Elliptic Curves

We can relate points on an elliptic curve to maximal ideals in the ring $R = K[x,y]/(y^2 - f(x))$

So to the point $P = (\alpha, \beta) \in K^2$ s.t. $\beta^2 = f(\alpha)$, we associate the ideal $(x-\alpha, y-\beta)$.

In the ring R we can define a group ~~action~~ : the class group.

$$Cl(R) = \text{free gp on the ideals } \mathfrak{p} \text{ modulo principal ideals.}$$

For $\mathfrak{p} = (x-\alpha, y-\beta)$ and $\mathfrak{p}' = (x-\alpha, y+\beta)$, note that

$$\mathfrak{p}\mathfrak{p}' = (x-\alpha) \equiv [1]$$, so the inverse of a point is easy.

For distinct points $P_i = (x-\alpha_i, y-\beta_i)$ $i = 1..3$ s.t. $ax+by+c \in P_1 \cap P_2 \cap P_3$,

then $P_1 P_2 P_3 = (ax+by+c) \equiv [1]$

What is the ideal class of $I = P_1 P_2 \cdots P_k$? $(k \geq 2)$

$P_{k-1} \cdot P_k \cdot q = (1)$, ~~for~~ some q, so

$$I \sim P_1 \cdots \underbrace{(P_{k-1} P_k q)}_{(1)} \cdot q' \sim P_1 \cdots P_{k-2} \cdot q'$$

Continuing in the same fashion, $I \sim \mathfrak{p}$ for some prime ideal $\mathfrak{p}$.

So it is enough to work with prime (maximal) ideals.

For two (distinct) primes $\mathfrak{p}$ and $\mathfrak{q}$, $\mathfrak{p} \not\sim \mathfrak{q}$ (why?) ← we'll see it later.

Conclusion: the class group of R can be uniquely represented by

$$\{P = (x-\alpha, y-\beta),\ \beta^2 = f(\alpha)\} \cup \{(1)\}$$ where $P_1 P_2 P_3 = (1) \Leftrightarrow ax+by+c \in P_1 \cap P_2 \cap P_3$

By the identification between the curve and its ring of functions, we see that there is a group structure on the set:

$$\{P=(\alpha,\beta)\in k^2 : \beta^2 = f(\alpha)\} \cup \{\mathcal{O}\}.$$

with addition law $P_1+P_2+P_3=\mathcal{O} \Leftrightarrow P_1, P_2, P_3$ are colinear.

Some geometry (~~differential?~~ no, algebraic).

Let $k=\bar{k}$ be an algebraically closed field.

A closed algebraic subset of k^n is a set V consisting of all roots of a finite set of polynomial equations.

$$V=\{(x_1,\dots x_n)\in k^n : f_1(x_1,\dots,x_n)=f_2(x_1,\dots,x_n)=\dots=f_m(x_1,\dots,x_n)=0\}$$

Let $A=(f_1,\dots,f_m)\subseteq \overbrace{k[x_1,\dots,x_n]}^{R}$, then V depends on A but not on the choice of its generators.

Define $V(A)=\{\underline{x}\in k^n : f(\underline{x})=0 \ \forall f\in A\}$.

Example: $V((0))=k^n$, $V((1))=\emptyset$.

The closed sets are a topology for k^n:

- $V(A)\cup V(B)=V(A\cap B)$
- $\bigcap_\alpha V(A_\alpha)=V\left(\sum_\alpha A_\alpha\right)$

(exercise)

For a closed algebraic set V, let $I(V)=\{f\in R : f(x)=0 \ \forall x\in V\}$.

- Clearly, the maps $I(\cdot)$ and $V(\cdot)$ are inclusion reversing.
- For any closed alg. set V_1,

$$V_1=V(I(V_1)) \quad \text{(exercise)}$$

Thm: (Hilbert Nullstellensatz).

$$I(V(A))=\sqrt{A}$$

Note that for a prime ideal $\mathfrak{p}$, $\sqrt{\mathfrak{p}} = \mathfrak{p}$

<u>Noether's decomposition Theorem</u>: The radical ideals in $k[X_1, \dots, X_n]$ are the ideals:

$$A = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \quad \text{for prime ideals } \mathfrak{p}_1, \dots, \mathfrak{p}_r .$$

The decomposition is unique if we remove primes that contain other primes in the list. (i.e. if no prime ideal $\mathfrak{p}_i$ contains another prime ideal $\mathfrak{p}_j$.

What we obtain is a 1-1 correspondence:

$$\left\{ \begin{array}{l} \text{closed algebraic} \\ \text{subsets of } k^n \\ V = V_1 \cup \cdots \cup V_n,\ V_n \text{ irreducible.} \end{array} \right\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{ \begin{array}{l} \text{radical} \\ \text{ideal } A \subseteq k[X_1, \dots, X_n] \\ A = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r \end{array} \right\}$$

If V cannot be written as a proper union $V = V_1 \cup V_2$, then V is called "irreducible".

<u>Def</u> A topological space X is said to be <u>noetherian</u> if it satisfies the descending chain condition on closed subsets.

<u>Example</u>:

$I = (xy, z) \subseteq k[X, Y, Z]$.

$I = (X, Z) \cap (Y, Z)$ and both are prime, so it is a decomposition.

So $V(I) = \{x = 0 \ \& \ z = 0\} \cup \{y = 0 \ \& \ z = 0\} = (y\text{-axis}) \cup (x\text{-axis})$

<u>Def</u> An <u>affine variety</u> is an irreducible closed algebraic subset of k^n.

<u>Rk</u>: If V is a variety, $V = V(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$.

<u>Def</u>: The affine coordinate ring $k[V]$ of V is the ring $k[V] = k[X_1, \dots, X_n]/\mathfrak{p}$

<u>Rk</u>: $k[V]$ is a finitely generated integral domain over k.

(in fact, all f.g. integral domains over k are of the form $k[X_1, \dots, X_n]/\mathfrak{p}$).

~~Def~~ A curve is an affine variety of dimension 1.

~~Def~~ Let $A = (f_1, \dots, f_m) \subseteq k[X_1, \dots X_n]$

Let $V = V(A)$. Then ~~P~~ V is nonsingular at P if.

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

(it does not depend on the choice of the f's, only on A!).

Example: $y^2 = x^3 - x$ is nonsingular at $P=(0,0)$: $f = y^2 - (x^3 - x)$.

$$\begin{pmatrix} \frac{\partial f}{\partial x}(P) & \frac{\partial f}{\partial y}(P) \\ 1, & 0 \end{pmatrix} \neq 0 \quad \text{is of rank } n - \dim V = 2-1 = 1.$$

But the curves $y^2 = x^3$, $y^2 = x^3 - x^2$ are singular at $(x,y) = (0,0)$.

Maps between affine varieties

Let $V_1 \subseteq K^{n_1}$, $V_2 \subseteq K^{n_2}$ be two affine varieties with ideals $I_1 \subseteq k[X_1, \dots, X_{n_1}]$, $I_2 \subseteq k[Y_1, \dots, Y_{n_2}]$.

A morphism from V_1 to V_2 is a map $\varphi : V_1 \longrightarrow V_2$ such that $\exists\, \varphi_1, \dots, \varphi_{n_2} \in k[X_1, \dots, X_{n_1}]$ with $\varphi(\underline{x}) = (\varphi_1(\underline{x}), \dots, \varphi_{n_2}(\underline{x}))$.

The morphism $\varphi : V_1 \longrightarrow V_2$ induces a K-homomorphism of K-algebras

$$\varphi^* : k[V_2] \longrightarrow k[V_1]$$
$$g \longmapsto \varphi^*(g) = g \circ \varphi.$$

~~Prop~~: The two categories

$$\left\{ \begin{matrix} \text{Affine varieties} \\ + \\ \text{morphisms} \end{matrix} \right\} \quad \text{and} \quad \left\{ \begin{matrix} \text{f.g. integral domains} \\ \text{over } K \\ + \\ K\text{-homomorphisms} \end{matrix} \right\}$$

are equivalent under the contravariant functor $\begin{bmatrix} V \mapsto k[V] \\ \varphi \mapsto \varphi^* \end{bmatrix}$.

Example

$V_1 = V(XY - 1) \subseteq k^2$ hyperbola $\quad k[V_1] = k[x,y]/(xy-1) \simeq k[x, \frac{1}{x}]$

$V_2 = V(y - x^2) \subseteq k^2$ Parabola $\quad k[V_2] = k[x,y]/(y-x^2) \simeq k[x]$ not isomorphic.

$\rightsquigarrow V_1 \not\cong V_2$.

~~Def~~ $\mathbb{P}^n(k) = \{(x_0 : \dots : x_n) : x_i \in k \text{ not all } x_i = 0\}/\sim$, where $(x_0 : x_1 : \dots : x_n) \sim (\lambda x_0 : \lambda x_1 : \dots : \lambda x_n)$ for all $\lambda \neq 0$.

$S = k[x_0, \dots, x_n] = \bigoplus_{d \geq 0} S_d$ is a graded ring.

An ideal $I \subseteq S$ is an <u>homogeneous ideal</u> if I is generated by homogeneous elements.

Ex: $I = (xy, z) \subseteq k[x,y,z]$ is homogeneous, but $(xy+z)$ is not.

For a homogeneous ideal I, define a <u>closed algebraic set</u>:

$V(I) = \{P \in \mathbb{P}^n(k) : f(P) = 0 \text{ for all}_{\text{homogeneous}}\ f \in I\}$. (well defined!)

The closed algebraic subsets define a topology on $\mathbb{P}^n(k)$, called the Zariski topology.

The maps $V(-)$ and $I(-)$ set up a 1-1 correspondence:

$$\left\{\begin{array}{l}\text{closed algebraic}\\ \text{subsets}\end{array}\right\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{\begin{array}{l}\text{homogeneous radical ideals}\\ I \subseteq S,\\ I \neq S_+ = (x_0, x_1, \dots, x_n)\end{array}\right\}$$

For $P \in V$, let (now working in affine algebraic sets)

$k[V]_P := \{f \in k(V) : f = g/h,\ g, h \in k[V],\ h(P) \neq 0\}$. (the local ring of V at P.)

Then $k[V] \subseteq k[V]_P \subseteq k(V)$.

Let V now be a projective variety (ie. V is irreducible).

~~Def~~ A <u>regular function</u> is a pair (U, f) where $U \subseteq V$ is an open subset, and $f = \frac{g}{h}$ for some $g, h \in S_d$ (homogeneous of the same degree), such that $h \neq 0$ on all U.

~~Def~~ Two regular functions (U_1, f_1) and (U_2, f_2) are equivalent iff $f_1 = f_2$ in $U_1 \cap U_2$

(For V irreducible the intersection of two opens will always be nonempty!).

Example:

$V = V(XY - Z^2) \subseteq \mathbb{P}^2$

Let U_X be the open $\{X \neq 0\}$ and let U_Z be the open $\{Z \neq 0\}$.

$$V \cap U_X \cong V(Y - Z^2) \subseteq k^2$$

$$V \cap U_Z \cong V(XY - 1) \subseteq k^2$$

Also, $(U_X, Z/X) \sim (U_Z, \frac{Y}{Z})$ (they agree on $U_X \cap U_Z$).

Def The function field of a proj variety V is

$$\kappa(V) = \{(U, f)\}/\sim \qquad \text{(note that this is a field).}$$

Prop: Let $U \subseteq V$ be an affine open subset.
Then $\kappa(V) \cong \kappa(U)$.

An element of $\kappa(V)$, that is, an equivalence class, is called a rational function.

Def A rational map ~~morphism~~ $\phi: V_1 \longrightarrow V_2$ of projective varieties $V_1 \subseteq \mathbb{P}^{n_1}$, $V_2 \subseteq \mathbb{P}^{n_2}$
is an n_2-tuple $\phi = (\phi_0, \dots, \phi_{n_2})$ of rational functions $\phi_0, \dots, \phi_{n_2} \in K(V_1)$

Def A rational map is regular at $P \in V_1$ if there exists $g \in k(V_1)$
s.t. $g\phi_0, \dots, g\phi_{n_2}$ are regular at P and not all zero at P.

A rational map is regular (i.e. it is a morphism) if it is regular at all P.

Example:

$\mathbb{P}^1(k) = \{(x_0, x_1) : \text{not both } 0\}/\sim \ = U_0 \cup U_1$

$k(U_0)$? $\quad k[U_0] = k\left[\frac{x_1}{x_0}\right] \Rightarrow k(U_0) = k\left(\frac{x_1}{x_0}\right)$ and, similarly, $k(U_1) = k\left(\frac{x_0}{x_1}\right)$

A variety V is nonsingular at P if there is an affine open $P \in U \subseteq V$ s.t. U is nonsingular at P.

<u>Thm 5.1 Hartshorne</u>: V is nonsingular at P iff $k[V]_P$ is a <u>regular</u> local ring.
(i.e. if m is the maximal ideal, then $\dim_k (m/m^2) = \dim R$.

(For curves: $\dim R = 1$, and then a regular local domain of $\dim = 1$ is called a Discrete Valuation Ring).

(For curves if the curve C is nonsingular at P, then a generator t for m/m^2 is called a <u>uniformizer</u> (or a local parameter)).

<u>Example</u>: $\phi : \left(\frac{x}{y} : \frac{y}{z} : \frac{z}{x}\right) : \mathbb{P}^2 \to \mathbb{P}^2$

ϕ is certainly regular on the open $U = \{xyz \neq 0\}$.

Let $P = (0 : a : 1)$, $a \neq 0$.

$\phi = \left(\frac{x}{y} : \frac{y}{z} : \frac{z}{x}\right) = \left(\frac{x}{y} \cdot \frac{x}{z} : \frac{y}{z} \cdot \frac{x}{z} : \frac{z}{x} \cdot \frac{x}{z}\right) = \left(\frac{x^2}{yz} : \frac{xy}{z^2} : 1\right)$ does not vanish in P ($\phi(P) = (0 : 0 : 1)$).

Let $O = (0 : 0 : 1)$. Is it then regular? Multiply the original by $\frac{xy}{z^2}$:

$\phi = \left(\frac{x^2}{z^2} : \frac{xy^2}{z^3} : \frac{yz}{z^2}\right)$ and $\phi(O) = (0 : 0 : 0) \Rightarrow$! this form is not regular, either.

So the rational map ϕ is <u>not</u> regular at O, O', O''.

A different way to write a rational map $\phi: V_1 \to V_2$ is by "clearing denominators": write $\phi = (\phi_0 : \dots : \phi_n)$ where $\phi_0, \dots, \phi_n$ are homogeneous polynomials of the same degree, such that:

(1) Not all $\phi_i \in I(V_1)$

(2) $\forall f \in I(V_2)$, $f(\phi_0(\underline{x}), \dots, \phi_n(\underline{x})) \in I(V_1)$

Example: $\phi = \left(\frac{x}{y} : \frac{y}{z} : \frac{z}{x}\right)$ is the same as $\tilde{\phi} = (x^2 z : x y^2 : y z^2)$.

Prop 2.1 [Silv]: Let $\phi : C \to V$ be a rational map from a curve to a variety (both projective). If C is nonsingular at P, then ϕ is regular at P.

Corollary: If C is a smooth curve, then $\phi: C \to V$ any rational map is regular (is a morphism).

Pf Let $P \in U \subset C$, U open with coordinate ring $k[U]$.
Then $R = k[U]_P$ is a regular local ring. Let $t \in \mathfrak{m} \setminus \mathfrak{m}^2$ be a uniformizing element
For $\phi = (\phi_0 : \phi_1 : \phi_2 : \dots : \phi_n)$, ~~write $\phi_i = \sum a_i$~~
Let M be minimal such that $t^M \phi_i \in R$ for all $i = 0, 1, \dots, m$
Then $\phi(t^M \phi_0 : \dots : t^M \phi_n)$ is regular, as if all $t^M \phi_i$ vanish simultaneously we'd have chosen a smaller M.

Klein quartic

Example: Let $\phi = (xy : yz : zx) : C \to \mathbb{P}^2$, where $C : x^3 y + y^3 z + z^3 x = 0$
What is the image of $O = (0:0:1)$?

$z(O) \neq 0$
$(x=0) \cap C$: $O\ (3\times)$, $(0:1:0)\ (1\times)$ $\Rightarrow \frac{x}{z} \in \mathfrak{m}^3$
$(y=0) \cap C$: $O\ (1\times)$, $(1:0:0)\ (3\times)$ $\Rightarrow \frac{y}{z} \in \mathfrak{m} \setminus \mathfrak{m}^2 \Rightarrow t = \frac{y}{z}$ is a uniformizing param.
$(xy : yz : zx) = \Big(\underbrace{\tfrac{x}{z}}_{\in \mathfrak{m}^3} : 1 : \underbrace{\tfrac{x}{y}}_{\in \mathfrak{m}^2}\Big) \Rightarrow \phi(O) = (0:1:0)$.

(continue with the example).

What is the image of C in $\mathbb{P}^2$. ~~Ie~~ i.e. what is the vanishing ideal for this image?

$$\phi: (\underbrace{xy}_{X} : \underbrace{yz}_{Y} : \underbrace{zx}_{Z}) : C \longrightarrow \mathbb{P}^2$$

i.e. what is the relation among X, Y, Z knowing that $x^3y + y^3z + z^3x = 0$?

General solution:

Eliminate x, y, z from the equations.

$$\begin{cases} x^3y + y^3z + z^3x = 0 \\ xy - X = 0 \\ yz - Y = 0 \\ zx - Z = 0 \end{cases} \Rightarrow x^2y^2z^2\left(x^3y + y^3z + z^3x\right) = 0 \rightarrow$$

$$\Rightarrow X^3Z^2 + Y^3X^2 + Z^3Y^2 = 0$$

So the image is contained in the curve $\{X^3Z^2 + Y^3X^2 + Z^3Y^2 = 0\} =: C_2$.

Then we've found a morphism $\phi: C_1 \longrightarrow C_2 \subseteq \mathbb{P}^2$.

Theorem 2.3 [Sil]: Let $\phi: C_1 \longrightarrow C_2$ be a morphism of curves. Then, ϕ is either constant or ϕ is surjective.

Is there a morphism $\psi: C_2 \to C_1$? First, is there a rational map $C_2 \to C_1$?

- We need to know some results from Silverman's book

Chap I

P1.1 P1.2

P2.1 T2.3 (R2.5) P2.6

P3.1

P4.3 ace

P5.2 T5.4(RR)

To a curve C/k (irreducible, projective) we can associate the function field $k(C)$.

To a $\overset{\text{surjective}}{}$ morphism $\phi: C_1 \longrightarrow C_2$ corresponds an injection of function fields,

$$\phi^*: k(C_2) \hookrightarrow k(C_1).$$

There is a more statement: the above maps define an equivalence of categories:

$$\left\{\begin{array}{c}\text{Smooth curves}/k \\ + \\ \text{Surjective } (=\text{nonconstant}) \\ \text{morphisms}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{function fields of} \\ \text{dimension 1 over } k \\ + \\ \text{injective } k\text{-homomorphisms}\end{array}\right\}$$

For it, the additional fact we have to prove is that $k(C_1) \simeq k(C_2) \Rightarrow C_1 \simeq C_2$.

If $k(C_1) \simeq k(C_2) \Rightarrow \exists\, U_1 \subsetneq C_1,\ U_2 \subseteq C_2$ opens s.t. $k(U_1) \overset{\sim}{=} k(U_2)$.

But if C_1, C_2 are smooth then the ~~rat~~ rational map can be extended to a regular map.

(See Hartshorne, I 6.7 or II 6.8).

A <u>function field of dimension 1</u> over k is a finite generated field extension K/k, of transcendence degree 1, such that $K \cap \bar{k} = k$

<u>Def</u> The <u>degree</u> of a surjective morphism $\phi: C_1 \longrightarrow C_2$ is $[k(C_1) : \phi^* k(C_2)]$

<u>Example</u>: $E/k : y^2 = x^3 + ax + b$

$\phi = (x:1) : E \longrightarrow \mathbb{P}^1$; $\phi' : (y;1) : E \longrightarrow \mathbb{P}^1$

The degree of ϕ is $[k(x,y) : k(x)] = 2$, because

The degree of ϕ' is $[k(x,y) : k(y)] = 3$.

$$\begin{array}{c} k(x,y) \\ \mid 2 \\ k(x) \\ \mid \text{tr deg} = 1 \\ k \end{array}$$

Let $\phi: C_1 \longrightarrow C_2$ be a nonconstant morphism, and let $\phi(P) = Q$.

$$\begin{array}{lll} \kappa(C_1) & P & t_P, \text{ local parameter for } P \\ \quad | & & \\ \phi^* \kappa(C_2) & Q & t_Q, \text{ local parameter for } Q. \end{array}$$

The <u>ramification index</u> of P above Q, $e_{P|Q} :=$ order of Q at P.
(i.e. $t_Q \in (t_P)^e \setminus (t_P)^{e+1}$).

