labeled) so coefficients of y^2 and x^3 are nonzero.
(i.e. if omit both y^2, x^3, get basis, so no lin dep. If omit one, also no lin dep. Hence coefficient of both $\neq 0$)
Rescaling x and y, we get

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

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

Let E' be the projective closure of the curve defined by Weierstrauss form.

There is a morphism

$$\phi : E \to E'$$

$$p \mapsto (x(p) : y(p) : 1)$$

Left to show ϕ is an isomorphism. (i.e. $\deg(\phi) = 1$) Since separable, by thm 2.8 $\#\phi^{-1}(p) = 1$ always

We have

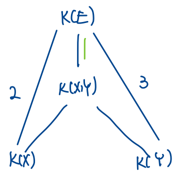
$$[K(E) : K(x)] = \deg(x : E \to \mathbb{P}^1) = \text{ord}_{O_E}\left(\tfrac{1}{x}\right) = 2$$ why $\text{ord}_E(\frac{1}{x})$, $\text{ord}_E(\frac{1}{y})$?

$$[K(E) : K(y)] = \deg(y : E \to \mathbb{P}^1) = \text{ord}_{O_E}\left(\tfrac{1}{y}\right) = 3$$ also isn't $\text{ord}_{O_E}(x) = 2$?

So by tower law $[K(E) : K(x,y)] = 1$ $\quad \deg \phi = \deg [K(E) : \phi^* K(E')]$

$= \deg [K(E) : K(x,y)]$

As $K(x,y) = \phi^* K(E')$, so $\deg \phi = 1$ so ϕ is birational.



If E' is singular, then E & E' are rational ※.

So E' is smooth and ϕ^{-1} is a morphism. (By remark 2.9)

So ϕ is an isomorphism.

To find image of O_E, we cannot plug O_E in as both x, y have poles at infinity.

Instead, we multiply through to get:

$$\phi : E \to E'$$

$$P \mapsto \left(\tfrac{x}{y}(P) : 1 : \tfrac{1}{y}(P)\right)$$

So $\phi(O_E) = (0 : 1 : 0)$ $\quad \frac{x}{y}(O_E)$ since x has 2-poly. y has 3-pole, so $\frac{x}{y}$ has 1-root.

$\frac{1}{y}(O_E)$ has a deg 3 root so it's 0 at that point.

Lecture 4

Finished the proof from last lecture.

Prop 3.2 Isomorphic elliptic curve only differ in Wierstrauss form by change of var.

Let E, E' be elliptic curve over K in Wierstrass form. Then $E \cong E'$ over K iff equations are related by change of variables.

i.e. $\left.\begin{array}{l} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{array}\right\}$ for some $u, r, s, t \in K$, $u \neq 0$

Proof: $\langle 1, x\rangle = \mathcal{L}(2.0_E) = \langle 1, x'\rangle$ since $1, x \in \mathcal{L}(2\cdot 0_E)$ and $\mathcal{L}(2.0_E)$ is a 2-diml vector space.

$\Rightarrow x = \lambda x' + r$ for some $\lambda, r \in K$, $\lambda \neq 0$.

$\langle 1, x, y\rangle = \mathcal{L}(3.0_E) = \langle 1, x', y'\rangle$

$\Rightarrow y = \mu y' + \sigma x' + t$ for some $\mu, \sigma, t \in K$, $\mu \neq 0$.

looking at the coefficients of x^3 and y^2 $\Rightarrow \lambda^3 = \mu^2$

Put $s = \sigma/u^2$ $\xleftarrow{\text{the } u \text{ arised here}}$ $\Rightarrow \begin{cases} \lambda = u^2 \\ \mu = u^3 \end{cases}$ for some $u \neq 0$

$\blacksquare$

Note: A weierstrass equation defines an elliptic curve $\Leftrightarrow$ it defines a smooth curve.

$\Leftrightarrow \Delta(a_1, \cdots a_6) \neq 0$ where $\Delta \in \mathbb{Z}[a_1, \cdots a_6]$ is a certain polynomial.

If $\mathrm{char}(K) \neq 2, 3$, we can reduce to the case

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

with discriminant $\Delta = -16(4a^3 + 27b^2)$

Corollary 3.3 ISO EC's of a certain form

Assume that $\mathrm{char}\, K \neq 2, 3$

Elliptic curves $E: \; y^2 = x^3 + ax + b$ are isomorphic over K

$E': \; y^2 = x^3 + a'x + b'$

$\Leftrightarrow \begin{cases} a' = u^4 a \\ b' = u^6 b \end{cases}$ for some $u \in K^*$.

$\begin{cases} x = u^2 x' \\ y = u^3 y' \end{cases}$ $\begin{cases} y^2 = x^3 + ax + b \\ u^6 y'^2 = u^6 x'^3 + a u^2 x' + b \end{cases}$

$\Rightarrow y'^2 = x'^3 + (a/u^4) x' + (b/u^6)$

Proof: E & E' are related by a substitution as prop 3.2 with $r = s = t = 0$.

Def j-invariant

The j-invariant of E is $j(E) = \dfrac{1728(4a^3)}{4a^3 + 27b^2}$ "recording ratio a^3 to b^2".

Corollary 3.4 relationship between j-inv and E

$E \cong E' \Rightarrow j(E) = j(E')$ & converse holds if $\bar{K} = K$.

Proof: $E \cong E' \Leftrightarrow \begin{cases} a' = u^4 a \\ b' = u^6 b \end{cases}$ for some $u \in K^*$.

$\Rightarrow (a^3 : b^2) = ((a')^3 : (b')^2)$ (apply mobius map)

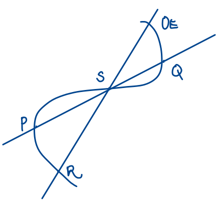
$\Leftrightarrow j(E) = j(E')$

& converse holds if $K = \bar{K}$ i.e. we can try solving for u & extract roots. ∎

§ 4. The group law.

$E \subset \mathbb{P}^2$ smooth plane cubic. $O_E \in E(K)$.

Def. Cord & Tangent process



E meets any line in 3 points counted with multiplicity

Define $P \oplus Q$:

$S =$ 3rd pt $\cap$ of E & PQ

$R =$ 3rd pt $\cap$ of E & $O_E S$.

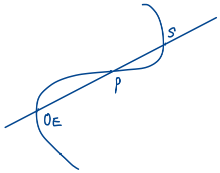
define $P \oplus Q = S$.

if $P = Q$ then take $T_P E$ instead of PQ.

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

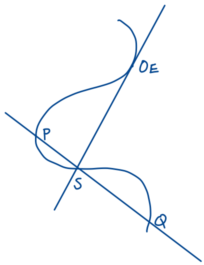
Proof (i) $\oplus$ is commutative

(ii) O_E is the identity



$O_E \oplus P = P$

iii) inverses :



Given $p \in E$

let $S = 3^{rd}$ pt $\cap$ of E & $T_{O_E} E$

let $Q = 3^{rd}$ pt $\cap$ of E & SP

Then $P \oplus Q = O_E$.

Construction scheme:

Consider $T_{O_E} E$

(iv) Associativity is harder to prove.

Def. linearly equivalent

$D_1, D_2 \in Div(E)$ are linearly equivalent if $\exists f \in \bar{K}(E)^*$ s.t. $div(f) = D_1 - D_2$.

Write $D_1 \sim D_2$ & $[D] = \{D' : D' \sim D\}$.

Def Pic group and Pic -0- group

$Pic(E) = Div(E)/\sim$

$Pic^0(E) = Div^0(E)/\sim$ where $Div^0(E) = \{D \in Div(E) \mid \deg D = 0\}$.

Def ψ

$\psi : E \longrightarrow Pic^0(E)$

$p \longmapsto [(p) - (O_E)]$

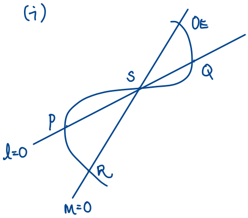
Prop 4.2

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

(ii) ψ is a bijection

Proof:

(i)



Recall that $\mathrm{div}(f) = \sum_{p \in C} \mathrm{ord}_p(f) \cdot P$

$$\mathrm{div}(l/m) = (P) + \cancel{(S)} + (Q) - (O_E) - \cancel{(S)} - (R)$$

$$= (P) + (Q) - (O_E) - (P \oplus Q)$$

so in $\mathrm{Pic}(E)$, $(P) + (Q) \sim (O_E) + (P \oplus Q)$

$$\Rightarrow (P) - (O_E) + (Q) - (O_E) \sim (P \oplus Q) - (O_E)$$

$$\Rightarrow \psi(P) + \psi(Q) = \psi(P \oplus Q)$$

Lecture 5.

Recall that ψ is defined by

$$\psi : E \to Pic^0(E)$$

$$P \mapsto [(P) - (0_E)]$$

Prop 4.2 (i) $\psi(Q \oplus P) = \psi(Q) + \psi(P)$ (shown last class)

ii) is a bijection

Proof (ctd):

injective:

so $[P]=[Q]$ in Picard group. defn of linearly equivalent divisor.

Suppose $\psi(P) = \psi(Q)$, $P \neq Q$. Then $\exists f \in \bar{K}(E)^*$ s.t. $div(f) = (P) - (Q)$

fact from 2.2 $deg(\phi) = 1 \Leftrightarrow \phi$ is an isomorphism.

$\Rightarrow E \xrightarrow{f} \mathbb{P}^1$ has degree 1. i.e. $deg(f) = ord_P(f) = 1$, and coefficient of (P) in $div(f)$ is 1. (degree is the points in fibre.)

$\Rightarrow E \cong \mathbb{P}^1$ as get morphism $E \to \mathbb{P}^1$.

※ because E has genus 1 and $\mathbb{P}^1$ genus 0.

Surjectivity:

let $[D] \in Pic^0(E)$. Then $\underset{deg\,0}{D} + \underset{deg\,1}{(0_E)}$ has degree 1.

Riemann Roch $\Rightarrow dim\, \mathcal{L}(D + 0_E) = 1$ Riemann-Roch for genus 1: $dim\, \mathcal{L}(D) = deg\, D$, $D > 0$

$\Rightarrow \exists f \in \bar{K}(E)^*$ s.t. $\underbrace{div(f) + D + 0_E}_{\text{degree 1, an effective divisor.}} \geq 0$ By definition of Riemann-Roch space.

$\Rightarrow div(f) + D + (0_E) = (P)$ for some $P \in E$. As an effective divisor of deg 1 is exactly one term.

$\Rightarrow (P) - (0_E) \sim D$

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

∎

Therefore, prop 4.2 $\Rightarrow \psi$ identifies $(E, \oplus)$ with $(Pic^0(E), +)$

Therefore $\oplus$ is associative.

Scheme: want ① $\psi(P \oplus Q) = \psi(P) + \psi(Q)$
② ψ is bij

① observe 2 lines l_1, l_2

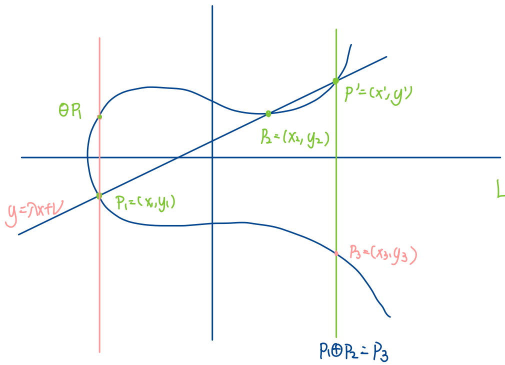
② inj. if $\psi(P) = \psi(Q)$, then get $f : E \to \mathbb{P}^1$ deg 1

surj: $deg(D + 0_E) = 1 \Rightarrow$ Riemann Roch $\Rightarrow div(f) + D + 0_E$ is point P.

Formulas for E in Wierstrauss form:

$E: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (*)$

in picture, $a_1 = a_3 = 0$ so it's symmetric across the y axis.



Why is this?

Note: points of infinity are vertical lines.

↳ As by the picture, we can characterise the group law as follows:

$P_1 \oplus P_2 \oplus P_3 = O_E \iff P_1, P_2, P_3$ are collinear.

the inverse of $P = (x_1, y_1)$ is the intersection of PO_E, which is the vertical line & E,

so, $\ominus P_1 = (x_1, \underbrace{-(a_1x_1 + a_3) - y_1}_{\text{a root other than } y_1 \text{ to the}})$ $\qquad \underbrace{y_1^2 + a_1xy_1 + a_3y_1}_{*} = \underbrace{x_1^3 + a_2x_1^2 + a_4x_1 + a_6}_{\text{Remain same}}$

same x-coord.

the parametrisation of line who meets EC @ 3 points

quadratic here * so Σ of roots is $-(a_1x_1 + a_3)$, one root is y_1

Substituting $y = \lambda x + \nu$ into $(*)$ $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ & looking at coefficient of x^2 gives

$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + \underbrace{x'}_{= x_3}$ $\qquad$ As coefficient of x^3 is the sum of x-coord of 3 roots.

$\therefore \quad x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$

$y_3 = -(a_1x_3 + a_3) - y'$ $\qquad$ By the $\ominus P$ formula.

$\quad = -(a_1x_3 + a_3) - (\lambda x' + \nu)$

$\quad = -(\lambda + a_1)x_3 - \nu - a_3.$

It remains to find formula for λ & ν.

Note: if either of P, Q is O_E, then we know summing = taking identity. Suffices to only look at affine pieces).

Case I: $x_1 = x_2$, $P_1 \neq P_2$, then $P_1 \oplus P_2 = O_E$.

Case II: $x_1 \neq x_2$, $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ $\quad \nu = y_1 - \lambda x_1 = \frac{y_1(x_2-x_1) - (y_2-y_1)x_1}{x_2 - x_1} = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1}$.

Case III: $P_1 = P_2$ (Most complicated)

then
$$\begin{cases} \lambda = \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} \\ \nu = \dfrac{-x_1^3 + a_4 x_1 + 2a_6 - a_3 y_1}{2y_1 + a_1 x_1 + a_3} \end{cases}$$

As we need to compute equation for tangent line.

<u>Corollary 4.3 Group structure on E(K)</u>

Earlier calculation showed that $E(\bar{K})$ points form a group. H.B. E(K)?

E(K) is an Abelian group.

<u>Proof</u>: It's a subgroup of $(E, \oplus)$.

Closure / inverses: see formula above.

More over, looking at coefficients, 3 points sum to 0. looking at sum of roots, (coefficient of y^1 & x^2) two rational $\Rightarrow$ 3^{rd} also is.

Associativity / Commutativity: inherited

$\blacksquare$

<u>Thm 4.4. Elliptic curves are group varieties.</u>

The group operations are morphisms of varieties.

i.e. $[-1]: E \to E$; $P \mapsto \ominus P$

$\oplus: E \times E \to E$; $(P, Q) \mapsto P \oplus Q$ are morphisms of algebraic varieties.

<u>Proof</u>:

Above formula shows $[-1]$ and $\oplus$ are rational maps

Two steps: i) show $[-1]$ is a morphism. ii) Show $\oplus$ is a morphism.

1) Above formula shows that $[-1]: E \to E$ is a rational map, (allowed to switch to different affine pieces)

As rational maps on smooth projective curves is a morphism, $[-1]$ is a morphism.

Proof Scheme

· Rational maps on smooth proj curves are morphisms
↳ $\ominus : E \to E$ is a morph
↳ $\oplus$ $E \times E \to E$ is a morph
factor using $\tau_P : E \to E$.

ii) WTS $\oplus$ is a morphism.

(Note that the above argument does not work for smooth surfaces, i.e. $E \times E$,)

Above formula $\Rightarrow$ $\oplus : E \times E \longrightarrow E$ is a rational map, that is regular on

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

(nonempty open set in Zariski set of E. It contains all except some points).

idea is to translate by P } for $P \in E$, let $\tau_P : E \to E$, $x \mapsto P \oplus x$ (note: we extend the map to be defined everywhere, checking agreements still needs some calculation!)

τ_P is a rational map, hence a morphism. (it's on smooth projective curve)

We factor $\oplus$ as

$$E \times E \xrightarrow{\tau_{\ominus A} \times \tau_{\ominus B}} E \times E \xrightarrow[\text{group law}]{\oplus} E \xrightarrow{\tau_{A \oplus B}} E$$

This shows $\oplus$ is regular on $(\tau_A \times \tau_B)(U)$, $\forall A, B \in E$, therefore $\oplus$ is regular on $E \times E$.

■

Statement of results

(The isomorphism on (i), (ii), (iv) respect the relevant topologies.)

i) $K = \mathbb{C}$, $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ where Λ is a lattice. ($\mathbb{Z}$ span of $\mathbb{C}$ vectors)

$\cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$

ii) $K \cong \mathbb{R}$ $E(\mathbb{R}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \text{if } \Delta > 0 \\ \mathbb{R}/\mathbb{Z} & \text{if } \Delta < 0 \end{cases}$ Recall that $\Delta = -16(4a^3 + 27b^2)$

iii) $K \cong \mathbb{F}_q$ (field with q elements) $\# |E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$ (Hasse's Theorem)

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

v) $[K : \mathbb{Q}] < \infty$ $E(K)$ is a finitely generated abelian group (Mordell-Weil thm)

In this course, mainly focus on iii), iv), v).

~~The Weierstrass p- theorem~~ (for case (i) of above)

Brief Remarks on $K=\mathbb{C}$

let $\Lambda = \{aw_1 + bw_2 : a, b \in \mathbb{Z}\}$ where w_1, w_2 is a basis for $\mathbb{C}$ as an $\mathbb{R}$ vector space.

Then,

$$\left\{ \begin{array}{c} \text{Meromorphic functions} \\ \text{on } \mathbb{C}/\Lambda \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{c} \Lambda\text{- invariant functions} \\ \text{on } \mathbb{C} \end{array} \right\}$$

The function field for $\mathbb{C}/\Lambda$ is generated by $\wp(z)$ and $\wp'(z)$.

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

and

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

They satisfy

$$\wp'(z)^2 = 4\wp(z)^3 - g_2 \wp(z) - g_3$$ for some constants $g_2, g_3 \in \mathbb{C}$ depending only on Λ.

(isomorphism as groups & Riemann surface)

One shows $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ where E is given by

$$y^2 = 4x^3 - g_2 x - g_3$$

this is not monic cubic but it's ok.

Point of inflection corresponds to 0 in $\mathbb{C}/\Lambda$.

uniformisation thm.

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

Lecture 6.

§ 5. Isogenies

Let E_1, E_2 be elliptic curves defined (over the same field)

thm 2.8, surjective on $\bar{K}$ points : either non-constant or surjective.

Defn isogeny, isogenous

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

ii) say E_1, E_2 are isogenous.

Def. $\mathrm{Hom}(E_1, E_2)$

$\mathrm{Hom}(E_1, E_2) = \{ \text{isogenies } E_1 \to E_2 \} \cup \{0\}$.

This is an abelian group under

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

Note. composition of isogenies

If $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ are isogenies, then $\psi\phi$ is an isogeny $E_1 \to E_3$.

(thm 2.8: $\psi\phi$ is surjective as they both are)

Tower law & degree law ($\deg \phi = [K(C_1) : \phi^* K(C_2)]$) implies that $\deg(\psi \circ \phi) = \deg \psi \cdot \deg \phi$.

def the $[n]$ map

$n \in \mathbb{Z}$, $[n] : E \to E$

$$p \mapsto \underbrace{p + p + \cdots + p}_{n \text{ copies}} \quad \text{if } n > 0$$

and $[-n] = [-1] \circ [n]$ (same as $[n] \circ [-1]$)

The above process is same as turning an abelian group into a $\mathbb{Z}$-module.

def. n-torsion subgroup

The n-torsion subgroup of E is

$E[n] = \ker(E \xrightarrow{[n]} E)$. for now consider $\bar{K}$ points.

Example of $E(\mathbb{C})$

If $K=\mathbb{C}$ then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$

thne $\begin{cases} E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 & ① \\ \deg[n] = n^2 & ② \end{cases}$

We will show ② holds for any field K and

① holds if char $K \nmid n$.

Lemma 5.1 Computing $E[2]$

Assume char $K \neq 2$.

let $E: \ y^2 = f(x) = (x-e_1)(x-e_2)(x-e_3)$ $e_i \in \overline{K}$ (distinct)

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

Proof: (this is a trick as opposed to "bashing")

let $P=(x,y) \in E$. Then

$P \in E[2] \Leftrightarrow [2]P = 0$

$\Leftrightarrow P = -P$

$\Leftrightarrow (x,y) = (x,-y)$ Curve is symmetric in y, OE vertical, so x are same & y flips sign.

$\Leftrightarrow y=0$ ∎

Prop 5.2. $[n]$ is an isogeny

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

Proof: $[n]$ is a morphism by Thm 4.4 ($\oplus: E \times E \to E$; $(P,Q) \mapsto P \oplus Q$ is a morphism)

Must show that $[n] \neq [0]$.

(also uses trick & lemma)

Assume that char $K \neq 2$.

Case $n=2$: lemma 5.1 $\Rightarrow E[2] \neq E$ (has 4 points)

$\Rightarrow [2] \neq [0]$. as $E[2] = \ker[2]$

$E = \ker[0]$.

Scheme:

char $K \neq 2$. o.w. replace lem w/ 3-torsion

char $K = 2$.

case $[n] = 2 \Rightarrow [0] \neq [2]$ cuz diff kernel.

case $[n]$ odd

then $[mn] = [m][n]$.

Case n odd: let T be a nonzero torsion point, say for contradiction, apply n to T, we would get 0.

lemma 5.1 $\Rightarrow \exists T$, s.t. $0_E \neq T \in E[2]$

then $nT = T \neq 0$, so $[n] \neq [0]$.

Now we use $[mn] = [m] \circ [n]$, to show $0 \neq n \in \mathbb{Z}$, $[n]$ is an isogeny.

Now if char $K = 2$, we can replace lemma 5.1 with an explicit lemma about 3-torsion points.

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

i.e. give isogeny ϕ, $\phi \cdot n \neq$ the zero map, so by thm 5.2 it's torsion free.

Theorem 5.3

let $\phi : E_1 \to E_2$ be an isogeny. (contrast this with the earlier

Then $\phi(P+Q) = \phi(P) + \phi(Q)$ $\forall P, Q \in E$. $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ then $(\phi + \psi)(P) = \phi(P) + \psi(P)$.)