<u>Prop 2.6 [Sil]</u>: (if $\kappa = \bar{\kappa}$)

a) For $Q \in C_2$, $\displaystyle\sum_{P \in \phi^{-1}(Q)} e_{P|Q} = \deg \phi$.

b) For almost all of $Q \in C_2$, $\# \phi^{-1}(Q) = \deg_s \phi$

c) Let $\begin{array}{ccccc} C_1 & \xrightarrow{\phi} & C_2 & \xrightarrow{\psi} & C_3 \\ P & \longmapsto & Q & \longmapsto & R \end{array}$. Then $e_{P|R} = e_{P|Q} \cdot e_{Q|R}$.

Pf: Theory of finite extensions of Dedekind domains //

The divisor group $\mathrm{Div}(C)$ is the free abelian group generated by the points $P \in C$. (An element $D = \sum_{P \in C} n_P P$ is called a divisor).

For $f \in \kappa(C)$, $f \neq 0$, define $(f) = \sum_{P \in C} \mathrm{ord}_P(f) \cdot P$ $\quad \left(\mathrm{ord}_P(f) = \max\{a : f \in (t_P^a)\} \right)$

<u>Claim</u>: (f) is a divisor (i.e. $\mathrm{ord}_P(f) = 0$ for almost all P).

Pf: For $f \in \kappa(C)^*$, let $\phi = (f:1) : C \longrightarrow \mathbb{P}^1$. Then $\mathrm{ord}_P(f) \neq 0 \iff P$ is a zero or a pole (i.e. $P \in \phi^{-1}((0:1))$ or $P \in \phi^{-1}((1:0))$).

But $\# \phi^{-1}((0:1)) \leq \deg \phi$ and $\# \phi^{-1}((1:0)) \leq \deg \phi$.

Riemann-Roch problem

For a divisor $D \in \mathrm{Div}(C)$, let

has poles supported by D

$$\mathcal{L}(D) := \{ f \in \bar{k}(C)^* : (f) + D \geq 0 \} \cup \{0\}.$$

What is the dimension of $\mathcal{L}(D)$? $\dim_{\bar{k}} \mathcal{L}(D)$?

Thm 5.4 [Sil].

$$\dim_{\bar{k}} \mathcal{L}(D) = \deg(D) + 1 - g + \dim_{\bar{k}} \mathcal{L}(K - D)$$

where $\deg(D) = \sum n_P$ if $D = \sum n_P P$. ; $g = g(C)$ is the genus of the curve,

and K is the canonical divisor (will see later on).

Genus g of a plane curve

Let $C = V(F_d) \subseteq \mathbb{P}^2$, $F_d = F_d(X, Y, Z)$ a degree d polynomial.

Let H_m be homogeneous of degree m. (will fix the poles).

What is the dimension of the vector space $L = \{ f = \frac{G}{H_m} \in \bar{k}(C)^*,\ G \text{ homogeneous of degree } m \} \cup \{0\}$.

$$\dim_{\bar{k}} L = \binom{m+2}{2} - \binom{m-d+2}{2} \quad \text{for } m \geq d.$$

$$= \underbrace{md}_{\#(C \cap H_m)} + 1 - \underbrace{\binom{d-1}{2}}_{\text{genus of } C} \qquad \frac{(d-1)(d-2)}{2} = \begin{cases} 1 & \text{for } d = 3 \\ 0 & \text{for } d = 1, 2 \end{cases}$$

Th (Riemann-Roch): Let $C/\bar{k}$ be a smooth (irr. proj.) curve over $\bar{k}$, $k = \bar{k}$.

For any divisor D on C,

$$\ell(D) - \ell(K - D) = \deg D + 1 - g$$

where $\ell(D) = \dim_{\bar{k}} \mathcal{L}(D)$, $\mathcal{L}(D) = \{ f \in \bar{k}(C)^* : (f) + D \geq 0 \}$.

and K is a canonical divisor.

g genus of the curve C.

Riemann Th (corollary of RR):

there exists $g \in \mathbb{Z}_{\geq 0}$ such that $\ell(D) = \deg D + 1 - g$ for all D with $\deg D \gg 0$.

Proof of RR: elementary in [Chevalley], [Stichtenoth], fancy proof in [Hartshorne], more geometric proof in [Fulton].

Algebraic Function Fields (Undergrad Springer)

(in Hartshorne, $\ell(D) = \dim H^0(X, \lambda(D))$, $\ell(K-D) = \dim H^1(X, \lambda(D))$).

Differentials:

Let C/K be a curve with function field $K(C)$.

The $K(C)$-module $\Omega(C)$ of differentials on C is the module with generators df where $f \in K(C)$ and relations

$$d(f+g) = df + dg$$
$$d(fg) = f\,dg + g\,df$$
$$d(a) = 0 \quad \forall a \in K$$

Prop 4.2 [Sil] (a) $\Omega(C)$ is a 1-dimensional $K(C)$-vectorspace.

Prop 4.3 [Sil] Let $\omega \in \Omega(C)$. Assume $\operatorname{char} K = 0$.

(a) For a point $P \in C$ and local parameter $t = t_P$, there exists $f \in K(C)$ s.t. $\omega = f\,dt$.

(c) $\operatorname{ord}_P(f)$ depends on ω and on P but not on the choice of t.

We write $\operatorname{ord}_P(\omega)$ for $\operatorname{ord}_P(f)$.

(e) For given $\omega \in \Omega(C)$, $\operatorname{ord}_P(\omega) = 0$ for almost all $P \in C$.

Pf of (e): write $\omega = f\,dx$ for some $x \in K(C)$.

Consider $\phi: C \xrightarrow{(x:1)} \mathbb{P}^1$, $P \longmapsto x(P)$. Then $x - x_P$ vanishes at P and is a local parameter for P at all points where ϕ is unramified. (suppose $x(P) \in K$). (not a pole)

So for all points P with $x_P \neq \infty$ and P unramified under ϕ, ~~$\mathrm{ord}_P(\omega) = \mathrm{ord}_P f$~~

$\omega = f\,dx = f\,d(x - x_P) \Rightarrow \mathrm{ord}_P(\omega) = \mathrm{ord}_P(f)$. But $\mathrm{ord}_P(f) \neq 0$ only at finitely many points (zeros / poles). //

Def: The <u>divisor of a differential</u> $\omega \in \Omega(C)$ is:

$$(\omega) := \sum_{P \in C} \mathrm{ord}_P(\omega) P$$

By <u>prop 4.2(a)</u>, for any two differentials $\omega_1, \omega_2 \in \Omega(C)$, $(\omega_1) \sim (\omega_2)$.

(we say that two divisors are $\sim$ iff they differ by a principal divisor; (a principal divisor is a divisor $D = (f)$ for some $f \in \kappa(C)^*$.))

So as $\omega_1 = f\omega_2 \Rightarrow (\omega_1) = (f) + (\omega_2) \Rightarrow (\omega_1) - (\omega_2) = (f)$.

Def The Divisor class group (or Picard group) is $\mathrm{Pic}(C) := \mathrm{Div}(C)/\sim$.

All principal divisors have degree 0

Def $\mathrm{Pic}^0(C) := \mathrm{Div}^0(C)/\sim$ where $\mathrm{Div}^0(C) = \{\text{divisors of degree } 0\}$.

Let E/k be a smooth irreducible projective curve of genus 1, with a point $O \in E$.

- For $D = 0$, $g = 1$:

$$\ell(D) - \ell(K - D) = \deg D + \cancel{1} - g \qquad L(0) = \{f \in \kappa(C)^* : (f) + 0 \geq 0\} \cup \{0\} = K$$

$$1 - \ell(K) = 0 \Rightarrow \ell(K) = 1.$$

- Substitute $D = K$.

$$\ell(K) - \ell(0) = \deg K \Rightarrow \deg(K) = 0.$$

$\dim L(D) = 1$ and $\deg D = 0 \Rightarrow D \sim (f)$. Thus $K \sim (f)$.

Claim: $\dim_k L(m\mathcal{O}) = \begin{cases} 1 & \text{if } m=0 \\ m & \text{if } m \geq 1 \end{cases}$

Pf $l(m\mathcal{O}) = \deg m\mathcal{O} + \dim(-m\mathcal{O}) = m + \overbrace{\dim(-m\mathcal{O})}^{0 \text{ or } 1 \text{ if } m=0}$ (in general, $L(D)=\{0\}$ when $\deg D<0$).

choose a basis $L(0\mathcal{O}) = \langle 1 \rangle$

$L(1\mathcal{O}) = \langle 1 \rangle$

$L(2\mathcal{O}) = \langle 1, x \rangle$

$L(3\mathcal{O}) = \langle 1, x, y \rangle$

$\dim L(6\mathcal{O}) = 6$. But $\underbrace{1, x, y, x^2, xy, x^3, y^2}_{7 \text{ elements}} \in \overbrace{L(6\mathcal{O})}^{\dim = 6} \Rightarrow$

$\Rightarrow \exists$ relation $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$

We've ~~proven~~ (a) in next prop.

Prop 3.1 [Si:I]: Let E/k be an elliptic curve.

a) There exist functions $x, y \in k(E)$ such that $\phi: (x:y:1): E \to \mathbb{P}^2$ gives an isomorphism into a curve $C: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$. $(*)$ with $a_1, a_2, a_3, a_4, a_6 \in k$ and such $\phi(\mathcal{O}) = (0:1:0)$.

The equation for C is called a Weierstrass equation for E.

b) Any two Weierstrass equations for E are related by a linear change of variables $\begin{cases} X = u^2X' + r \\ Y = u^3Y' + sX' + t \end{cases}$ $u, r, s, t \in k$, $u \neq 0$.

c) Every smooth cubic curve C given by an equation $(*)$ is an elliptic curve with point $\mathcal{O} = (0:1:0)$.

P1

a) By R-R, $\exists\, x, y \in k(E)$ s.t. $L(O) = \langle 1 \rangle$, $L(2O) = \langle 1, x \rangle$, $L(3O) = \langle 1, x, y \rangle$.

Both x^3, y^2 live in $L(6O) \setminus L(5O)$.

Thus, there exist nonzero constants A_6, A_7 s.t.

$$A_6 y^2 - A_7 x^3 \in L(5O) \iff A_7^2 A_6^4 y^2 - A_7^3 A_6^3 x^3 \in L(5O) \iff$$

$$\iff \tilde{y}^2 - \tilde{x}^3 \in L(5O).$$

So can choose x, y s.t. $y^2 - x^3 \in L(5O)$ (but $x^3, y^2 \in L(6O) \setminus L(5O)$).

$L(5O) = \langle 1, x, y, x^2, y^2 \rangle \Rightarrow \exists\, a_1, a_2, a_3, a_4, a_6$ s.t.

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

We have shown $\phi(E) \subseteq C \subseteq \mathbb{P}^2$.

$\phi : E \to C$ is a rational map defined on a smooth curve,

so ϕ is a morphism. ϕ is non-constant, so ϕ is surjective.

Want ϕ to be of degree 1, ~~so it is injective~~.

$K(C) = k(x, y)$

Consider $k(x,y)$ as a subfield of $k(E)$ (identify $\phi^* k(C)$ with $k(C)$).

$$\begin{tikzcd} & k(E) \arrow[dl, dash, "2"'] \arrow[d, dash] \arrow[dr, dash, "3"] & \\ k(x) \arrow[dr, dash] & k(x,y) \arrow[l, dash] \arrow[r, dash] & k(y) \arrow[dl, dash] \\ & k & \end{tikzcd}$$

$\phi_x : E \to \mathbb{P}^1$, $P \mapsto (x : 1)$ is of degree 2, because $x \in L(2O) \setminus L(O)$.

$\phi_y : E \to \mathbb{P}^1$, $P \mapsto (y ; 1)$ is of degree 3, because $y \in L(3O) \setminus L(2O)$

$\deg\ [k(E) : k(x,y)] \mid \gcd(2,3) = 1$. That shows that $\deg \phi = 1$.

Still want to see that the inverse ϕ^{-1} is of degree 1.

As $k(E) \xrightarrow{\sim} k(C)$, there exists a rational map $\psi: C \to E$.

C is a cubic plane curve of genus 1 (because the function fields coincide).

Now use that singular plane cubic curves have genus 0 to conclude that C is smooth.

Pf. If O is a singular point on the curve, any line l through O will intersects the curve in only another point P (because it is tangent at O).

This map defines a birational map $\mathbb{P}^1 \to C$ $\Rightarrow$ genus(C) = genus$(\mathbb{P}^1) = 0$.
$$l \mapsto P$$

So ψ is smooth $\Rightarrow$ ψ is surjective and morphism. Thus $C \cong E$.

(b) Let $\langle 1, x\rangle = \langle 1, x'\rangle$
$\langle 1, x, y\rangle = \langle 1, x', y'\rangle$

then we get $x = \mu_1 x' + r$ but $x^3 - y^2 \in L(5O)$
$y = \mu_2 \cancel{y'} + s_2 x' + t$ $\quad x'^3 - y'^2 \in L(5O)$

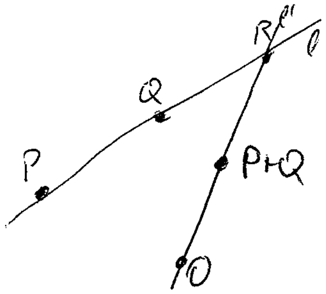
This means that $\mu_1 = \mu^2$, $\mu_2 = \mu^3$ and take $s_2 = s\mu^2$ for convenience

(c) $C: y^2 + \dots$ is an elliptic curve? we only need to show that genus$(C) = 1$.

We know, for smooth cubic curves of degree d, that $\ell(mL) = dm + 1 - \binom{d-1}{2}$ divisor of a line.

Comparing with R-R, for $d = 3$, $g = 1$.

- <u>Addition Law on (E, O).</u>



- Three ways to verify the axioms (associativity is the only nontrivial one).
  - → Use coordinates for a Weierstrass equation (not enlightening).
  - → Use R-R to show that $\langle E(K), + \rangle \simeq \mathrm{Pic}^0(E)$, $P \mapsto [P-O]$
  - → Geometric proof (Fulton, Cassels) (see photocopies).

<u>Lemma</u>: Let $P_1, \ldots, P_8$ be points in the plane in "general position". Then every cubic curve through $P_1, \ldots, P_8$ passes through P_9, a ninth point, ~~dependent~~ only on $P_1, \ldots, P_8$

Pf The space of all cubics is $\{a_0 X^3 + a_1 X^2 Y + \ldots + a_9 Z^3\}$ $\left(\binom{5}{2} = 10\right)$.
i.e. is of projective dimension 9.

The subspace of cubics through $P_1, \ldots, P_8$ is $\{\lambda F + \mu G : (\lambda:\mu) \in \mathbb{P}^1\}$.

In particular, $F \cap G \supseteq \{P_1, \ldots, P_8\}$. But $\underbrace{\#(F \cap G) = 9}_{\text{why?}} \Rightarrow P_9 \in \{\lambda F + \mu G\}$ $\forall (\lambda:\mu) \in \mathbb{P}^1$.

This automatically proves associativity.

- Models for Elliptic Curves:

If char $K \neq 2$, multiply by 4 and a new variable for $2y + a_1 x + a_3$ gives

$$E: y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$

If furthermore char $K \neq 3$, we can force $b_2 = 0$ and get

$$E: y^2 = x^3 - 27c_4 x - 56 c_6$$

And write

$$E: y^2 = x^3 + Ax + B \qquad (\text{char } K \neq 2, 3). \quad (\text{Weierstrass Normal Form})$$

The only isomorphism that transforms a normal form to another normal form is $\begin{cases} x = u^2 x \\ y = u^3 y \end{cases}$. If so, then $A' = \frac{A}{u^4}$, $B' = \frac{B}{u^6}$

So an invariant in E can be $\frac{A^3}{B^2}$

Lemma: Up to isomorphism, E is determined by $(A^3 : B^2) \in \mathbb{P}^1$.

Def: Let $\Delta = \text{disc}(x^3 + Ax + B) = -(4A^3 + 27B^2)$ (Silverman puts 16 in front (!!))

The discriminant can be scaled $\Delta' = \frac{\Delta}{u^{12}}$ by isomorphism.

Def: The <u>j-invariant</u> of the elliptic curve E is defined as

$$j = 1728 \frac{4A^3}{4A^3 + 27B^2} = -1728 \frac{4A^3}{\Delta}$$

Thm: The <u>j-invariant</u> is an isomorphism invariant.

$$\Big(E \underset{\substack{\uparrow \\ \text{isomorphic} \\ \text{over } K = \overline{K}}}{\xrightarrow{\sim}} E' \iff j(E) = j(E') \Big).$$

Examples: $E: y^2 = x^3 + x \longrightarrow j(E) = 1728$

$E': y^2 = x^3 + 1 \longrightarrow j(E') = 0$

The discriminant is well defined because $\Delta \neq 0$ (E is smooth!)

Example:

$E: y^2 = x^3$ has $\Delta = 0$. E is singular with a cusp at the origin $(0,0)$

Let $\phi : E \xrightarrow{(x:y)} \mathbb{P}^1$ be a rational map.

The image of ϕ. $\phi(E_{ns}) \subseteq \mathbb{P}^1 \setminus (1:0)$:

$y^2 z = x$ and $(x : y) = (1:0) \Rightarrow$ If $y = 0 \Rightarrow x = 0$, so only have $(0:0:1)$,

singular!

Now, let $\phi\big((x:y:z)\big) = (t:1) \in \mathbb{P}^1 \setminus (1,0)$.

Then $\frac{x}{y} = \frac{t}{1}$, or $x = yt$.

Get $y^2 = (yt)^3 \Rightarrow \begin{cases} y = 0 \\ \text{or } 1 = yt^3 \Leftrightarrow y = \frac{1}{t^3} \end{cases}$

So the only preimage of $(t:1)$ in E_{ns} is $\left(\frac{1}{t^2} : \frac{1}{t^3} : 1\right) = (t, 1, t^3)$

So we have a degree-1 map, which is an isomorphism:

$$E_{ns} \xrightarrow{(x:y:z)\mapsto(x:y)} \mathbb{P}^1 \setminus (1:0)$$
$$(t,1,t^3) \mapsfrom (t:1)$$

Let $(t_1:1:t_1^3)$, $(t_2:1:t_2^3)$ $(t_3:1:t_3^3)$, ~~be colinear~~

The three points are colinears $\Leftrightarrow$ there $\exists\ \alpha, \beta \in k$ s.t. $\alpha t_i + \beta + t_i^3 = 0 \ \forall i = 1..3$

$\Leftrightarrow \exists\ \alpha, \beta \in k$ st $t^3 + \alpha t + \beta = (t-t_1)(t-t_2)(t-t_3) \Longleftrightarrow t_1 + t_2 + t_3 = 0$

As groups, $\langle E_{ns}(k), + \rangle \simeq \langle \mathbb{P}^1 \setminus (1,0), + \rangle$

<u>Example</u>: $E: y^2 = x^3 + x^2$

Then $\varphi: E \to \mathbb{P}^1 \setminus \{\underset{(0:1)}{0}, \underset{(1:0)}{\infty}\}$ is an isomorphism on E_{ns}
$(x,y,z) \mapsto (y+x : y-x)$

and $\phi: E_{ns}(k) \simeq (k^*, \times)$ $\left(P \mapsto (t_p:1) \quad t_p = \frac{y+x}{y-x} \right)$

then $P_1 + P_2 + P_3 = 0 \Leftrightarrow t_1 t_2 t_3 = 1$.

We've seen that every elliptic curve E/K char $K \neq 2,3$ is of the form
$E: y^2 = x^3 + Ax + B$, $j(E) = 1728 \dfrac{4A^3}{4A^3+27B^2}$

Conversely, the elliptic curve:

$$E: y^2 + xy = x^3 - \frac{36}{j_0 - 1728} x - \frac{1}{j_0 - 1728} \quad \text{has } j(E) = j_0 \quad \text{for } j_0 \neq 1728, 0$$

Also, $E_1: y^2 = x^3 + 1$ has $j(E) = 0$, and $E_2: y^2 = x^3 + x$ has $j(E) = 1728$.

If char $K = 3$, $1728 = 0$ and use E_2 for $j = 0$.

If char $K = 2$, $1728 = 0$, use $y^2 + y = x^3 =: E_3$

For char $K \neq 2,3$, every elliptic curve has an equation in Legendre form:

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

The j-invariant of E_λ is $j_\lambda = \dfrac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda-1)^2} \cdot 2^8$

Pf Let $E: y^2 = x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$

Since E is nonsingular, e_1, e_2, e_3 are distinct.

Now use an affine transformation that brings $e_1 \to 0$, and $e_2 \to 1$ and let λ be the image of that transformation. //

Rk: The morphism $j: \mathbb{P}^1 \longrightarrow \mathbb{P}^1$, $\lambda \longmapsto j(E_\lambda)$ is of degree 6.

1.	$0, 1, \infty$	λ
2.	$1, 0, \infty$	$1-\lambda$
3.	$\infty, 1, 0$	$\frac{1}{\lambda}$
4.	$0, \infty, 1$	$\frac{\lambda}{\lambda-1}$
5.	$1, \infty, 0$	$\frac{1}{1-\lambda}$
6.	$\infty, 0, 1$	$\frac{\lambda-1}{\lambda}$

But above $j = \infty$, only 3 preimages: $0, 1, \infty$

$j = 0$, only 2 preimages: $\zeta_6, \bar{\zeta}_6$

$j = 1728$, only 3 " : $-1, \frac{1}{2}, 2$

By Hurwitz, $(2g_L - 2) = n \cdot (2g_K - 2) + \sum (e_p - 1)$

$-2 = 6 \cdot -2 + 10 \Rightarrow \sum (e_p - 1) = 10$

Example:

Let $C: y^2 = f(x)$, $\deg f = 4$

$f(x) = (x-a)(x-a_1)(x-a_2)(x-a_3)$ with a, a_1, a_2, a_3 distinct.

Use the substitution $\begin{cases} x = \frac{1}{u} + a \\ y = \frac{v}{u^2} \end{cases}$ and get $\frac{v^2}{u^4} = \frac{1}{u}\left(\frac{1}{u} + b_1\right)\left(\frac{1}{u}+b_2\right)\left(\frac{1}{u}+b_3\right)$

$\iff v^2 = (1+ub_1)(1+ub_2)(1+ub_3)$.

So it is an elliptic curve.

We've mapped $(a, a_1, a_2, a_3) \longmapsto \left(\infty, \frac{1}{a_1 - a}, \frac{1}{a_2-a}, \frac{1}{a_3-a}\right) = (\infty, e_1, e_2, e_3)$

Rk:

$$\begin{array}{llll} L = k(x,y),\ y^2 = x^3+Ax+B & g_L = 1 & (x,y) \quad (x,-y) & (e_i, 0) \\ 2\,\Big| & & \quad\searrow \quad \swarrow & \quad \Big| \\ K = k(x) & g_K = 0 & \qquad x & \quad e_i \end{array}$$

By Hurwitz, $0 = 2\cdot(-2) + 4$ so we need four points which have to ramify, but only have e_1, e_2, e_3. The fourth is the ∞.

A morphism in the category of elliptic curves is called an isogeny.

Def An isogeny between two elliptic curves $E_1 \to E_2$ is a morphism

$\phi: E_1 \to E_2$ s.t. $\phi(O_{E_1}) = O_{E_2}$

We define also $\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } \phi: E_1 \to E_2\}$.

It is a group with the addition law in the codomain $((\phi+\psi)(P) = \phi(P) + \psi(P))$.

Thm 4.8 [S,I]: Let $\phi: E_1 \to E_2$ be an isogeny. Then

$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$

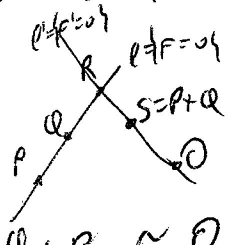
~~Idea of Pf~~: verify that the following diagram is well defined and commutes:

$$\begin{array}{ccc} E_1 & \xrightarrow[\cong]{\kappa_1} & \mathrm{Pic}^\circ(E_1) \\ \downarrow & & \downarrow \\ E_2 & \xrightarrow[\cong]{\kappa_2} & \mathrm{Pic}^\circ(E_2) \end{array} \qquad \begin{array}{ccc} P & \longmapsto & [P-\mathcal{O}_1] \\ \downarrow & & \downarrow \\ & & [\phi P - \phi \mathcal{O}_1] \text{ as } \phi\mathcal{O}_1 = \mathcal{O}_2 \\ & & \| \\ \phi P & \longmapsto & [\phi P - \mathcal{O}_2] \end{array}$$

1) So we only need to see that $E \xrightarrow[\cong]{\kappa} \mathrm{Pic}^\circ(E)$ is well defined isomorphism of groups.

Use R.R to show that $\kappa(P) = [P - \mathcal{O}]$ is both surjective and injective.

~~Let P+Q~~



$$\left(\frac{F}{F'}\right) = (P+Q+R) - (\mathcal{O}+R+S)$$

Thus $P+Q+\cancel{R} \sim \mathcal{O} + \cancel{R} + S \iff (P-\mathcal{O}) + (Q - \mathcal{O}) \sim (S - \mathcal{O}) \iff$

$\iff [P-\mathcal{O}] + [Q - \mathcal{O}] = [S - \mathcal{O}] \iff \kappa(P) + \kappa(Q) = \kappa(P+Q)$.

2) We need to show that $[P - \mathcal{O}_1] \longmapsto [\phi P - \phi \mathcal{O}_1]$ is well defined:

For $\phi : C_1 \to C_2$ a morphism of curves,

$\phi_* : \mathrm{Pic}^\circ(C_1) \to \mathrm{Pic}^\circ(C_2)$ is a well defined group homomorphism.

(A map in the other direction is the pullback $\phi^* : \mathrm{Pic}^\circ(C_2) \to \mathrm{Pic}^\circ(C_1)$).

We have - given $\phi : C_1 \to C_2$, a pullback $\phi^* : k(C_2) \to k(C_1)$.

So there is a Norm map: $\mathrm{Norm} : k(C_1) \xrightarrow{\mathrm{Norm}} \phi^* k(C_2)$

$$\begin{array}{ccc} k(C_1) & \xrightarrow{\mathrm{Norm}} & \phi^* k(C_2) \\ & \searrow^{\phi_*} & \uparrow \wr\, \phi^* \\ & & k(C_2) \end{array}$$

So we get a push-forward $\phi_* : k(C_1) \to k(C_2)$.

We also have $\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ by decomposing P in $k(C_1)$.

Also, $\phi_* : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ is the one obtained from $\phi_* : k(C_1) \to k(C_2)$.

To see that ϕ^*, ϕ_* are in fact defined over the $\mathrm{Pic}^\circ(C_i)$,
note that $\begin{cases} \deg(\phi^* D_2) = (\deg\phi)\cdot \deg D_2. \\ \deg(\phi_* D_1) = \deg(D_1). \end{cases}$ (so ~~takes~~ 0 deg to 0 deg)

~~ϕ^*~~ ~~Also~~ $\phi^*((f_2)) = (\phi^* f_2)$
$\phi_*((f_1)) = (\phi_* f_1)$ $\Big\{$ takes principal divisors to principal divisors.

Corollary: if $\phi : E_1 \to E_2$ is a nonzero isogeny, then
$\ker\phi = \phi^{-1} O_2$ is a finite group of order $\deg\phi$.

Remark: if $\phi : E_1 \to E_2$ is a nonzero isogeny then ϕ is unramified.
Pf/. Use Hurwitz-Zeuthen: $(2\cancel{g}-2) = (\deg\phi)(\cancel{2}g-2) + \sum(e_\phi - 1) \Rightarrow$ unramified.
Another (more enlightening proof):
if ϕ is a group homomorphism, then $\phi^{-1}P_2'$ is a translate of $\phi^{-1}P_2$.
So it would be either unramified or everywhere ramified.

Addition law on $E : y^2 = x^3 + ax + b$

Let $P \neq Q$, $P, Q \neq O = (0:1:0)$.
The line ℓ through $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ is ℓ: $y = \dfrac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1$, $y = \lambda x + \mu$.
Let $\ell \cap E = (P, Q, R)$ and $R = (x_3, y_3)$.

Then $(\lambda x + \mu)^2 = x^3 + ax + b$ for $x = x_1, x_2, x_3 \Rightarrow x_1 + x_2 + x_3 = \lambda^2$

Finally, $y_3 = \lambda x_3 + \mu$.
Then $S = P + Q = (x_3, -y_3)$.

Special case $P = Q$.
Observe $2y\,dy = (3x^2 + a)\,dx \Rightarrow$ the tangent line ℓ_P at P has equation:
$y - y_1 = \left(\dfrac{3x_1^2 + a}{2y_1}\right)(x - x_1) = \lambda x + \mu$ and do the same.

<u>Prop 4.2</u>: Let $m \in \mathbb{Z}$

a) Multiplication by m, $[m]: E \to E$ is a nonzero morphism.

(First, there are exactly four points in $\ker[2]$: $(e_1,0), (e_2,0), (e_3,0), \mathcal{O}$
(e_i are roots of x^3+ax+b).
Let $P_0 \neq \mathcal{O}$ be a point with $[2]P_0 = \mathcal{O}$.
Then, for m odd, $[m]P_0 = P_0 \neq \mathcal{O}$, and thus $[m] \neq [0]$.

b) $\mathrm{Hom}(E_1, E_2) = \{$isogenies $\phi: E_1 \to E_2\}$ is a torsion-free $\mathbb{Z}$-module.
(Let $\phi: E_1 \to E_2$ be nonzero.
Assume, for $m \neq 0$, $\underset{\text{nonconstant}}{[m]} \circ \phi = \underset{\text{constant}}{[0]} \Rightarrow \phi = 0$.)

c) $\mathrm{End}(E) = \mathrm{Hom}(E,E)$ is a ring of characteristic zero without zero divisors.
(in general, it is <u>not</u> commutative).

((b) $\Rightarrow$ char. 0, because $[m]\circ\phi = 0 \Rightarrow \phi = 0$.
Let ϕ, ψ be isogenies $\phi \circ \psi = [0]$.
But then either $\phi = 0$ or $\psi = 0$ (since composition of surjectives is surjective).)

As group homomorphism, we got the diagram:

$$\begin{tikzcd}
E_1 \arrow[r, "\sim"] \arrow[d, "\phi"'] & \mathrm{Pic}^0(E_1) \arrow[d, "\phi_*"] & {[P - O_1]} \arrow[d] \\
E_2 \arrow[r, "\sim"] \arrow[d, dashed, "\hat{\phi}"'] & \mathrm{Pic}^0(E_2) \arrow[d, "\phi^*"] & {[Q - O_2]} \arrow[d] \\
E_1 \arrow[r, "\sim"] & \mathrm{Pic}^0(E_1) & {\left[\sum_{i=1}^{m}(P+T_i) - \sum_{i=1}^{m}(O_1+T_i)\right] = [m(P-O_1)]}
\end{tikzcd}$$

Let $\ker\phi = \{T_1, \ldots, T_m\}$ where $m = \deg\phi$.

So $\exists\ \hat{\phi}$ s.t. $\hat{\phi}\circ\phi = [\deg\phi]$ as group homomorphism.
Need to show that $\hat{\phi}$ is, in fact, an isogeny.

Prop 4.10: Let $\phi : E_1 \to E_2$ be a separable, nonconstant isogeny.
↑ the extension $\phi^* k(E_2) \subseteq k(E_1)$ is separable.

Let $m = \deg \phi$.

$$\begin{array}{ccc} E_1 & & k(E_1) \\ \phi \big\downarrow & & \big| m \\ E_2 & & \phi^* k(E_2) \end{array}$$

Then, $k(E_1) / \phi^* k(E_2)$ is Galois, with

$$\mathrm{Gal}\left(k(E_1) / \phi^* k(E_2) \right) \simeq \mathrm{Ker}\, \phi.$$

~~Pf~~

The isomorphism is given by:

$$\ker \phi \xrightarrow{\sim} \mathrm{Gal}\left(k(E_1) / \phi^* k(E_2) \right)$$
$$T \longmapsto \tau_T^*$$

Where $\tau_T : E_1 \to E_1$, $P \mapsto P+T$ (a degree-one morphism) $\Rightarrow$ induces an automorphism on $k(E_1)$.

Now, we show that τ_T^* fixes $\phi^* k(E_2)$:

Let $f \in k(E_2)$. $\tau_T^*(\phi^* f) = f \circ \phi \circ \tau_T = (\phi \circ \tau_T)^* f \overset{\text{because } T \in \ker\phi}{=} \phi^* f$

If we show now that we have m different elements τ_T^*, we are done (the ext. will be normal).

If $T \mapsto \tau_T^*$ is injective ($\Rightarrow$ it) so need to show that it is injective.

Prop 4.11: Let

$$\begin{tikzcd} & E_1 \arrow[dl, "\phi"'] \arrow[dr, "\psi"] & \\ E_2 & & E_3 \end{tikzcd}$$

such that $\underline{\ker \phi \subseteq \ker \psi}$. Then,

$$\begin{tikzcd} & k(E_1) \arrow[dl, dash, "\mathrm{Ker}\,\phi"'] \arrow[dr, dash, "\mathrm{Ker}\,\psi"] & \\ \phi^* k(E_2) \arrow[rr, dash, "\mathrm{Ker}\,\lambda"'] & & \psi^* k(E_3) \end{tikzcd}$$

And thus

$$\begin{array}{c} k(E_1) \\ | \\ \phi^* k(E_2) \\ | \\ \psi^* k(E_3) \end{array}$$

is a tower

Note that $\phi^{*-1}\psi\, k(E_3) \subseteq k(E_2)$.

Let $\lambda^* = \phi^{*-1}\psi^*$. Then the diagram commutes:

$$\begin{tikzcd} & E_1 \arrow[dl, "\phi"'] \arrow[dr, "\psi"] & \\ E_2 \arrow[rr, "\lambda"'] & & E_3 \end{tikzcd}$$

$\Updownarrow$

$\phi^*\lambda^* = \psi^* \iff (\lambda\circ\phi)^* = \psi^* \iff \boxed{\lambda\circ\phi = \psi}$

(to complete the proof of 6.1, apply this to

$$\begin{tikzcd} & E_1 \arrow[dl, "\phi"'] \arrow[dr, "{[m]}"] & \\ E_2 \arrow[rr, "\exists\hat\phi"'] & & E_1 \end{tikzcd}$$

Shows the existence. Need to prove the uniqueness!

Suppose $\exists\ \hat\phi'$ st $\hat\phi'\circ\phi = [m]$.

Then $(\hat\phi - \hat\phi')\circ\phi = [0]$, so as ϕ is nonconstant $\Rightarrow$ $\hat\phi = \hat\phi'$.

Example: Let $E: y^2 = x^3 + ax^2 + bx$ (not normal form!!), and let $Q = (0,0) \in E$.

Then $(x) = 2Q - 2O$, and so $[2]Q = O$. $\Rightarrow$ Q has order 2.

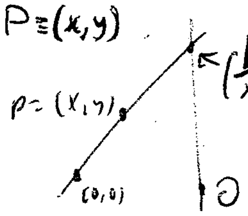
We want to construct an isogeny:

$$\phi : E_1 \longrightarrow E_2 \quad \text{with} \quad \operatorname{Ker}\phi = \{O, Q\}.$$

Let $\tau_Q : E_1 \to E_1$, $P \mapsto P + Q$. So τ_Q^* gives an automorphism on $k(E_1)$, of order 2.

What is the fixed field of τ_Q^*?

Let $P \equiv (x, y)$



$\left(\frac{b}{x}, \frac{b}{x^2}y\right) \to P' = \left(b/x, -\frac{b}{x^2}y\right)$

The functions u, v are fixed by τ_Q^*:

$u := x + \frac{b}{x} + a$

$v = y - \frac{b}{x^2}y$

Then (u, v) generate the fixed field under τ_Q^*. (check it!)

If we insert it,

$$u = x + \frac{b}{x} + a = \frac{y^2}{x^2} \quad \rightsquigarrow \quad \phi = (y^2 ; y(x^2 - b) : x^2)$$

$$v = y - \frac{b}{x^2} y$$

Then $E_2 = \phi(E_1)$: $v^2 = u^3 - 2au + (a^2 - 4b)u$.

So get

$$E_1 : y^2 = x^3 + ax^2 + bx \xrightarrow{\phi \text{ degree-2}} E_2 : v^2 = u^3 - 2au^2 + (a^2 - 4b)u$$

$b \neq 0$, $a^2 - 4b \neq 0$

Special case: $a = 4, b = 2$.

$$E_1 : y^2 = x^3 + 4x^2 + 2x \longrightarrow E_2 : v^2 = u^3 - 8u^2 + 8u$$

Now, scaling by $\sqrt{-2}$, we get $E_1 \cong E_2$.

If $\mathrm{End}(E) \neq \mathbb{Z}$, then E is called Complex Multiplication Curve. (CM).

- Properties of isogenies (prop 6.2 [Sil]).

(C) Let $\phi : E_1 \to E_2$, $\psi : E_1 \to E_2$ be isogenies. Then $\widehat{(\phi + \psi)} = \hat{\phi} + \hat{\psi}$.

i.e. $\mathrm{Hom}(E_1, E_2) \xrightarrow{\wedge} \mathrm{Hom}(E_2, E_1)$ is a group homomorphism.

(a) Let $m = \deg \phi$. Then

$\hat{\phi} \circ \phi = [m]_{E_1} \leftarrow$ from (6.1)

$\phi \circ \hat{\phi} = [m]_{E_2} \leftarrow (\phi \circ \hat{\phi}) \circ \phi = \phi \circ (\hat{\phi} \circ \phi) = \phi \circ [m]_{E_1} = [m]_{E_2} \circ \phi$ // $[m]$ commutes!

($\Rightarrow$ $\phi \circ \hat{\phi} = [m]_{E_2}$ because there are no zero divisors in $\mathrm{End}(E)$.)

(b) Let $\lambda : E_2 \to E_3$ be an isogeny. Then $\widehat{(\lambda \circ \phi)} = \hat{\phi} \circ \hat{\lambda}$

(Pf: $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\lambda} E_3 \Rightarrow E_3 \xrightarrow{\hat{\lambda}} E_2 \xrightarrow{\hat{\phi}} E_1$. If $m = \deg \phi$, $n = \deg \lambda$,

$$(\hat{\phi} \circ \hat{\lambda}) \circ (\lambda \circ \phi) = \hat{\phi} \circ [n] \circ \phi = \hat{\phi} \circ \phi \circ [n] = [m][n] = [mn].$$

By uniqueness of dual isogeny, $\hat{\phi} \circ \hat{\lambda} = \widehat{\lambda \circ \phi}$.

• Formal Groups.

Let R be a ring.

Def: A formal group $\mathcal{F}$ over R is a power series $F(X,Y) \in R[[X,Y]]$, which satisfies:

a) $F(X,Y) = X + Y + (\text{higher order terms})$.

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

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

d) $\exists!\ i(T) \in R[[T]]$ s.t. $F(X, i(X)) = 0$.

e) $F(X,0) = X$, $F(0,Y) = Y$

F is called the formal group law of $\mathcal{F}$.

Def An homomorphism of formal groups $(\mathcal{F}, f)$, $(\mathcal{G}, g)$ is a p.s. $f(T) \in R[[T]]$, <u>with no constant</u> term and satisfying:

$$f(F(X,Y)) = G(f(X), f(Y)).$$

Example:

- Formal additive group: $\hat{G}_a$: $F(X,Y) = X + Y$
- Formal multiplicative group: $\hat{G}_m$: $F(X,Y) = X + Y + XY$

Given a formal group $(\mathcal{F}, F)$.

Def: The multiplication-by-m homomorphism is defined:

$[m] : \mathcal{F} \to \mathcal{F}$. inductively:

$[0](T) = 0$; $[m+1](T) = F([m](T), T)$

$[m-1](T) = F([m](T), i(T))$.

Prop 2.3: Let $\mathcal{F}/R$, $m \in \mathbb{Z}$.

a) $[m](T) = mT + (\text{h.o.t.})$

b) If $m \in R^{\times}$, then $[m]$ is an isomorphism.

Pf a) $m=0$ ✓, $m \geq 0$. $[m+1](T) = F([m](T), T) = [m](T) + T + (\text{hot}) = (m+1)T + (\text{hot})$

b) $[mT] = mT + \text{hot}$. We construct an inverse:

Lemma 2.4: If $a \in R^{\times}$ & $f(T) \in R[[T]]$ s.t. $f(T) = aT + \cdots$ Then, $\exists!$ inverse $g(T) \in R[[T]]$ s.t $g(f(T)) = T$ & $f(g(T)) = T$.

Pf Construct the sequence of polynomials $g_n(T) \in R[T]$ s.t.

$f(g_n(T)) \equiv T \pmod{T^{n+1}}$, $g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$

Set $g_1(T) = a^{-1}T$. If have $g_{n-1}(T)$.

$f(g_{n-1}(T)) \equiv T \pmod{T^n} = T + bT^n \pmod{T^{n+1}}$. for some $b \in R$.

Set $\lambda = -a^{-1}b$, and $g_n(T) = g_{n-1}(T) + \lambda T^n$.

$f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n) = f(g_{n-1}(T)) + a\lambda T^n + \text{hot}$

$= T + bT^n + \text{hot} = T + (b + \lambda a)T^n + \text{hot} \equiv 0 \bmod T^{n+1}$.

For uniqueness,

if have $h(T)$ with $f(h(T)) = T$ then $g(T) = g(f(h(T))) = (g \circ f)(h(T)) = h(T)$ //

Suppose now that R is a <u>complete</u> local ring, with maximal $\mathfrak{m}$.

$\forall x, y \in \mathfrak{m}$, $F(x,y)$ and $i(x)$ will converge in R.

So define

Def The <u>group associated</u> to $\mathcal{F}/R$, denoted $\mathcal{F}(\mathfrak{m})$ to be $(\mathfrak{m}, \overset{\text{evaluating } F \text{ on points of } \mathfrak{m}}{F})$ $x \ast y := F(x,y)$.