(in point addition, use $\mathrm{Pic}^0(E)$ instead.)

Sketch proof:

Remember: ϕ^* is dual

ϕ_* is induced p.w. Σ on divisors.

ϕ induces $\phi_* : \mathrm{Div}^0(E_1) \longrightarrow \mathrm{Div}^0(E_2)$

$$\sum_{P \in E_1} n_P \cdot P \longmapsto \sum_{P \in E_1} n_P \cdot \phi(P)$$

(Divisor of the form (f))

Recall $\phi^* : K(E_2) \longrightarrow K(E_1)$

$$\begin{array}{l} K(E_1) \\ \big| \Big\downarrow \text{norm} \\ K(E_2) \end{array}$$

field extension $K(E_1)/K(E_2)$ so get norm:

$N_{K(E_1)/K(E_2)} : K(E_1) \to K(E_2)$

Fact. If $f \in K(E_1)^*$, then

$\mathrm{div}(N_{K(E_1)/K(E_2)} f) = \phi_* \mathrm{div}(f)$ (result in commutative algebra

So ϕ_* sends principal divisors to prin divisors. Similar to norm of ideals & localisation)

Scheme:

$\phi_* : Pic^0(E_1) \longrightarrow Pic^0(E_2)$

fact: maps prin to prin

get comm diagram.

ϕ_* is gp hom $\Rightarrow \phi$ is.

Since $\phi(O_{E_1}) = O_{E_2}$, the following diagram commutes:

$$\begin{tikzcd} P \arrow[d, mapsto] & E_1 \arrow[r, "\phi"] \arrow[d, "\wr S"] & E_2 \arrow[d, "\wr S"] & Q \arrow[d, mapsto] \\ {[(P)-(O_{E_1})]} & Pic^0(E_1) \arrow[r, "\phi_*"] & Pic^0(E_2) & {[(Q)-(O_{E_2})]} \end{tikzcd}$$

ϕ_* is a group homomorphism $\Rightarrow \phi$ is. ∎

The following 2 lemmas help prove that $\deg [n] = n^2$.

<u>Lemma 5.4. Commutative diagram involving E_i's and $\mathbb{P}$s.</u>

Let $\phi : E_1 \longrightarrow E_2$ be an isogeny.

Then exists morphism ξ that makes following commute.

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

$(x_1 : 1)$ $(x_2 : 1)$

New coordinates only depend on old x coordinates

not old y coordinate? ???

x_i is the x-coord on a Weierstrass eqn for E.

Moreover, if $\xi(t) = \frac{r(t)}{s(t)}$ $r, s \in K[t]$ coprime, then the

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

(Note: the morphism ξ only depend on the x-coordinates).

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

Thm 5.3 $\Rightarrow [-1] \cdot \phi = \phi \circ [-1]$. ???

So if $f \in K(x_2)$, then $[-1]^* f = f$ $\quad [-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f$ $\quad \therefore \phi^* f \in K(x_1)$. ???

$$\begin{tikzcd} & K(E_1) = K(x_1, y_1) \arrow[d, "\deg \phi"] \\ K(x_1) \arrow[ur, "2"] & K(E_2) = K(x_2, y_2) \\ K(x_2) \arrow[u, phantom] \arrow[ur, "2"'] & \end{tikzcd}$$

$\deg(\xi)$: $K(x_1) \to K(x_2)$

Now $K(x_2) \hookrightarrow K(x_1)$

$x_2 \longmapsto \xi(x_1)$

this ξ defines a morphism $\mathbb{P}^1 \xrightarrow{\xi} \mathbb{P}^1$ making diagram commute.

Tower law: $\cancel{2} \deg \phi = \cancel{2} \deg \xi$

(now, it's computing degree of morphism, nothing to do with Es).

Write $\xi(x_1) = \frac{r(x_1)}{s(x_1)}$ $r, s \in K[t]$ coprime.

Claim that min poly of x_1 over $K(x_2)$ is:

$$f(t) = r(t) - s(t)x_2 \in K(x_2)[t].$$

Check: 1) $f(x_1) = 0$ ✓ $r(x_1) - s(x_1) \cdot x_2 = 0 \iff x_2 = \frac{r(s_1)}{s(s_1)}$

2) f irreducible in $K[x_2, t]$ since r, s coprime and it's linear in x_2.

so f is indeed min poly of x_1 over $K(x_2)$.

Gauss's lemma: f is irreducible in $K(x_2)[t]$. (irred over ring $\Rightarrow$ irred over field)

$\therefore$ $\deg \phi = \deg \xi = [K(x_1) : K(x_2)]$? Why?

$= \deg f$

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

■

Lemma 3.5 $\deg[2] = 4$.

Proof: Assume that $K \neq 2, 3$. Write

$$E \cdot y^2 = f(x) = x^3 + ax + b.$$

If $P = (x, y)$ then

$$x(2P) = \underbrace{\left(\frac{3x^2+a}{2y}\right)^2}_{\text{square of } \lambda} - \underbrace{2x}_{\text{sum of } x\text{-coords}} = \frac{(\overbrace{3x^2+a}^{f'(x)})^2 - 8x f(x)}{4f(x)} = \frac{x^4 + \cdots}{4f(x)}.$$

the numerator and denom are coprime.

Indeed, o.w. $\exists$ $\theta \in \bar{K}$ s.t. $f(\theta) = f'(\theta) = 0$ then f has multiple root ✗.

By lemma 5.4, $\deg[2] = \max(3, 4) = 4$.

■

Lecture 7.

Defn. Quadratic forms

Let A be an abelian group.

$q: A \to \mathbb{Z}$ is a quadratic form if

i) $q(nx) = n^2 q(x) \quad \forall n \in \mathbb{Z},\ x \in A$

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

lemma 5.6 Quadratic form $\Leftrightarrow$ parallelogram law.

$q: A \to \mathbb{Z}$ is a quadratic form iff it satisfies the parallelogram law:

$$q(x+y) + q(x-y) = 2q(x) + 2q(y) \quad \forall x, y \in A.$$

Proof:

$\Rightarrow$ let $\langle x, y \rangle = q(x+y) - q(x) - q(y)$

then $\langle x, x \rangle = q(x+x) - 2q(x) = 2q(x)$ (by (i), $n=2$)

But by (ii), $\frac{1}{2}\langle x+y, x+y\rangle + \frac{1}{2}\langle x-y, x-y\rangle = \langle x, x\rangle + \langle y, y\rangle$

i.e. $\frac{1}{2}\langle x+y, x+y\rangle + \frac{1}{2}\langle x-y, x-y\rangle$

$= \frac{1}{2}\langle x, x\rangle + \frac{1}{2}\langle x, y\rangle + \frac{1}{2}\langle y, x\rangle + \frac{1}{2}\langle y, y\rangle + \frac{1}{2}\langle x, x\rangle + \frac{1}{2}\langle y, y\rangle - \frac{1}{2}\langle x, y\rangle - \frac{1}{2}\langle y, x\rangle$

$= \langle x, x\rangle + \langle y, y\rangle$

But by the above $\langle z, z\rangle = 2q(z)$, we get

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

$\Leftarrow$ on example sheet 2.

Thm 5.7. Degree is a quadratic form.

must be defined this way to be true.

$\deg: \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form (define $\deg 0 = 0$)

$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies}\} \cup \{0\}$.

Remarks for the proof, we assume $\deg K \neq 2, 3$, so

Write $E_2: y^2 = x^3 + ax + b$

let $P, Q \in E_2$ with $P, Q, P+Q, P-Q \neq 0$ (i.e. them on standard affine piece)

let x_1, x_2, x_3, x_4 be the x-coordinate of these 4 points.

lemma 5.8 write x-coordinates in terms w_0, w_1, w_2. (idea: get coordinate of one point in terms of the others.)

$\exists\, w_0, w_1, w_2 \in \mathbb{Z}[a,b][x_1, x_2]$ of deg ≤ 2 in x_1 and degree ≤ 2 in x_2, s.t.

$$\underbrace{(1 : x_3+x_4 : x_3x_4)}_{\text{they are rational func on } x_1, x_2} = \underbrace{(w_0 : w_1 : w_2)}_{\text{each of them are polynomials in } x_1, x_2}$$

Proof: Method ①: direct calculation (explicit group law + formula sheet)

$$w_0 = (x_1 - x_2)^2$$
$$w_1 = \cdots\ 2(x_1x_2 + a)(x_1+x_2) + 4b$$
$$w_2 = \cdots\ x_1^2x_2^2 - 2ax_1x_2 - 4b(x_1+x_2) + a^2$$

see formula sheet

Method ②: idea: get $P, Q, P+Q$, get line PQ, look at intersection

let $y = \lambda x + \nu$ be the line through P & Q.

then, EC & $\lambda x + \nu$ intersect at 3 point of intersections:

$$x^3 + ax + b - \underbrace{(\lambda x + \nu)^2}_{=y^2} = (x - x_1)(x - x_2)(x - x_3) = x^3 - s_1 x^2 + s_2 x - s_3$$

$s_i = i^{th}$ elementary symmetric poly in x_1, x_2, x_3.

compare the coefficients we get
$$\begin{cases} \lambda^2 = s_1 \\ -2\lambda\nu = s_2 - a \\ \nu^2 = s_3 + b \end{cases}$$

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

$F(x_1, x_2, x_3)$ has degree ≤ 2 in each x_i once plug each s_i in.

(as x_3 must satisfy the above poly)

x_3 is a root of the quadratic $W(t) = F(x_1, x_2, t)$. (as x_1, x_2 already known)

Repeat the above computation for $P, -Q$, shows x_4 is another root. (of $W(t)$)

So $w_0(t - x_3)(t - x_4) = W(t) = w_0 t^2 - w_1 t + w_2$

its roots include x_3, x_4

therefore $(1 : x_3 + x_4 : x_3 x_4) = (w_0 : w_1 : w_2)$.

∎

Now, show if $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ then $\deg(\phi+\psi) + \deg(\phi-\psi) \leq 2\deg\phi + 2\deg\psi$.

We may assume $\phi, \psi, \phi+\psi, \phi-\psi \neq 0$ (o.w. trivial or use $\deg[-1]=1$, $\deg[2]=4$).

If any is 0, get $2\deg(\phi) \leq 2\deg(\phi)$. If $\phi=\psi$, $\deg(2\psi)+\deg(0) \leq 2\deg(\psi)+2\deg(\psi)$

If $\phi=-\psi$, similar.

We write (using lemma 3.4 in the background)

$\phi : (x,y) \mapsto (\xi_1(x), \cdots\cdots)$

$\psi : (x,y) \mapsto (\xi_2(x), \cdots)$

$\phi+\psi : (x,y) \mapsto (\xi_3(x), \cdots)$

$\phi-\psi : (x,y) \mapsto (\xi_4(x), \cdots)$

lemma 5.8 $\Rightarrow$ $(1 : \xi_3+\xi_4 : \xi_3\xi_4) = ((\xi_3-\xi_4)^2 : \cdots\cdots)$ (formula sheet)

Put each $\xi_i = \frac{r_i}{s_i}$, $r_i, s_i \in K[t]$, coprime.

then $(s_3s_4 : r_3r_4 + r_4r_3 : r_3r_4) = ((r_1s_2 - r_2s_1)^2 : \cdots)$ $(*)$ Clear the denom by multiply s_3, s_4

coprime

lemma 5.8 $\Rightarrow$ everything has degree ≤ 2.

therefore

lemma 5.4

$\deg(\phi+\psi) + \deg(\phi-\psi) = \max(\deg(r_3), \deg(s_3)) + \max(\deg(r_4), \deg(s_4))$

check & split into 4 cases.

$= \max(\deg(s_3s_4), \deg(r_3s_4+r_4s_3), \deg(r_3r_4))$

by $(*)$ as LHS of $(*)$ is coprime.

$\leq 2\max(\deg(r_1), \deg(s_1)) + 2\max(\deg(r_2), \deg(s_2))$??? why follows?

$= 2\deg(\phi) + 2\deg(\psi)$ ——— ①

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

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

But $\deg[2]=4$, so

$2\deg(\phi) + 2\deg(\psi) \leq \deg(\phi+\psi) + \deg(\phi-\psi)$ ——— ②

①+② $\Rightarrow$ degree satisfy parallelogram law.

$\Rightarrow$ degree is a quadratic form. (lemma 5.6) $\blacksquare$

~~Cor 5.9 $\deg[n]=n^2$~~

$\deg(n\phi) = n^2\deg(\phi)$ $\forall n \in \mathbb{Z}$, $\phi \in \mathrm{Hom}(E_1, E_2)$

In particular $\deg[n] = n^2$

Example 5.10 An isogeny that is not [n].

Let E/K be an elliptic curve. Suppose char $K \neq 2$, $0 \neq T \in E(K)[2]$ (2-torsion point)

w.l.o.g. $E: y^2 = x(x^2+ax+b)$, $a, b \in K$, $\underbrace{b(a^2-4b) \neq 0}$. Then, we have that $T = (0,0)$.

there's no double root as if $b=0$, get double. If $a^2-4b=0$, also double.

It is a 2-torsion point since its tangent is vertical.

If $P=(x,y)$, and $P' = P+T = (x',y')$ then

$$\begin{cases} x' = \underbrace{\left(\frac{y}{x}\right)^2 - a - x}_{\text{Formal gp law}} = \frac{x^2+ax-b}{x} - a - x = \frac{b}{x} \\ y' = \underbrace{\left(-\frac{y}{x}\right)x'}_{\text{gp law again, } \nu=0} = \frac{by}{x^2} \end{cases}$$

Isogeny obtained by adding point w/ $(0,0)$

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

then $\eta^2 = \left(\frac{y}{x}\right)^2 \left(\left(x + \frac{b}{x}\right)^2 - 4b\right)$

$= \xi\left((\xi - a)^2 - 4b\right)$

$= \xi\left(\xi^2 - 2a\xi + a^2 - 4b\right)$

let $E': y^2 = x^2 + a'x + b'$ where $a' = -2a$, $b' = a^2 - 4b$, then we get an isogeny

$\phi: E \to E' \subseteq \mathbb{P}^2$ $\quad \phi: E \to E'$

$(x,y) \mapsto (\xi : \eta : 1)$ $\quad (x,y) \mapsto \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2-b)}{x^2}\right)$ or $\left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2-b)}{x^2} : 1\right)$

left to show $\phi(O_E) = O_{E'}$, the three coordinates have a pole of order ~~-2, -3, 0~~ 1 0 3 resp.

at O_E, so we multiply by uniformizer of power 3, get $(0:1:0)$.

so $O_E \mapsto (1:0:1)$

(keep using smooth proj curves $\Rightarrow$ morphism)

$\left(\frac{y}{x}\right)^2 = \frac{x^2+ax+b}{x}$ coprime since $b \neq 0$

lemma 3.3 $\Rightarrow \deg(\phi) = 2$ so that ϕ is a 2-isogeny.

It's a diff isogeny than [2].

Lecture 8

(switched to annotating typed notes by Qiangru Kuang)

§6. Invariant differential.

Let C be an algebraic curve over $K=\bar{K}$.

defn. Space of differentials

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

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

Idea, given $K(C)$, we quotient out by these relations?

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

def. Order of vanishing

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

Since $\omega \in \Omega_C$, and Ω_C is 1-dim $K(C)$ v.s. anything nonzero is a basis, so that can write $\omega = f\,dt$.

Fact. Taking differential decrease the exponent by 1.

Suppose $\underbrace{f \in K(C)^*}_{\text{nonzero rational}}$ and $\mathrm{ord}_P(f) = n \neq 0$. If $\mathrm{char}\, K \nmid n$ then

$$\mathrm{ord}_P(df) = n-1.$$ (think as $f = x^n$, $df = nx^{n-1}$).

We now assume C is a smooth projective curve.
(before we assumed C is an alg curve).

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

def. $\mathrm{div}(\omega)$

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

def. Genus of C

define the genus of C to be

canonical divisor.

effective divisors $\Leftrightarrow$ no poles

$$g(C) = \dim_K \underbrace{\{ \omega \in \Omega_C : \mathrm{div}(\omega) \geq 0 \}}_{\text{the space of regular differentials.}}$$

not a v.s. over $K(C)$
But is a v.s. over K.

As a consequence of Riemann Roch, we have

$$0 \neq \omega \in \Omega_C \Rightarrow \deg(\mathrm{div}(\omega)) = 2g(C) - 2.$$

this is choice of ω up to multiply by rational functions.

Lemma 6.1. $\omega \in \Omega_C$ s.t. it has no poles & no zeroes.

Assume $\mathrm{char}\, K \neq 2$ and $E: y^2 = (x-e_1)(x-e_2)(x-e_3)$. e_1, e_2, e_3 distinct.

Then $\omega = \frac{dx}{y}$ is a (regular differential) differential on E with no zeroes or poles.

In particular, $g(E) = 1$ and the K-vector space of regular differentials on E is 1-dim'l, spanned by ω. (as $\omega \neq 0$ so it spans)

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

$$\mathrm{div}(y) = (T_1) + (T_2) + (T_3) - 3(O_E) \quad ①$$

had choice of picking $(1,1,1)$ as coefficients, T_i are uniformizers, & know 3 zeroes.

T_i appear with multiplicity 1 in $\mathrm{div}(y)$ as we know $\deg(\mathrm{div}(y)) = 0$. ??? Riemann Roch?

If $P \in E\setminus\{O\}$, then

$$\mathrm{div}(x - x_P) = (P) + (-P) - 2(O_E)$$

coefficient of this

If $P \in E \setminus E[2]$, then $\mathrm{ord}_P(x - x_P) = 1$ so $\mathrm{ord}_P(dx) = 0$ ($d(x-x_P) = dx$ and take d drop

If $P = T_i$, then $\mathrm{ord}_P(x - x_P) = 2$ ($(P) = (-P)$ so coefficient is 2). So $\mathrm{ord}_P(dx) = 1$. by 1).

If $P = O_E$ then ~~$\mathrm{ord}_P(x) = -2$~~ $\mathrm{ord}_P(x - x_P)$ so $\mathrm{ord}_P(dx) = -3$.

Therefore,

$$\mathrm{div}(dx) = (T_1) + (T_2) + (T_3) - 3(O_E) \quad ②$$

so ① + ② $\Rightarrow \mathrm{div}\left(\frac{dx}{y}\right) = 0$ ← this 0 is the 0 divisor

■

Recall how we have pullback of rational fcn, now pb of differentials.

<u>defn. pullback of differentials</u>

If $\phi: C_1 \to C_2$ is a nonconstant morphism then we have:

(pb of differentials):

$$\phi^*: \Omega_{C_2} \to \Omega_{C_1}$$

$$f\,dg \mapsto (\phi^* f)\, d(\phi^* g)$$

Recall $\phi: C_1 \to C_2$

$\phi^*: K(C_2) \to K(C_1)$

$\phi^*(f) = \underbrace{f \circ \phi}_{C_1 \to K}$

$f: C_2 \to K$, $C_2 \to K$, $C_1 \to C_2$

<u>lemma 6.2 invariant differential.</u>

let $P \in E$, $\tau_P: E \to E$, $x \mapsto P + x$. if $\omega = \frac{dx}{y}$ then $\tau_P^* \omega = \omega$.

ω is called the invariant differential.

note: Regular differentials ⇔ no poles

so translation also no poles.

$VS = \mathrm{span}(\omega)$

<u>Proof</u>:

$\tau_P^* \omega$ is again a regular differential on E so $\tau_P^* \omega = \lambda_P \omega$ for some $\lambda_P \in K^*$. (lemma 6.1. The reg. differentials is a K-vec space) λ_P depend on P.

The map $E \to \mathbb{P}^1$, $P \mapsto \lambda_P$ (after a calculation we know it's rational)

so it's a morphism of smooth projective curves but not surjective, as it misses 0 and ∞.

Thm 2.8 $\Rightarrow$ it's constant. Hence $\exists \lambda \in K^*$ s.t. $\tau_P^* \omega = \lambda \omega \quad \forall P \in E$.

Take $P = O_E \Rightarrow \lambda = 1$.

translation by O: do nothing

hence pushback is identity $\Rightarrow \lambda = 1$. $\blacksquare$

<u>Remark</u> If $K = \mathbb{C}$, recall $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ so

$z \mapsto (\wp(z), \wp'(z))$

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

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

<u>Lemma 6.3. invariant differential vs. Hom.</u>

let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, ω the invariant differential on E_2.

Then $(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$. $\quad \phi^*, \psi^* : \Omega_{E_2} \to \Omega_{E_1}$

group law on E_2.

<u>Proof</u>:

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

$$E \times E \to E$$

$$\mu : (P, Q) \mapsto P + Q$$

$$Pr_1 : (P, Q) \mapsto P$$

$$Pr_2 : (P, Q) \mapsto Q.$$

$E \times E$ is 2-dimensional

<u>Fact</u> $\Omega_{E \times E}$ is a 2 dimensional $K(E \times E)$ vector space with basis $Pr_1^* \omega, Pr_2^* \omega$.

Then $\mu^* \omega = f Pr_1^* \omega + g Pr_2^* \omega$ for some $f, g \in K(E \times E)$.

For fixed $Q \in E$, let $\tau_Q : E \to E \times E$, $p \mapsto (P, Q)$ Applying τ_Q^* gives

$$(\mu \tau_Q)^* \omega = \tau_Q^*(\mu^*(\omega)) = (\tau_Q^* f)\underbrace{(Pr_1 \tau_Q)}_{= \mathrm{id}}{}^* \omega + (\tau_Q^* g)\underbrace{(Pr_2 \tau_Q)}_{\text{constant map}}{}^* \omega$$

Question: how does pullback distribute?

so $\omega \underset{\text{lemma 6.2.}}{=} \tau_Q^* \omega = (\tau_Q^* f)\, \omega + 0$

so $\tau_Q^* f = 1$ for all $Q \in E$, so $f(P, Q) = 1$ for all $P, Q \in E$.

Similarly $g(P, Q) = 1$, $\forall P, Q \in E$.

thus $\mu^* \omega = \pi_1^* \omega + \pi_2^* \omega$. Now, pullback by $V : E_1 \to E_2 \times E_2$

$P \mapsto (\phi(P), \psi(P))$ to get

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

$u^* : E \to E \times E$

$V^* : E \times E \to E$

$V^* u^* \omega = V^* \pi_1^* \omega + V^* \pi_2^* \omega$

$(uV)^* \omega = (\pi_1 V)^* \omega + (\pi_2 V)^* \omega$

$(\phi(p) + \psi(p))^* \omega = \phi(p)^* \omega + \psi(p)^* \omega$ $\blacksquare$

Lecture 9

Lemma 6.4. Check if a morphism is separable.

Let $\phi: C_1 \to C_2$ be a non constant morphism.

Then ϕ is separable if and only if

$\phi^*: \Omega_{C_2} \to \Omega_{C_1}$ is nonzero.

Proof: omitted. Idea is basically check if $f(x)$, $f'(x)$ has common roots.

Example: Consider the group variety $\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\} = \mathbb{P}^1 \setminus \{0, \infty\}$, group law is multiplication.

let $n \geq 2$ and $\phi: \mathbb{G}_m \to \mathbb{G}_m$

$x \mapsto x^n$

two ways to show char $K \nmid n$ implies $\#\ker(\phi) = n$

1^{st} way:

??? not seen before — Galois theory $\Rightarrow$ if char $K \nmid n$, then $\#\ker(\phi) = n$.

2^{nd} way:

? why equal?

Consider the differentials. $\phi^*(dx) = dx^n = nx^{n-1}\,dx$

so if char $K \nmid n$, ϕ^* nonzero, 6.4 $\Rightarrow$ ϕ is separable.

So $\#\phi^{-1}(Q) = \deg \phi$ for all but finitely many $Q \in \mathbb{G}_m$. degree = count fibres at most points

ϕ is a group homomorphism, so $\#\phi^{-1}(Q) = \#\ker(\phi)$ $\forall Q \in \mathbb{G}_m$. as fibres form cosets of the kernel.

So, $\#\ker\phi = \#\phi^{-1}(Q) = \deg\phi = n$

Therefore, $K (= \bar{K})$ contains exactly n n^{th} roots of unity.

Thm 6.5 Structure of the n-torsion group

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

proof idea uses invariant differential ω.

Proof: By induction + lemma 6.3, $[n]^*\omega = n\omega$. $(\phi^* + \psi^*)\omega = \phi^*\omega + \psi^*\omega$ so $n^*\omega = 1^*\omega + \dots + 1^*\omega = n\omega$

So, if char $K \nmid n$, then $n\omega \neq 0$ so $[n]: E \to E$ is separable.

By thm 2.8, $\#[n]^{-1}Q = \deg[n]$ for all but finitely many $Q \in E$. degree is #fibre for almost all Q.

But, $[n]$ is a group hom so $\#[n]^{-1}(Q) = \#E[n]$ for all $Q \in E$. Since $\#[n]^{-1}(Q) = \#[n]^{-1}(O) = \#E[n]$
the size of cosets equal

so $\#E[n] = \#[n]^{-1}(Q) = \deg[n] = n^2$
quadratic form thm.

Now we know the order of the group $E[n]$.

By classification of finite abelian groups,

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

with $d_1 | d_2 | \cdots | d_t | n$ and $\prod d_i = n^2$.
since any element is n-torsion so order of everything must divide n

If p is a prime, $p | d_1$, $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$ as $E[p]$ is subgp of $E[n]$, $p | d_i$ $\forall i$, get iso btwn them.

But $\#E[p] \cong p^2$ so $t = 2$, hence $d_1 | d_2 | n$, $d_1 d_2 = n^2 \Rightarrow d_1 = d_2 = n$.

■

Remark inseparable isogenies

If $\mathrm{char}\, K = p$, then $[p]$ is inseparable as $[p]^* \omega = 0$ for $p \mid \mathrm{char}(K)$ & lemma 6.4.

It can be shown that

① $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ $\forall r \geq 1$. Called ordinary

or

② $E[p^r] = 0$ $\forall r \geq 1$ called supersingular.
(p-torsion don't exist)

§7. Elliptic curves over finite fields

Lemma 7.1 A form of Cauchy Schwartz.

the degree map.

let A be an abelian group and $q: A \to \mathbb{Z}$ is a positive definite quadratic form,
If $x, y \in A$ then

$$\underbrace{|q(x+y) - q(x) - q(y)|}_{\text{write } := \langle x, y \rangle} \leq 2\sqrt{q(x) q(y)}$$

also note $\langle x, x \rangle = 2q(x)$

Proof: Assume $x \neq 0$, ($x = 0$ quickly check $0 \leq 0$)

let $m, n \in \mathbb{Z}$ then consider lin comb of x, y.

$0 \le q(mx+ny)$

$= \frac{1}{2}\langle mx+ny, mx+ny\rangle$

$= \frac{m^2}{2}\langle x,x\rangle + \frac{2mn}{2}\langle x,y\rangle + \frac{n^2}{2}\langle y,y\rangle$

$= m^2 q(x) + mn\langle x,y\rangle +$

$q(x) \ne 0$
& completing the square $= q(x)\left(m + \frac{\langle x,y\rangle}{2q(x)}n\right)^2 - \frac{\langle x,y\rangle^2}{4q(x)}n^2 \quad + n^2 q(y))$

$= q(x)\left(m + \frac{\langle x,y\rangle}{2q(x)}n\right)^2 + \left(q(y) - \frac{\langle x,y\rangle^2}{4q(x)}\right)n^2$

take $m = -\langle x,y\rangle$, $n = 2q(x)$, we get

$\Rightarrow \quad 0 \le \left(q(y) - \frac{\langle x,y\rangle^2}{4q(x)}\right)n^2$

or $\quad \langle x,y\rangle^2 \le 4q(x)q(y)$

$|\langle x,y\rangle| \le 2\sqrt{q(x)q(y)}$ ∎

Now, given an EC, want the # of points defined over $E(\mathbb{F}_q)$.

Recall that

let $\mathbb{F}_q$ be field of q elements, $q=p^m$, p prime, Then

$Gal(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is cyclic of order r generated by the Frobenienious element $x \mapsto x^q$.

Galois group generated by Frobenius.

Thm 7.2 Hasse

let $E/\mathbb{F}_q$ be an elliptic curve. Then

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

Note: Something about the estimation of $\#E(\mathbb{F}_q)$?

Proof:

let E have Weierstrass equation with coefficients $a_1, \cdots a_6 \in \mathbb{F}_q$,

So that $a_i^q = a_i$ for all i. (over $\bar{\mathbb{Q}}$, elements in $\mathbb{F}_q$ fixed by Frob map)

Scheme

↳ $E(\mathbb{F}_q) = \ker(1-\phi)$

↳ ϕ is not separable, $1-\phi$ is

↳ so $\underbrace{\#(\ker 1-\phi)}_{\#\text{ fibre}} = \deg(1-\phi)$

↳ use cauchy-schwartz thing.

<u>def. Frobenius Endomorphism</u> (for elliptic curves)

$\phi : E \to E$

$(x,y) \mapsto (x^q, y^q)$ this is an isogeny of degree q. (field extension is of degree q)

Then

$E(\mathbb{F}_q) = \{ P \in E : \phi(P) = P \} = \ker(1-\phi)$ } note: you see it both as an isogeny & action over Gal.

Now, want to calculate $\#\ker$ in same way.

Examine $1-\phi$

Note that ϕ is not separable because

$$\phi^* \omega = \phi^*\left(\frac{dx}{y}\right) = \frac{dx^q}{y^q} = \frac{q x^{q-1}}{y^q} \underset{\text{char } p}{=} 0$$

But $1-\phi$ is separable

$$(1-\phi)^*\omega \overset{6.3}{=} 1^*\omega - \phi^*\omega = \omega - \phi^*\omega = \omega \neq 0$$

Thm 28 $\Rightarrow$ (thm 28 basically says separable $\Rightarrow$ can count fibre)

so $\#E_1(\mathbb{F}_q) = \#\ker(1-\phi) = \deg(1-\phi)$ is this counting the fibre over 0?

note $\deg : \mathrm{Hom}(E,E) \to \mathbb{Z}$ is a positive definitive quadratic form, so

By 7.1,

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

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

■

7.1 Zeta function

<u>Defn Zeta function for number field & function field.</u>

for K a number field

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

for K a function field, i.e. $K = \mathbb{F}_q(C)$, $C/\mathbb{F}_q$ is a smooth projective curve,

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

where $|C|$ is the set of closed points of C, and is same as the orbit of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on $C(\overline{\mathbb{F}_q})$.

$Nx = q^{\deg x}$, $\deg(x)$ = size of the orbit. (i.e. conjugate pts/ quad exts)

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

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

The next part gives us some motivation to why taking this series

Take logarithm of the formal power series, get

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

using power series expansion for $-\log(1-x) = x + \frac{x^2}{2} + \cdots + \frac{x^n}{n} + \cdots$

to fix the $T^{m \deg x - 1}$ back

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

set $n = m \deg x$

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

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

Reversing the process,

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

Where did division by n from?

divide by n b/c it gives similar Riemann zeta fcn.

Silverman page 140: given $F(T)$ we can recover the $\# V(\mathbb{F}_{q^n})$.

def tr

$$\mathrm{tr} : \mathrm{End}(E) \to \mathbb{Z}$$

$$\phi \mapsto \langle \phi, 1 \rangle.$$

Lecture 10.

def : $\langle \phi, \psi \rangle$ and the trace

for $\phi, \psi \in End(E, E)$, we put $\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg \phi - \deg \psi$.

$$tr(\phi) = \langle \phi, 1 \rangle.$$

lemma 7.3: Something links $tr(\phi)$ and $\deg(\phi)$

If $\phi \in End(E)$, then $\phi^2 - \underbrace{tr(\phi)}_{\in \mathbb{Z}} \phi + \deg(\phi) = 0.$

Proof: ex sh 2. (related to Cayley Hamilton thm 2x2 matrices?)

defn. Zeta function for curves

the zeta function of a variety $C/\mathbb{F}_q$ is the formal power series

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

Recall by Hasse's thm, $|\# E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$

Lemma 7.4. Zeta function for EC expressed as rational function.

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

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

Proof let $\phi: E \to E$ be q-th power Frobenius. Proof of Hasse's thm yields

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

detail in Hasse's # $\bar{\mathbb{Q}}$ point fixed by $1-\phi$ — defn of trace.

So $a = tr\phi$, $\deg \phi = q$.

So lemma 7.3: $\phi^2 - tr(\phi)\phi + \deg(\phi) = 0 \Rightarrow \phi^2 - a\phi + q = 0$

$$\Rightarrow \phi^{n+2} - a\phi^{n+1} + q\phi^n = 0$$

taking the trace, $\langle \cdot, \cdot \rangle$ is bilinear

$$\Rightarrow tr(\phi^{n+2}) - a\, tr(\phi^{n+1}) + q\, tr(\phi^n) = 0$$

why solutions are of this form?

This gives us a second order difference equation with init conditions $\begin{cases} tr\, 1 = 2 & \langle 1,1 \rangle = \deg(2) - 2\deg(1) = 2 \\ tr\phi = a \end{cases}$

It gives us solutions $tr(\phi^n) = \alpha^n + \beta^n$, $\alpha, \beta \in \mathbb{C}$, as roots of $x^2 - ax + q = 0$.

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

$\bar{\mathbb{Q}}$ points fixed by ϕ^n Frobenius. — isogeny degree — composition multiplicative.

Scheme
- $\hookrightarrow \# E(\mathbb{F}_{q^n}) = ?$
- $\hookrightarrow \phi^2 - a\phi + q = 0$
- $\hookrightarrow$ pad with ϕ^n
- $\hookrightarrow$ take trace
- $\hookrightarrow tr(\phi^n)$ is 2^{nd} order DE
- $\hookrightarrow$ write $\# E(\mathbb{F}_{q^n})$ in terms of α^n, β^n.
- $\hookrightarrow$ use log to get result.

Thus, the zeta function is: substitute (*) into $Z_C(T)$

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

using $-\log(1-x) = \sum_{m=1}^{\infty} \frac{x^m}{m}$. $-\log(RHS) = -\log(1-\alpha T) - \log(1-\beta T) + \log(1-T) + \log(1-qT)$

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

■

Remark: Hasse's thm & Riemann Hypothesis for elliptic curves:

Hasse's thm $\Rightarrow |a| \le 2\sqrt{q}$ since α, β solves $1-aT+qT^2$ $\sqrt{b^2-4ac} = \sqrt{a^2-4q} < 0$, both $\notin \mathbb{R}$

$\Rightarrow \alpha = \overline{\beta}$

since $\alpha\beta = q$ $\Rightarrow |\alpha| = |\beta| = \sqrt{|q|}$ —— (*)

Let $K = \mathbb{F}_q(E)$, then $\zeta_K(s) = 0 \Leftrightarrow Z_E(q^{-s}) = 0$ (because $\zeta_K(s) = Z_E(q^{-s})$)

$\Rightarrow q^s = \alpha$ or β, so $q^{re(s)} = \sqrt{q}$ by (*) $\Rightarrow \mathrm{Re}\, s = \frac{1}{2}$.

numerator of $Z_E(T)$ is $(1-\alpha T)(1-\beta T)$ look into raise $\mathbb{C}$ to $\mathbb{C}$.

So we have proven the Riemann hypothesis.

§8. Formal groups (in preparation for EC in local fields).

Def I-adic topology

Let R be ring, $I \subset R$ ideal, the I-adic topology is the topology on R with basis $\{r + I^n : \substack{r \in R \\ n \ge 1}\}$.

Def. Cauchy Sequence.

A sequence (x_n) in R is cauchy if $\forall k \ge 1$, $\exists N$, s.t. $\forall m, n \ge N$, $x_m - x_n \in I^k$.

Def. Ring complete w.r.t. I-adic topology

R is complete if

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

Remark $1-x \in R^*$

If R is complete, if $x \in I$, then $\frac{1}{1-x} = \underbrace{1+x+x^2+\cdots}_{\text{cauchy}}$ hence $1-x$ has an inverse, so $1-x \in R^*$.

Example

1. $R = \mathbb{Z}_p$, $I = p\mathbb{Z}_p$ } complete by construction

$R = \mathbb{Z}[[t]]$, $I = (t)$ } think why it's complete?

Notation $a \equiv b \mod I$ means $(a-b) \in I$.

Lemma 8.1 Hensel's lemma

let R be a ring, complete w.r.t. ideal I.

let $F \in R[x]$, and $s \geq 1$.

Suppose $a \in R$ satisfies $\begin{cases} F(a) = 0 \mod I^s \\ F'(a) \in R^* \end{cases}$

then there exists unique $b \in R$ s.t. $\begin{cases} F(b) = 0 \\ b = a \mod I^s. \end{cases}$

Proof. We start with some w.l.o.g. business.

let $u \in R^\times$ with $F'(a) \equiv u \mod (I)$ any unit works as $F'(a) \in R^\times$. This u only helpful way later.

replace F by $\frac{F(X+A)}{u}$ we may assume $a = 0$ and $F'(0) = 1 \mod (I)$ work it out explicitly.

We define $\begin{cases} x_0 = 0 \\ x_{n+1} = x_n - F(x_n) \end{cases}$ —— ①

An easy induction $\Rightarrow$ $x_n \equiv 0 \mod (I^s)$, $\forall n$ —— ② $\begin{cases} x_0 = 0 \;\checkmark \\ x_{n+1} - x_n \equiv F(x_n), \; (F(x_n) \equiv F(0) \equiv 0, \mod I^s) \end{cases}$

Also, have

$$F(X) - F(Y) = (X-Y)\,(\underbrace{F'(0)}_{\text{coefficient of } x \text{ in } F} + XG(X,Y) + YH(X,Y)) \quad \text{—— ③}$$ (similar to local fields factorise)

for some $G, H \in R[X,Y]$.

Claim that $x_{n+1} \equiv x_n \pmod{I^{n+s}}$ $\forall n \geq 0$

Proof of claim

induction on n.

- $n=0$, $x_1 \equiv x_0 \mod I^s$ this is already true by ②.
- $n>0$, suppose that $x_n \equiv x_{n-1} \pmod{I^{n+s-1}}$ then

$F(x_n) - F(x_{n-1}) = (x_n - x_{n-1})(1+c)$, for some $c \in I$. (plug into ③, get $\underset{1 \bmod I}{F'(0)} + x_n(\text{smth}) + x_{n-1}(\text{smth})$ $\in I$ by ①)

modulo by I^{n+s}, get

$$F(x_n) - F(x_{n-1}) \equiv (x_n - x_{n-1}) + \underbrace{(x_n - x_{n-1})c}_{\in I^{n+s}} \equiv (x_n - x_{n-1}) \mod I^{n+s}$$

Rearrange $\Rightarrow$ $\underbrace{x_n - F(x_n)}_{= x_{n+1}} \equiv \underbrace{x_{n-1} - F(x_{n-1})}_{= x_n} \mod I^{n+s}$ ■

continue proof of hensel's lemma.

By completeness & claim, $x_n \to b \in R$ as $n \to \infty$.

Taking limit of ① & continuity gives $b = b - F(b) \Rightarrow F(b) = 0$.

Taking limit in $x_n \equiv 0 \mod I^s$ in ② gives $b \equiv 0 \mod I^s$. $\Rightarrow b \equiv a \mod I^s$.

uniqueness follows in ③. i.e. if X, Y two different roots, then

$$\underbrace{F(X) - F(Y)}_{0} = \underbrace{(X-Y)}_{\neq 0} \underbrace{(F'(0) + XG(X,Y) + YH(X,Y))}_{1 \bmod I.}$$

R is ID, ※.

completes the proof ■

<u>Remark Approx E with Power series</u>

Consider the homogenous version of E:

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

want to study the power series passing thru affine piece.

Idea: solve for w in power series of t.

Want to study the behaviour near O_E, use affine piece $Y \neq 0$ (or $Y=1$)

let $t = -X/Y$, $w = -Z/Y$, then

$$w = \underbrace{t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3}_{f(t,w)}.$$

Apply Hensel's lemma to $R = \mathbb{Z}[a_1, \cdots a_6][[t]]$, $I = (t)$ (complete w.r.t. I-adic topology)

and $F(X) = X - f(t, X) \in R[X]$.

The approximate root is $a=0$ for $S=3$. Check $F(0) = -f(t,0) = -t^3$, $F'(0) = 1 \underbrace{- a_1t - a_2t^2}_{\text{basically all linear terms in } t} \in R^*$ in R^*, form of $1-(\text{smth})$.

Then Hensel's lemma $\Rightarrow \exists$ unique $w(t) \in \mathbb{Z}[a_1, \cdots, a_6][[t]]$ s.t. $w(t) = f(t, w(t))$ and $w(t) \equiv 0 \mod (t^3)$

So given t the x-coordinate on E, Hensel helps you to solve for w, the y-coordinate, in a power series of t.

scheme for the above:
↳ hom Weierstrass.
Leaffine piece $Y=1$
↳ $t=-X/Y$, $w=-Z/Y$.

then substitute
use Hensel on
$w=f(t,w)$
$F(x)= x-f(t,x)$.

Lecture 11

To see $w(t)$ explicitly, following Hensel's lemma with $u=1$,

get $w(t) = \underbrace{\lim_{n\to\infty} w_n(t)}_{\text{as sequence of polynomials}}$ where $\begin{cases} w_0(t)=0 \\ w_{n+1}(t)= f(t, w_n(t)). \end{cases}$

In fact,

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

where $A_1=a_1$, $A_2=a_1^2+a_2$, $A_3=a_1^3+2a_1a_2+a_3$, ... Pattern, each additive term, sum of subscrip is the index of A_i.

Lemma 8.2

Let R be an integral domain (so $\mathrm{Frac}(R)$ exists), complete w.r.t I.

let $a_1, \cdots, a_6 \in R$, $K=\mathrm{Frac}(R)$ then

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

is a subgroup of $E(K)$.

(i.e. the points on E with both coordinates in a certain ideal of R forms a group on $E(\mathrm{Frac}(R))$.

Remark. Another way to write $\hat{E}(I)$

By uniqueness of Hensel's lemma, $(s=1)$, we also describe $\hat{E}(I)$ as

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

Proof

taking $(t,w)=(0,0)$ shows $0_E \in \hat{E}(I)$. (as $(0,0)$ corresponds to $\begin{matrix}(X:Y:Z)\\(0:1:0)\end{matrix}$)

Thus suffices to show $P_1, P_2 \in \hat{E}(I)$ then $-P_1-P_2 \in \hat{E}(I)$ (shows inverses & group law)

Now, suppose that $P_i=(t_i, w_i)$. So t_1, t_2, $w_1=w(t_1)$, $w_2=w(t_2) \in I$

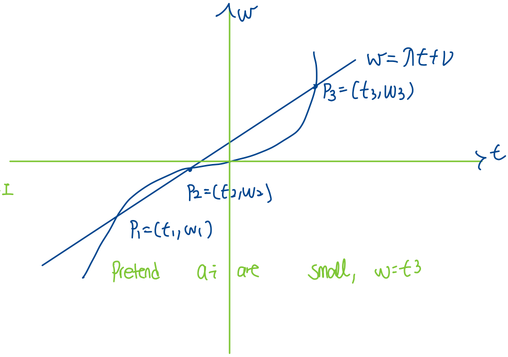
so $w(t)=\sum_{n=2}^{\infty} A_{n-2}t^{n+1}$, $(A_0=1)$

P_1P_2 given by $w=\lambda t+\nu$. Where $\lambda = \begin{cases} \dfrac{w(t_2)-w(t_1)}{t_2-t_1} & t_1\neq t_2 \\ w'(t_1) & t_1=t_2 \end{cases}$

since all $t_i \in I$

So, $\lambda = \sum_{n=2}^{\infty} A_{n-2}\,(t_1^n + t_1^{n-1}t_2 + \cdots + t_2^n) \in I$

$\nu = w_1 - \lambda t_1$ $\in I$ since all $t_i, w_i \in I$



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

$$\lambda t+\nu = t^3 + a_1 t(\lambda t+\nu) + a_2 t^2(\lambda t+\nu) + a_3(\lambda t+\nu)^2 + a_4 t(\lambda+4\nu)^2 + a_6(\lambda+\nu)^3.$$

A = coeff of t^3 = $1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3$

B = coeff of t^2 = $a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu$.