So $\hat{\mathcal{F}}(\mathfrak{m})$ is a group and, $\forall m \geq n$, $\hat{\mathcal{F}}(\mathfrak{m}^n)$ are subgroups.

Example:

$\hat{G}_a(\mathfrak{m}) = (\mathfrak{m}, +)$: $F(x,y) = x+y$

$\hat{G}_a(\mathfrak{m}) \simeq 1 + \mathfrak{m}$, $(1+a)(1+b) = 1 + a + b + ab$

Prop 3.2:

a) $\forall n \geq 1$, $\hat{\mathcal{F}}(\mathfrak{m}^n) / \hat{\mathcal{F}}(\mathfrak{m}^{n+1}) \xrightarrow{\sim} \mathfrak{m}^n / \mathfrak{m}^{n+1}$ induced by the identity map of sets is an isomorphism

b) Let $p = \operatorname{char} k (= R/\mathfrak{m})$. Then every torsion element in $\hat{\mathcal{F}}(\mathfrak{m})$ has order a power of p.

Pf (a) The map is clearly a bijection of sets, $a + \hat{\mathcal{F}}(\mathfrak{m}^{n+1}) \longmapsto a + \mathfrak{m}^{n+1}$.
Need to check it is an homomorphism:

If $x, y \in \mathfrak{m}^n$, then $x + y + (\text{hot}) \equiv x + y \bmod \mathfrak{m}^{n+1}$ //

(b) $[p^a k](x) = 0 \Rightarrow [k][p^a](x) = 0$, so it is enough to show $\nexists$ nonzero torsion elements of order prime to p.

Pick $m \in \mathbb{Z}$ s.t $[m](x) = 0$ with $(p, m) = 1$.

$|m|_p = 1 \Rightarrow m \notin \mathfrak{m} \Rightarrow m \in R^\times$, so $[m]$ is an isomorphism, and hence $x = 0$. //

Start now with E/K : $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$.

Want $\hat{E}$:

Change variables $z = -\frac{x}{y}$, $w = -\frac{1}{y}$. $O = (0,0)$ in the zw-plane.

Also z is a local uniformizer at O.

Divide by $-y^3$ the original curve, and get

$w + \cdots = z^3 + \cdots \quad \Leftrightarrow w = f(z,w) = z^3 + (a_1 z + a_2 z^2) w + (a_3 + a_4 z) w^2 + a_6 w^3$

Recursively plug-in for w:

and get $W = z^3(1 + A_1 z + A_2 z^2 + \cdots)$

with $A_n \in \mathbb{Z}[a_1 \ldots a_6]$.

<u>Prop 1.1</u>: (a) This procedure converges to a <u>unique</u> power series:

$W(z) = \cdots$

Satisfying $w(z) = f(z, w(z))$.

(b) If weight$(a_i) = i$, then A_j are homogeneous of weight j.

We can change the coefficients back,

$x(z) = \frac{z}{w(z)}$, $y(z) = \frac{-1}{w(z)}$ obtain $(x(z), y(z))$, a <u>formal point</u> in E.

If k is complete, then $\mathcal{O}_k = R \supseteq \mathfrak{m}$. Then

$\forall z \in \mathfrak{m}$, $(x(z), y(z))$ converges to a point $\in E(k)$.

$\mathfrak{m} \hookrightarrow E(k)$

$z \longmapsto (x(z), y(z))$

The image of $\mathfrak{m}$ in $E(k)$ is $\{(x,y) \in E(k) \mid xy^{-1} \in \mathfrak{m}\}$

If $(x,y) \in$ Image then we can recover z by $z := \frac{x}{y}$.

Pick z_1, z_2 indeterminates, let $w_i := w(z_i)$, so (z_i, w_i) are two points on E.

$\lambda := \frac{w_2 - w_1}{z_2 - z_1} \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]$ is the slope of the line through (z_i, w_i)

~~Then $v = w_1 - \lambda z_1$ is the~~ So $w = \lambda z + v$ → line through the points. ($v = w_1 - \lambda z_1$)

Plug this into the Weierstrass equation for E.

Get a cubic in z, with 2 roots being z_1, z_2 and solve for the 3rd, z_3.

and then express z_3 in terms of z_1 and z_2.

So get a power series $Z_3(Z_1, Z_2) \in \mathbb{Z}[a_1, \dots, a_6][[Z_1, Z_2]]$.

In the xy-plane, the eq. for the negative for (x, y) is $(x, -y - a_1x - a_3)$.

As $z = \frac{-x}{y}$, the z-coordinate of $-(z_1 \cdot w_3)$ is $\dfrac{x(z)}{y(z) + a_1 x(z) + a_3} =: i(z)$

Define now $F(z_1, z_2) := i(z_3(z_1, z_2)) = z_1 + z_2 + \underbrace{(-a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2)) \cdots}_{\text{terms of order} \geq 2.}$ $\in \mathbb{Z}[a_1, \dots, a_6][[z]]$

check that linear terms ok!

- $F(z_1, z_2) = F(z_2, z_1)$
- $F(z_1, F(z_2, z_3)) = F(F(z_1, z_2), z_3)$
- $F(z, i(z)) = 0$.

easy!

So $F(z_1, z_2)$ is a formal group law. Given an elliptic curve E, then the <u>formal group associated</u> to E, noted $\hat{E}$, is defined by $F(z_1, z_2)$.

<u>Fact</u>: The map $\hat{E}(m) \longrightarrow E(k)$, $z \longmapsto (x(z), y(z))$ is a <u>group homomorphism</u>. (by construction).

- Elliptic Curves over Local Fields (chap VII).

Let K be a (complete) local field. (complete wrt a discrete valuation v) s.t. $\bar{k} = \mathcal{O}_K/m\mathcal{O}_K$ is finite

$\mathcal{O}_K : R : \{x \in K \mid v(x) \geq 0\}$, $m = \{x : v(x) > 0\}$, $R^* : \{x : v(x) = 0\}$.

Let π be a uniformizer for R $(m = \pi R)$, $k = R/m$. $(v(\pi) = 1,\ v(0) := \infty)$.

Let E/K be an elliptic curve over E, with Weierstrass model $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

Recall that the only iso's of E preserving $[0:1:0]$ and the Weierstrass equation.

$$(x, y) \longmapsto (u^2x + r,\ u^3y + u^2sx + t).$$

If we apply $(x, y) \mapsto (u^2x, u^3y)$, $u \in K^*$ then it sends a_i to $u^i a_i$

So for a sufficiently large u, we can express E over R.

The discriminant Δ is a polynomial in a_i's, so if we have E/R,

then $\Delta \in R$, so $v(\Delta) \geq 0$.

Since v is discrete, can choose an eq'n for E s.t. E/R and $v(\Delta)$ is minimal.

Def: Such an equation is called the (unique up to units!) minimal Weierstrass eq'n of E at v.

Question: How can one tell if a W. eq'n is minimal?

Ans: By chap 3.1 [Sil], $(x,y) \overset{(*)}{\mapsto} (u^{-2}x, u^{-3}y)$ changes Δ to $u^{12}\Delta$, so

(I) looking at the discriminant is enough: if $a_i \in R$ and $v(\Delta) < 12$ then the eq'n is minimal.

(II) Also, have c_4 and c_6 invariants. These change under $(*)$ with $\begin{cases} c_4 \mapsto u^4 c_4 \\ c_6 \mapsto u^6 c_6 \end{cases}$

So another test is: if $a_i \in R$ and $v(c_4) < 4$ or $v(c_6) < 6$ then eq'n is minimal.

Example: $y^2 + xy + y = x^3 + x^2 + 22x - 9$ over $\mathbb{Q}_p$.

has $\Delta = -2^{15}5^2$

Test I is inconclusive, but test II says $c_4 = -5 \cdot 211$, so eqn is minimal at every prime p.

Example: $y^2 = x^3 + 16$, has $\Delta = -2^{12}3^3$, $c_4 = 0$

Prop:

a) Every elliptic curve $/K$ has a minimal Weierstrass equation (at v). (Pf: v is discrete)

b) A minimal W. eqn is unique up to $(x,y) \overset{(*)}{\mapsto} (u^2x + r, u^3y + u^2sx + t)$. $\begin{cases} u \in R^\times \\ r,s,t \in R. \end{cases}$

• Reduction mod π:

K a field, $R=\{x\in K: v(x)\geq 0\}$, $m=\{x\in K; v(x)>0\}$; $m=\pi R$, π an uniformizer.

We have a map $\rho: R\to k=R/m$
$t\mapsto t+\pi R=\tilde{t}$

If $x\in K$, and $v(x)<0$, then define $\rho(x):=\infty$. So we get $\rho: \mathbb{P}^1(K)\to\mathbb{P}^1(k)$

$E/K: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ a minimal model.

We can then set the reduction of E at π, by reducing the coefficients.

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

Note: $\tilde{E}$ can be singular, even if E is nonsingular.

If $P\in E(K)$, $P=[x_0,y_0,z_0]$, with at least one of the coordinates in $R^\times$ (and the rest in R)

Can define $\tilde{P}=[\tilde{x}_0,\tilde{y}_0,\tilde{z}_0]\in\tilde{E}(k)$.

So we get $\rho: E(K)\to\tilde{E}(k)$.

Even if $\tilde{E}(k)$ is singular, by [prop III 2.5] it contains $\tilde{E}_{ns}(k)$, which is a group (open).

Def: $E_0(K):=\{P\in E(K): \tilde{P}\in\tilde{E}_{ns}(k)\}$.
$E_1(K):=\{P\in E(K): \tilde{P}=\tilde{O}\}$.

Prop 2.1: $\exists$ an exact sequence of AbGp $0\to E_1(K)\to E_0(K)\to\tilde{E}_{ns}(k)\to 0$

Pf/ First, show that E_0 and E_1 are Abgps:

$P_1,P_2\in E_0(K)$, on line ℓ. Then $Q=-(P_1+P_2)\in\ell$, but $Q\in E(K)$.

As $\rho:\mathbb{P}^2(K)\to\mathbb{P}^2(k)$ takes lines to lines, so $\tilde{Q}$ lies in the line through $\tilde{P}_1$ and $\tilde{P}_2$. But as $\tilde{P}_1$ and $\tilde{P}_2\in\tilde{E}_{ns}(k)$, $\tilde{Q}\in\tilde{E}_{ns}(k)\Rightarrow E_0$ gp.

As $\rho(P_1+P_2)=-\tilde{Q}=\tilde{P}_1+\tilde{P}_2=\rho(P_1)+\rho(P_2)$, so ρ is a homomorphism,

and $E_1(K)$ is also a group because it is the kernel of ρ.

~~So~~ We get exactness because ρ is ~~everything~~ a surjection.

Write $f(x,y)=0$ for the eq. of E. Let $\tilde{f}(x,y)=0$ the corresponding reduced poly'l.
Let $\tilde{P}=(\alpha,\beta)\in \tilde{E}_{ns}(k)$. Since $\tilde{P}$ is nonsingular, one of $\frac{\partial \tilde{f}}{\partial x}(\tilde{P})\neq 0$ or $\frac{\partial \tilde{f}}{\partial y}(\tilde{P})\neq 0$.
Suppose $\frac{\partial \tilde{f}}{\partial x}(\tilde{P})\neq 0$.

Pick any $y_0\in R$ s.t. $\tilde{y}_0=\beta$, so $f(x,y_0)$ is a polynomial in K such that $\tilde{f}(x,\tilde{y}_0)=0$ has α as a simple root (because $\frac{\partial \tilde{f}}{\partial x}(\alpha,\beta)\neq 0$).
By Hensel's lemma, $\exists x_0\in R$ s.t. $\tilde{x}_0=\alpha$ and $f(x_0,y_0)=0$.
So $P=(x_0,y_0)$ is s.t. $\rho(P)=\tilde{P}$, and $P\in E_0(K)$. //

Aside: If $v(\Delta)=0 \Rightarrow \Delta\in R^\times \Rightarrow \tilde{E}$ is nonsingular. So in this case, $\tilde{E}_{ns}=\tilde{E}$ and $E_0(K)=E(K)$, so we get $0\to E_1(K)\to E(K)\to \tilde{E}(k)\to 0$

Prop: Let E/K be given by a minimal Weierstrass equation.
Let $\hat{E}(R)$ be the associated formal group.
$w(z)=z^3(1+\cdots)\in R[[z]]$ be the power series corresponding to $\hat{E}$.
Then, $\hat{E}(m)\longrightarrow E_1(K)$ is an isomorphism.

$$z\longmapsto\left(\frac{z}{w(z)},\frac{-1}{w(z)}\right)$$
$$0\longmapsto \mathcal{O}$$

Pf/

By Chap 4, $\left(\frac{z}{w(z)},\frac{-1}{w(z)}\right)\in E(K)\ \forall z\in m$.
$v\left(\frac{-1}{w(z)}\right)=-v(w(z))=-3v(z)$ and $v\left(\frac{z}{w(z)}\right)=-2v(z)$.
So $\left(\frac{z}{w(z)},\frac{-1}{w(z)}\right)\xrightarrow{\rho}\tilde{\mathcal{O}}\in\tilde{E}_{ns}(k)$, so $\left(\frac{z}{w(z)},\frac{-1}{w(z)}\right)\in E_1(K)$ and thus the map is well-defined.

(cont proof).

We have already shown that this is a group homomorphism.

It is injective, because $w(z)=0 \iff z=0$.

Let $(x,y) \in E_1(K)$. Since $(x,y) \xmapsto{f} \textcircled{o}$, $v(x)<0$, $v(y)<0$.

But from $y^2+\cdots = x^3+\cdots \Rightarrow 2v(y)=3v(x) = -6r$, $r \in \mathbb{Z}^+$.

So $v\left(\frac{x}{y}\right) = v(x)-v(y) = r > 0$, and thus $\frac{x}{y} \in \mathfrak{m}$.

And hence $\begin{array}{ccc} E_1(K) & \longrightarrow & \hat{E}(\mathfrak{m}) \\ (x,y) & \longmapsto & \left(\frac{-x}{y}\right) \end{array}$ is well defined.

This map is also an homomorphism, by construction of F.

It is injective because only $O \longmapsto 0$.

So we get $\begin{array}{ccccc} \hat{E}(\mathfrak{m}) & \hookrightarrow & E_1(K) & \hookrightarrow & \hat{E}(\mathfrak{m}) \\ z & \longmapsto & \left(\frac{z}{w(z)}, \frac{-1}{w(z)}\right) & \longmapsto & z \end{array}$ $\Rightarrow$ //

<u>Prop 3.1</u>: E/K, $m \geq 1$ integer relatively prime to $\operatorname{char}(k)$.

a) $E_1(K)$ has no torsion of order m.

b) If $\tilde{E}$ is nonsingular, then $E(K)[m] \xhookrightarrow{\rho} \tilde{E}(k)$ is injective

Pf

(a) $E_1(K) \cong \hat{E}(\mathfrak{m})$ and have shown that (IV. 3.2(b)) $\hat{E}(\mathfrak{m})$ has no torsion of order m.

(b): If $\tilde{E}$ is nonsingular, have $0 \longrightarrow \hat{E}(\mathfrak{m}) \longrightarrow E(K) \xrightarrow{f} \tilde{E}_{ns}(k) \longrightarrow 0$

$$\hat{E}(\mathfrak{m}) = E_1(K), \quad E(K) = E_0(K), \quad \tilde{E}_{ns}(k) = \tilde{E}_{ns}(k)$$

Since $\hat{E}(\mathfrak{m})$ has no m-torsion, apply the torsion "functor" and done //

(Back to isogenies, chap 6)

We prove property (c) of 6.2 [Sil]: $\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$.

It suffices to show that for a generic point,

$[(x_2, y_2) - O] \in \mathrm{Pic}^0(E_2)$.

a "generic point"

$(\phi+\psi)^*(x_2,y_2) - \phi^*(x_2,y_2) - \psi^*(x_2,y_2) = 0 \in \mathrm{Pic}^0(E_1/K(x_2,y_2))$

Let $K(E_2) = K(x_2, y_2)$, the function field of E_2/K $\quad (E_2 : F_2(x_2,y_2) = 0)$

Let $K(E_1) = K(x_1, y_1)$ $\quad (E_1 : F_1(x_1, y_1) = 0)$

Then $K(x_1, x_2, y_1, y_2) = \underbrace{K(x_2,y_2)(E_1)}_{\text{f.f. of } E_1/K(x_2,y_2)} = \underbrace{K(x_1,y_1)(E_2)}_{\text{f.f. of } E_2/K(x_1,y_1)}$

So have:

$$E_1 \xrightarrow{\phi} E_2 \qquad (x_1,y_1) \longmapsto Q_\phi = \phi(x_1,y_1)$$

$$E_2 \xrightarrow{\psi} E_1 \qquad (x_1,y_1) \longmapsto Q_\psi = \psi(x_1,y_1)$$

and

$$E_1 \xrightarrow{\phi+\psi} E_2 \qquad (x_1,y_1) \longmapsto Q_{\phi+\psi} = (\phi+\psi)(x_1,y_1)$$

So $\exists f \in K(E_1)(x_2,y_2)$ $(= K(x_1,y_1,x_2,y_2))$ s.t. $(f) = Q_{\phi+\psi} + O_2 - Q_\phi - Q_\psi$

As a function in (x_2,y_2), f has a zero at $(\phi+\psi)(x_1,y_1)$ and at O_2, and a pole at $\phi(x_1,y_1)$ and $\psi(x_1,y_1)$

Now consider f as a function in x_1, y_1 (i.e. $f \in K(E_2)(x_1,y_1)$

$f(x_1,y_1,(\phi+\psi)(x_1,y_1)) = 0$

$f(x_1,y_1,\phi(x_1,y_1)) = \infty$ $\longrightarrow$ $f(-,-,x_2,y_2)$ has

$f(x_1,y_1,\psi(x_1,y_1)) = \infty$ ")

a zero at P's when $(\phi+\psi)(P) = (x_2,y_2)$, or when P is independent of (x_2,y_2)

and a pole at Q's where $\phi(Q) = (x_2,y_2)$ or $\psi(Q) = (x_2,y_2)$

(and at $f(x_1,y_2,O_2) = 0$)

So we get, for $f \in K(E_2)(x_1,y_1)$, $(f) = (\phi+\psi)^*(x_2,y_2) + \overset{\text{does not depend on } (x_2,y_2)}{R} - \phi^*(x_2,y_2) - \psi(x_2,y_2)$

In $\mathrm{Pic}^0(K(E_2)(x_1,y_1))$ we see that ~~$(\phi+\psi)^*\ldots+R$~~ $[R] = [0]$ so done! //

(more properties) (6.2)

(d) For $m \in \mathbb{Z}$, $\widehat{[m]} = [m]$. (OK for $m = -1, 0, 1$. Now use (c) + induction).

(e) $\deg \hat{\phi} = \deg \phi$.

Pf For $\phi = [m]$, note that $\deg \hat{\phi} = \deg \phi = \deg [m] = m^2$.

$\underbrace{\hat{\phi} \circ \phi}_{\text{degree } m} = [m] \leftarrow$ degree m^2 $\Rightarrow \deg \hat{\phi} = m$ //

(f) $\hat{\hat{\phi}} = \phi$: $\widehat{\hat{\phi} \circ \phi} \overset{\text{by (b)}}{=} \hat{\phi} \circ \hat{\hat{\phi}}$. Also, since

$(\hat{\phi} \circ \phi) \circ (\hat{\phi} \circ \phi) = [m^2]$, have $\hat{\phi} \circ \phi = \widehat{\hat{\phi} \circ \phi}$. So $\hat{\phi} \circ \phi = \hat{\phi} \circ \hat{\hat{\phi}} \Rightarrow \phi = \hat{\hat{\phi}}$ //

__Corollary 6.3:__
The degree map $\deg : \mathrm{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$ is a positive definite quadratic form.

Def A map $d : A \to \mathbb{R}$, A an Ab Gp, is a __quadratic form__ if

(1) $d(\alpha) = d(-\alpha)$

(2) The map $A \times A \to \mathbb{R}$

$(\alpha, \beta) \longmapsto d(\alpha+\beta) - d(\alpha) - d(\beta)$ is __bilinear__.

A quadratic form is __positive definite__ if, moreover:

(3) $d(\alpha) \geq 0 \quad \forall \alpha \in A$

(4) $d(\alpha) = 0 \iff \alpha = 0$

__Pf of corollary:__

(1) OK, (3) OK, (4) OK.

(2) Need to verify that $\deg(\alpha+\beta) - \deg(\alpha) - \deg(\beta)$ is bilinear.

As $\mathbb{Z} \hookrightarrow \mathrm{End}(E_1)$, can work in $\mathrm{End}(E_1)$.