So $\begin{cases} A \in R^\times & \text{(something } +1 \text{ is unit)} \\ B \in I & (\lambda, \nu \text{ in } I) \end{cases}$

So $t_3 = \underbrace{-B/A}_{\Sigma \text{ of roots in x-coord}} - t_1 - t_2 \in I$, $w_3 = \lambda t_3 + \nu \in I$. ∎

Pf scheme:

$(0,0) \in \hat{E}(I)$

and say $P_1, P_2 \in \hat{E}(I)$,

then want: $-P_1 - P_2 \in \hat{E}(I)$.

write: $P_1 = (t_1, w(t_1))$

$P_2 = (t_2, w(t_2))$

substitute $w=\lambda t+\nu$ into f.

look at coefficients $\Rightarrow$ result.

<u>Remarks. The motivation of group law</u>

Taking $R=\mathbb{Z}[a_1,\cdots a_6][[t]]$, $I=(t)$, lemma 8.2 ($\hat{E}(I)$ is a group)

shows there exists $\iota(t) \in \mathbb{Z}[a_1 \cdots a_6][[t]]$, $\iota(0)=0$, $[-1](t, w(t)) = (\iota(t), w(\iota(t)))$.

lemma 8.2 shows $\hat{E}(t)$ is closed under inverses, so the inverse can be expressed as a power series.

Take $R=\mathbb{Z}[a_1,\cdots a_6][[t_1,t_2]]$, $I=(t_1,t_2)$ then $8.2 \Rightarrow \exists F \in \mathbb{Z}[a_1,\cdots a_6][[t]]$, with $F(0,0)=0$,

s.t. $\underline{(t_1, w(t_1)) + (t_2, w(t_2)) = (F(t_1,t_2), w(F(t_1,t_2)))}$.

t_1, t_2 are concrete element of ring.

i.e. $(t_1, w(t_1)), (t_2, w(t_2)) \in \hat{E}((t_1,t_2))$, so that their sum is of form $(pt, w(pt))$

which we denote by $pt = F(t_1,t_2)$.

In fact, $\iota(x) = -x - a_1x^2 - a_2x^3 - (a_1^3+a_3)x^4 + \cdots$ notice the pattern.

$F(x,y) = x+y - a_1xy - a_2(x^2y+xy^2) + \cdots$

Properties of the group law, have

$$\begin{cases} 1. & F(X,Y) = F(Y,X) & \text{gp law is comm} \\ 2. & F(X,0) = X, \quad F(0,Y)=Y & \\ 3. & F(F(X,Y),Z) = F(X,F(Y,Z)) & \text{gp law is assoc.} \\ 4. & F(X,\iota(X)) = 0 & \end{cases}$$

defn. Formal group

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

Excercise ex sh 2 $\Rightarrow$ in any formal group, 4 is established with unique τ, $\tau(t) = -t + \cdots \in R[[t]]$

Example

1. $F(X,Y) = X+Y$, $\hat{G}_a$ "affine line, add 2 pts" ??!
2. $F(X,Y) = XY + X + Y = (X+1)(Y+1) - 1$ $\hat{G}_m$ "affine line, origin deleted, fully shift by 1, identity at 0 rather than 1."
3. $F(X,Y)$ = see above, call it $\hat{E}$

defn. Morphisms and isomorphisms of formal group.

let $\mathcal{F}$ and $\mathcal{G}$ be formal groups over R, given by power series F and G,

1. a morphism $f: \mathcal{F} \to \mathcal{G}$ is a power series $f \in R[[t]]$ with $f(0)=0$,

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

2. $\mathcal{F} \cong \mathcal{G}$ if there exists homs $f: \mathcal{F} \to \mathcal{G}$, $g \to \mathcal{G} \to \mathcal{F}$, s.t

$f(g(X)) = X$, $g(f(X)) = X$.

Thm 8.3. Reducing a mysterious formal group into additive formal group

If Char $R = 0$, then every formal group $\mathcal{F}$ over R is isomorphic to $\hat{G}_a$ over $\boxed{R \otimes \mathbb{Q}}$. More precisely This means coefficient need not be in R, But "in the form of R/integer.

1. There exists unique power series $\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \cdots\cdots$ with $a_i \in R$ s.t.

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

2. There exists a unique power series $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \cdots\cdots$ $b_i \in R$ s.t. $\exp\log(T) = \log\exp(T) = T$. ~~Something shift by 1?~~

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

To show uniqueness, let

$$p(T) = \frac{d}{dT}\log T = 1 + a_2 T + a_3 T^2 + \cdots$$

differentiating (*) w.r.t x gives

$$\log(F(x,y)) = \log(x) + \log(y) \qquad (*)$$

$\Rightarrow \quad p(F(x,y))\,F_1(x,y) = p(x)$

Putting $x=0$ gives $\quad p(y)\,F_1(0,y) = 1 \quad$ so $\quad p(y) = F_1(0,y)^{-1}$ thus is unique.

$\Rightarrow$ log is unique.

scheme: ↳ uniqueness shown by derivatives
↳ existence by differentiating commutativity
↳ 2^{nd} part standard.

note: prove uniqueness first. you get some identities. using these, show existence.

remember: setup $\quad F_1(x,y) = \frac{\partial}{\partial x} F(x,y)$

$p(T) = \frac{d}{dT} \log T$

uniqueness $\quad p(T) \cdot F_1(0,T) = p(0) = 1.$

Lecture 12.

Now, continue last lecture. Show existence of the log.

Write $p(T) := F_1(0,T)^{-1} = 1 + a_2 T + a_3 T^2 + \cdots$ $a_i \in R$. we know what $F_1(0,Y)^{-1}$ is.

let $\log(T) = T + \frac{a_2}{2} T^2 + \cdots$ .. we define $\log(T)$ w.r.t coeff we get at $F_1(0,T)^{-1}$.

have gp law $F(F(X,Y),Z) = F(X, F(Y,Z))$

differentiate w.r.t. X

$F_1(F(X,Y),Z) F_1(X,Y) = F_1(X, F(Y,Z))$

sub $X=0$ & use $F(0,Y)=Y$

$F_1(Y,Z) F_1(0,Y) = F_1(0, F(Y,Z))$

$F_1(Y,Z)\, p(Y)^{-1} = p(F(Y,Z))^{-1}$

$F_1(Y,Z)\, p(F(Y,Z)) = p(Y)$

integrate w.r.t Y

$\log(F(Y,Z)) = \log(Y) + h(Z)$ for some power series h of Z.

$$\frac{d\log(T)}{dT} = p(T)$$

$$\frac{d\log(F(Y,Z))}{dY} = p(F(Y,Z))\, F_1(Y,Z).$$

Symmetry in $Y, Z \Rightarrow h(Z) = \log(Z)$.

Hence part (i) is proven.

2. (exist exp s.t. $\exp(\log(T)) = \log(\exp(T)) = T$).

lemma 8.4 Inverse to power series. Similar to a prob in local fields.

let $f(T) = aT + \cdots \in R[[T]]$ with $\boxed{a \in R^\times.}$ this condition is all you need to get an inverse

then exists a unique $g = a^{-1}T + \cdots \in R[[T]]$ s.t. $f(g(T)) = g(f(T))$.

Proof:

make $g_n(T) \in R[T]$ s.t. $\begin{cases} f(g_n(T)) \equiv T & \text{mod } (T^{n+1}) \\ g_{n+1}(T) \equiv g_n(T) & \text{mod } (T^{n+1}) \end{cases}$

then $g(T) = \lim_{n\to\infty} g_n(T)$ exists and satisfies $f(g(T)) = T$.

Now, work with induction.

to start, $g_1(T) = a^{-1} T$

for $n \geq 2$, suppose $g_{n-1}(T)$ exists. so $f(g_{n-1}(T)) = T \mod T^n$

so $f(g_{n-1}(T)) = T + bT^n \pmod{T^{n+1}}$ for some $b \in R$.

we put $g_n(T) = g_{n-1}(T) + \lambda T^n$ for some $\lambda \in R$ T.B.D.

then, $f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n)$

$= f(g_{n-1}(T)) + \lambda a T^n \pmod{T^{n+1}}$.

$= T + (b + \lambda a) T^n \pmod{T^{n+1}}$

quadratic term vanishes. mod T^{n+1}
write it out you'll see

take $\lambda = -b/a$, allowed as $a \in R^\times$. $\Rightarrow \lambda \in R$.

We obtain $g(T) = a^{-1}T + \dots \in R[[T]]$ s.t $f(g(T)) = T$. Applying same argument to g,

get $h(T) = (a^{-1})^{-1} T + \dots = aT + \dots \in R[[T]]$ s.t. $g(h(T)) = T$. now

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

Similar to how uniqueness of inverse proven in gp theory

shows can write $g^{-1} = f$. $\blacksquare$

then, thm 8.3 ii follows except for showing $b_n \in R$, (not just $R \otimes \mathbb{Q}$).

See example sheet 2.

$\blacksquare$

Notation. $\mathcal{F}$ (e.g. $\hat{\mathbb{G}}_a$, $\hat{\mathbb{G}}_m$, $\hat{E}$) be a formal group given by $F \in R[[X, Y]]$.

Suppose R is complete w.r.t. I. Then for $x, y \in I$, put $x \oplus_F y = F(x, y) \in I$.

Then $\mathcal{F}(I) = (I, \oplus_F)$ is an abelian group.

e.g.
$$\begin{cases} \hat{\mathbb{G}}_a(I) = (I, +) \\ \hat{\mathbb{G}}_m(I) \cong (1+I, \times) \\ \hat{E}(I) \leq E(K) \quad \text{as in lemma 8.2} \end{cases}$$

i.e. power series in $R[[X, Y]]$ is fixed. gp addition is as plugging two arguments into two places of power series and if $x, y \in I$, $x \oplus_{\mathcal{F}} y \in I$.

Cor 8.5 $[n]$'s properties

let $\mathcal{F}$ be a formal group over R and $n \in \mathbb{Z}$.

Suppose $n \in R^\times$ then

1. $[n] : \mathcal{F} \to \mathcal{F}$ is an iso.
2. If R is complete w.r.t. I, then $\mathcal{F}(I) \xrightarrow{x n} \mathcal{F}(I)$ is an iso of groups.

In particular $\mathcal{F}(I)$ has no $[n]$ torsion.

Proof: The notation $[n]$ is defined inductively as

$$\begin{cases} [1]T = T \\ [n]T = F([n-1]T, T) \text{ if } n \geq 2 \\ [-1]T = \iota(T) \quad \text{for } n<0. \end{cases}$$

An easy induction $\Rightarrow$ $[n](T) = nT + \cdots \in R[[T]]$, by lemma 8.4 it's an isomorphism.

Try to show this. also see LF notes. ∎

§ 9. Elliptic curves over local fields.

let K be a field, complete w.r.t. a discrete valuation $v: K^* \twoheadrightarrow \mathbb{Z}$.

↳ The valuation ring, aka ring of integers is

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

↳ with unit group

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

↳ and max ideal $\quad \pi \mathcal{O}_K$, $v(\pi) = 1$.

↳ residue field $\quad k = \mathcal{O}_K / \pi \mathcal{O}_K$

Assume char $K = 0$ char $k = p > 0$, e.g. $\begin{cases} K = \mathbb{Q}_p \\ \mathcal{O}_K = \mathbb{Z}_p \\ k = \mathbb{F}_p \end{cases}$

let E/K be an elliptic curve.

defn. integral/minimal Weierstrass equation.

A Weierstrass eqn for E with coefficients $a_1, \cdots a_6 \in K$ is

$\begin{cases} \text{integral} \quad \text{if} \quad a_1, \cdots a_6 \in \mathcal{O}_K \quad \text{(you can clear denominators)} \\ \text{minimal} \quad \text{if} \quad v(\Delta) \text{ is minimal among all integral weierstrass eqn for } E. \end{cases}$

"don't overclear denominators to get huge valuation).

Remarks

1. Putting $x = u^2 x'$, $y = u^3 y'$, gives $a_i = u^i a_i'$ so integral eqns exist.
2. If $a_1, \cdots a_6 \in \mathcal{O}_K$ then $\Delta \in \mathcal{O}_K$ so $v(\Delta) \geq 0$ so min. Weierstrass eqn exists.

If not, then either Δ won't stay the same or integrality

3. If char $k \neq 2,3$, then exist a min. Wierstrass eqn of form $y^2 = x^3 + ax + b$.

Lemma 9.1. Related to ex sheet Q.

Let E/K have an integral Wierstrass eqn,

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

Let $0 \neq P \in E(K)$. Say $P = (x, y)$.
POI

then either $x, y \in \mathcal{O}_K$
or $v(x) = -2s$, $v(y) = -3s$, for some $s \geq 1$.

Proof:

since $a_1xy + a_3y \in \mathcal{O}_K$, $y^2 + a_1xy + a_3y \notin \mathcal{O}_K$.

Case $v(x) \geq 0$: If $v(y) < 0$, $v(LHS) < 0$, $v(RHS) \geq 0$, ※ so $x, y \in \mathcal{O}_K$.

Case $v(x) < 0$:

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

in each 3 cases, $v(y) < v(x)$ so $2v(y) = 3v(x)$.

■

Lecture 13.

K complete $\Rightarrow \mathcal{O}$ complete w.r.t. the ideal $\pi^r \mathcal{O}_K$ any $r \geq 1$.

Fix a minimal Wierstrass equation for E/K, get a formal group $\hat{E}$ over K and

$(t, w(t))$??? where this came from?

$$\hat{E}(\pi^r \mathcal{O}_K) = \{(x,y) \in E(K) : -\frac{x}{y}, -\frac{1}{y} \in \pi^r \mathcal{O}_K\} \cup \{0\}.$$

lemma 9.1

$$= \{(x,y) \in E(K) : v(\tfrac{x}{y}) \geq r, v(\tfrac{1}{y}) \geq r\} \cup \{0\}$$

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

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

this is a π neighbourhood of 0.

Thm 8.2 $\Rightarrow$ this is a subgroup of $E(K)$, say $E_r(K)$, then we get a nested sequence (filtration of groups)

$$E_1(K) \supset E_2(K) \supset E_3(K) \supset \cdots \cdots$$

Recall $E_n(K) = \mathcal{F}(\pi^n \mathcal{O}_K)$

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

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

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

and for all $r \geq 1$, $\dfrac{\mathcal{F}(\pi^r \mathcal{O}_K)}{\mathcal{F}(\pi^{r+1} \mathcal{O}_K)} \cong (k, +)$

Reminder: Working with char $K = 0$, char $k = p$.

Prop. log induces iso between $\mathcal{F}$ and $\hat{G}_a$

Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$.

let $e = v(p)$. If $r > \dfrac{e}{p-1}$ then

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

is an iso with inverse exp.

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

Proof: For $x \in \pi^r O_K$ we must show power series exp and log in thm 8.3 converge.

Recall $\exp(T) = T + \frac{b_2}{2!}T^2 + \cdots$ $b_n \in O_K$.

Note: Big denominator is "good" in Archimedean but "bad" in non-archimedean.

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

Proof of claim:

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

$n = p^5$ $\quad p^5+p^4+p^3 \leq p^5+p^1$

hence, $(p-1)v_p(n!) < n$. But $(p-1)v_p(n!) \in \mathbb{Z}$ so $(p-1)v_p(n!) \leq n$.

why $v(n!) \leq v(p)\left(\frac{n-1}{p-1}\right)$? as $\boxed{v_p(x) = \frac{v(x)}{v(p)}}$ unclear! ∎

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

this is always $\geq r$.

It goes to infinity as $n \to \infty$, so exp x converges and belongs to $\pi^r O_K$. (In non-arch, only need $|x_{n+1} - x_n|$ converge to be a cauchy seq)

log x similar but easier. Recall how $\log(F(X,Y)) = F(X) + F(Y)$. this completes the proof of iso. ∎

Prop 9.3. quotient of formal gp of ideals.

for $r \geq 1$, $\frac{\mathcal{F}(\pi^r O_K)}{\mathcal{F}(\pi^{r+1} O_K)} \cong (k, +)$.

no higher powers of standalone x or standalone y.

Proof: Recall $F(X,Y) = X + Y + XY(\cdots\cdots)$

so if $x, y \in O_K$, $F(\pi^r x, \pi^r y) \equiv \pi^r(x+y) \pmod{\pi^{r+1}}$.

Thus, $\mathcal{F}(\pi^r O_K) \to (k, +)$

$\pi^r x \mapsto x \pmod{\pi}$

shows that $\pi^r x \mapsto x$ is a surj hom by $\begin{cases} \pi^r x + \pi^r y \mapsto x+y \\ \& \ \pi^r(x+y) \mapsto x+y. \end{cases}$

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

Corollary If $|k| < \infty$, $\mathcal{F}(\pi O_K)$ contains a subgroup of finite index and is isomorphic to $(O_K, +)$.

Notation ~ $\qquad \mathcal{O}_K \mapsto \frac{\mathcal{O}_K}{\pi \mathcal{O}_K} \overset{def}{=} k.$

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

Prop 9.4

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

Proof: look at back of formula sheet.
Say weierstrass eqns are related by $[u; r, s, t]$, $u \in K^\times$, $r, s, t \in K$.
then $\Delta_1 = u^{12} \Delta_2$
minimality of equations imply that $u \in \mathcal{O}_K^\times$. ? why this true ?
Transformation formulas for a_i, b_i, conclude $r, s, t \in \mathcal{O}_K$.
The wierstrass equation for reductions mod π are related by $[\tilde{u}; \tilde{r}, \tilde{s}, \tilde{t}]$.
Note that all these are to ensure things work in char 2 or 3. ∎

why is good reduction well defined? i.e. over min W-eqns?

Defn reduction, good reduction, bad reduction:

curve defined over k

The reduction $\tilde{E}/k$ of E/K is defined to be a reduction of a minimal Weierstrass equation.

E has a good reduction if $\tilde{E}$ is nonsingular (and so is an EC)

E has bad reduction o.w.

Note: it's important to take the minimal W-equation.

For an integral weierstrass equation,

$v(\Delta) = 0$ is a sufficient condition for good reduction. ???

$0 < v(\Delta) < 12$, by $\Delta_1 = u^{12} \Delta_2$, we have a bad reduction. ???

$v(\Delta) \geq 12$, the equation might not be minimal.

u cannot have a strictly between 0 & 1 valuation ?

There is a well defined map

$$\mathbb{P}^2(K) \longrightarrow \mathbb{P}^2(k)$$
$$(x:y:z) \longmapsto (\tilde{x}:\tilde{y}:\tilde{z})$$

this is in the projective coords $\Rightarrow$ we can clear denominators

where we choose representatives $\min(v(x), v(y), v(z)) = 0$ to ensure we don't get $(0:0:0)$.

(otherwise, reduce mod π gives $(0:0:0)$.

we restrict to get $E(K) \to E(k)$
$$P \mapsto \tilde{P}.$$

if $P=(x,y) \in E(K)$, then either $\begin{cases} x, y \in \mathcal{O}_K \text{ so } \tilde{P} = (\tilde{x}, \tilde{y}) \\ v(x) = -2s,\ v(y) = -3s, \text{ we choose } P = (\pi^{3s}x : \pi^{3s}y : \pi^{3s}) \end{cases}$
or

which reduces to $\tilde{P} = (0:1:0)$.

thus $E_1(K) = \hat{E}(\pi\mathcal{O}_K) = \{P \in E(K) : \tilde{P} = 0\}$ is the kernel of reduction.

Lecture 14

Idea: $\tilde{E}_{ns}$ is original $\hat{E}(\mathcal{O}_K)$ if good.
If bad, delete point & make $\hat{G_a}$ and $\hat{G_m}$.

Recall the following:

def: Kernel of reduction.

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

as in the point of infinity

defn $\tilde{E}_{ns}$

Set of nonsingular points on $\tilde{E}$.

$\begin{cases} \text{if } E \text{ has a good reduction, then } \tilde{E}_{ns} = \tilde{E} \\ \text{o.w. no good reduction, then } \tilde{E}_{ns} = \tilde{E} \setminus \{\text{singular pt}\} \end{cases}$

the chord & tangent law still define a group law on $\tilde{E}_{ns}$ (since 3^{rd} pt has multiplicity 1.)

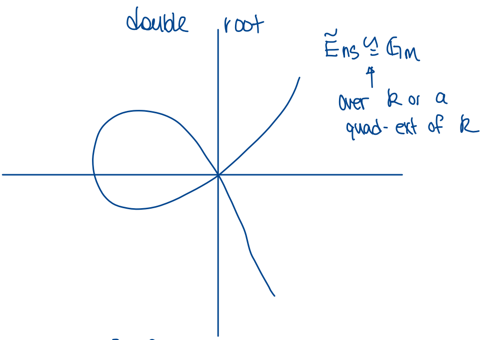
In case of bad reduction, $\tilde{E}_{ns} \cong \hat{G_a}$ or $\hat{G_m}$ (over $\bar{k}$)

$\hat{G_a}$: additive reduction; $\hat{G_m}$: multiplicative reduction

Assume char $k \neq 2$, we have $\tilde{E}: y^2 = f(x)$.

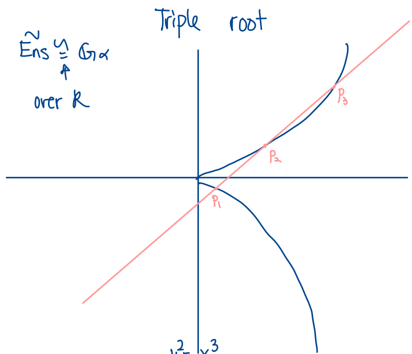
then $\tilde{E}$ is singular $\Leftrightarrow$ f has a repeated root.

Two situations:



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

Curve with node
multiplicative reduction



$y^2 = x^3$

Curve with cusp
additive reduction.

For triple root, $y^2=x^3$, get curve with cusp and additive reduction.

$$\begin{aligned} \tilde{E}_{ns} &\xrightarrow[\phi]{\sim} G_a \\ (x,y) &\mapsto \frac{x}{y} \\ (t^{-2}, t^{-3}) &\leftarrow t \\ \infty &\leftarrow 0 \end{aligned}$$

We check the above is a group homomorphism.

let $P_1, P_2, P_3 \in ax+by=1$.