$[\deg(\alpha+\beta)] - [\deg(\alpha)] - [\deg(\beta)] = \widehat{(\alpha+\beta)} \circ (\alpha+\beta) - \hat{\alpha} \circ \alpha - \hat{\beta} \circ \beta \overset{6.3c}{=}$

$= (\hat{\alpha} + \hat{\beta}) \circ (\alpha+\beta) - \hat{\alpha} \circ \alpha - \hat{\beta} \circ \beta = \hat{\alpha} \circ \beta + \hat{\beta} \circ \alpha$ This expression is bilinear (by again 6.3 C) //

Proposition 6.4: Let m be coprime to $\mathrm{char}(K)$. Then,

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

as $p \nmid m$, $\deg_s[m] = \deg[m]$

Pf/ We know that $\# E[m] = m^2$ $(= \mathrm{Ker}\,[m] = \deg_s[m] = m^2)$.

The torsion $E[m]$ cannot be of rank ≥ 3, for then there exists $p \mid m$, $E[p] \supseteq (\mathbb{Z}/p\mathbb{Z})^3 \Rightarrow$ contradiction.

Example (of an inseparable morphism):

Let $E/\mathbb{F}_2 : y^2 + y = x^3 - x$

Then $\phi : (x,y) \longmapsto (x^2, y^2)$ is inseparable of degree 2. (Frobenius)

Def/ The ℓ-adic Tate Module for E/K (ℓ a prime $\ell \nmid \mathrm{char}\,K$) is

$$T_\ell(E) := \varprojlim_n E[\ell^n]$$

(Note that $\phi : E_1 \to E_2$ induces maps $\phi : E_1[\ell^n] \to E_2[\ell^n]$, and so ϕ induces $\tilde{\phi} : T_\ell(E_1) \to T_\ell(E_2)$)

$$\left(\begin{tikzcd} & T_\ell(E) \arrow[dl, "\pi^{n+1}"'] \arrow[dr, "\pi^n"] & \\ E[\ell^{n+1}] \arrow[rr, "{[\ell]}"] & & E[\ell^n] \end{tikzcd} \right)$$

Prop 7.1: For ℓ prime, $\ell \nmid \mathrm{char}\,K$, $T_\ell(E) \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ as $\mathbb{Z}_\ell$-modules

ℓ-adic integers

Theorem 7.4:

$$\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E_1), T_\ell(E_2))$$ is injective.

Corollary 7.5: $\mathrm{rk}_{\mathbb{Z}}\, \mathrm{Hom}(E_1, E_2) \leq 4$.

In particular, $\mathrm{rk}_{\mathbb{Z}}\, \mathrm{End}(E) \leq 4$

Pf/

$$\mathrm{Hom}_{\mathbb{Z}_\ell}(\underbrace{T_\ell(E_1)}_{\cong\, \mathbb{Z}_\ell \times \mathbb{Z}_\ell}, \underbrace{T_\ell(E_2)}_{\cong\, \mathbb{Z}_\ell \times \mathbb{Z}_\ell}) \simeq M_2(\mathbb{Z}_\ell)$$

//

(iii) How does the result of (ii) square with the result proved in the text that a cubic curve has at most one singularity?

3. Let $F(\mathbf{x})$ be as in the previous question and suppose that $F(\mathbf{x}) = 0$ is non-singular.

(i) Let $F(\mathbf{x}) = 0$. Show that the third intersection $\mathbf{t}$ of the tangent at $\mathbf{x}$ is given by

$$t_j = x_j(a_{j+1}x_{j+1}^3 - a_{j+2}x_{j+2}^3) \quad (j = 1, 2, 3),$$

where the suffixes are taken mod 3.

(ii) Let $\mathbf{x}$, $\mathbf{y}$ be distinct points on $F(\mathbf{X}) = 0$. Show that the third intersection $\mathbf{z}$ of the line joining them is given by

$$z_j = x_j^2 y_{j+1} y_{j+2} - y_j^2 x_{j+1} x_{j+2}.$$

[Formulae of Desboves].

4. Starting with the solution $(2, -1, -1)$ of $X^3 + Y^3 + 7Z^3 = 0$, find 10 distinct solutions.

7

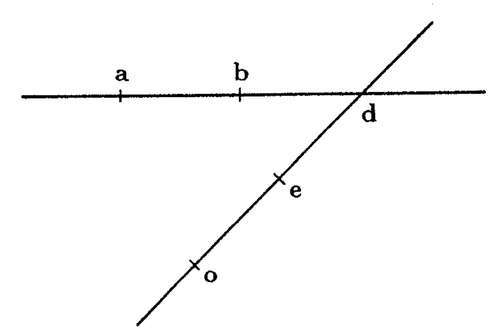
Non-singular cubics. The group law

Let $\mathcal{C}$ be a non-singular cubic curve and let $\mathbf{o}$ be a rational point on $\mathcal{C}$. We show that the set of rational points on $\mathcal{C}$ has a natural structure of commutative group with $\mathbf{o}$ as neutral element ("zero").

Here the ground field is arbitrary, the curve $\mathcal{C}$ is defined over it; and by rational point we mean point defined over the ground field.

The group law is defined as follows. Let $\mathbf{a}$, $\mathbf{b}$ be rational points. Let $\mathbf{d}$ be the third point of intersection with $\mathcal{C}$ of the line through $\mathbf{a}$, $\mathbf{b}$. Let $\mathbf{e}$ be the third point of intersection of the line through $\mathbf{o}$, $\mathbf{d}$. Then we write

$$\mathbf{a} + \mathbf{b} = \mathbf{e}.$$



The construction has to be interpreted appropriately if two or more of the points involved coincide. For example if $\mathbf{b} = \mathbf{a}$ we take the tangent at $\mathbf{a}$.

Pf (of thm 7.4):

Let $M \subseteq \mathrm{Hom}(E_1, E_2)$ be a finitely generated subgroup (note that then M is torsion free)

Let $M^{div} := \{ \phi \in \mathrm{Hom}(E_1,E_2) : [m] \circ \phi \in M, \text{ for some } m \geq 1 \} \supseteq M$.

Claim: M^{div} is finitely generated:

Consider M^{div} as a discrete subgroup of a finite-dimensional real vectorspace.

If we can do so, then it is f-gen (discrete subgps of fin-dim. vecspaces are f-gen).

M has no torsion + f-generated!

For f.d. vectorspace, choose $M \otimes_{\mathbb{Z}} \mathbb{R}$. ($M$ is free as $\mathbb{Z}$-module).

Now, see that $M^{div} \subseteq M \otimes \mathbb{R}$ is discrete.

Use the pairing $(\alpha, \beta) := \deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta)$.

$(\cdot,\cdot) : M \times M \longrightarrow \mathbb{R}$

This can be extended to a pairing $(\cdot,\cdot) : M \otimes \mathbb{R} \times M \otimes \mathbb{R} \longrightarrow \mathbb{R}$.

Use this pairing to degree map to $M \otimes \mathbb{R}$, using $(\alpha,\alpha) = 2\deg(\alpha)$.

open

Then $M^{div} \cap \{ \phi \in M \otimes \mathbb{R} : \underbrace{\deg \phi}_{\frac{(\phi,\phi)}{2}} < 1 \} = \{ \phi = 0 \}$.

Consider now $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E_1), T_\ell(E_2))$

$$\phi \longmapsto \phi_\ell$$

Suppose $\phi_\ell = 0$.

We may choose $M \subseteq \mathrm{Hom}(E_1, E_2)$, M f-gen s.t. $\phi \in M \otimes \mathbb{Z}_\ell$.

Say $\phi = \alpha_1 \phi_1 + \dots + \alpha_t \phi_t$, where $\alpha_i \in \mathbb{Z}_\ell$, $\phi_i \in M^{div}$, $\{\phi_i\}$ a $\mathbb{Z}_\ell$-basis for M^{div}.

Choose $n \in \mathbb{Z}_{>0}$. There exists $a_i \in \mathbb{Z}$ s.t. $a_i \equiv \alpha_i \pmod{\ell^n}$

Then $\psi := a_1 \phi_1 + \dots + a_t \phi_t \in M$, and $\psi \equiv \phi \pmod{[\ell^n]}$

Since ϕ annihilates $E_1[\ell^n]$, then $E_1[\ell^n] \subseteq \ker \psi$. (because ϕ and $\phi - \psi$ vanish in $E_1[\ell^n]$).

$$\begin{tikzcd} & E_1 \arrow[dl, "{[\ell^n]}"'] \arrow[dr, "\psi"] & \\ E_1 \arrow[rr, dotted, "\exists\lambda"] & & E_2 \end{tikzcd}$$

$\exists \lambda : E_1 \longrightarrow E_2$ s.t. $\psi = \lambda \circ [\ell^n]_{E_1} = [\ell^n]_{E_2} \circ \lambda \Rightarrow \lambda \in M^{div}$

As $\lambda \in M^{div}$, write $\lambda = b_1\phi_1 + \cdots b_t\phi_t$, with $b_i \in \mathbb{Z}$.
$\psi = a_1\phi_1 + \cdots + a_t\phi_t$

Because $\psi = \lambda \circ [\ell^n] = [\ell^n]\circ\lambda$, get.

$[a_i] = [\ell^n]\circ[b_i]$ and $a_i \equiv 0 \pmod{\ell^n}$.

As n is arbitrary, $a_i = 0 \Rightarrow \alpha_i = 0 \Rightarrow \phi = 0$ //

Corollary: $rk_{\mathbb{Z}}(\mathrm{End}(E)) \leq 4$.

End(E) has the following properties.

Prop:

(1) End(E) is a characteristic-0 integral domain of $rk_{\mathbb{Z}}(\mathrm{End}(E)) \leq 4$.

(2) End(E) possesses an anti-involution $\phi \mapsto \hat{\phi}$ $\left(\begin{array}{l}\widehat{\phi+\psi} = \hat{\phi}+\hat{\psi} \\ \widehat{\phi\psi} = \hat{\psi}\hat{\phi} \\ \hat{\hat{\phi}} = \phi\end{array}\right)$

(3) $\hat{\phi}\phi \in \mathbb{Z}$, $\hat{\phi}\phi \geq 0$ and equality holds iff $\phi = 0$.

Theorem 9.3: A ring R with properties (1), (2), (3) is of one of the following types:

a) $R = \mathbb{Z}$

b) R is an order in a imaginary quadratic number field

c) R is an order in a quaternion (definite) algebra.

Def An order R in a $\mathbb{Q}$-algebra K is a subring R of K such that R is finitely-generated over $\mathbb{Z}$ and $R \otimes_{\mathbb{Z}} \mathbb{Q} = K$.

Def A quaternion algebra is an algebra of the form.

$K = \mathbb{Q} \oplus \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ s.t $\alpha^2, \beta^2 \in \mathbb{Q}$, $\beta\alpha = -\alpha\beta$.

K is definite if $\alpha^2 < 0$ and $\beta^2 < 0$

<u>Proof of thm 9.3:</u>

If $K=\mathbb{Q}$, we are done: type (a).

Otherwise, let $\alpha \in K \setminus \mathbb{Q}$.

Let $T\alpha := \hat{\alpha}+\alpha$. After replacing, if necessary, α with $\alpha - \frac{T\alpha}{2}$, we may assume that $T\alpha = 0$.

the norm is always nonnegative.

Then the norm of α, $N\alpha = \hat{\alpha}\alpha = -\alpha^2 > 0$

If $K=\mathbb{Q}(\alpha)$, then we are done (Type b).

Otherwise, let $\beta \in K \setminus \mathbb{Q}(\alpha)$. We may assume that $T\beta = T\alpha\beta = 0$

(after replacing β with $\beta - \frac{\overset{\in\mathbb{Q}}{T\beta}}{2} - \frac{1}{2}\left(\underbrace{\frac{T(\alpha\beta)}{\alpha^2}}_{\in\mathbb{Q}}\right)\alpha$)

$0 < N\beta = \hat{\beta}\beta = -\beta^2$.

We only need to verify that $\beta\alpha = -\alpha\beta$:

$$T(\alpha\beta)=0 \iff \widehat{\alpha\beta}+\alpha\beta=0 \iff \hat{\beta}\hat{\alpha}+\alpha\beta=0 \iff (-\beta)(-\alpha)+\alpha\beta=0 \iff \beta\alpha=-\alpha\beta.$$

If $K=\mathbb{Q}(\alpha,\beta)$, then K is of Type c

$$\begin{tikzcd} K=\mathrm{End}(E)\otimes\mathbb{Q} \arrow[d, dash] \\ \mathbb{Q}(\alpha,\beta) \arrow[d, dash, "4"] \\ \mathbb{Q} \end{tikzcd} \Rightarrow K=\mathbb{Q}(\alpha,\beta) \text{ as vectorspaces}$$

Now we prove the Riemann Hypothesis for Elliptic Curves over finite fields.

<u>Thm IV.1.</u>: Let $k=\mathbb{F}_q$ be a finite field, and let E/k an elliptic curve.

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

Pf Consider $\phi: E \to E$ be the q-Frobenius endomorphism, $\phi(x,y)=(x^q,y^q)$

For $P \in E(\mathbb{F}_q)$, $\phi(P)=P$. Also, $\phi(P)=P \Rightarrow P\in E(\mathbb{F}_q)$.

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

<u>Claim</u>: $1-\phi$ is a separable morphism.

If we assume $1-\phi$ is separable, $\# \ker(1-\phi) = \deg 1-\phi =$
$\left(= (1-\phi)\widehat{(1-\phi)} = (1-\phi)(1-\hat{\phi}) = 1 - T(\phi) + N(\phi). \right)$

As $L(\phi,\psi) = \deg(\phi - \psi) - \deg(\phi) - \deg(\psi)$ is a quadratic form,

$|L(\phi,\psi)| \leq 2\sqrt{\deg(\phi)\deg(\psi)}$ by ~~Cauchy-Schwarz~~. Cosine rule: $(a^2 = b^2 + c^2 - 2bc\cos\theta)$ $\Rightarrow |a^2 - b^2 - c^2| \leq 2bc$)

$\Big[0 \leq \deg(m\phi - n\psi) = m^2 \deg(\phi) - mn\, L(\phi,\psi) + n^2 d(\psi) \quad \forall m,n \in \mathbb{Z}$

Thus $(L(\phi,\psi))^2 - 4\deg(\phi)\deg(\psi) \leq 0$

If $1-\phi$ was not separable, $|E(k)| = \deg_s(1-\phi) \leq \deg 1-\phi$

So we get anyway that $\#E(k) \leq q+1+2\sqrt{q}$. Still want the lower bound!

Let $E: y^2 = x^3 + ax + b$ have $\#E(k) = q+1-t$, and let

d be a nonsquare in K.

Then $E': dy^2 = x^3 + ax + b$ has $\#E'(k) = q+1+t$.

Putting this information together, we conclude that $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$

- Classification of elliptic curves in char $= 2$.

$j \neq 0$ $E: y^2 + xy = x^3 + a_2 x^2 + a_6 \qquad \Delta = a_6,\ j = \frac{1}{a_6} \quad (a_6 \neq 0)$

$j = 0$ $E: y^2 + a_3 y = x^3 + a_4 x + a_6 \qquad \Delta = a_3^4,\ j = 0 \quad (a_3 \neq 0)$

These are all the non-isomorphic elliptic curves.

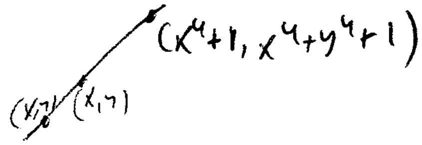
<u>Ex:</u> over $\mathbb{F}_2$, the complete list is:

	# points	j-inv
$E_1: y^2 + y = x^3 + x + 1$	1	0
$E_2: y^2 + xy = x^3 + 1$	2	1
$E_3: y^2 + y = x^3$	3	0
$E_4: y^2 + xy = x^3 + x^2 + 1$	4	1
$E_5: y^2 + y = x^3 + x$	5	0

<u>Example</u>: $E_5: y^2+y=x^3+x$

We will compute the number of solutions $\#E(\mathbb{F}_{2^m})$ for all $m \geq 1$.

Let $P=(x,y)$ be ~~a~~ point in $E(\bar{K})$



As $dy=(x^2+1)\,dx$, get the line tangent to (x,y) is $(Y-y)=(x^2+1)(X-x)$.

For $X=x^4+1$, $x^4+y^4+y+1=(x^2+1)(x^4+x+1)$. So $2(x,y)=(x^4+1, x^4+y^4)$

$$\begin{tikzcd}
E \arrow[rr, "{[2]}"] \arrow[dr, "\phi"'] & & E \\
& E \arrow[ur, "\hat{\phi}"'] &
\end{tikzcd}$$

$(x,y) \longmapsto (x^4+1, x^4+y^4)$

$(x,y) \longmapsto (x^2,y^2)$

So $\boxed{\hat{\phi}(x,y)=(x^2+1, x^2+y^2)}$

<u>Remark</u>: for E_5, ϕ and $\hat{\phi}$ are inseparable (purely inseparable) and thus $[2]$ is purely inseparable.

In particular, $E_5[2]=\{O\}$.

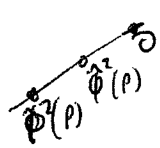
So $\phi+\hat{\phi} \in \mathbb{Z} \subseteq \text{End}(E)$.

<u>Lemma</u>: $[\#E(\mathbb{F}_q)] = [q+1] + [-1]\circ(\phi+\hat{\phi})$

Pf $\deg(1-\phi) = (1-\phi)(1-\hat{\phi}) = 1-(\phi+\hat{\phi}) + \overbrace{\phi\hat{\phi}}^{\deg\phi} \in \mathbb{Z} \Rightarrow \phi+\hat{\phi} \in \mathbb{Z}$.

<u>Note</u>: $\phi^2(x,y)=(x^4,y^4)$
$\hat{\phi}^2(x,y)=(x^4,y^4+1)$ $\Big\} \Rightarrow \phi^2+\hat{\phi}^2=[0]$

So, $\forall P$,



$\Rightarrow \#E(\mathbb{F}_4) = 4+1-(\phi^2+\hat{\phi}^2) = 5$. ($\hat{\phi}^2=\widehat{\phi^2}$)

Compute $\phi(P)+\hat{\phi}(P) = (x^4+1, x^4+y^4+1) = [-2](P)$

So $\#E(\mathbb{F}_2) = 2+1-(-2) = 5$.

Now, $\#E(\mathbb{F}_{2^m}) = 2^m + 1 - (\phi^m + \hat{\phi}^m)$.

$$(t-\phi)(t-\hat{\phi}) = t^2 - (\phi+\hat{\phi})t + \phi\hat{\phi} = t^2 - 2t + 2 \implies$$

$$1\cdot(\phi^{m+2} + \hat{\phi}^{m+2}) + 2(\phi^{m+1} + \hat{\phi}^{m+1}) + 2(\phi^m + \hat{\phi}^m) = 0$$

Let $k = \mathbb{F}_q$

Let C be a curve, $C = V(I) \subseteq \mathbb{P}^n(k)$, some (prime) ideal $I \subseteq k[x_0, \dots, x_n]$.

Then $\phi: C \to C$, $(x_0 : x_1 : \dots : x_n) \longmapsto (x_0^q : x_1^q : \dots : x_n^q)$ is called the <u>q-power</u> Frobenius.

<u>Remark</u>: if, more generally, k is of char $p > 0$, $q = p^r$, then $\phi: C \to C^{(q)}$ where $C^{(q)}$ is the curve defined by ~~def~~ raising the coefficients in the equations to the q^{th}-power.

<u>Prop 2.11</u>: Let $\phi: C \to C$ be a q-power Frobenius.

a) $\phi^* k(C) = \{ f^q : f \in k(C) \}$.

b) ϕ is purely inseparable.

c) $\deg \phi = q$.

Pf

(a) $\phi^* k(C) = \{ f(x_0^q, x_1^q, \dots, x_n^q) : f \in k(C) \}$.

but $f(x_0^q, \dots, x_n^q) = \dfrac{g(x_0^q, \dots, x_n^q)}{h(x_0^q, \dots, x_n^q)} = \dfrac{g(x_0, \dots, x_n)^q}{h(x_0, \dots, x_n)^q} = \left(\dfrac{g(x_0, \dots, x_n)}{h(x_0, \dots, x_n)}\right)^q = f^q(x_0, \dots, x_n)$.

(2) For $f \in k(C) \setminus \phi^* k(C)$, f is a root of $X^q - f^q = 0$. $\Rightarrow$ purely inseparable.

(3) Choose $t \in k(C)$ such that $k(C)/k(t)$ is separable (for example, chose t to be the local parameter at a smooth point P).

$$\begin{tikzcd}
 & k(C) \arrow[dr, dash, "q"] & \\
k(t) \arrow[ur, dash, "sep"] \arrow[dr, dash, "\deg q"'] \arrow[rr, Rightarrow] & & \phi^* k(C) \\
 & k(t^q) \arrow[ur, dash, "sep"'] &
\end{tikzcd}$$

Prop 2.12:

Let $\psi: C_1 \to C_2$ be a morphism of smooth curves over K, char $K = p$.
Then, ψ factors as:

$$\begin{tikzcd} C_1 \arrow[rr, "\psi"] \arrow[dr, "\phi"', "\text{insep}"] & & C_2 \\ & C_1 \arrow[ur, "\text{sep}"', "\lambda"] & \end{tikzcd}$$

such that $\phi = \mathrm{Frob}_q$ for some $q = \deg_i \psi$.

Pf

$$\begin{array}{l} k(C_1) \\ \big| \text{ insep} \\ L \\ \big| \text{ sep} \\ \psi^* k(C_2) \end{array}$$

$k(C_1)^q$ (insep over $k(C_1)$)

Let $q = \deg_i \psi$, and let $\phi = \mathrm{Frob}\, q$.

Claim: $k(C_1)^q = L$ (by uniqueness of maximum separable ext.

//

Thm V.3.1: (Deuring, 1941): Let k be a perfect field, char $k = p > 0$, and let E/k be an elliptic curve.
For an integer $r \geq 1$, let $\phi^r : E \to E^{(p^r)}$, $\hat{\phi}^r : E^{(p^r)} \to E$ be the p^r-power Frobenius and its dual isogeny.
TFAE:

1) $E[p^r] = 0 \quad \forall r \geq 1$
2) $\hat{\phi}^r$ is purely inseparable $\forall r \geq 1$.
3) $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.
4) End(E) is an order in a quaternion algebra.

Pf 1 ⟺ 2

$$\begin{tikzcd} E \arrow[r, "\phi_r"] \arrow[rr, bend right, "{[p^r]}"'] & E^{(p^r)} \arrow[r, "\hat{\phi}_r"] & E \end{tikzcd}$$

If $\hat{\phi}_r$ is pur. insep. $\Leftrightarrow [p^r]$ pur. insep $\Leftrightarrow$ $\Leftrightarrow \ker [p^r] = \{0\}$.

~~Also~~

$2 \Rightarrow 3$: If $\hat{\phi}_r$ is purely insep. $\forall r \geq 1$, in particular $\hat{\phi}_1$ is pur. insep, so $\hat{\phi}_1 \circ \phi = [p]$ is purely insep.

$$\begin{tikzcd} E^{(p)} \arrow[r, "\hat{\phi}_1"] \arrow[dr, "\mathrm{Frob}_p"'] & E \\ & E^{(p^2)} \arrow[u, "\lambda"'] \end{tikzcd}$$

$(2.12) \Rightarrow$

$\Rightarrow \deg \lambda = 1 \Rightarrow$ isomorphism $E \simeq E^{(p^2)} \Rightarrow$
$\Rightarrow j(E) = j(E^{(p^2)}) = j(E)^{p^2}$ //

$\underline{3 \Rightarrow 4}$: Assume $[p]: E \to E^{(p)}$ is purely insep and $j(E) \in \mathbb{F}_{p^2}$

Suppose not (4). Then $K = \mathrm{End}(E) \otimes \mathbb{Q}$ is a number field.

Let $\psi: E \to E'$ be an isogeny from E to a (different) curve E'.

$$\begin{tikzcd} E \arrow[r, "{[p]}"] \arrow[d, "\psi"'] \arrow[dr, phantom, "G"] & E \arrow[d, "\psi"] \\ E' \arrow[r, "{[p]}"] & E' \end{tikzcd}$$

$\Rightarrow [p]: E' \to E'$ is inseparable, and therefore $j(E') \in \mathbb{F}_{p^2}$

There can be only finitely many elliptic curves E' isogenous to E, up to isomorphism.

<u>Claim</u>: If $E \sim E'$, then $\mathrm{End}(E) \otimes \mathbb{Q} \simeq \mathrm{End}(E') \otimes \mathbb{Q}$.

pf

$$E' \xrightarrow{\hat{\psi}} E \xrightarrow{\phi} E \xrightarrow{\psi} E'$$

Define $\mathrm{End}(E) \otimes \mathbb{Q} \to \mathrm{End}(E') \otimes \mathbb{Q}$ it's an isomorphism.

$$\phi \longmapsto \frac{\hat{\psi} \circ \phi \circ \psi}{\deg \psi}$$

$$\frac{\psi \circ \phi' \circ \hat{\psi}}{\deg \psi} \longleftarrow \phi'$$

Thus all $E' \sim E$ have $\mathrm{End}(E')$ inside the same $K = \mathrm{End}(E) \otimes \mathbb{Q}$.

~~Claim~~ Choose a prime $\ell \neq p$, s.t. ℓ is inert in all $\mathrm{End}(E')$, $E' \sim E$

(fine, because only finitely many such E').

Since $\ell \neq p$, $E[\ell^i] \simeq \mathbb{Z}/\ell^i\mathbb{Z} \times \mathbb{Z}/\ell^i\mathbb{Z}$ $\forall i \geq 1$.

Choose a filtration of subgroups

$$\Phi_1 \subset \Phi_2 \subset \cdots \subset E(\bar{K}) \quad \text{with} \quad \Phi_i \simeq \mathbb{Z}/\ell^i\mathbb{Z}.$$

Let $E_i = E/\Phi_i$ (i.e. E_i the image under an isogeny $E \to E_i$ with kernel Φ_i).

So get $E \to E_1 \to E_2 \to \cdots\cdots$

We have constructed an infinite sequence of elliptic curves that are all isogenous to E. So $\exists m, n$ s.t $j(E_m) = j(E_{m+n})$ (ie $E_n \simeq E_{n+m}$).

Then $E_m \sim E_{m+n}$, and $\lambda : E_m \longrightarrow E_{m+n}$ with kernel $\simeq \mathbb{Z}/\ell^n\mathbb{Z}$.

$$\begin{tikzcd} E_m \arrow[r, "\lambda"] \arrow[rr, bend right, "{[\ell^n]}"'] & E_{m+n} \arrow[r, "\hat{\lambda}"] & E_n \end{tikzcd}$$

The factorization of $[\ell^n] \in \mathrm{End}(E)$ is $[\ell^n] = [\ell] \circ [\ell] \circ \cdots \circ [\ell]$, so λ and $\hat{\lambda}$ are $[\ell^{n/2}]$ (n has to be even).

This contradicts $\ker \lambda \simeq \mathbb{Z}/\ell^n\mathbb{Z}$, because $\ker [\ell^{n/2}] \simeq \mathbb{Z}/\ell^{n/2}\mathbb{Z} \times \mathbb{Z}/\ell^{n/2}\mathbb{Z}$ //

<u>4 ⇒ 2</u>: Assume $\hat{\Phi}_r$ is separable $\forall r \geq 1$. We show that $\mathrm{End}(E)$ is commutative (so not a quat. alg!).

As $\hat{\Phi}_r$ is separable, $E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z}$

Let $\mathrm{End}(E) \longrightarrow \mathrm{End}(T_p(E))$ $\left(T_p(E) = \varprojlim_r E[p^r] \simeq \mathbb{Z}_p \right)$.
$\psi \longmapsto \psi_p$

<u>Claim</u>: The map $\psi \mapsto \psi_p$ is injective:

$\psi_p(T_p(E)) = 0 \Rightarrow \psi(E[p^r]) = 0 \ \forall r \geq 1$ and $\mathbb{Z}/p^r\mathbb{Z} \simeq E[p^r] \subseteq \ker \psi \ \forall r \geq 1$

$\Rightarrow \psi = 0$ (an isogeny has always finite kernel).

So $\mathrm{End}(E) \hookrightarrow \mathrm{End}(\mathbb{Z}_p) \simeq \mathbb{Z}_p \Rightarrow \mathrm{End}(E)$ is commutative.

//

Terminology:

There are two possibilities for E/k, char $k = p$.

→ if $\hat{\phi}$ is inseparable, say E is <u>supersingular</u>. (say E has Hasse invariant 0)

→ if $\hat{\phi}$ is separable, say E is <u>ordinary</u> (say E has Hasse invariant 1) ← rank of p-torsion.

In general,

$\#E(\mathbb{F}_q) = q+1 - (\phi + \hat{\phi})$.

What can we say when E is supersingular?

Clearly, $p \nmid \#E(\mathbb{F}_q)$ (E has no p-torsion), so $\phi + \hat{\phi} \not\equiv 1 \bmod p$.

Claim: $\phi + \hat{\phi} \equiv 0 \pmod p$:

Pf we know also that $\forall i \geq 1$, $\phi^i + \hat{\phi}^i \not\equiv 1 \pmod p$. but still not enough.

Let $\omega \in \Omega_{E_2}$, with $(\omega) = 0$.

Then, $(\phi \underset{E_2}{+} \psi)^*(\omega) = \phi^*(\omega) \overset{\Omega_{E_1}}{+} \psi^*(\omega)$.

Example:

$E/\overline{\mathbb{Q}}$: $y^2 = x^3 - x$, $\mathrm{End}(E) = \mathbb{Z}[i]$, $j = 1728$.

$E/\overline{\mathbb{Q}}$: $y^2 = x^3 + 1$, $\mathrm{End}(E) = \mathbb{Z}[\omega]$, $\omega^2 + \omega + 1 = 0$, $j = 0$

Reducing mod p, will they be supersingular or ordinary?

Suppose $E/\mathbb{F}_p$ is ordinary, and $\mathrm{End}(E/\mathbb{Q}) \subseteq K = \mathbb{Q}(\sqrt{d})$ $d < 0$.

Its endomorphism ring will be the same.

p factors in $\mathrm{End}(E)$ as $p = \phi \circ \hat{\phi}$.

This gives a contradiction when $\mathrm{End}(E) \subseteq K$ and p is inert in $K/\mathbb{Q}$.

The conclusion is, therefore:

Prop/If $E/\mathbb{Q}$ has CM by K and p is inert in $K/\mathbb{Q}$, then $E/\mathbb{F}_p$ is supersingular.

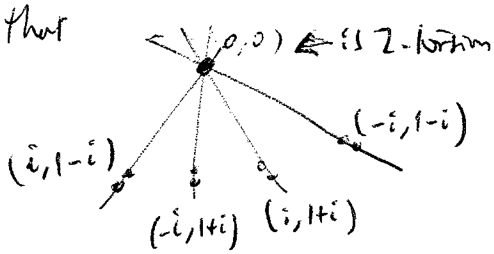
So in the example, $E/\mathbb{Q}: y^2 = x^3 - x$, $E/\mathbb{F}_p$ supersingular if $p \equiv 3\ (4)$
$y^2 = x^3 + 1$, $E/\mathbb{F}_p$ " " $p \equiv 2\ (3)$

In general, $\#E(\mathbb{F}_p) = p + 1 - (\phi + \hat{\phi})$.
When $E/\mathbb{F}_p$ is supersingular, $\phi + \hat{\phi} \equiv 0\ (p)$ (and hence for $p > 3$, $\phi + \hat{\phi} = 0$).

For the curve $y^2 = x^3 - x$, we have seen that $p \equiv 3\ (4) \Rightarrow E/\mathbb{F}_p$ supersingular.
But it has 4 points over $\mathbb{Q}$, so if $p \equiv 1\ (4)$ and it were supersingular, $\#E(\mathbb{F}_p) \equiv 2\ (4) \Rightarrow$!! (has to have $\equiv 0\ (4)$). So if $p \equiv 1\ (4) \Rightarrow E$ is ordinary over $\mathbb{F}_p$.

In this case,
$\mathrm{End}(E) \subseteq \mathbb{Q}(i)$ implies that $p = \phi \cdot \hat{\phi}$ corresponds to a factorization $p = (a+bi)(a-bi) \in \mathbb{Q}(i)$.
Thus $\phi + \hat{\phi}$ is either $2a, -2a, 2b, -2b$.
Let $p = a^2 + b^2$, such that $b \equiv 0 \pmod 2$
$a \equiv 1 \pmod 4$
$4 \mid p + 1 - (\phi + \hat{\phi}) \Rightarrow \phi + \hat{\phi} \equiv 2\ (4)$

Note, further, than when $p \equiv 1\ (4)$, $i = \sqrt{-1} \in \mathbb{F}_p$. Note then $(i, 1-i) \in E(\mathbb{F}_p)$.
We get that



So have $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subseteq E(\mathbb{F}_p)$

So $8 \mid \#E(\mathbb{F}_p)$, and thus

$$\phi + \hat{\phi} \equiv \begin{cases} 2\ (8) & \text{if } p \equiv 1 \\ 6\ (8) & \text{if } p \equiv 5 \end{cases} = \begin{cases} 2a & (\text{if } p \equiv 1) \\ -2a & (\text{if } p \equiv 5) \end{cases}$$

Let's go back and prove that, if E is supersingular, $\phi + \hat{\phi} \equiv 0 \ (p)$.

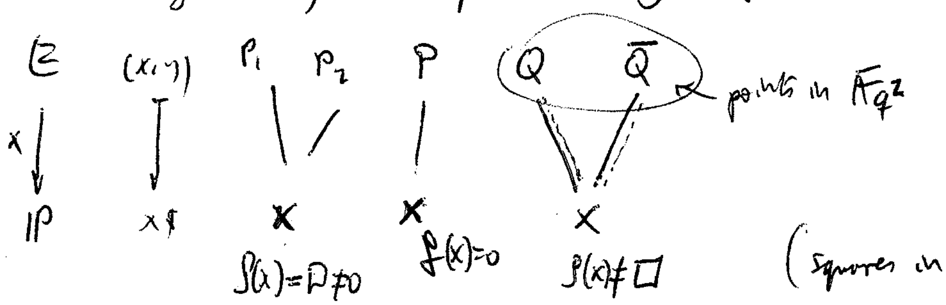
Pf/ $(t-\phi)(t-\hat{\phi}) = t^2 - at + p$

$$\left.\begin{array}{l} \phi + \hat{\phi} \equiv a \quad (p) \\ \phi^2 + \hat{\phi}^2 \equiv a^2 \quad (p) \\ \vdots \\ \phi^i + \hat{\phi}^i \equiv a^i \quad (p) \end{array}\right\} \Longrightarrow a \equiv 0 \ (p)$$

(because if not, for some i would have $a^i \equiv 1 \ (p)$!!)

V.4: How to count $\#E(\mathbb{F}_q)$ mod p? $(q = p^r)$

Let E be given by an equation in Legendre form $E: y^2 = \underbrace{x(x-1)(x-\lambda)}_{f(x)}$



(squares in $\mathbb{F}_q$)

$$\#\text{contributions from } x \in \mathbb{P}^1 = \begin{cases} 2 & \text{if } \left(\frac{f(x)}{q}\right) = 1 \\ 1 & \text{if } \left(\frac{f(x)}{q}\right) = 0 \\ 0 & \text{if } \left(\frac{f(x)}{q}\right) = -1 \end{cases} \Rightarrow \#E(\mathbb{F}_q) = \overset{\text{for infinity}}{1} + q + \sum_{x \in \mathbb{F}_q} \left(\frac{f(x)}{q}\right)$$

$$\left(\frac{f(x)}{q}\right) = f(x)^{\frac{q-1}{2}} = A_0 + A_1 x + \dots + A_{q-1} x^{q-1} + \dots + A_{\frac{3(q-1)}{2}} x^{\frac{3(q-1)}{2}}$$

So $\displaystyle\sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}} \equiv (q-1) A_{q-1} \pmod p$

So $\phi + \hat{\phi} \equiv A_{q-1} \pmod p$

For $f(x) = x(x-1)(x-\lambda)$, $\displaystyle A_{q-1} = (-1)^{\frac{q-1}{2}} \sum_{i=0}^{\frac{q-1}{2}} \binom{\frac{q-1}{2}}{i}^2 \lambda^i$ ← Hasse polynomial for p. $H_p(\lambda)$

Recall that, if $E/\mathbb{F}_q : y^2 = (x)(x-1)(x-\lambda)$, then if $m = \frac{q-1}{2}$, then:

$$\#E(\mathbb{F}_q) = 1 - (-1)^m \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i \pmod{p}.$$

$$\#E(\mathbb{F}_q) = q+1 - Tr(\phi), \quad Tr(\phi) = (-1)^m H_q(\lambda).$$

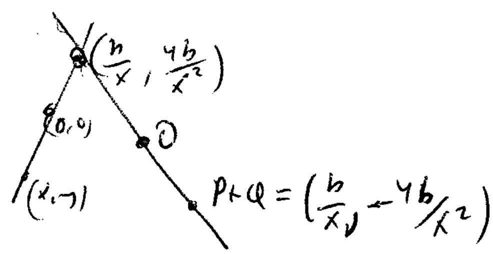
Example:

Let $E: y^2 = x^3 + ax + b$. Let $Q = (0,0) \in E[2]$.

For $P = (x_P, y_P) \in E$, let $P+Q = (x_{P+Q}, y_{P+Q}) \in E$.

Translation by Q gives an isomorphism

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



Let $\omega = \frac{dx}{y} \in \Omega_E$.

$$\tau_Q^*(\omega) = \tau_Q^*\left(\frac{dx}{y}\right) = d\left(\tau_Q^*(x)\right) / \tau_Q^*(y) =$$

$$= d(b/x) \Big/ -\frac{yb}{x^2} = \left(-\frac{b}{x^2} dx\right) \Big/ \left(-\frac{b}{x^2} y\right) = \frac{dx}{y} = \omega. \quad \Rightarrow$$

$$\Rightarrow \quad \begin{array}{l} k(E) \\ \quad | \deg = 1 \\ \tau_Q^* k(E) \end{array}$$

Proposition: Let $\tau_Q : E \to E$ via $P \mapsto P+Q$. Let $\omega \in \Omega_E$, with $div(\omega) = 0$ (for $E: y^2 = f(x)$, then $\omega = dx/y$ will work). Then $\tau_Q^* \omega = \omega$.
Such ω is called an <u>invariant differential</u>.

Note that if $\varphi: E_1 \to E_2$ and we have functions f, then
$\operatorname{div}(\varphi^* f) = \varphi^*(\operatorname{div} f)$.

Similarly for differentials: $\operatorname{div}(\varphi^*\omega) = \varphi^*(\operatorname{div}\omega)$ if φ is unramified.

Let $\varphi: C_1 \to C_2$ be unramified, let $\omega \in \Omega_{C_2}$, let $\varphi(P) = Q$. Let also $\omega = f_Q dt_Q$. Then $\operatorname{ord}_\omega(Q) = \operatorname{ord}_Q(f_Q)$. $\varphi^*\omega = (\varphi^* f)\, d(\varphi^* t_Q)$.

If $P \overset{\varphi}{\mapsto} Q$ is unramified, then $\varphi^*(t_Q)$ is a local parameter at P, and so $\operatorname{ord}_P(\varphi^*\omega) = \operatorname{ord}_P(\varphi^* f_Q)$.

Also, $\operatorname{div}(\varphi^*\omega) = \sum \operatorname{ord}_P(\varphi^*\omega)(P) = \sum_Q \sum_{P \mapsto Q} \operatorname{ord}_P(\varphi^* f_Q)(P) = \sum_Q \operatorname{ord}_Q(f_Q)\varphi^*(Q) =$
$= \varphi^*\left(\sum_Q \operatorname{ord}_Q(\omega) Q\right) = \varphi^*(\operatorname{div}\omega)$.

<u>Proof (of Prop)</u>: $\operatorname{div}(\tau_Q^*\omega) = \tau_Q^*(\operatorname{div}\omega) = 0$, so $\tau_Q^*\omega = a_Q\omega$, $a_Q \in k$.

Note that the map $\begin{array}{l} E \to \mathbb{P}^1 \\ Q \mapsto (a_Q : 1) \end{array}$ is a morphism, and $a_Q \neq (0, \infty)\ \forall Q$, it is not surjective, so it is constant. Thus, $a_Q = 1\ \forall Q$. //

Next, we prove a similar result to the one for dual isogenies, but for differentials.

<u>Theorem</u>: Let $\varphi: E_1 \to E_2$, $\psi: E_1 \to E_2$ be isogenies. Let $\omega \in \Omega_{E_2}$, with $\operatorname{div}(\omega) = 0$. Then $(\varphi +_{E_2} \psi)^*(\omega) = \varphi^*(\omega) +_{\Omega_{E_1}} \psi^*(\omega)$.

Pf Let $x_3, y_3 \in k(x_1, y_1, x_2, y_2)$ be such that $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$.
We claim that $\frac{dx_3}{y_3} = \frac{dx_1}{y_1} + \frac{dx_2}{y_2}$ if $E_2: y^2 = f(x)$.

From this, the theorem will follow easily.

Prop/ If we have $E_1 \xrightarrow{\varphi} E_2$, $E_1 \xrightarrow{\psi} E_2$, $\omega \in \Omega_{E_2}$, $\mathrm{div}(\omega) = 0$

(e.g. $\omega = \frac{dx}{y}$ if $E_2 : y^2 = f(x)$).