Write $P_i = (x_i, y_i)$. $t_i := \frac{x_i}{y_i}$.

then $x_i^3 = y_i^2 = y_i^2 \cdot 1 = y_i^2(ax_i+by_i)$. so, t_1, t_2, t_3 are roots of $x^3-ax-b=0$.

divide by $y^3 \Rightarrow$ $x^3 = ax+b$. looking at the coefficient of $x^2 \Rightarrow t_1+t_2+t_3=0$.

to check gp hom, shows P_1,P_2,P_3 Σ to $0 \Rightarrow \phi(P_1)\ \phi(P_2), \phi(P_3)$ Σ to 0 in $\hat{G}_a$? ???

the node case is on ex. sheet.

Confirm this!

Show homomorphism WTS $\Sigma \to 0 \Rightarrow \Sigma \to 0$???

<u>Defn. $E_0(K)$</u>

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

i.e. points whose reduction is nonsingular.

<u>Prop 9.5.</u> $E_0(K)$ (aka. ignore points whose reduction is singular) is a subgroup of $E(K)$ and reduction mod π is a surjective group homomorphism

$$E_0(K) \twoheadrightarrow \tilde{E}_{ns}(k)$$

<u>Proof</u>

<u>Check group hom:</u> Why check gp hom $\Rightarrow$ collinear Σ to 0?

A line l in $\mathbb{P}^2$ defined over K has equation $aX+bY+cZ=0$, $a,b,c \in K$.

We may assume $\min(v(a), v(b), v(c))=0$

Reduction mod $\pi \Rightarrow$ $\tilde{l} : \tilde{a}X+\tilde{b}Y+\tilde{c}Z=0$.

Now, if $P_1, P_2, P_3 \in E(K)$ with $P_1+P_2+P_3=0$, then they lie on a line l.

then $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ lie on $\tilde{l}$.

If $\tilde{P}_1, \tilde{P}_2 \in \tilde{E}_{ns}(K)$ then $\tilde{P}_3 \in \tilde{E}_{ns}(K)$ (since it's a subgroup)

$\Rightarrow \tilde{P}_3 \in \tilde{E}_{ns}(k)$

So, if $P_1, P_2 \in E_0(K)$ then $P_3 \in E_0(K)$ and $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = 0$

It is an exercise to check it still work if $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3$ not distinct.

this shows E_0 is a subgroup.

Now show surjectivity:

let $f(x,y) = y^2 + a_1xy + a_3y - (x^3 + \cdots)$ be the Weierstrass eqn.

let $\tilde{P} \in \tilde{E}_{ns}(k) \setminus \{0\}$. Say $\tilde{P} = (\tilde{x}_0, \tilde{y}_0)$, $\hat{x}_0, \hat{y}_0 \in O_K$.

$\tilde{P}$ nonsingular $\Rightarrow$ either $\begin{cases} \frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \mod \pi \\ \text{or } \frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \mod \pi. \end{cases}$

In first case, put $g(t) = f(t, y_0) \in O_K[t]$. then,

$$\begin{cases} g(x_0) \equiv 0 \mod \pi & \text{since } f(x_0, y_0) \equiv 0 \bmod \pi, \ 0 \bmod \pi) \\ g'(x_0) \in O_K^* \end{cases}$$

Hensel's lemma $\Rightarrow \exists b \in O_K$, s.t. $g(b) = 0$, $b \equiv x_0 \mod \pi$.

So $P = (x, y_0) \in E(K)$ has reduction $\tilde{P}$.

Second case similar.

Scheme: Given reduced pt in $\tilde{E}_{ns}$, find a repn. use nonsingularity to hack out the Hensel (equality in π & derivative a unit) to get point on $E(K)$.

<u>Remark. Nested sequence of groups</u>

Recall for $r \geq 1$, we put

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

and we get a nested seq of groups

$$\text{for } r > \frac{e}{p-1}, \quad (O_K, +) \cong E_r(K) \subseteq \cdots \subseteq \underset{\hat{E}(\pi^2 O_K)}{\underset{\cong}{E_2(K)}} \subseteq \underset{\hat{E}(\pi O_K)}{\underset{\cong}{E_1(K)}} \subseteq E_0(K) \subseteq E(K)$$

Prop 9.5

$\frac{E_0(K)}{E_1(K)} \cong \tilde{E}_{ns}(k)$

$$\begin{cases} \text{all quotient } \frac{E_{t+1}}{E_t} \cong (k, +) \\ \frac{E_0(K)}{E_1(K)} \cong \tilde{E}_{ns}(k) \end{cases}$$

now, what about $E_0(K) \subseteq E(K)$? Only cover special case.

lemma 9.7 & 9.8 & Remark & fact skipped in QK's notes.

Thm 9.6 relationship between $E(K)$, $E_r(K)$

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

Thm $E(K)_{\text{tors}} \hookrightarrow \dfrac{E(K)}{E_r(K)}$ hence is finite.

Some Recall from ANT

let $[K:\mathbb{Q}_p]<\infty$, L/K finite.

valuation of L restricted to K is $e\times$ valuation of K.

Then $[L:K]=ef$ with $v_L|_{K^*}=ev_K$ and $f=[k':k]$, k' res field L, k res field of K.

If L/K is Galois, then get a natural group hom $\mathrm{Gal}(L/K)\to\mathrm{Gal}(k'/k)$.

this map is surjective with kernel order e.

$$\begin{array}{ccc} K^* & \xrightarrow{v_K} & \mathbb{Z} \\ \cap & & \downarrow{\scriptstyle \times e} \\ L^* & \xrightarrow{v_L} & \mathbb{Z} \end{array}$$

def. unramified extension

L/K is unram if $e=1$.

Fact for each integer $m\geq1$,

1. k has a unique extension of deg m, say k_m.
2. K has a unique unram extension, say K_m.

unique either
1. up to iso
2. choice of alg closure
But they're same.

def. Max unram extension.

$$K^{nr}=\bigcup_{m\geq1}K_m \quad (\text{inside } \bar{K})$$

thm 9.7 "dividing a point by n"

Suppose $[K:\mathbb{Q}_p]<\infty$. E/K an E.C. with good reduction. $p\nmid n$.

If $P\in E(K)$, then $K([n]^{-1}P)/K$ is unramified.

Notation Recall we do not specify a base field, so we refer to the fibres over the algebraic closure:

$$[n]^{-1}P=\{Q\in E(\bar{K}) \mid [n]Q=P\}$$

Also, $\quad K(\{Q_1,\cdots,Q_r\})=K(x_1,x_2,\cdots x_r,y_1,\cdots y_r)$, where $Q_i=(x_i,y_i)$.

Proof of 9.7.

for each $m \geq 1$, there's a SES:

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

Prop 9.5: $E_0(K) = \{ P \in E(K) : \tilde{P} \in \widetilde{E}_{ns}(k) \}$

$E_0(K) \twoheadrightarrow \widetilde{E}_{ns}(k)$ with kernel $E_1(K_m)$.

i.e. $E_1(K_m)$ injects into $E(K_m)$

$E(K_m)$ surjects into $\widetilde{E}(k_m)$,

and ker $=$ Im. so it's SES.

now take union over all $m \geq 1$ gives comm diagram with exact rows.

why allowed to take unions ?

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

observe left map & right map first.

left vertical map is an iso by thm 8.5. (applies since $p \nmid n \Rightarrow n \in \mathcal{O}_K^*$)

right vertical map serjective by thm 2.8, has Ker $\cong (\mathbb{Z}/n\mathbb{Z})^2$ by thm 6.5.

??? don't get.

By Snake lemma,

$$\begin{array}{ccccccccc}
 & & 0 & & \text{so } \cong & & & & \\
0 & \longrightarrow & \ker & \longrightarrow & \ker & \longrightarrow & \ker & & \\
0 & \longrightarrow & E_1(K^{nr}) & \longrightarrow & E(K^{nr}) & \longrightarrow & \widetilde{E}(\bar{k}) & \longrightarrow & 0 \\
 & & \downarrow n & & \downarrow n & & \downarrow n & & \\
0 & \longrightarrow & E_1(K^{nr}) & \longrightarrow & E(K^{nr}) & \longrightarrow & \widetilde{E}(\bar{k}) & \longrightarrow & 0 \\
 & & \text{coker} & \longrightarrow & \text{coker} & \longrightarrow & \text{coker} & \longrightarrow & 0 \\
 & & 0 & & \text{so } 0 & & 0 & &
\end{array}$$

$\left\{ \begin{array}{l} E(K^{nr})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2 \\ \dfrac{E(K^{nr})}{nE(K^{nr})} = 0 \end{array} \right.$ Cokernel of $x[n]$ is trivial.

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

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

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

subfield.

Lecture 15

Recall we want to prove if $|k| < \infty$, then $\mathbb{P}^n(K)$ is compact (w.r.t. π-adic topology)

points that reduce to nonsingular pt in res field. & is a subgroup.

Lemma 9.8. If $|k| < \infty$, then $E_0(K) \subset E(K)$ has finite index. Scheme next page.

Pf if $|k| < \infty$, then $\frac{\mathcal{O}_K}{\pi^r \mathcal{O}_K}$ is finite for $r \geq 1$. So $\mathcal{O}_K \cong \varprojlim \mathcal{O}_K / \pi^r \mathcal{O}_K$ is a profinite group hence is compact. (Every profinite group is compact & totally disconnected)

$\mathbb{P}^n(K)$ is the union of compact sets

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

and hence compact. (to write any point in $\mathbb{P}^n(K)$ in this form, take term with least valuation & scale it to 1).

" union of n cartesian prod of n-1 compact sets is compact).

$E(K) \subseteq \mathbb{P}^2(K)$ is a closed subset so $(E(K), +)$ is a compact topological group.

(As gp law is cts. and points satisfying Weierstrass eqn is closed)

If $\tilde{E}$ has a singular point $(\tilde{x}_0, \tilde{y}_0)$ then

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

Point in $E(K) \setminus E_0(K)$ are exactly the ones reduce to $(\tilde{x}_0, \tilde{y}_0)$ mod π, so $v(x - x_0)$, $v(y - y_0)$ is at least 1.

this set is a closed subset of $E(K)$. So $E_0(K)$ is an open subgroup of $E(K)$. The cosets of $E_0(K)$ form an open cover of $E(K)$. But since $E(K)$ is compact, & the cosets are disjoint. $E_0(K)$ has finite index in $E(K)$.

So $[E_0(K) \cdot E(K)] < \infty$.

This index is called the Tamagawa number, denoted $c_K(E)$. ▨

Remark Good reduction implies $c_K(E) = 1$. The converse is false. (Ex sheet)

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

either $c_K(E) = v(\Delta)$

or $c_K(E) \leq 4$

Proof scheme of $[E(K) : E_0(K)]$ is finite index :

↳ $E(K)$ is compact since $E(K) \subseteq \mathbb{P}^2(K)$, $\mathbb{P}^2(K)$ compact as union of compact sets $(a_1 : \cdots : a_{i-1} : 1 : a_{i+1} : \cdots a_n)$

↳ $E(K) \setminus E_0(K)$ = points that do not reduce to sin point:
$\{(x,y) \mid v(x-x_0) \geq 1, \ v(y-y_0) \geq 1\}$. closed set.

↳ $E_0(K)$ open subgroup.

↳ cosets form open cover of $E(K)$. But since cosets disjoint, $E(K)$ cpt, finite # cosets $\Rightarrow$ index finite.

§10. Elliptic curves over number fields

I. Torsion subgroup.

Notation

Suppose $[K:\mathbb{Q}]<\infty$. E/K an elliptic curve.

let $\mathfrak{p}$ be a prime of K, $K_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of K,

$k_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$.

K a num field $\Rightarrow$ $K_\mathfrak{p}$ a local field?

defn. Prime of good reduction

yes $K_\mathfrak{p}$ falls into "finite ext of $\mathbb{Q}_p$" in characterisation of LFs.

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

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

Proof Take a Weierstrass eqn for E. with coefficients $a_1, \cdots a_6 \in \mathcal{O}_K$.

E non-singular $\Rightarrow$ $0 \neq \Delta \in \mathcal{O}_K$. Write $(\Delta) = \mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}\cdots\mathfrak{p}_r^{\alpha_r}$ for factorisation into prime ideals.

let $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$ if $\mathfrak{p} \notin S$ then $v_\mathfrak{p}(\Delta) = 0$. So $E/K_\mathfrak{p}$ has good reduction.

Note we have $\{\text{bad primes}\} \subset S$. But it's possible to also have good prime in S.

Recall that $v(\Delta)=0$ is sufficient condition for a good reduction!

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

How? all ideals principal. $\Rightarrow$ $v(\Delta) \exists$ s.t. $v(\Delta)=0$?

Basic group theory:

If A is a f.g. abelian gp, $A \cong \underbrace{(\text{finite gp})}_{\text{torsion subgroup}} \times \mathbb{Z}^r$ $r = \operatorname{rank}(A)$.

???

lemma 10.2 $E(K)_{tor}$ is finite (Same result if replace K by $K_\mathfrak{p}$)

Proof take any $\mathfrak{p}$. $K \subset K_\mathfrak{p}$. ~~thm 9.8 $\Rightarrow$ $|k|<\infty$ $\Rightarrow$ $E_0(K) \subseteq E(K)$ has finite index.~~

we know $E(K_\mathfrak{p})$ has a subgroup A of finite index with $A \cong (\mathcal{O}_{K_\mathfrak{p}}, +)$.

In particular, A is torsion free.

Don't quite get this arg.

consider $E(K)_{tor} \subset E(K_\mathfrak{p})_{tor} \longrightarrow \dfrac{E(K_\mathfrak{p})}{A}$, A torsion free, to be in kernel, must be in kernel of $E(K_\mathfrak{p})$ which is 0. $\Rightarrow$ this map is injective here torsion free.

Lemma 10.3. injection $E(K)[n] \hookrightarrow \tilde{E}(k_p)[n]$?

let p be a prime of good reduction, $p \nmid n$.

then reduction mod p gives an injective group hom

$$E(K)[n] \hookrightarrow \tilde{E}(k_p)$$

studied formal gp of

Proof Prop 9.5 $\Rightarrow$ $E(K_p) \to \tilde{E}(k_p)$ is a group hom with kernel $E_1(K_p)$.

then, cor 8.5 $\Rightarrow$ $E_1(K_p)$ has no n-torsion. (as a formal gp)

Recall 8.5

Cor 8.5 [n] 's properties

let $\mathcal{F}$ be a formal group over R and $n \in \mathbb{Z}$.

Suppose $n \in R^\times$ then

1. $[n] \cdot \mathcal{F} \to \mathcal{F}$ is an iso.
2. If R is complete w.r.t. I, then $\mathcal{F}(I) \xrightarrow{xn} \mathcal{F}(I)$ is an iso of groups.

In particular $\mathcal{F}(I)$ has no [n] torsion.

$$\boxed{E(K)[n] \hookrightarrow E(K_p)[n] \to \tilde{E}(k_p) \quad \text{kernel} = E_1(K_p)}$$

Key

So the only way for it to fail to be inj is to get mapped to $E_1(K_p)$. But $E_1(K_p)$ has no n-torsion points, so cannot get mapped to $E_1(K_p)$, so trivial kernel.

Example 1 $E/\mathbb{Q}$: $y^2+y = x^3-x^2$. verify? $\Delta = -11$. E has good reductions at all primes $\neq 11$.

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

B/C $E(K)[n] \hookrightarrow \tilde{E}(k_p)$

so $E(K)[n]$ is factor of $\tilde{E}(k_p)$?

Look at 2, $\#(E(\mathbb{Q})_{tor}) \mid 5 \cdot 2^a$, some $a \geq 0$ — kill the 2 torsion first

at 3, $\#(E(\mathbb{Q})_{tor}) \mid 5 \cdot 3^b$, some $b \geq 0$ — b/c 2 torsion don't work with injectivity

so $\#(E(\mathbb{Q})_{tor}) \mid 5$. let $T = (0,0) \in E(\mathbb{Q})$, we can check $5T = 0$. so $E(\mathbb{Q})_{tor} \cong \mathbb{Z}/5\mathbb{Z}$.

Example 2 let $E/\mathbb{Q} \cdot y^2 + y = x^3+x$. verify? $\Delta = -43$.

E has good reduction at all $p \neq 43$. consider primes 2, 11,

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

Lemma 10.3, $E(\mathbb{Q})_{tor} \mid 5 \cdot 2^a$
$E(\mathbb{Q})_{tor} \mid 9 \cdot 11^a$
$\Rightarrow$ $E(\mathbb{Q})_{tor} = \{0\}$. So $P = (0,0) \in E(\mathbb{Q})$ has infinite order.

so rank $E(\mathbb{Q}) \geq 1$.

Does this not contradict lemma 10.2 ?

?

Example 3. let $E_D : y^2 = x^3 - D^2 x$. $D \in \mathbb{Z}$ square free, and a congruent number.

$\Delta = 2^6 D^6$. We know the torsion group contains $\{0, (0,0), (\pm D, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$

let $f(x) = x^3 - D^2 x$.

We count # of points using Legendre symbol.

if $\underbrace{p \nmid 2D}_{\text{ensure good division.}}$, then

$$\# \tilde{E}_D(\mathbb{F}_p) = \underset{\text{pt of infty}}{1} + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{f(x)}{p} \right) + 1 \right)$$

if $f(x)$ is quad res, 2 pts. We know $\neq 0$
if $f(x)$ is non-res, $-1+1=0$ pts.

$p \nmid 2D$ ensures $\left(\frac{f(x)}{p}\right) = \pm 1$.

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

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

-1 is QNS mod p.

so all $\left(\frac{f(x)}{p}\right) + \left(\frac{f(-x)}{p}\right)$ cancel out, add $\mathbb{F}_p$ # of 1's.

so $\# \tilde{E}_D(\mathbb{F}_p) = p+1$.

Proof idea:
$E_D = y^2 = x^3 - D^2 x$
$E_D(\mathbb{F}_p) = p+1 \quad \forall p \equiv 3 \bmod 4$

$4 \mid m \mid p+1 \Rightarrow \# E_D(\mathbb{Q})_{tor} = 4$
$\operatorname{rank}(E_D) \geq 1 \Leftrightarrow$ exists some points not in torsion i.e. $y \neq 0$.
so the cong # argument.

Lecture 16

Continue with $E_D: y^2 = x^3 - D^2 x$.

why $m \mid p+1$? b/c $\# \tilde{E}_D(\mathbb{F}_p) = p+1$?

let $m = \# E_D(\mathbb{Q})_{tor}$.

We have $4 \mid m \mid p+1$ for all sufficiently large primes p with $p \equiv 3 \bmod 4$.

then, $m=4$. o.w. it contradicts the prime number theorem

i.e. if $m=8$, then $m \mid p+1$, $p \equiv 7 \bmod 8$, then $\Rightarrow$ ~~only finitely many primes $7 \bmod 8$ exist.~~

I don't see why only finitely many those?

Thus, $E_D(\mathbb{Q})_{tor} \cong (\mathbb{Z}/2\mathbb{Z})^2$. Recall $E_D(\mathbb{Q}) \cong$ tor $\times$ free part.

$\Rightarrow \operatorname{rank} E_D(\mathbb{Q}) \geq 1 \Leftrightarrow \exists\, x, y \in \mathbb{Q},\ y \neq 0,\ y^2 = x^3 - D^2 x$

$\Leftrightarrow D$ is a congruent number.

Says, $\operatorname{rank} E_D(\mathbb{Q}) \geq 1 \Leftrightarrow$ exist free part

$\Leftrightarrow$ exist no-torsion part

$\Leftrightarrow \exists$ point (x,y), $(x,y) \notin \{0_E, (0,0), (\pm 1, 0)\}$.

Lemma 10.4. $E(\mathbb{Q})_{tor}$ points have "almost integer" coordinates.

let $E/\mathbb{Q}$ be given by a W-equation with $a_1, \cdots, a_6 \in \mathbb{Z}$.

Suppose $0 \neq T = (x,y) \in E(\mathbb{Q})_{tors}$. Then

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

Proof

1. the W-equation defines a formal group $\hat{E}$ over $\mathbb{Z}$. (after lemma 9.1)

for $r \geq 1$, recall

Concept check, why $v_p(x)$, $v_p(x)$ is small yet in $\hat{E}(p^r\mathbb{Z}_p)$?

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

dir of inequality makes no sense

Prop 9.2 $\Rightarrow \hat{E}(p^r\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ if $r > \frac{1}{p-1}$.

If p is odd prime, $r=1$ works. if $p=2$, $r \geq 2$.

Thus $\left\{ \begin{array}{ll} \hat{E}(4\mathbb{Z}_2) & \\ \hat{E}(p\mathbb{Z}_p) & p \text{ odd prime} \end{array} \right\}$ are torsion free.

So, if $0 \neq T = (x,y) \in E(\mathbb{Q})_{tors}$ then $T \notin \hat{E}(4\mathbb{Z}_2)$ so $v_2(x) \geq -2$, $v_2(y) \geq -3$

so $T \in \hat{E}(2\mathbb{Z}_2)$

$T \notin \hat{E}(p\mathbb{Z}_p)$ so $v_p(x) \geq 0$, $v_p(y) \geq 0$.

so $T \in \hat{E}(\mathbb{Z}_p)$

2. Recall if $T \in \tilde{E}(\mathbb{Z}_p)$ we already saw $(x,y) \in \mathbb{Z}$.

Recall $0 \neq T \in E(\mathbb{Q})_{tors}$

2. Suppose that $T \in \tilde{E}(2\mathbb{Z}_2)$. i.e. $V_2(x) = -2$, $V_2(y) = -3$.

Since $\frac{\tilde{E}(2\mathbb{Z}_2)}{\tilde{E}(4\mathbb{Z}_2)} \cong (\mathbb{F}_2, +)$, have $\tilde{E}(4\mathbb{Z}_2)$ is torsion free, $2T \in \tilde{E}(4\mathbb{Z}_2)$ (since $T+T \cong \mathbb{F}_2$ addition).

But $\tilde{E}(4\mathbb{Z}_2)$ is torsion free, and $2T$ is torsion, hence $2T = 0$.

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

so $2y + a_1x + a_3 = 0$

$\Rightarrow$ $8y + 4a_1x + 4a_3 = 0$

note: $8y$, $4x$ are odd integers since $V_2(x) = -2$ $V_2(y) = -3$

$4a_3$ is even. so a_1 is odd.