Then $(\varphi \underset{E_2}{+} \psi)^* \omega = \varphi^* \omega \underset{\Omega_{E_1}}{+} \psi^* \omega$

Pf/ Let $(x_1, y_1) \in E_2$ be a generic point, $(x_2, y_2) \in E_2$ be another generic point,

Then $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ (formally, for $x_3 = x_3(x_1, y_1, x_2, y_2) \in k(x_1, y_1, x_2, y_2)$
$y_3 = y_3(x_1, y_1, x_2, y_2) \in k(x_1, y_1, x_2, y_2)$)

Claim ($E_2 : y^2 = f(x)$): $\frac{dx_3}{y_3} = \frac{dx_1}{y_1} + \frac{dx_2}{y_2}$

Pf/ $\exists\, f_1, f_2 \in k(x_1, y_1, x_2, y_2)$ s.t. $\frac{dx_3}{y_3} = f_1 \frac{dx_1}{y_1} + f_2 \frac{dx_2}{y_2}$ (*)

Apply (*) to $(x_2, y_2) = (x_Q, y_Q) \in E(k)$. Then,

$\frac{dx_3}{y_3} = f_1(x_1, y_1, x_Q, y_Q) \frac{dx_1}{y_1}$ { it is the same as $\tau_Q^* \omega = \omega$.

Thus $f_1(x_1, y_1, x_Q, y_Q) = 1$ $\forall (x_1, y_1) \in E \Rightarrow f_1 \equiv 1$ $\forall (x_Q, y_Q) \Rightarrow f_1 \equiv 1$.

Similarly, $f_2 \equiv 1$ also, and that proves the claim //

So now, $(\varphi + \psi)^* \omega = \varphi^* \omega + \psi^* \omega$, very easily:

$$\begin{array}{l} E_1 \longrightarrow E_2 \\ (x, y) \xmapsto{\varphi} (x_1, y_2) \\ (x, y) \xmapsto{\psi} (x_2, y_2) \\ (x, y) \xmapsto{\varphi + \psi} (x_3, y_3) \end{array} \qquad \frac{dx_3}{y_3} = \frac{dx_1}{y_1} + \frac{dx_2}{y_2}$$

//

Note that the proof is similar to the one used to prove $\widehat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$.

Application: Let $E : y^2 = f(x)$, $\omega = \frac{dx}{y}$

Then $[m]^* \omega = m\omega$.

Pf by induction, $m = 1$ ok.

$$(m+1)^* \omega = m^* \omega + 1^* \omega = m\omega + \omega = (m+1)\omega \quad //$$

In char $= p$, $[p]^* \omega = 0$.

It can also be seen as follows: $\left(\phi(x,y) = (x^p, y^p) \right)$

$$[p] = \hat{\phi} \circ \phi$$

Use $\phi^*\left(\frac{dx}{y}\right) = \left(\frac{d(x^p)}{y^p}\right) = 0$

2) Under multiplication by m, let $[m](x_P, y_P) = (x_{mP}, y_{mP})$.

Let $x_{mP} = R(x_P)$ (rational function in one variable).

$[m]^* \omega = m\omega$ gives $\frac{dx_{mP}}{y_{mP}} = m \frac{dx_P}{y_P}$, thus

$$\frac{y_{mP}}{y_P} = \frac{dx_{mP}}{m\, dx_P} = \frac{1}{m} R'(x_P).$$

III §10 : Automorphism groups of elliptic curves.

For $E: y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$, the automorphisms are $\begin{cases} x = u^2 x + r \\ y = u^3 y + sx + t \end{cases}$

Examples: $E: y^2 = x^3 + ax + b$, $(x,y) \mapsto (x,-y)$ of order 2.

We can actually check that all elliptic curves have an automorphism of order 2.

$E: y^2 = x^3 + 1$ $(j=0)$ $(x,y) \mapsto (\omega x, -y)$ of order 3.

$E: y^2 = x^3 - x$, $(x,y) \mapsto (-x, iy)$ of order 4.

This is the whole story for char $\neq 2, 3$.

$\#\mathrm{Aut}(E)$:	char $\neq 2, 3$	char 3	char 2
$j \neq 0, 1728$	2	2	2
$j = 1728$	4	$\boxed{12}$	$\boxed{24}$
$j = 0$	6		

$E_1: y^2 - y = x^3 - x^2$ good reduction for $p \neq 11$

$E_2: y^2 - y = x^3 - x$ good reduction for $p \neq 37$

Both curves obviously contain the points $O, (0,0), (0,1), (1,0), (1,1)$.

But $E_1(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$, $E_2(\mathbb{Q}) \simeq \mathbb{Z}$.

Let E be a curve defined over $\mathbb{F}_p$.

$$N_m = \# E(\mathbb{F}_{p^m}) = p^m + 1 - (\alpha^m + \bar{\alpha}^m).$$

$$Z(T) := \exp\left(\sum_{m \geq 1} \frac{N_m}{m} T^m\right) = \frac{(1-\alpha T)(1-\bar{\alpha}T)}{(1-T)(1-pT)} = \frac{(1-aT+pT^2)}{(1-T)(1-pT)}$$

because: $\frac{1}{1-T} = 1 + T + T^2 + \cdots \Rightarrow -\ln(1-T) = T + \frac{T^2}{2} + \frac{T^3}{3} + \cdots$

$$\Rightarrow -\ln(1-\alpha T) = (\alpha T) + \frac{\alpha^2 T^2}{2} + \frac{\alpha^3 T^3}{3} + \cdots \qquad \Rightarrow \frac{1}{1-\alpha T} = \exp\left(\sum \alpha^m \frac{T^m}{m}\right)$$

Theorem (Mordell): For K a number field, $E(K)$ is finitely generated.

Pf/ We will prove that $E(K)/mE(K)$ is finite (weak Mordell), and then use the descent method:

If A is an abelian group s.t. A/mA is finite, and there is a height function $h: A \to \mathbb{R}$, then A is f.g. //

We start with the descent method:

Theorem: Let A be an abelian group with a height function $h: A \to \mathbb{R}$.

(that is, h satisfies: (1) For a given $Q \in A$, $h(P+Q) \leq 2h(P) + C_1$ $(C_1 = C_1(G,Q))$

(2) $\exists m \geq 2$ s.t. $h(mP) \geq m^2 h(P) - C_2$ $(C_2 = C_2(A, m))$.

(3) $\{P \in A : h(P) \leq C_3\}$ is finite $\forall C_3$)

Then A/mA is finite $\iff$ A is finitely-generated.

Pf ($\Leftarrow$) trivial

($\Rightarrow$) Let $S = \{Q_1, \dots, Q_r\} \subseteq A$ be representatives for A/mA.

Let $P \in A$ be any point.

Write
$$P = mP_1 + Q_{i_1} \quad \text{for some } P_1 \in A, \ 1 \leq i_1 \leq r$$
$$P_1 = mP_2 + Q_{i_2}$$
$$\vdots$$
$$P_j = mP_{j+1} + Q_{i_{j+1}}$$

Compute $h(P_j)$:

$C_1' := \max\{C_1(A, Q_i)\}_{1 \leq i \leq r}$

$$h(P_j) \underset{(2)}{\leq} \frac{1}{m^2}\left(h(mP_j) + C_2'\right) = \frac{1}{m^2}\left(h(P_{j-1} - Q_{i_j}) + C_2'\right) \leq \frac{1}{m^2}\left(2h(P_{j-1}) + C_1' + C_2'\right) \leq$$

$$(m \geq 2) \leq \frac{1}{2} h(P_{j-1}) + \frac{C_1' + C_2'}{4} \leq 2^{-j} h(P) + \frac{C_1' + C_2'}{4}\left(1 + \frac{1}{2} + \dots\right) \leq 2^{-j} h(P) + \frac{C_1' + C_2'}{2}$$

For j sufficiently large, $h(P)\,2^{-j} \leq 1$, so $h(P_j) \leq 1 + \frac{c_1'+c_2'}{2}$. ← independent of P!!

By axiom (3), $\{P \in A : h(P) \leq 1 + \frac{c_1'+c_2'}{2}\}$ is finite, so

$\{P_1, \dots, P_{j-1}\} \cup \{ \quad \}$ is finite.

$P = m^j P_j \in \langle Q_1, \dots, Q_r \rangle$. Thus A is generated by this finite set.

Lemma: Let L/K be finite Galois of number fields. Then,

$$E(K)/mE(K) \text{ is finite iff } E(L)/mE(L) \text{ is finite.}$$

Pf.

$$0 \to \Phi \to E(K)/mE(K) \xrightarrow{\varphi} \underbrace{E(L)/mE(L)}_{\text{finite}} \to 0$$

It suffices to show that Φ ($= \ker \varphi$) is finite.

$$\Phi = \frac{E(K) \cap mE(L)}{mE(L)}$$

For any $P \in E(K) \cap mE(L)$, let $P = m\,Q_P$ (not uniquely), $Q_P \in E(L)$.

Define a map (setwise) $\lambda_P : G_{L/K} \to E[m]$

$$\sigma \longmapsto Q_P^\sigma - Q_P$$

λ_P is well-defined: $m(Q_P^\sigma - Q_P) = (mQ_P)^\sigma - mQ_P = P^\sigma - P = 0$ (because $P \in E(K)$)

↑ σ and $[m]$ commute, as $[m]$ has coeffs in K.

(Note: $\sigma\tau \longmapsto Q_P^{\sigma\tau} - Q_P = (Q_P^\sigma)^\tau - Q_P = (Q_P^\sigma - Q_P)^\tau + (Q_P^\tau - Q_P)$

So it is not an homomorphism unless τ acts trivially on $Q_P^\sigma - Q_P$ $\forall \sigma, \tau$).

It is called a crossed homomorphism (or a 1-cocycle).

(cont pf of lemma):

__Claim__: The map $\delta : \bar{P} \longmapsto \lambda_P$ is injective (and well-defined).

Pf Suppose $\lambda_P = \lambda_{P'}$, $P, P' \in E(K) \cap mE(L)$.

Then $(Q_P^\sigma - Q_P) = (Q_{P'}^\sigma - Q_{P'})$ $\forall \sigma \in G_{L/K}$ $\Leftrightarrow (Q_P - Q_{P'})^\sigma = Q_P - Q_{P'}$

$\Leftrightarrow Q_P - Q_{P'} \in E(K)$.

But then $P - P' = mQ_P - mQ_{P'} \in mE(K)$, so $\bar{P} = \bar{P'}$ //

Since both $G_{L/K}$ and $E[m]$ are finite, there are only finitely-many λ_P, and so finitely-many classes in Φ. //

Due to the lemma, we can assume that $E[m] \subseteq E(K)$ (K large enough).

__Def__: Let $\kappa : E(K) \times G_{\bar{K}/K} \longrightarrow E[m]$
$(P, \sigma) \longmapsto Q^\sigma - Q$ where $P = mQ$ (Q lives in some extension of K)

__Prop__: The following hold for κ.

(a) κ is well defined.

(b) κ is bilinear

(c) The left kernel of κ is $mE(K)$

(d) The right kernel of κ is $Gal_{\bar{K}/L}$, where $L = K([m]^{-1}E(K)) = K(Q : mQ \in E(K))$.

Pf (a) As before, $Q^\sigma - Q \in E[m]$ (using that σ and $[m]$ commute).
We need to show that it doesn't depend on the choice of Q. Let $Q' = Q + T$, $T \in E[m]$.
Then $T \in E(K) \Rightarrow Q'^\sigma - Q' = Q^\sigma - Q$.

(b) It is linear in the first component, clearly.

$Q^{\sigma\tau} - Q = (\underbrace{Q^\sigma - Q}_{E[m] \subseteq E(K)})^\tau + (Q^\tau - Q)$ so τ acts trivially on $Q^\sigma - Q$.

(cont pf)

(c) To prove that the left kernel is $mE(K)$:

[$\supseteq$] Let $P = mQ$, $Q \in E(K)$. Then $Q^\sigma - Q = O$ $\forall \sigma \in Gal_{\bar{K}|K}$ (as $Q \in E(K)$).

[$\subseteq$] Let $P = mQ$, $Q \in E(\bar{K})$ s.t. $Q^\sigma - Q = O$ $\forall \sigma \in Gal_{\bar{K}|K}$ $\Rightarrow Q \in E(K)$ $\Rightarrow$ ok.

(d) To prove that the right kernel is $\left(L = K(Q : mQ \in E(K))\right)$ $Gal_{\bar{K}|L}$:

$\sigma \in$ right kernel of $k \Leftrightarrow Q^\sigma = Q$ $\forall P \in E(K), P = mQ \Leftrightarrow Q^\sigma = Q$ $\forall Q \in E(\bar{K}) : mQ \in E(K)$
$\Leftrightarrow \sigma \in Gal_{\bar{K}|L}$.

<u>Remark</u>: As a right kernel, $Gal_{\bar{K}|L} \triangleleft Gal_{\bar{K}|K}$,

and $L|K$ is Galois, with group $Gal_{L|K}$.

k induces a perfect bilinear pairing (perfect := left and right kernels are trivial).

$$\frac{E(K)}{mE(K)} \times Gal_{L|K} \longrightarrow E[m]$$

Now, to each point $\bar{P} \in E(K)/mE(K)$, we can associate a group homomorphism $k(\bar{P}, \cdot) : Gal_{L|K} \to E[m]$. If we show that L/K is finite, then there are only a finite amount of possibilities for $k(P, \cdot)$, and so only finitely many classes.

<u>Prop</u>: Let $L = K(Q : mQ \in E(K))$.

(a) Then $L|K$ is abelian of exponent m.

(b) $L|K$ is unramified at almost primes $\mathfrak{p}$ of K.

Pf/

(a): $Gal_{L|K} \hookrightarrow Hom\left(E(K)/mE(K), E[m]\right)$ so it is abelian and is killed by m.

(b) prove it later.

Prop: Let L/K be Galois abelian of exponent m, and unramified almost everywhere. Then L/K is finite.

But first let us prove that:

Prop: L/K is unramified almost everywhere (i.e. $\forall\, \mathfrak{p} \notin S$ – S a finite set).

Pf/ L is the composition of all $K' = K(Q)$, in $Q \in E(K)$.

It suffices to show that K'/K is unramified outside S.
↖ Galois Ext!

$$\begin{array}{lll} & K' & \mathfrak{q} \\ & \mid e & \\ \text{inertia field} & K_I & \\ & \mid f & \\ \text{decomp field} & K_D & \\ & \mid r & \\ & K & \mathfrak{p} \end{array}$$

we need to show that $e=1$, i.e. Inertia group $I = I(\mathfrak{q}/\mathfrak{p}) = \{id\}$.

(recall: $D = \{\sigma \in \mathrm{Gal}_{K'/K} : \sigma\mathfrak{q} = \mathfrak{q}\}$.

$I = \{\sigma \in \mathrm{Gal}\, K'/K : \sigma\alpha \equiv \alpha \pmod{\mathfrak{q}}\}$)

We will show that $I = \{id\}$ whenever $E/K_{\mathfrak{p}}$ has good reduction and $\mathfrak{p} \nmid m$

From Chap VII, (3.1):

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

For a given prime $\mathfrak{p}$ of K, $E/K_{\mathfrak{p}}$ is a minimal model iff
$$\begin{cases} a_1, a_2, \dots, a_6 \in R_{\mathfrak{p}} \\ \operatorname{ord}_{\mathfrak{p}}(\Delta) \text{ is minimal} \end{cases}$$

unit in $R_{\mathfrak{p}}$

In particular, $E/K_{\mathfrak{p}}$ is minimal for all $\mathfrak{p}$ with $a_1, a_2, \dots, a_6$ integral and $\operatorname{ord}_{\mathfrak{p}}(\Delta) = 0$

Let $\tilde{E}/k_{\mathfrak{p}}$ be the reduction of $E/k_{\mathfrak{p}}$ (it's an e.c. outside some finite set of primes).

Then, if $\tilde{E}/k_{\mathfrak{p}}$ is nonsingular,

$E(k_{\mathfrak{p}})[m] \hookrightarrow \tilde{E}(k_{\mathfrak{p}})$ (m prime to char $k_{\mathfrak{p}}$, i.e. $\mathfrak{p} \nmid m$).

Need to show that, $\forall \sigma \in I$, $Q^{\sigma} = Q \iff Q^{\sigma} - Q = O$.

The image of $Q^{\sigma} - Q$ in $\tilde{E}(k_{\mathfrak{q}})$ (as Δ is a unit in $R_{\mathfrak{p}}^{*}$, it is also a unit in $R_{\mathfrak{q}}^{*}$).

is trivial (because $\sigma \in I \Rightarrow \sigma\alpha \equiv \alpha \bmod \mathfrak{q}$).

$\widetilde{Q^{\sigma} - Q} = \tilde{Q}^{\sigma} - \tilde{Q} = \tilde{Q} - \tilde{Q} = \tilde{O}$

Also, $Q^{\sigma} - Q \in E(K')[m]$:

$m(Q^{\sigma} - Q) = (mQ)^{\sigma} - mQ = mQ - mQ = O$.

So $Q^{\sigma} - Q \in E(k_{\mathfrak{q}})[m]$ s.t. the reduction (injective) is $\tilde{O}$. So it is O before the reduction. $Q^{\sigma} - Q = O \Rightarrow \sigma = \mathrm{id}$.

So if $S = \{\mathfrak{p} : \mathfrak{p} \mid m\} \cup \{\mathfrak{p} : a_1, a_2, \dots, a_6 \text{ not all integral}\} \cup \{\mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(\Delta) \neq 0\}$.

Now, prove that if L/k is Galois abelian of exponent m, and ~~L/k~~ unramified almost everywhere, then L/k is finite.

Pf Assume $K \supseteq \mu_m$.

Theory of Kummer extensions gives that L is of the form

$L = K(\sqrt[m]{a} : a \in T)$.

$$\begin{array}{ll} \mathfrak{q} & K(\sqrt[m]{a}) \\ & \big| \\ \mathfrak{p} & K \end{array}$$

$X^m - a$, $\alpha^m = a$

if $\mathfrak{q}/\mathfrak{p}$ is unramified

$\mathrm{ord}_{\mathfrak{q}}(a) = \mathrm{ord}_{\mathfrak{q}}(\alpha^m) = m \cdot \mathrm{ord}_{\mathfrak{q}}(\alpha) \Rightarrow m \mid \mathrm{ord}_{\mathfrak{p}}(a)$

$\mathrm{ord}_{\mathfrak{q}}(a) = e \cdot \mathrm{ord}_{\mathfrak{p}}(a)$

(cont pf)

So let $T_S := \{ a \in K^*/K^{*m} : m \mid \mathrm{ord}_{\mathfrak{p}}(a) \text{ for all } \mathfrak{p} \notin S \}$.

Enlarge S, if necessary, such that the primes $\mathfrak{p} \in S$ generate Cl_K (Cl_K is finite)

For $a \in T_S$, write $(a) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n_{\mathfrak{p}}} \cdot \prod_{\mathfrak{p} \notin S} (\mathfrak{p}^{n_{\mathfrak{p}}})^m$

Let $J := \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{n_{\mathfrak{p}}}$. In general, J is not principal. However, there exists $J' \overset{\text{in } Cl_K}{\sim} J$ s.t it has support in S (because S generates Cl_K).

Let $(b) = J' \cdot J^{-1}$

Then (ab^m) has support in S

But ab^m generates the same extension as a. So we can find representatives for T_S s.t (a) is supported on S.

So $(a) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n_{\mathfrak{p}}}$. For each $\mathfrak{p}$, $\mathfrak{p}^{h_K \cdot m} = (b^m)$ for some $b \in K$,

So $n_{\mathfrak{p}}$ may not take values greater than $h_K m - 1$.

Thus the representative in T_S can be chosen of the form:

$$(a) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{n_{\mathfrak{p}}}, \quad 0 \leq n_{\mathfrak{p}} < m h_K$$

But now, if $a_1 \neq a_2$ s.t $(a_1) = (a_2)$, means that $a_2 = u a_1$ for some u in the unit group.

Modulo m^{th}-powers, and using Dirichlet's Unit Thm, they are finite.

So T_S is generated by finitely many a's.

__Example__: $E_1: y^2 = x(x-7)(x+10) = x^3 + 3x^2 - 70x$

$E_2: v^2 = u^3 - 6u^2 + 289u$

E_1 is 2-isogenous to E_2.

(in general, $E_1: y^2 = x^3 + ax^2 + bx$ is 2-isogenous (with kernel $\{O, (0,0)\}$) to

$E_2: y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$

↖ WLOG, we'll assume from now on that $a, b \in \mathbb{Z}$.

$$\begin{tikzcd} E_1 \arrow[rr, "{[2]}"] \arrow[dr, "\phi"'] & & E_1 \\ & E_2 \arrow[ur, "\hat{\phi}"'] & \end{tikzcd}$$

So instead of asking whether $P \in [2]E_1$, we ask

we ask if $P_1 \in \hat{\phi}(E_2)$ (necessary, not sufficient condition).

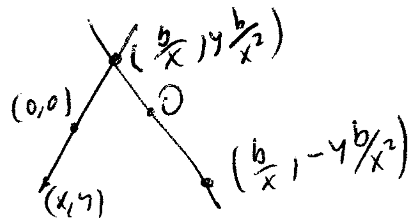
Similarly, is P_2 an element of $\phi(E_1)$ for a given P_2?

If we can answer these two questions, we will be done.