Thus, if $2T \neq 0$ $\Rightarrow$ $(T \in \hat{E}(\mathbb{Z}_p))$ $\Rightarrow$ $x, y \in \mathbb{Z}$.

or if a_1 is even $\overset{\neg \Rightarrow \neg}{\Rightarrow}$ $2T \neq 0$ $\Rightarrow$ $T \notin \tilde{E}(2\mathbb{Z}_2)$. $\Rightarrow$ $x, y \in \mathbb{Z}$.

$\blacksquare$

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

$\downarrow$ Finitely many points for (x,y) in $E(\mathbb{Q})_{tors}$

<u>Thm 10.5 (Lutz Nagell) (Nice result that help you find torsion on E)</u>

let $E/\mathbb{Q}: y^2 = \underbrace{x^3 + ax + b}_{f(x)}$, $a, b \in \mathbb{Z}$. Suppose $0 \neq T \in E(\mathbb{Q})_{tor}$, then $x, y \in \mathbb{Z}$

and either $y = 0$ or $y^2 \mid 4a^3 + 27b^2$.

<u>Proof</u>

note in lemma 10.4, a_1 is even, so $x, y \in \mathbb{Z}$.

If $2T = 0$ then $y = 0$.

O.w. $0 \neq 2T = (x_2, y_2)$ is torsion, so $x_2, y_2 \in \mathbb{Z}$.

then formula sheet $\Rightarrow$ $x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x$

Every thing is integer $\Rightarrow$ $y \mid f'(x)$.

E non-singular $\Rightarrow$ $f(x)$, $f'(x)$ are coprime

$\Rightarrow$ $f(x)$, $f'(x)^2$ are coprime

$\Rightarrow$ $\exists g, h \in \mathbb{Q}[x]$ s.t. $g(x)f(x) + h(x)f'(x)^2 = 1$

A calculation & clearing denominator yields <u>NOT clear</u>

$$(3x^3 + 4a)f'(x)^2 - 27(x^3 + ax - b)f(x) = 4a^3 + 27b^2$$

Plug in x for X, y for Y, since $y \mid f'(x)$, $y^2 = f(x)$, $\Rightarrow y^2 \mid 4a^3 + 27b^2$. $\blacksquare$

<u>Remark (Mazur)</u>: Pf beyond this course

If $E/\mathbb{Q}$ is an elliptic curve then $E(\mathbb{Q})_{tors}$ is isomorphic to one of below.

$$\begin{cases} \mathbb{Z}/n\mathbb{Z}, & \text{for } 1 \le n \le 12 \quad n \ne 11 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & \text{for } 1 \le n \le 4 \end{cases}$$

Moreover, all 15 possibilities occur. (Silverman show all 15 of them).

§ 11. Kummer Theory

let K be a field, with char $K \nmid n$, assume $\mu_n \subseteq K$.

<u>lemma 11.1 an iso between Gal and Hom.</u>

let $\Delta \subseteq K^*/(K^*)^n$, be a finite subgroup. (think as in cosets)

let $L = K(\sqrt[n]{\Delta})$ then, L/K is Galois and $\Delta^{\frac{1}{n}} = \{\sqrt[n]{a} : a \in K^\times,\ a\cdot(K^*)^n \in \Delta\}$.

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

Q: How to think of this field ex? not just n^{th} root of 1, but n^{th} root of a bigger subgp mod $(K^*)^n$?

<u>Proof</u> to show Galois, WTS normal & separable. $\begin{cases} \text{Normal: } \mu_n \in K. \\ \text{Separable: } x^n + a \text{ don't have repeated roots, true as } p \nmid n. \end{cases}$

define Kummer pairing:

$$\langle \cdot, \cdot \rangle : \mathrm{Gal}(L/K) \times \Delta \to \mu_n$$

$$(\sigma, x) \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}} \quad \leftarrow x \in K^*, \text{ pick repn of } x. \text{ though } x \in K^*/(K^*)^n.$$

this is well defined. i.e. regardless of repn in $\Delta \subseteq K^*/(K^*)^n$.

i.e. if $\alpha, \beta \in L^*$, $\alpha^n = \beta^n = x$, $\Rightarrow \left(\frac{\alpha}{\beta}\right)^n = 1$, since K contains n roots of unity

$\Rightarrow \frac{\alpha}{\beta} = \mu_n \subseteq K$

$\Rightarrow \sigma\left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta}$ since $\sigma \in \mathrm{Gal}(L/K)$

this BC this $\Rightarrow \frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\beta)}{\beta}$.

well defined.

$$\langle \sigma\tau, x \rangle = \frac{\sigma(\tau\sqrt[n]{x})}{\tau\sqrt[n]{x}} \cdot \frac{\tau\sqrt[n]{x}}{\sqrt[n]{x}} = \langle \sigma, x \rangle \langle \tau, x \rangle$$

$$\langle \sigma, xy \rangle = \frac{\sigma\sqrt[n]{xy}}{\sqrt[n]{xy}} = \frac{\sigma\sqrt[n]{x}}{\sqrt[n]{x}} \cdot \frac{\sigma\sqrt[n]{y}}{\sqrt[n]{y}} = \langle \sigma, x \rangle \langle \sigma, y \rangle$$

Bilinear

This pairing is non-degen in both arguments:

In 1st argument: let $\sigma \in Gal(L/K)$. if $\langle \sigma, x \rangle = 1 \ \forall x \in \Delta$, then $\sigma \sqrt[n]{x} = \sqrt[n]{x} \ \forall x \in \Delta$.

so σ fixes L pointwise $\Rightarrow \sigma = 1$. (since $L = K(\sqrt[n]{\Delta})$)

In 2nd argument: let $x \in \Delta$. If $\langle \sigma, x \rangle = 1$, $\forall \sigma \in Gal(L/K)$, then $\sigma \sqrt[n]{x} = \sqrt[n]{x} \ \forall \sigma \in Gal(L/K)$.

so $\sqrt[n]{x} \in K^*$, so $x \in (K^*)^n$. i.e. the trivial coset. so $x \sim 0 \in \Delta$.

$\Big\}$ non-degenerate in both argument.

By bilinearity, get two injective group homomorphisms:

1. $Gal(L/K) \hookrightarrow Hom(\Delta, \mu_n)$ since $\langle \cdot, \cdot \rangle : Gal(L/K) \times \Delta \to \mu_n$,
2. $\Delta \hookrightarrow Hom(Gal(L/K), \mu_n)$ get: given $Gal(L/K)$, fix it, get $Hom(\Delta, \mu_n)$ likewise.

1. $\Rightarrow$ $Gal(L/K)$ is abelian gp whose exponent divides n. (exponent of a gp = lcm of order of elements)

Similar to the fact that a group to its (dual gp of a finite abelian gp) has same size.

have $|Hom(\Delta, \mu_n)| = |\Delta|$. $|Gal(L/K)| \leq |\Delta|$ b/c $|Gal(L/K)|$ inject into $Hom(\Delta, \mu_n)$ with size $|\Delta|$.

$\Rightarrow |Gal(L/K)| \underset{1}{\leq} |\Delta| \underset{2}{\leq} |Gal(L/K)|$

and 1, 2 are isomorphisms.

$\blacksquare$

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

Lecture 17 Kummer Theory Ctd.

Thm 11.2 Kummer theory bijection

There is a bijection

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

exponent of a finite abelian group is smallest n s.t. $g^n = 1$ $\forall g \in G$

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

$$\frac{(L^*)^n \cap K^*}{(K^*)^n} \longleftarrow L$$

Proof: Show two maps compose to identity on both sides.

Δ maps back to Δ:

let $\Delta \subseteq K^*/(K^*)^n$ be a finite subgroup.

let $L = K(\sqrt[n]{\Delta})$ and $\Delta' = \frac{(L^*)^n \cap K^*}{(K^*)^n}$

$\Delta \subseteq \Delta'$ by definition.

to show equality, just need to check same order.

$$L = K(\sqrt[n]{\Delta}) \subseteq K(\sqrt[n]{\Delta'}) \overset{\text{have } n^{th} \text{ power in } L}{\subseteq} L$$

so $K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\Delta'})$ so $|\Delta| = |\Delta'|$ by lemma 11.1. Hence equality.

L maps back to L

let L/K be a finite abelian extension of exponent dividing n.

let $\Delta = \frac{(L^*)^n \cap K^*}{(K^*)^n}$. Then, $K(\sqrt[n]{\Delta}) \subseteq L$.

want = here

We want to show equality by showing $[K(\sqrt[n]{\Delta}):K] = [L:K]$.

let $G = \mathrm{Gal}(L/K)$. The Kummer pairing defines an injective gp hom $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$.

injectivity, see pf of 11.1.

Claim this is surjective.

Granted this claim,

$$[K(\sqrt[n]{\Delta}):K] \underset{\text{By 11.1's proof}}{=} |\Delta| \underset{\text{By claim}}{=} |\mathrm{Hom}(G,\mu_n)| = |G| = [L:K] \quad \blacksquare$$

Proof of claim "$\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$ is surjective".

Let $\chi : G \to \mu_n$ be a group homomorphism.

Basic Galois theory, distinct automorphisms are linearly independent ???

so $\underbrace{\sum_{\tau \in G} \chi(\tau)^{-1} \cdot \tau}_{\text{nonzero. comb of elements}}$ is not zero so $\exists\, a \in L$, $\underbrace{\sum_{\tau \in G} \chi(\tau)^{-1} \cdot \tau(a)}_{:= y} \neq 0$

let $\sigma \in G$ then

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

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

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

$$= \chi(\sigma)\, y \qquad (*)$$

thus $\sigma(y^n) = y^n \quad \forall\, \sigma \in G$ Why ? How?? ???

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

So, the map $\Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$ sends x to χ. ▨

whole part is shaky. ???

Prop 11.3 finitely many extensions L/K with certain properties

let K be a number field and $\mu_n \subseteq K$.

let S be a finite set of primes of K.

then, there are only finitely many extensions L/K s.t.

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

Proof:

& cond #1

11.2 $\Rightarrow$ $L = K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subseteq K^*/(K^*)^n$.

let p be a prime of K s.t.

$$p\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad \mathfrak{P}_i \text{ distinct primes of } L.$$

If $x \in K^*$ represents an element of Δ then

why? ram index? look @ it upstairs & downstairs?

$$n v_{\mathfrak{p}_i}(\sqrt[n]{x}) = v_{\mathfrak{p}_i}(x) \overset{\downarrow}{=} e_i v_p(x)$$

If $p \notin S$ (p unram) then $e_i = 1$ $\forall i$, so $n v_{\mathfrak{p}_i}(\sqrt[n]{x}) = v_p(x) \Rightarrow v_p(x) \equiv 0 \mod n$. limits our choice of what Δ can be.

Thus $\Delta \subseteq K(S,n)$ where

$$K(S,n) = \{x \in K^*/(K^*)^n : v_p(x) = 0 \pmod n \quad \forall p \notin S\}.$$

Proof is completed by lemma 11.4, which shows $K(S,n)$ is finite. ∎

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

Proof: the map

$$K(S,n) \to (\mathbb{Z}/n\mathbb{Z})^{|S|}$$
$$x \mapsto (v_p(x) \mod n)_{p \in S}$$

is a group homomorphism with kernel $K(\phi, n)$. ← why?

So it suffices to prove lemma with $S = \phi$. ??? ← why?

So if $x \in K^*$ represents an element for $K(\phi, n)$, then $(x) = \mathfrak{a}^n$ for some ideal $\mathfrak{a}$.

There's an exact sequence

* Check injection & surjection & exactness!

$$0 \longrightarrow O_K^*/(O_K^*)^n \longrightarrow K(\phi, n) \longrightarrow Cl_K[n] \longrightarrow 0$$

Algebraic number theory $\begin{cases} |Cl_K| < \infty \\ O_K^* \text{ is finitely generated (Dirichlet's unit thm)} \end{cases}$

So $K(\phi, n)$ is finite. ∎

§ 12. Elliptic curves over number fields II.

↳ Mordell-Weil theorem.

lemma 12.1 $E(K)/nE(K) \to E(L)/nE(L)$ has finite kernel.

let E/K be an elliptic curve, and L/K be a finite Galois extension.

then the map $E(K)/nE(K) \to E(L)/nE(L)$ has finite kernel.

* Note how this lemma resembles Kummer theory.

Proof idea:

let P be a coset rep for kernel. Then, $P = nQ$ for $Q \in E(L)$.

finite choices for $Gal(L|K) \to E[n]$

$\sigma \mapsto \sigma Q - Q$.

But, if P_1, P_2, $nP_1 = Q_1$, $nP_2 = Q_2$, & they mapped to same element $\sigma Q_1 - Q_1 = \sigma Q_2 - Q_2$.

<u>Proof.</u> For each element in kernel, we pick a coset rep. $P \in E(K)$.

then $\exists Q \in E(L)$ s.t. $nQ = P$.

Bound # ker by this?

$Gal(L/K)$ is finite and $E[n]$ is finite so there are only finitely many possibilities for the map $Gal(L/K) \to E[n]$ i.e: $n(\sigma Q - Q) = \sigma P - P = 0$ since P in base

$\sigma \mapsto \sigma Q - Q$ $\Rightarrow \sigma Q - Q \in E[n]$.

But, if $P_1, P_2 \in E(K)$ with $P_i = nQ_i$

& $\sigma Q_1 - Q_1 = \sigma Q_2 - Q_2 \quad \forall \sigma \in Gal(L/K)$

then $\sigma(Q_1 - Q_2) = Q_2 - Q_1$, so $Q_1 - Q_2 \in E(K)$. so $P_1 - P_2 \in n E(K)$. ∎

??? why does it imply the lemma?

<u>lemma 12.2</u>

let $E(K)$ be an elliptic curve over a number field.

If $P \in E(K)$ then $K([n]^{-1}P)/K$ is Galois.

Moreover, if $E[n] \subset E(K)$, the Galois group is abelian of exponent dividing n.

<u>Proof</u>

Show is Galois

Since $Gal(\bar{K}/K)$ acts on $[n]^{-1}P$, we see that $Gal(\bar{K}/K([n]^{-1}P))$ is a normal subgroup of $Gal(\bar{K}/K)$. Hence $K([n]^{-1}P)/K$ is Galois.

Pick $Q \in [n]^{-1}P$, then $[n]^{-1}P = \{Q + T : T \in E[n]\}$

So, $K([n]^{-1}P) = K(Q)$ Reminds me of ex sheet #2 Q7.

There's a map $Gal(K(Q)/K) \to E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$

$\sigma \mapsto \sigma Q - Q$ $\in E[n]$ by lemma 12.1.

claim: this map is group hom & inj.

↳ Gp hom: $\sigma\tau Q - Q = \sigma(\tau Q - Q) + \sigma Q - Q$ since argument is in K Why is $\tau Q - Q \in K$?

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

↳ inj: $\sigma Q - Q = 0 \Rightarrow \sigma Q = Q$

$\Rightarrow \sigma$ fixes $K(Q)$

$\Rightarrow \sigma = 1$

therefore, $Gal(K(Q)/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^n$ proving the claim ∎

scheme:

extend L/K s.t.

↳ assume $\mu_n \in K$. assume $E[n] \subseteq E(K)$

↳ assume L/K Galois

↳ extend over $K([n]^{-1}P)/K$.

↳ unramified out of three prime. finitely many

$\Rightarrow$ $E(K)/nE(K) \to E(L)/nE(L)$ zero map, so ker is LHS.

finite kernel $\Rightarrow$ finite.

Lecture 18 (Did not attend in person)

Theorem: (Weak Mordell - Weil theorem)

E/K an EC over N.F.. let $n \geq 2$. then $E(K)/nE(K)$ is finite.

Proof: By a lemma from last time, (lemma 12.1)

$$\ker\left(E(K)/nE(K) \longrightarrow E(L)/nE(L) \right)$$

is finite, so we may extend our field.

So, WLOG, $\mu_n \subseteq K$ and $E[n] \subseteq E(K)$. (as in after extending)

Extending further, we may assume that L/K is Galois.

(lem 12.2)

The extensions $K([n]^{-1}P)/K$ as P runs over $E(K)$ are abelian of exponent dividing n.

We also saw these extensions are unramified outside of S in the set of primes

$S = \{p \mid n\} \cup \{$ primes of bad reductions over $E/K\}$ By thm 9.9 ???

By prop 11.3, there are only finitely many such extensions of K.

Hence, the compositum L of all these extensions is still finite & Galois over K.

By the construction of L, the map

$$E(K)/nE(K) \longrightarrow E(L)/nE(L)$$

is the zero map

Why is this map the zero map?

so $\left|E(K)/nE(K)\right| = \left|\ker(\dots)\right|$ which is finite by lemma 12.1.

∎

Remark. If $K = \mathbb{R}$ or $\mathbb{C}$ or $[K:\mathbb{Q}_p] < \infty$ then $\left|\frac{E(K)}{nE(K)}\right| < \infty$ yet $E(K)$ is not finitely generated (even uncountable). i.e. weak mordell weil thm is true for num fields. and local fields.

Yet strong Mordell weil thm is false.

* weak Mordell weil true for NF, C, R yet strong M-W only true for NF.

Fact: Existence & Properties of the canonical height

E/K an EC over NF. Then exists a quadratic form, called <u>canonical height</u>

$$\hat{h}: E(K) \to \mathbb{R}_{\geq 0}$$

s.t. $\forall B \geq 0$, $\{P \in E(K) \mid \hat{h}(P) \leq B\}$ is finite.

Thm 12.3 (Mordell Weil thm)

let K be a N.F. E/K an E.C.

Then $E(K)$ is a finitely generated abelian gp.

Proof fix integer $n \geq 2$.

Weak Mordell-Weil $\Rightarrow$ $\left|\frac{E(K)}{nE(K)}\right| < \infty$.

Pick coset representatives $P_1, \cdots, P_m$ (i.e. m cosets)

let $\Sigma = \{P \in E(K) : \hat{h}(P) \leq \max_{1 \leq i \leq n} \hat{h}(P_i)\}$. the union of all points whose height is at most the max of heights of the coset reps.

Claim Σ generates $E(K)$.

Proof of Claim

Suppose not, $\exists P \in E(K) \setminus \{\text{subgroup generated by } \Sigma\}$ of minimal height.

then $P = P_i + nQ$ for some $1 \leq i \leq m$ where $Q \in E(K) \setminus \{\text{subgp gen by } \Sigma\}$.

since P_i are coset reps

$Q \notin$ subgp gen by Σ o.w. $P \in$ subgp gen by Σ

then $\hat{h}(P) \leq \hat{h}(Q)$ by minimality. Then,

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

so $\hat{h}(P) \leq \hat{h}(P_i)$ so $P \in \Sigma$ by defn of Σ. contradiction. $\blacksquare$

Σ is finite so done. $\blacksquare$

Remark: the M-W thm $\Rightarrow$ rank $E(K) < \infty$. However there's no known algorithm to compute rank $E(K)$

§ 13. Heights

For simplicity, take $K = \mathbb{Q}$. Write $P \in \mathbb{P}^n(\mathbb{Q})$ as

$$P = (a_1 : \cdots : a_n), \quad a_1, \cdots a_n \in \mathbb{Z}, \quad \gcd(a_1, \cdots a_n) = 1.$$

<u>defn</u> Height $\quad H(P) = \max_{1 \le i \le n} |a_i|$

<u>lemma 13.1</u> (Lipschitz like condition for heights)

let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be coprime & hom poly of deg d.

let $\quad F : \mathbb{P}^1 \to \mathbb{P}^1$

$$(X_1, X_2) \mapsto (f_1(X_1, X_2), f_2(X_1, X_2))$$

then there exists $C_1, C_2 > 0$ s.t.

$$C_1 H(P)^d \le H(F(P)) \le C_2 H(P)^d \qquad \forall P \in \mathbb{P}^1(\mathbb{Q})$$

the height fcn resembles a Lipschitz like-condition

Takeaway

have $\mathbb{P}^1 \to \mathbb{P}^1$

we map

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

to get smth about ϕ.

<u>Proof</u> wlog $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$.

<u>upper bound</u>:

write $P = (a, b)$ then

$$H(F(P)) = \max_{i=1,2} |f_i(a, b)| \le C_2 (\max(|a|, |b|))^d = C_2 H(P)^d$$

C_2 is max of absolute values of coefficients in f_1 and f_2.

<u>lower bound</u>:

we claim that $\exists g_{ij} \in \mathbb{Z}[X_1, X_2]$ homogenous of deg $d-1$ & $\kappa \in \mathbb{Z}_{\ge 0}$ s.t.

$$\underbrace{\sum_{j=1}^{2} g_{ij} f_j}_{\text{hom of deg}(2d-1)} = \kappa X_i^{2d-1} \qquad (\dagger)$$

Proof:

Recall that f_1, f_2 coprime. Running Euclid's algorithm on $f_1(X, 1)$, $f_2(X, 1)$ gives $r, s \in \mathbb{Q}[X]$ s.t.

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

Homogenising and clearing dominators gives $(\dagger)$ for $i = 2$. Similarly $i = 1$.

done proof of claim. ∎

write $P = (a_1 : a_2)$ $a_1, a_2 \in \mathbb{Z}$ coprime. then $(\dagger)$ gives

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

so $\gcd(f_1(a,b), f_2(a,b)) \mid \gcd(Ka^{2d-1}, Kb^{2d-1}) = K$ b/c a,b coprime.

But also,

Where did this equation come from? Why K gives bound?

$$|Ka_i^{2d-1}| \leq \boxed{\underbrace{\max_{j=1,2} |f_j(a,b)|}_{\leq K H(F(P))}} \underbrace{\sum_{i=1}^{2} |g_{ij}(a,b)|}_{\leq \gamma_i H(P)^{d-1}}$$

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

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

for $i=1,2$.

Recall $H(P) = \max_{i=1,2} |a_i|$

Thus

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

take $C_1 = \max(\gamma_1, \gamma_2)^{-1}$!

■

Lecture 19 (did not attend in person).

Notation H defined on $\mathbb{Q}$.

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

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

defn Height (of $E(\mathbb{Q})$)

Height is defined as map

$$H : E(\mathbb{Q}) \to \mathbb{R}_{\geq 1}$$

$$P \mapsto \begin{cases} H(x) & P = (x,y) \\ 1 & P = O_E \end{cases}$$

height of the x-coord.

def logarithmic height

$$h = \log H.$$

lemma 13.2. $|h(\phi(P)) - \deg(\phi)\, h(P)|$ is bounded.

Let E, E' be elliptic curves over $\mathbb{Q}$.

$\phi : E \to E'$ an isogeny defined over $\mathbb{Q}$. Then $\exists\, c > 0$ s.t.:

$$|h(\phi(P)) - \deg \phi\; h(P)| \leq C$$

height in E' height in E

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

Note that c depends on E, E' and ϕ.

Proof.

lemma 5.4 gives us commutative diagrams:

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

Why is this true?

and $\boxed{\deg \phi = \deg \xi} := d$ note: deg of isogeny is same as hom deg.

B/C all $P \in E(\mathbb{Q})$ projects into $\mathbb{P}^1$.

lemma 13.1 $\Rightarrow$ $\exists\, c_1, c_2 > 0$ s.t. $c_1 H(P)^d \leq H(\phi(P)) \leq c_2 H(P)^d$ $\forall P \in E(\mathbb{Q})$.

Taking log gives us:

$$\begin{cases} \log c_1 + d\,h(P) \leq h(\phi(P)) \\ \log c_2 + d\,h(P) \geq h(\phi(P)) \end{cases}$$

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

$\blacksquare$

Example

If $\phi = [2] : E \to E$ then $\exists C > 0$ s.t.

$$|h(2P) - 4h(P)| \leq C \quad \forall P \in E(\mathbb{Q})$$

defn canonical height

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

Recall: we've seen 3 types of heights
↳ Height
↳ Log height
↳ Canonical height

Check that it converges

for $m \geq n$,

$$\left| \frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P) \right|$$
$$\leq \sum_{r=n}^{m-1} \left| \frac{1}{4^{r+1}} h(2^{r+1} P) - \frac{1}{4^r} h(2^r P) \right|$$
$$= \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} \left| h(2^{r+1} P) - 4h(2^r P) \right|$$
$$\leq C \sum_{r=n}^{m-1} \frac{1}{4^{r+1}}$$
$$\to 0 \quad (\text{as } n \to \infty)$$

this sequence is cauchy so this limit exists.

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

Put $n=0$ in above calculation yields

$$\left| \frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P) \right| \leq C \sum_{r=n}^{m-1} \frac{1}{4^{r+1}}$$

$$\left| \frac{1}{4^m} h(2^m P) - h(P) \right| \leq C \sum_{r=0}^{m-1} \frac{1}{4^{r+1}} \leq C \sum_{r=0}^{\infty} \frac{1}{4^{r+1}} = C \cdot \frac{1}{4} \frac{1}{1 - 1/4} = \frac{C}{3}$$

■

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

When $\hat{h}$ is bounded by B, lemma 13.3 $\Rightarrow$ $h(P)$ is bounded.

So only finitely many possibilities for x. (since $x \in \mathbb{Q}$, and denom / numerator can be at most some number).

each choice gives at most 2 choices for y.

■

Lemma 13.5. $\hat{h}(\phi(P)) = \deg(\phi)\, \hat{h}(P)$

Suppose $\phi: E \to E'$ is an isogeny defined over $\mathbb{Q}$. Then
$$\hat{h}(\phi P) = \deg \phi \; \hat{h}(P)$$
$\forall P \in E(\mathbb{Q})$.

Proof

Lemma 13.2 $\Rightarrow$ there exists $C > 0$ s.t.
$$|h(\phi P) - \deg(\phi) h(P)| < C. \qquad \forall P \in E(\mathbb{Q}).$$
Replace P with $2^n P$, divide by 4^n, take limits $n \to \infty$. $\blacksquare$
$$\left| \frac{h(\phi(2^n P))}{4^n} - \frac{\deg \phi \cdot h(2^n P)}{4^n} \right| \le \frac{C}{4^n}$$
$$= |\hat{h}(\phi(P)) - \deg(\phi)\, \hat{h}(P)| = 0$$

Remark

1. The case $\deg \phi = 1$ shows that $\hat{h}$ unlike h is independent of the choice of the Weierstrass equation. what does it even mean?
2. Taking $\phi: [n]: E \to E$ gives $\hat{h}([n]P) = n^2 \hat{h}(P)$ $\forall P \in E(\mathbb{Q})$.

(Now, going to prove $\hat{h}$ is a quadratic form by showing it satisfies the parallelogram law)

Lemma 13.6 help to show $\hat{h}$ satisfy parallelogram.

Let $E/\mathbb{Q}$ be an elliptic curve. There exists $C > 0$ s.t.
$$H(P+Q)\, H(P-Q) \le C\, H(P)^2 H(Q)^2$$
for all $P, Q, P+Q, P-Q \ne 0_E$.

Proof

Let E have Weierstrass equation $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$.

Let $P, Q, P+Q, P-Q$ have x-coordinates x_1, x_2, x_3, x_4.

Lemma 5.8, $\exists\, W_0, W_1, W_2 \in \mathbb{Z}[x_1, x_2]$ of degree ≤ 2 in x_1, deg ≤ 2 in x_2, s.t.
$$\begin{cases} (1 : x_3 + x_4 : x_3 x_4) = (W_0 : W_1 : W_2) \\ W_0 = (x_1 - x_2)^2 \end{cases}$$

check! forgot how it's proven!

Write $x_i = \frac{r_i}{s_i}$, r_i, s_i coprime, we get

$$(s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = ((r_1 s_2 - r_2 s_1)^2 : \cdots) = (w_0 : w_1 : w_2)$$

coprime

all deg = 2 in poly as s_1/r_1
" " " s_2/r_2

So,

$$H(P+Q)\,H(P-Q) = \max(|r_3|,|s_3|)\max(|r_4|,|s_4|)$$

By defn, $P+Q = r_3/s_3$, $P-Q = r_4/s_4$, h is the bigger of them.

$$\leq \max(|s_3 s_4|, |r_3 s_4 + r_4 s_3|, |r_3 r_4|)$$

?

$$\leq 2\max(|r_1 s_2 - r_2 s_1|^2, \cdots) = 2\max(|w_0|, |w_1|, |w_2|) \leq \text{const}\cdot \max(|r_1|,|s_1|)^2 \max(|r_2|,|s_2|)^2$$

?

$$\leq C\, H(P)^2 H(Q)^2$$

c depends on E, not on P & Q.

■

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

Proof lemma 13.6 & the fact that $|h(2P) - 4h(P)|$ is bounded imply that

(take logs & limits) $H(P+Q)\,H(P-Q) \leq C\, H(P)^2 H(Q)^2$

$$\Rightarrow h(P+Q) + h(P-Q) \leq C + 2h(P) + 2h(Q)$$

for $P, Q \in E(\mathbb{Q})$ (need to check several special cases) ???

replacing P, Q by $2^n P$, $2^n Q$ dividing 4^n, take limits $n \to \infty$ yields,

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

common trick in showing parallelog ram law.

replacing P, Q by $P+Q$, $P-Q$ & writing $\hat{h}(2P) = 4\hat{h}(P)$ gives reverse direction.

So $\hat{h}$ satisfy the parallelogram law & it's a quadratic form.

■

Remark. Able to replace all previous results $\mathbb{Q} \to K$

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

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

the product is over all places v, and the absolute values $|\cdot|_v$ are normalised

s.t. $\prod_v |\lambda|_v = 1 \quad \forall \lambda \in K^*$. always exist such

Then all result in this section genealises to K.

Lecture 20 (unable to attend in person)

§14. Dual Isogenies & Weil Pairings

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

Prop 14.1 universal-property-like thm for EC

what this means?

Let $\Phi \subseteq E(\bar{K})$ be a finite $Gal(\bar{K}/K)$-stable subgroup.

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

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

Proof: omitted. See silverman chapter 3. $\square$

Idea: Select a $Gal(\bar{K}/K)$ stable subgroup of E, to be Φ, to be ker.

Then $\exists!$ E' $\ker(E \to E') = \Phi$ and any E'', $\ker(E \to E'') \supseteq \Phi$ can factor through.

Prop 14.2. The unique existence of dual isogeny

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

$$\begin{tikzcd} E \arrow[r, "{[n]}"] \arrow[d, "\phi"'] & E \\ E' \arrow[ur, dashed, "\exists!\hat{\phi}"'] & \end{tikzcd}$$

Proof

Case ϕ is separable:

$|\ker\phi| = n$ so $\ker \phi \subseteq E[n]$.

Apply prop 14.1 with $\psi = [n]$ to get $\hat{\phi}$.

For uniqueness, if $\psi_1\phi = \psi_2\phi = [n]$

$\Rightarrow (\psi_1 - \psi_2)\circ\phi = 0$

$\Rightarrow \psi_1 = \psi_2$ since ϕ is non constant, hence surjective on $\bar{K}$ points.

Case ϕ is inseparable

Omitted. See Silverman. Suffice to check Frobenius map.

Remark

1. The relation of elliptic curves being isogenous is an equivalence relation.
   Write $E_1 \sim E_2$.
2. If $\deg \phi = [n]$, then $\deg [n] = n^2$, so $\deg \hat{\phi} = \deg \phi$
3. $[n] = \widehat{[n]}$
4. If $E \xrightarrow{\psi} E' \xrightarrow{\phi} E''$ then $\widehat{\phi\psi} = \hat{\psi} \circ \hat{\phi}$
5. $\phi\hat{\phi}\phi = \phi[n]_E = [n]_{E'}\phi$ implies $\phi\hat{\phi} = [n]_{E'}$, in particular $\hat{\hat{\phi}} = \phi$.
6. If $\phi \in \mathrm{End}(E)$ then by example sheet 2,

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

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

hence $\mathrm{tr}\,\phi = \phi + \hat{\phi}$ good to know.

Lemma 14.3 $\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$

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

Proof: If $E = E'$ this follows from $\mathrm{tr}(\phi+\psi) = \mathrm{tr}(\phi) + \mathrm{tr}(\psi)$.

In general, let $\alpha : E' \to E$ be any isogeny (i.e. $\hat{\phi}$) thus

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

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

$$(\widehat{\phi+\psi})\hat{\alpha} = (\hat{\phi} + \hat{\psi})\hat{\alpha} \qquad \text{using the law } \widehat{\phi\psi} = \hat{\psi}\hat{\phi}.$$

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

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

worth concerning for exams!

__Defn (sum)__

The sum map is defined as

$$\text{Sum}: \operatorname{Div}(E) \to E$$
$$\underbrace{\sum n_P (P)}_{\text{formal sum}} \mapsto \underbrace{\sum n_P P}_{\text{group law}}$$

__Recall__ we have a group isomorphism

$$E \to \operatorname{Pic}^0(E) \leftarrow \operatorname{Pic}^0(E) \text{ is Picard w/ deg} = 0.$$
$$P \mapsto [(P)-(O_E)]$$

thus sum $D \mapsto [D]$ for all $D \in \operatorname{Div}^0(E)$. (if deg $D = 0$) (Prop 4.2).

__lemma 14.4__

let $D \in \operatorname{Div}(E)$. Then $D \sim 0$ (is principle) $\Leftrightarrow$ deg $D = 0$ & Sum $D = 0$.

~~Proof proven ? intuitively true.~~ ?????

__Now, ready to define Weil Pairing__

let $\phi: E \to E'$ be an isogeny of degree n with dual isogeny $\hat{\phi}: \hat{E} \to E$.

Assume char $K \nmid n$. $\Rightarrow \phi, \hat{\phi}$ are separable.

We now define Weil Pairing $e_\phi: E[\phi] \times E[\phi'] \to \mu_n$.

eventually, e_ϕ is of form $e_\phi(S,T)$. kernels n^{th} root of unity.

let $T \in E'[\hat{\phi}]$. Then $nT = 0$ ($\hat{\phi}(T) = 0$ so $\phi\hat{\phi}(T) = [n]T = 0$)

so exists $f \in \bar{K}(E')^*$ s.t. $\operatorname{Div}(f) = n(T) - n(O)$. By definition of linearly equivalent divisor.

($nT = O$ same points, so $\exists$ function $\operatorname{Div}(f) = n\, T - O = nT - n \cdot O$ since O is id in the picard group).

Pick $T_0 \in E(\bar{K})$ with $\phi(T_0) = T$ (since ϕ is surjective) Then,

$$\underbrace{\phi^*(T)}_{\text{formal sum of points in } \phi^{-1}[T]} - \phi^*(O) = \sum_{P \in E[\phi]} (P + T_0) - \sum_{P \in E[\phi]} (P)$$

note $\phi^*(T) = \sum_{P \in \phi^{-1}(T)} P$
$= \sum_{P \in E[\phi]} P + T_0$ one pt of preimage plus each point in the kernel

has sum $= \sum_{P \in E[\phi]} T_0 = n T_0 = \hat{\phi}\phi T_0 = \hat{\phi} T = 0$

Hence, $\phi^*(T) - \phi^*(O) = 0$ So it's principle, $\phi^*(T) - \phi^*(O) = \operatorname{div}(g)$ for some $g \in \bar{K}(E)^*$.

Now, $\operatorname{div}(\phi^* f) = \phi^*(\operatorname{div} f)$ By defn of pullback of divisors

$= \phi^*(n(T) - n(O))$

$= n(\phi^*(T) - \phi^*(O)) = n \operatorname{div}(g)$

$= \operatorname{div}(g^n)$

Therefore, $\phi^* f = c g^n$ for some $c \in \bar{K}^*$.

After rescaling f, wlog $c = 1$, i.e. $\phi^* f = g^n$.

recall T_s^* translation invariant.

Now, if $s \in E[\phi]$, then $T_s^*(\operatorname{div} g) = \operatorname{div} g$.

$\Rightarrow \operatorname{div}(T_s^* g) = \operatorname{div} g$

$\Rightarrow T_s^* g = \zeta g$ for some $\zeta \in \bar{K}^*$

so $\zeta = \dfrac{g(x+s)}{g(x)}$ for all $x \in E(\bar{K}) \setminus \left\{ \begin{matrix} \text{poles or} \\ \text{zeroes of } g \end{matrix} \right\}$

Now, $\zeta^n = \dfrac{g(x+s)^n}{g(x)^n} = \dfrac{f(\phi(x+s))}{f(\phi(x))} = 1$

since $s \in E[\phi]$ (why implies this $=1$ still?)

thus $\zeta \in \mu_n$.

Finally, we define $e_\phi(s, T) = \dfrac{g(x+s)}{g(x)}$ for any $x \in E$.

Does not depend on x since isog. is constant.

Note: Construction still kind of shaky, needs review.

Prop 14.5 e_ϕ is bilinear and nondegenerate.

Proof

linearity in the first argument.

$$e_\phi(s_1 + s_2, T) = \frac{g(x + s_1 + s_2)}{g(x + s_2)} \cdot \frac{g(x+s_2)}{g(x)} = g(s_1, T) \cdot g(s_2, T).$$

continue in next lecture.

Lecture 21 (Did not attend in person).

★ useful readings: Pg 415 Silverman Group Cohomology (H^0 and H^1)

Continue the proof for weil Pairing bilinear & nondegenerate.

linearity in the second argument:

let $T_1, T_2 \in E'[\hat{\phi}]$, we can find f_i, g_i, $i=1,2$ s.t. $\mathrm{div}(f_i) = n(T_i) - n(0)$, $\phi^* f_i = g_i^n$.

There exists $h \in \bar{K}(E')^*$ s.t.

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

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

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

hence

$$\begin{aligned} e_\phi(S, T_1+T_2) &= \frac{g(X+S)}{g(X)} \qquad \text{as } S \in \ker\phi = E[\phi] \\ &= \frac{g_1(X+S)}{g_1(X)} \frac{g_2(X+S)}{g_2(X)} \underbrace{\frac{h(\phi(X))}{h(\phi(X+S))}}_{=1} \\ &= e_\phi(S, T_1)\, e_\phi(S, T_2) \end{aligned}$$

Now: on to showing that e_ϕ is nondegenerate:

1^{st} direction: fix $T \in E'(\hat{\phi})$. Suppose $e_\phi(S,T) = 1$ for all $S \in E[\phi]$

So $\tau_S^* g = g$ for all $S \in E[\phi]$ (*)

thus,

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

? Don't quite get this argument.

Is a Galois extension with group $E[\phi]$. with $S \in E[\phi]$ acting as τ_S^*.

So (*) $\Rightarrow$ $g \in \phi^* \bar{K}(E') = \bar{K}(E)^{Gal}$

$\Rightarrow$ $g = \phi^* h$ for some h

$\Rightarrow$ $\phi^* f = g^n = \phi^*(h^n)$

$\Rightarrow$ $f = h^n$ $\qquad$ ϕ^* is a field hom

So $\mathrm{div}(h) = (T) - (0)$

But a divisor of degree 0 is principal $\Leftrightarrow$ sum $=0$

$\therefore T=0$

2^{nd} direction: To get non-degeneracy in the other coordinate note that

$$E'[\hat{\phi}] \longrightarrow \mathrm{Hom}(E[\phi], \mu_n)$$
$$T \longmapsto e_\phi(-,T)$$

is injective because

$$|E'[\hat{\phi}]| = |\mathrm{Hom}(E[\hat{\phi}], \mu_n)| = n, \quad \text{it is an iso.}$$

$\square$

Remarks:

(i) If E, E', ϕ are defined over K then e_ϕ is Galois equivalent:

$$e_\phi(\sigma S, \sigma T) = \sigma\, e_\phi(S,T) \qquad \forall \sigma \in \mathrm{Gal}(\bar{K}/K).$$

Galois action on a point: act on its coords.

(ii) Taking $\phi = [n] : E \to E$ gives

$$e_n : E[n] \times E[n] \longrightarrow \mu_n, \quad \text{actually gets } \mu_n, \text{ not just } \mu_{n^2}.$$

this map

B/C e_n is linear & $E[n]$ has exponent n.

Corollary 14.6

If $E[n] \subseteq E(K)$ then $\mu_n \in K$.

Proof: e_n nondegenerate $\Rightarrow \exists\, S, T \in E[n]$ s.t. $e_n(S,T)$ is a primitive n^{th} root of unity. Say ζ_n.

Then, $\sigma(\zeta_n) = \sigma(e_n(S,T)) = e_n(\sigma S, \sigma T) = e_n(S,T) = \zeta_n$, $\forall \sigma \in \mathrm{Gal}(\bar{K}/K)$

Therefore, $\zeta_n \in K$.

$\square$

Example: There is no elliptic curve $E/\mathbb{Q}$ s.t.

$$E(\mathbb{Q})_{tors} \cong (\mathbb{Z}/3\mathbb{Z})^2 \qquad \text{b/c} \quad \zeta_3 \notin \mathbb{Q}.$$

(i.e. if $E[3] \subseteq E(\mathbb{Q})$ then $\zeta_3 \in \mathbb{Q}$ which is false).

Remark: It turns out that e_n is alternating:

$$e_n(T,T) = 1 \qquad \forall T \in E[n]$$

expanding $e_n(S+T, S+T)$ get $\quad e_n(S,T) = e_n(T,S)^{-1}$.

§ 15. Galois Cohomology

★ useful readings: Pg 415 Silverman Group Cohomology (H^0 and H^1)

Let G be a group. (usually the Galois group of a field extension)

Let A be a G-module (i.e. an abelian group with a G-action via group homomorphism)

Defn (group cohomology)

- $H^0(G, A) = A^G = \{a \in A \mid \sigma(a) = a \quad \forall \sigma \in G\}$ invariant elements of A under G.
- $C^1(G, A) = \{gp \text{ hom } G \to A\}$ 1-cochains
- $Z^1(G, A) = \{(a_\sigma)_{\sigma \in G} : a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\}$ 1-cocycles

  not quite understand why defined this way.
- $B^1(G, A) = \{(\sigma b - b)_{\sigma \in G} : b \in A\}$ 1-coboundaries
- $H^1(G, A) = Z^1(G, A) / B^1(G, A)$.

Check $B^1(G, A) \subseteq Z^1(G, A)$.

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

Now here are elementary results from homological algebra:

Thm 15.1 SES to LES:

A SES of G-modules

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

gives rise to a LES of abelian groups

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

Proof: Omitted. (See Qiangru Kuang's notes for defn of δ specifically)

Thm 15.2 (The Inflation-restriction exact sequence)

let A be a G-module and $H \trianglelefteq G$ a normal subgroup.

Then, there is a inflation restriction exact sequence:

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

Let K be a perfect field. Then $\mathrm{Gal}(\bar{K}/K)$ is a topological group with basis of open subgroups $\mathrm{Gal}(\bar{K}/L)$ for $[L:K]<\infty$.

If $G=\mathrm{Gal}(\bar{K}/K)$ we modify the definition of $H^1(G,A)$ by insisting :

1. The stabilizer of each $a\in A$ is an open subgroup of G.
2. All 1-cochains $G\to A$ are continuous, where A is given the product topology.

Then,

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

Here the direct limit is w.r.t. inflation maps.

<u>Thm 15.3 Hilbert 90</u>

Suppose L/K is a finite Galois extension, then

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

Lecture 22 (Did not attend in person)

Thm 15.3 Hilbert 90

Suppose L/K is a finite Galois extension, then

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

Proof

let $G = \mathrm{Gal}(L/K)$ and $(a_\sigma)_{\sigma\in G} \in Z^1(G, L^*)$.

Distinct automorphisms are linearly independent so $\exists y$ s.t.

$$\underbrace{\sum_{\tau\in G} a_\tau^{-1}\tau(y)}_{x} \neq 0 \qquad a_\tau, y \in A, \quad \tau\in G.$$

For $\sigma\in G$,

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

$\sigma(a_\tau)a_\sigma = a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma$

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

$\square$

Cor 15.4. $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$? Why? only allowed to use it on finite exts.

As an application of Cor 15.4 (Cor of Hilbert 90), assume char $K \nmid n$, we get a SES of $\mathrm{Gal}(\overline{K}/K)$-modules:

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

So we have a LES (By the SES → LES proposition)

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

Cor 15.4

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

Now, revisit Kummer theory. If $\mu_n \subseteq K$, then $\mathrm{Gal}(\overline{K}/K) \circlearrowright \mu$ trivially

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

$\boxed{\text{Why? lemma 11.1?}}$

cts

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

i.e. There's a bijection

$$\left\{ \begin{array}{c} \text{fin. abelian ext } L/K \\ \text{of exp } | n \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{fin subgroups of} \\ \mathrm{Hom}_{cts}(\mathrm{Gal}(\overline{K}/K), \mu_n) \end{array} \right\}$$

$$L \longmapsto \mathrm{Hom}_{cts}(\mathrm{Gal}(L/K), \mu_n)$$

$\Rightarrow$ We get another proof that fin. subgroups of $K^*/(K^*)^n$ parametrizes fin. abelian. exts. of exp $| n$.

Notation: Write $H^1(K, \_) = H^1(\mathrm{Gal}(\overline{K}/K), -)$

Now work on the construction of Selmer group

Let $\phi: E \to E'$ be an isogeny of ECs over K.

There is a SES of $\mathrm{Gal}(\overline{K}/K)$ modules

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

Which induces a LES

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

combined 2 steps?

$\boxed{?}$ How this achieved?

From which we get a SES

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

Now, take K a NF. for each place v of K, fix an embedding $\overline{K} \subseteq \overline{K_v}$.

Then $\mathrm{Gal}(\overline{K_v}/K_v) \subseteq \mathrm{Gal}(\overline{K}/K)$. We get a comm diagram:

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

Def (selmer group) (note that selmer gp depends on an isog.)

the ϕ selmer group $S^{(\phi)}(E/K)$ is the kernel of the dotted arrow:

$$\begin{tikzcd}
0 \arrow[r] & \frac{E'(K)}{\phi E(K)} \arrow[r] \arrow[d] & H^1(K, E[\phi]) \arrow[r] \arrow[d, "\mathrm{res}_V"] \arrow[dr, dotted] & H^1(K,E)[\phi_*] \arrow[r] \arrow[d, "\mathrm{res}_V"] & 0 \\
0 \arrow[r] & \prod_v \frac{E'(K_v)}{\phi E(K_v)} \arrow[r, "\delta_v"] & \prod_v H^1(K_v, E[\phi]) \arrow[r, "(t)"] & \prod_v H^1(K_v, E)[\phi_*] \arrow[r] & 0
\end{tikzcd}$$

so

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

(since $\mathrm{im}\ \delta_v = \ker t$).

Defn. Tate-Shafarevich group.

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

We now get a SES:

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

no ideal why this SES is true.

We can specialize ϕ to $[n]$. Rearranging our proof of weak Mordell Weil theorem $\Rightarrow$

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

Thm 15.5 $S^{(n)}(E/K)$ is finite

Proof for L/K a finite Galois extension, there is an exact sequence:

$$\begin{tikzcd}
0 \arrow[r] & \underbrace{H^1(\mathrm{Gal}(L/K), E(L)[n])}_{\text{Finite b/c both } \mathrm{Gal}(L/K),\ E(L)[n] \text{ are}} \arrow[r, "\mathrm{inf}"] & H^1(K, E[n]) \arrow[r, "\mathrm{res}"] & H^1(L, E[n]) \\
& & S^{(n)}(E/K) \arrow[u, phantom, "\supseteq"] \arrow[r] & S^{(n)}(E/L) \arrow[u, phantom, "\supseteq"]
\end{tikzcd}$$

Since $H^1(\_\_, \_\_)$ is finite, we may extend our field to assume $E[n] \subseteq E(K)$

$\Rightarrow$ $\mu_n \subseteq K$ using the Weil pairing

$\Rightarrow$ $E[n] \cong \mu_n \times \mu_n$ as $\mathrm{Gal}(\bar{K}/K)$-modules b/c both sides are trivial modules.

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

$\cong K^\times/(K^\times)^n \times K^\times/(K^\times)^n$

def The set S.

let $S = \{\text{primes of bad redn for } E\} \cup \{v \mid n\infty\}$

S is a finite set of places.

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

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

There is a commutative diagram with exact rows:

$$\begin{tikzcd}
E(K_v) \arrow[r, "\times n"] \arrow[d] & E(K_v) \arrow[r, "\delta_v"] \arrow[d] & H^1(K_v, E[n]) \arrow[d, "\mathrm{res}"] \\
E(K_v^{\mathrm{nr}}) \arrow[r, "\times n", "(*)"'] & E(K_v^{\mathrm{nr}}) \arrow[r, "0", "(+)"'] & H^1(K_v^{\mathrm{nr}}, E[n])
\end{tikzcd}$$

Recall that $(*)$ is surjective for $\forall v \notin S$. } ???

$\Rightarrow$ $(+)$ is the zero map.

now, $\mathrm{im}(\delta_v) \subseteq \ker(\mathrm{res})$

$\Rightarrow$ $S^{(n)}(E/K) = \{\alpha \in H^1(K, E[n]) \mid \mathrm{res}_v(\alpha) \in \mathrm{im}(\delta_v) \ \forall v\}$

$\subseteq H^1(K, E[n]; S)$ By Hilbert 90

$= H^1(K, \mu_n; S) \times H^1(K, \mu_n; S)$

$\subseteq K(S, n) \times K(S, n)$ since $K_v(\sqrt[n]{x}) \subseteq K_v^{nr}$ $\Rightarrow v(x) = 0 \mod n$

But $K(S,n)$ is finite $\Rightarrow$ $S^{(n)}(E/K)$ is too.

$\square$

Done proof!

__Remark.__ $S^{(n)}(E/K)$ is finite and effectively computable.

It is conjectured that $|Ш(E/K)| < \infty$.

This would imply $\operatorname{rank}(E(K))$ is effectively computable.

§ 16. Descent by cyclic isogeny

Let $E, E'/K$ a number field.

Let $\phi: E \to E'$ an isogeny of degree n.

Assume $E'[\hat{\phi}] \cong \mathbb{Z}/n\mathbb{Z}$ is generated by $T \in E'(K)$. So all torsion is defined $/K$.

Then $E[\phi] \cong \mu$ as a $\mathrm{Gal}(\bar{K}/K)$-modules

$S \mapsto e_\phi(S,T)$

So we get a SES of $\mathrm{Gal}(\bar{K}/K)$-modules.

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

gives rise to a LES:

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

Lecture 23 (Did not attend in person).

Thm 16.1

let $f \in K(E')$, $g \in K(E)$ be s.t.

$$\mathrm{div}(f) = n(T) - n(0)$$

$$\phi^* f = g^n$$

then, $\alpha(P) = f(P) \mod (K^*)^n$ $\quad \forall P \in E'(K) \setminus \{0, T\}$.

Recall that α is a map $E'(K) \to K^*/(K^*)^n$.

Proof

let $Q \in \phi^{-1}(P)$. Then, $\delta(P) \in H^1(K, \mu_n)$ is represented by the cocycle

$$\sigma \mapsto \sigma Q - Q \in E[\phi] \cong \mu_n$$

$$S \mapsto e_\phi(S, T).$$

Now, $e_\phi(\sigma Q - Q, T) = \dfrac{g(X + \sigma Q - Q)}{g(X)}$ for any X not zero or poles of g

$$= \frac{g(\sigma Q)}{g(Q)} \quad \text{taking } X = Q$$

$$= \frac{\sigma(g Q)}{g(Q)}$$

$$= \frac{\sigma(\sqrt[n]{f(P)})}{\sqrt[n]{f(P)}} \qquad \phi^* f = g^n \Rightarrow f(P) = g(Q)^n$$

Therefore, $\delta(P)$ is represented by cocycle $\sigma \longmapsto \dfrac{\sigma \sqrt[n]{f(P)}}{\sqrt[n]{f(P)}}$. 1

But, $H^1(K, \mu_n) \cong K^* / (K^*)^n$

$$\left(\sigma \mapsto \frac{\sigma \sqrt[n]{x}}{\sqrt[n]{x}}\right) \longleftarrow x \qquad 2$$

therefore, $\alpha(P) = f(P) \mod (K^*)^n$. $\square$

Don't quite get this pf.

1 & 2

Descent by 2-isogeny

let $E: y^2 = x(x^2 + ax + b)$ ← $b(a^2 - 4b) \neq 0$

$E': y^2 = x(x^2 + a'x + b')$ and $a' = -2a$, $b' = a^2 - 4b$

$\phi: E \to E'$ $\qquad$ $\hat{\phi}: E' \to E$

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

Check that they're duals to each other.

Write $E[\phi] = \{0, T\}$ $\quad T = (0,0) \in E(K)$

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

Prop 16.2.

There is a group homomorphism

$$E'(K) \longrightarrow K^*/(K^*)^2$$

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

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

Proof either apply previous thm 16.1, with $f = x \in K(E')$, $g = \frac{y}{x} \in K(E)$, or direct calculation. (see ex 4). $\square$

Therefore, we get:

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

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

Remark: It is easy to check that $\operatorname{rank}(E(K)) = \operatorname{rank}(E'(K))$

Lemma 16.3.

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

Proof: If $A \xrightarrow{f} B \xrightarrow{g} C$ are homomorphisms of abelian groups, then we get an exact sequence:

$$0 \longrightarrow \ker(f) \longrightarrow \ker(gf) \xrightarrow{f} \ker(g) \longrightarrow \operatorname{Coker}(f) \xrightarrow{g} \operatorname{coker}(gf) \longrightarrow \operatorname{coker}(g) \longrightarrow 0$$

Since $\hat{\phi}\phi = [2]_E$, we get

$$0 \longrightarrow \underbrace{E(K)[\phi]}_{\cong \mathbb{Z}/2\mathbb{Z}} \longrightarrow E(K)[2] \xrightarrow{\phi} \overbrace{E'(K)[\hat{\phi}]}^{\cong \mathbb{Z}/2\mathbb{Z}}$$

$$\longrightarrow \underbrace{\frac{E'(K)}{\phi E(K)}}_{\cong \operatorname{Im}(\alpha_{E'})} \xrightarrow{\hat{\phi}} \frac{E(K)}{2E(K)} \longrightarrow \underbrace{\frac{E(K)}{\hat{\phi} E'(K)}}_{\cong \operatorname{Im}(\alpha_E)} \longrightarrow 0$$

Why is this?

Why?

Taking group order now gives $\dfrac{|E(K)/2E(K)|}{|E(K)[2]|} = \dfrac{|\operatorname{Im}(\alpha_E)| \cdot |\operatorname{Im}(\alpha_{E'})|}{4}$ $\quad (\dagger)$

Mordell - Weil theorem $\Rightarrow E(K) \cong \Delta \times \mathbb{Z}^r$ $\to \Delta$ a finite gp
$\to r =$ rank $E(K)$

so $\frac{E(K)}{2E(K)} \cong \Delta/2\Delta \times (\mathbb{Z}/2\mathbb{Z})^r$

$E(K)[2] \cong \Delta[2]$ since Δ is finite, $\frac{\Delta}{2\Delta}$ and $\Delta[2]$ have same order.

Thus LHS of $(\dagger) = 2^r$.

The result follows.

$\square$

$$K(S,2) = \left\{ x \in K^\times/(K^\times)^2 \mid v_p(x) \equiv 0 \mod p \ \forall p \notin S \right\}.$$

lemma 16.4.

If K is a number field and $a, b \in \mathcal{O}_K$, then

$$\text{im}(\alpha_E) \subseteq K(S, 2)$$

where $S = \{$ primes dividing $b\}$.

Proof:

? why

Must show that if if $(x,y) \in E(K)$, so $y^2 = x(x^2+ax+b)$ & $v_p(b) = 0$ then, $\boxed{v_p(x) \equiv 0 \mod 2.}$

if $v_p(x) < 0$, then $v_p(x) = -2s$, $v_p(y) = -3s$, for some $s \geq 1$.

$\Rightarrow v_p(x) \equiv 0 \mod 2$.

if $v_p(x) > 0$, then $v_p(x^2+ax+b) = 0$ b/c $p \nmid b$

$\Rightarrow v_p(x) = v_p(y^2) = 2v_p(y) \equiv 0 \mod 2$.

$\square$

lemma 16.5.

If $b_1 b_2 = b$ then $b_1 (K^*)^2 \in \text{Im}\, \alpha_E$ if and only if

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

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

Proof: If $b_1 \in (K^*)^2$ or $b_2 \in (K^*)^2$ then both conditions are satisfied.

So WLOG $b_1, b_2 \notin (K^*)^2$.

Now $b_1 (K^*)^2 \in \text{Im}\, \alpha_E \Leftrightarrow \exists (x,y) \in E(K)$ s.t. $x = b_1 t^2$ for some $t \in K^\times$.

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

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

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

Conversely if (u,v,w) is a solution then $uv \neq 0$ because $b_1, b_2 \notin (K^*)^2 \Rightarrow (b_1(\frac{u}{v})^2, b_2 \frac{vw}{v^3}) \in E(K)$ has $a=b$.

$\square$

Example

Consider $E: y^2 = x^3 - x$ $/\mathbb{Q}$ so $a=0$, $b=-1$

since $(0,0) \in \alpha_E$, equality

Lemma 16.4 $\Rightarrow$ $\operatorname{im}(\alpha_E) \subseteq \langle -1 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E': y^2 = x^3 + 4x \Rightarrow S = \{2\}$

so $\operatorname{im}(\alpha_{E'}) \subseteq \langle -1, 2 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$

lemma 16.5 $\Rightarrow$ $b_1 = -1 \in \operatorname{im}(\alpha_{E'}) \Leftrightarrow w^2 = -u^4 - 4v^4$

try $b_1 b_2 = b = 4$ since $\mathbb{Q}^*/\mathbb{Q}^2$ we only try b_1 square free.

$b_1 = 2 \in \operatorname{im}(\alpha_{E'}) \Leftrightarrow w^2 = 2u^4 + 2v^4$

$b_1 = -2 \in \operatorname{im}(\alpha_{E'}) \Leftrightarrow w^2 = -2u^4 - 2v^4$

The 1st and 3rd are not soluble over $\mathbb{R}$. The second has solution $(u,v,w) = (1,1,2)$

So $\operatorname{im} \alpha_{E'} = \langle 2 \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$

Now, $2^{\operatorname{rank} E(\mathbb{Q})} = \frac{2 \cdot 2}{4} = 1 \Rightarrow \operatorname{rank} E(\mathbb{Q}) = 0$

$\Rightarrow$ 1 is not a congruent number.

o.w. this would have solution

Example

Consider $E: y^2 = x^3 + px$ $/\mathbb{Q}$, where p is prime, $p \equiv 5 \mod 8$.

Then, $\operatorname{im}(\alpha_E) \subseteq \langle -1, p \rangle$.

$b_1 = -1 \in \operatorname{im}(\alpha_E) \Leftrightarrow w^2 = -u^4 - pv^4$ insoluble over $\mathbb{R}$.

So $\operatorname{im}(\alpha_E) = \langle p \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.

Also, $E': y^2 = x^3 - 4px \Rightarrow S = \{2, p\}$

so $\operatorname{im}(\alpha_{E'}) \subseteq \langle -1, 2, p \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$

Note: $\alpha_{E'}(T') = (-4p)(\mathbb{Q}^*)^2 = (-p)(\mathbb{Q}^*)^2$ so only need to consider

① $b_1 = 2 \in \operatorname{im}(\alpha_{E'}) \Leftrightarrow w^2 = 2u^4 - 2pv^4$

② $b_1 = -2 \in \operatorname{im}(\alpha_{E'}) \Leftrightarrow w^2 = -2u^4 + 2pv^4$

③ $b_1 = p \in \operatorname{im}(\alpha_{E'}) \Leftrightarrow w^2 = pu^4 - 4v^4$

Suppose 1 is soluble. wlog. $u, v, w \in \mathbb{Z}$, $\gcd(u,v)=1$, if $p|u$ then $p|w$ then $p|v$ ※

Thus, $w^2 = 2u^4 \neq 0 \mod p$. so $\left(\frac{2}{p}\right) = 1$. contradicting $p \equiv 5 \mod 8$.

likewise, 2 has no solution over $\mathbb{Q}$ since $\left(\frac{-2}{p}\right) = -1$.

so 1 and 2 are insoluble over $\mathbb{Q}$.

Lecture 24.

Example continued.

To Recall,

$E: y^2 = x(x^2+ax+b)$, $\phi: E \to E'$ a 2-isogeny.

$w^2 = b_1u^4 + au^2v^2 + b_2v^4$ $(*)$

We have an SES

$$0 \longrightarrow \frac{E'(\mathbb{Q})}{\phi E(\mathbb{Q})} \longrightarrow S^{(\phi)}(E/\mathbb{Q}) \longrightarrow \text{Ш}(E/\mathbb{Q})[\phi_*] \longrightarrow 0$$

$$\frac{E'(\mathbb{Q})}{\phi E(\mathbb{Q})} \xrightarrow{\alpha_{E'}} \mathbb{Q}^*/(\mathbb{Q}^*)^2 \supset S^{(\phi)}(E/\mathbb{Q})$$

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

only primes fit for proving insolubility.

Fact: using ex sheet 3 Q9 & Hensel's lemma: if $a, b_1, b_2 \in \mathbb{Z}$, and $p \nmid 2b(a^2-4b)$ then $*$ is soluble over $\mathbb{Q}_p$.

not necessarily

Example 2 continued.

$E: y^2 = x^3 + px$, $p \equiv 5 \mod 8$

$w^2 = pu^4 - 4v^4$ $(\dagger)$

?

$E(\mathbb{Q})$ has rank 0 if $\dagger$ is insoluble and 1 if soluble.

By the fact we only have to look at p-adic & 2-adic.

③ soluble $\Rightarrow$ image size 4

③ insoluble $\Rightarrow$ image size 2.

By fact
- $(\dagger)$ is soluble over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right)=1$ so $(-1) \in (\mathbb{Z}_p^*)^2$ (By Hensel's lemma)
- soluble over $\mathbb{Q}_2$ since $p-4 \equiv 1 \mod 8$, Hensel $\Rightarrow$ $p-4 \in (\mathbb{Z}_2^*)^*$
- soluble over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$.

$u=1, v=1$, get from local fields that 1 mod 8 is a 2-adic square.

why p-adic square matters?

We can try to spot solutions:

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

Conjecture: $\mathrm{rank}(E(\mathbb{Q}))=1 \quad \forall$ primes $\equiv 5 \mod 8$

Example 3 (Lind)

$E: y^2 = x^3+17x.$ $\qquad \mathrm{Im}\,\alpha_E = \langle 17\rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E': y^2 = x^3-68x.$ $\qquad \mathrm{Im}\,\alpha_{E'} \subseteq \langle -1,2,17\rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$

Consider $b_1=2.$ $\qquad w^2 = 2u^4-34v^4$

Replace w by $2w$ and divide through by 2 to get $C: 2w^2 = u^4-17v^4.$

Notation

$C(K) = \{(u,v,w)\in K^3\setminus\{0\}$ satisfying $C\}/\sim.$ ← Weighted projective space.

Where $(u,v,w)\sim(\lambda u, \lambda v, \lambda^2 w) \quad \forall \lambda\in K^*$

- $C(\mathbb{Q}_2)\neq\emptyset$ as $17\in(\mathbb{Z}_2^*)^4$ (example in local fields)
- $C(\mathbb{Q}_{17})\neq\emptyset$ since $2\in(\mathbb{Z}_{17}^*)^2$ Legendre + hensel, $u=1$, $v=0$, 2 is a square
- $C(\mathbb{R})\neq\emptyset$ since $\sqrt{2}\in\mathbb{R}.$

Thus, $C(\mathbb{Q}_v)\neq 0$ for all places of $\mathbb{Q}$.

However, it has no solution over $\mathbb{Q}$. (Trick is to use quadratic reciprocity)

Suppose $(u,v,w)\in C(\mathbb{Q})$, wlog $u,v\in\mathbb{Z}$, $\gcd(u,v)=1$. Then $w\in\mathbb{Z}$. assume $w>0$.

- If $17\mid w$, then $17\mid u$, then $17\mid v$. ※
- So if $p\mid w$, then $p\neq 17$ and $\boxed{\left(\frac{17}{p}\right)=1}$?why? so by quadratic reciprocity,

for p odd, $\left(\frac{p}{17}\right)=\left(\frac{17}{p}\right)=1$

for $p=2$, $\left(\frac{2}{17}\right)=1$

thus $\left(\frac{w}{17}\right)=1$

w is a square, so w^2 is 4^{th} power

But $2w^2 = u^4 \mod 17$ so $2 \in (\mathbb{F}_{17}^*)^4 = \{\pm1, \pm4\}$, $\times$.

so $C(\mathbb{Q}) = \phi$.

C is a counter-example to the Hasse-principle.

It represents a non-trivial element of Ш$(E/\mathbb{Q})$.

(looking at the LES, it's smth in Selmer not coming from left. so it goes to right).

Birch Swinnerton-Dyer Conjecture

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

defn L-function for Elliptic curves

$L(E,s) = \prod_p L_p(E,s)$, $s \in \mathbb{C}$, where

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

where $\# E(\mathbb{F}_p) = p+1-a_p$.

Hasse's thm: $|a_p| \leq 2\sqrt{p}$, so $L(E,s)$ converge for $Re(s) > 3/2$.

As a consequence of modularity thm:

Thm 16.6 (Wiles, Breuil, Conrad, Diamond, Taylor)

$L(E,s)$ is the L-function of a weight 2-modular form and hence an analytic continuation to all of $\mathbb{C}$. And has a functional equation relating $L(E,s)$ and $L(E, 2-s)$.

Conjecture (weak BSD conj)

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

Assuming weak BSD, and let $r = \mathrm{ord}_{s=1} L(E,s)$ be the analytic rank, we have

<u>conjecture (Strong BSD conj)</u>

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

- $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ = tamagawa number of $E/\mathbb{Q}_p$.
- $\dfrac{E(\mathbb{Q})}{E(\mathbb{Q})_{tors}} = \langle P_1, \cdots, P_r \rangle$
- $\mathrm{Reg}\, E(\mathbb{Q}) = \det([P_i, P_j])_{ij}$

  where $[P, Q] = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$
- $\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{|2y + a_1 x + a_3|}$ where a_i is the coefficient of a globally minimal Weierstrass equation for E.

Best result so far

<u>thm 16.7 (Kolyvagin)</u>

If $\mathrm{ord}_{s=1} L(E,s) = 0$ or 1, then the weak BSD is true and $|Ш(E/\mathbb{Q})| < \infty$.