$\phi: E_1 \to E_2$

$(x, y) \mapsto (u, v)$ where $u = \left(\frac{y}{x}\right)^2 = x + \frac{b}{x} + a$

$v = \left(\frac{y}{x}\right)\left(x - \frac{b}{x}\right) = y - y\frac{b}{x^2}$



__Lemma__: If (u, v) $(\neq O)$ $\in E_2(\mathbb{Q})$ is of the form $\phi(x,y)$, $(x,y) \in E_1(\mathbb{Q})$

$\iff u \in \mathbb{Q}^{*2}$

Pf. ($\Rightarrow$) easy, since $u = \left(\frac{x}{y}\right)^2$.

($\Leftarrow$) Let $\lambda = \sqrt{u} \in \mathbb{Q}^*$. $\begin{cases} u = x + \frac{b}{x} + a \in \mathbb{Q} \\ \lambda^{-1} v = \left(x - \frac{b}{x}\right) \in \mathbb{Q} \end{cases} \Rightarrow 2x + a \in \mathbb{Q}$,

hence $x \in \mathbb{Q}$, $y = \lambda x \in \mathbb{Q}$.

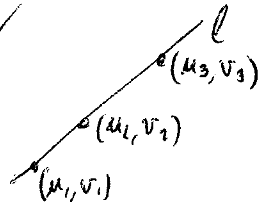
Def $q: E_2(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$

$$(u,v) \longmapsto \begin{cases} u \\ a^2-4b & \text{if } (u,v)=0 \\ 1 & \text{if } (u,v)=\mathcal{O} \end{cases}$$

Lemma:

q is a homomorphism, with $\operatorname{Ker} q = \phi(E_1(\mathbb{Q}))$.

Pf



We need to show that $q(u_1,v_1)\,q(u_2,v_2)\,q(u_3,v_3) = u_1u_2u_3 \in \mathbb{Q}^{*2}$ (the general case)

Let $l: V = rU+s$.

We know that $(rU+s)^2 - (U^3 - 2aU^2 + (a^2-4b)U) = (U-u_1)(U-u_2)(U-u_3)$

For $U=0$, $s^2 = u_1u_2u_3$.

The kernel is assured by the previous lemma.

Lemma: $q: E_2(\mathbb{Q})/\phi E_1(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ has finite image.

Pf **Claim:** let $r \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ (assume r squarefree integer). Then,

$$r \in \operatorname{Im}(q) \Rightarrow r \mid a^2-4b. \quad \text{(and then, only finite possibilities)}$$

Pf of claim:

We solve for (u,v) with $(u,v) \mapsto r \in \mathbb{Q}^*/\mathbb{Q}^{*2}$.

Write $u = rt^2$ for some $t \in \mathbb{Q}$.

product:

$$\begin{array}{lr} & u^2 - 2au + (a^2-4b) = rs^2 \\ \times & u = rt^2 \\ \hline & v^2 = (rst)^2 \end{array}$$

Write $t = l/m$, $l,m \in \mathbb{Z}$, $\gcd(l,m)=1$.

Substitute $v = rt^2$ in $u^2 \cdots = rs^2$.

Multiply by m^4, and get:

$$r^2\ell^4 - 2ar\ell^2m^2 + (a^2-4b)m^4 = \overbrace{rs^2m^4}^{\text{integer because LHS is an integer.}} = rn^2 \text{ where } n = sm^2 \in \mathbb{Z}.$$

Let $p \mid r$, p prime (suffices to do it for all primes).

$\Rightarrow p \mid (a^2-4b)m^4$.

Assume $p \nmid (a^2-4b)$. So $p \mid m^4 \Rightarrow p \mid m$. $\Rightarrow p \mid n \Rightarrow p \mid \ell \Rightarrow$!!

<u>Remark</u>: we have $r \in \mathrm{Im}\, q$ only if $r \mid a^2-4b$.

Moreover, we see that $r \in \mathrm{Im}\, q$ precisely when

$$r^2\ell^4 - 2ar\ell^2m^2 + (a^2-4b)m^4 = rn^2$$

has a solution in $(\ell, m, n) \in \mathbb{Z}^3$.

(In that case, $\left(u = r\ell^2/m^2,\ v (= rst) = \dfrac{r\ell n}{m^3}\right) \longmapsto r$).

In our example, $r \mid a^2-4b = 289 \Rightarrow r \in \{\pm 1, \pm 17\}$.

$r=1$: $\ell^4 - 6\ell^2m^2 + 289m^4 = n^2 \to (0,1,17)$

$r=-1$ $-\ell^4 - 6\ell^2m^2 - 289m^4 = n^2 \to \times$

$r=17$ $17\ell^4 - 6\ell^2m^2 + 17m^4 = n^2 \to -6$ is not a square mod 17

$r=-17$ $-17\ell^4 - 6\ell^2m^2 - 17m^4 = n^2 \to \times$

We conclude that $E_2(\mathbb{Q}) / \phi(E_1(\mathbb{Q})) = \{1\}$.

So $E_2(\mathbb{Q}) = \phi(E_1(\mathbb{Q}))$.

Similarly, determine $E_1(\mathbb{Q}) / \hat{\phi}(E_2(\mathbb{Q}))$

With $E_2(\mathbb{Q}) = \phi(E_1(\mathbb{Q}))$ we get:

$$E_1(\mathbb{Q}) / \hat{\phi} E_2(\mathbb{Q}) = E_1(\mathbb{Q}) / 2E_1(\mathbb{Q})$$ ← we were looking for this!

In this case $E_1(\mathbb{Q}) / \hat{\phi}(E_2(\mathbb{Q})) = (\mathbb{Z}/2\mathbb{Z})^4$.

To prove M-W, still need to define a height function $h: E(\mathbb{Q}) \to \mathbb{R}$ and verify conditions (1), (2), (3).

__Example__: Height function on $\mathbb{P}^1(\mathbb{Q})$: $H((p:q)) = \max\{|p|, |q|\}$, $p, q \in \mathbb{Z}$, $\gcd(p,q) = 1$.

Let $M_{\mathbb{Q}}$ be the set of standard absolute values of $\mathbb{Q}$:

→ $|x|_\infty = \max\{x, -x\}$.

→ $|x|_p = p^{-n}$ if $x = p^n \frac{a}{b}$, $a, b \in \mathbb{Z}$, $\gcd(p, ab) = 1$.

Let M_K be the set of standard absolute values of K ($[K:\mathbb{Q}] < \infty$).
(standard means that agree on $M_{\mathbb{Q}}$ when restricted).
($v \in M_K$ is in standard form iff ~~...~~ $v|_{\mathbb{Q}} \in M_{\mathbb{Q}}$) ~~...~~

Define $n_v := e_v \cdot f_v \left(= [K_v : \mathbb{Q}_v]\right)$ $\quad$ $K \,|\, \mathbb{Q}$: $n = e \cdot f \cdot$ (# primes that lie over (p))

$$\begin{array}{cc} L & w \\ | & | \\ K & v \\ | & \\ \mathbb{Q} & \end{array} \qquad \text{Then } \sum_{w|v} e_{(w|v)} f_{(w|v)} = [L:K]$$

__Lemma 5.2__: $\sum_{w|v} n_w = [L:K] \cdot n_v$

Pf: $\sum_{w|v} n_w = \sum_{w|v} e_w \cdot f_w = \sum_{w|v} e_{(w|v)} \cdot e_v \cdot f_{(w|v)} \cdot f_v = n_v \sum_{w|v} e_{(w|v)} \cdot f_{(w|v)} = n_v [L:K]$. //

5.3 (Product formula for $x \in K^\times$):

$$\prod_{v \in M_K} |x|_v^{n_v} = 1$$

Pf/ Reduce to the case $K = \mathbb{Q}$, and there it is easy.

Def/ Let $P \in \mathbb{P}^N(K)$, $P = (x_0 : x_1 : \cdots : x_N)$

$$H_K(P) := \prod_{v \in M_K} \max\{|x_0|_v, \ldots, |x_N|_v\}^{n_v}$$

Prop 5.4:

a) $H_K(P)$ is well defined (does not depend on the homogeneous coordinates).

b) $H_K(P) \geq 1$.

c) For a finite extension L/K and P defined over K, $H_L(P) = H_K(P)^{[L:K]}$

Pf/ (a)
$$\prod_{v \in M_K} \max\{|\lambda x_i|_v\}^{n_v} = \prod_{v \in M_K} |\lambda|_v^{n_v} \max\{|x_i|_v\}^{n_v} = \underbrace{\left(\prod |\lambda|_v^{n_v}\right)}_{1 \text{ by the product formula!}} \prod \max\{|x_i|_v\}^{n_v} \quad //$$

(b) At least one of the $x_i \neq 0$, multiply it by λ s.t. $\lambda x_i = 1$. Then $|x_i|_v = 1 \ \forall v$.

Also, can make all $x_0, \ldots, x_N \in \mathcal{O}_K$, and then the valuation at ∞ is at least 1.

(c) $$H_L(P) = \prod_{w \in M_L} \max\{|x_i|_w\}^{n_w} = \prod_{v \in M_K} \prod_{w | v} \max\{|x_i|_v\}^{n_w} = \prod_{v \in M_K} \max\{|x_i|_v\}^{\sum_{w|v} n_w} \quad //$$

Def/ The absolute height of $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ is

$$H(P) := H_K(P)^{\frac{1}{[K:\mathbb{Q}]}}$$ for any field K over which P is defined.

Rk: If $P \in \mathbb{P}^N(\mathbb{Q})$, choose $P = (x_0 : x_1 : \cdots : x_N)$ with $x_0, x_1, \ldots, x_N \in \mathbb{Z}$ s.t. $\gcd(x_0, \ldots, x_N) = 1$. Then $H_{\mathbb{Q}}(P) = \prod_{v \in M_{\mathbb{Q}}} \max\{|x_i|_v\} = \max_i \{|x_i|_\infty\}$ ← agrees on the Naive height! //

~~Def~~ A <u>morphism of degree d</u> on projective spaces is a map

$$F : \mathbb{P}^N \to \mathbb{P}^M \qquad (x_0 : \cdots x_N) \longmapsto (f_0(x_0 : \cdots x_N) ; \cdots : f_M(x_0 : \cdots x_N)),$$

where $f_0, \ldots, f_M \in \overline{\mathbb{Q}}[x_0, \ldots, x_N]_d$ are homogeneous of degree d, such that $V(f_0, \ldots, f_M) = \phi \subseteq \mathbb{P}^N$ (i.e. $V(f_0, f_1, \ldots, f_M) = \{(0,0,\ldots,0)\} \subseteq \mathbb{A}^{N+1}$)

<u>Theorem</u>: There exists $c_1, c_2 > 0$ s.t.

$$C_1 H(P)^d \leqslant H(F(P)) \leqslant C_2 H(P)^d$$

Here, C_1 and C_2 depend on d, N, M and F, but <u>Not</u> on P.

~~Pf~~

- First, the upper bound:

Choose K s.t. F and P are defined over K.

Let $|P|_v = \max\limits_{0 \leqslant i \leqslant N} \{|x_i|_v\}$ and $|F(P)|_v = \max\limits_{0 \leqslant j \leqslant M} \{|f_j(P)|_v\}$.

Also, let $|F|_v := \max\{|a|_v : a \text{ is a coeff in some } f_j\}$.

$$H_K(P) = \prod_{v \in M_K} |P|_v^{n_v}$$

$$H_K(F(P)) = \prod_{v \in M_K} |F(P)|_v^{n_v}$$

Convention: $\epsilon_v = \begin{cases} 1 & v \in M_K^\infty \text{ (the infinite primes)} \\ 0 & v \in M_K^0 \end{cases}$

For $v \in M_K^\infty$, $|a+b| \leqslant 2 \max\{|a|, |b|\}$

$v \in M_K^0$, $|a+b| \leqslant \max\{|a|, |b|\}$

(So we get $|t_1 + \cdots + t_n|_v \leqslant n^{\epsilon_v} \cdot \max\{|t_1|_v, \ldots, |t_n|_v\}$)

Have, for each j, $|f_j(P)|_v \leqslant C_3^{\epsilon_v} \cdot |F|_v \cdot |P|_v^d$

C_3 an upper bound for the # terms, ~~of the~~

Now, ~~KNX~~ $|F(P)|_v \leqslant C_3^{\epsilon_v} |F|_v |P|_v^d \Rightarrow H(F(P)) \leq \overbrace{\left(\prod C_3^{\epsilon_v n_v}\right)}^{C_3} \overbrace{H(F)}^{\text{some constant}} H(P)^d$

finite number of infinite primes!

So letting $C_2 := C_3 \cdot H(F)$, we are done.

For the lower bound, we need to do some more work.

We actually need that $V(f_0, \dots, f_M) = \{(0,0,\dots 0)\} \subset \mathbb{A}^{N+1}$.

Applying Hilbert's Nullstellensatz, $\left(I(V(J)) = \sqrt{J}\right)$

x_0 vanishes at $(0,0,\dots 0)$ so $x_0 \in I(V(I)) = \sqrt{I}$

So $x_0^m \in I = (f_0, \dots, f_N)$ for some m. effective versions of Nullstellensatz bound this for any x_i!

Choose e large enough so that $x_i^e \in I$ $(\forall i = 0..N)$.

Let $x_i^e = \sum_j g_{ij} f_j$ for $i = 0..N$

Can choose the g_{ij} to be homogeneous of degree $e-d$.

(note that g_{ij} live in some extension, so choose a large K s.t. all $g_{ij}, f_i \in k[x_0, \dots, x_N]$).

Let $|G|_v = \max\{|b|_v : b$ a coefficient of some $g_{ij}\}$.

$H_K(G) := \prod_{v \in M_K} |G|_v^{n_v}$

upper bound for the number of terms in $g_{ij} f_j$, $i = 0..N$, $j = 0..M$

Have $|x_i|_v^e \leq C_4^{\varepsilon_v} \max_{i,j} \{|g_{ij}(P) f(P)|_v\}$

Also, $|g_{ij}(P)|_v \leq C_5^{\varepsilon_v} |G|_v |P|_v^{e-d}$

bound for # terms in g_{ij}

So $|P|_v^e \leq C_4^{\varepsilon_v} C_5^{\varepsilon_v} |G|_v |P|_v^{e-d} |F(P)|_v$

Thus $|P|_v^d \leq C_6^{\varepsilon_v} |G|_v |F(P)|_v$

$$H(P)^d \leq \underbrace{C_6 H(G)}_{C_1^{-1}} H(F(P))$$

Theorem 5.9: Let $f(T) = a_0T^d + \cdots + a_d$ a degree-d polynomial, that factors $a_0(T-\alpha_1)\cdots(T-\alpha_d) \in \bar{\mathbb{Q}}[T]$, $a_0 \neq 0$

Then $H(f) \left(= H((a_0:\cdots:a_d))\right)$ satisfies:

$$2^{-d}\prod_{j=1}^{d} H(\alpha_j) \overset{\text{not so obvious!}}{\leq} H(f) \leq 2^{d-1}\prod_{j=1}^{d} H(\alpha_j) \qquad \left(H(\alpha_j) := H((\alpha_j:1))\right).$$

Pf/ Let $C_v = \begin{cases} 2 & \text{if } v \in M_K^\infty \\ 1 & \text{if } v \in M_K^0 \end{cases} \rightarrow |x+y|_v \leq C_v \max\{|x|_v, |y|_v\}$

For a given valuation v, choose k s.t. $|\alpha_k|_v \geq |\alpha_j|_v$ $j=1\ldots d$

Write $f(T) = (T-\alpha_k)\,g(T)$.

$g(T) = b_0T^{d-1} + \cdots + b_{d-1}$ and $a_i = b_i - \alpha_k b_{i-1}$

So $\max\{|a_i|_v\} = \max_i\{|b_i - \alpha_k b_{i-1}|\} \leq C_v \max_i\{|b_i|_v, |\alpha_k|_v |b_{i-1}|_v\} \leq$

$$\leq C_v \underbrace{\max_i\{|b_i|_v\}}_{\text{will apply induction on this}} \cdot \max\{|\alpha_k|_v, 1\} \underset{\text{induction}}{\leq} C_v^{d-1}\prod \max\{|\alpha_j|_v\}$$

For the other bound;

- Case $|\alpha_k|_v \leq C_v$:

Then $\prod_j \max\{|\alpha_j|_v\} \leq \prod_j(\max\{|\alpha_k|_v, 1\}) = |\alpha_k|_v^d \leq C_v^d \Rightarrow$

$\Rightarrow C_v^{-d}\prod_j \max\{|\alpha_j|_v\} \leq 1 \leq \max_i\{|a_i|_v\}$ $\Rightarrow$ done.

- Case $|\alpha_k|_v > C_v$

if $v \in M_K^0$: $\max_i\{|b_i - \alpha_k b_{i-1}|_v\} = \max_i\{|b_i|\}\cdot \max\{|\alpha_k|, 1\}$

if $v \in M_K^\infty$ $(C_v = 2)$, $|\alpha_k|_v > 2$, $\max\{|b_i - \alpha_k b_{i-1}|\} \geq \max_i\{|\alpha_k||b_{i-1}| - |b_i|\}\ldots$

$$\max_i\{|a_i|_v\} = \max_i\{|b_i - \alpha_k b_{i-1}|_v\} \geq C_v^{-1}\max_i\{|b_i|_v\}\max\{|\alpha_k|_v, 1\}.$$

Lemma: For $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$, $\sigma \in \mathrm{Gal}_{\bar{\mathbb{Q}}|\mathbb{Q}}$, $H(P^\sigma) = H(P)$.

Pf/ σ permutes the factors in $\prod_v \max\{|x_i|_v\}^{n_v}$.

Note: σ can be any in $\mathrm{Gal}\,\bar{\mathbb{Q}}|\mathbb{Q}$: it can move elements in K!

So $H_{K^\sigma}(P^\sigma) = \prod_{v \in M_K} \max_i \{|x_i^\sigma|_{v\sigma}|^{n_{v\sigma}} \ldots$ //

Theorem: For given $C \overset{\in\mathbb{R}}{>} 0$, $d \in \mathbb{Z}_{>0}$,

$\{P \in \mathbb{P}^N(\bar{\mathbb{Q}}) : H(P) \leq C$ and $[\mathbb{Q}(P):\mathbb{Q}] \leq d\}$ is a finite set.

Pf/ Let $K = \mathbb{Q}(P)$.

$$H_K(P) = \prod_{v \in M_K} \max_i \{|x_i|_v\}^{n_v} \geq \max_i \left\{ \prod_{v \in M_K} \max\{|x_i|_v, 1\} \right\} = \max_i H_K((x_i:1))$$

Thus it suffices to show it for $N=1$.

Let x_i s.t. $H((x_i:1)) \leq C$, and let $e = [\mathbb{Q}(x_i):\mathbb{Q}] \leq d$.

$f(T) = T^e + \cdots + a_e$ be the minimal polynomial of x_i over $\mathbb{Q}$.

Then ~~$H(f(T))$~~ $H(f) \leq 2^{e-1} \prod_{\substack{x' \text{ conjugate of } x_i \\ \text{prev}}}^{e} H(x') \underset{\substack{\uparrow \\ \text{prev Lemma}}}{=} 2^{e-1} H(x_i)^e \leq (2C)^d$

But there are only finitely many polynomials of bounded height over $\mathbb{Q}$. (because bounded height $\Rightarrow$ bounded height of its coefficients), and

$\{H(p/q) \leq C' : \frac{p}{q} \in \mathbb{Q}\}$ is finite. //

- Height functions for <u>elliptic curves</u>.

Def: $h : \mathbb{P}^N(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}_{\geq 0}$ <u>logarithmic height</u>
$$P \longmapsto \log(H(P))$$

Def: Let E be an elliptic curve over K. Let $\bar{K}$ be the alg. closure of K, and let $f \in \bar{K}(E)$, $E \xrightarrow{(f:1)} \mathbb{P}^1$

Then $h_f : E(\bar{K}) \longrightarrow \mathbb{R}_{\geq 0}$
$$P \longmapsto h(f(P)) = \log H(\underbrace{f(P)}_{\in \mathbb{P}^1(\bar{K})})$$
(we will use $f = x : E \to \mathbb{P}^1$)

<u>Prop 6.1</u>: If K is a number field, and $f \in \bar{K}(E)$ is of finite degree,
$\{P \in E(K) : h_f(P) \leq C\}$ is finite. (evident)

<u>Theorem 6.2</u>:
Let $K(E) = K(x,y)$, let $f \in K(x)$ (we will use $f = x$).
Then, $\forall P, Q \in E(\bar{K})$, $h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + \mathcal{O}(1)$
where $\mathcal{O}(1)$ is a constant, independent of P and Q.

Pf
<u>Idea</u>:
$$(P,Q) \longmapsto (P+Q, P-Q)$$
$$\begin{tikzcd}
(P,Q) \arrow[d, mapsto] & E \times E \arrow[r, "G"] \arrow[d] & E \times E \arrow[d] & (P+Q, P-Q) \arrow[d, mapsto] \\
(x_1, x_2) \arrow[d, mapsto] & \mathbb{P}^1 \times \mathbb{P}^1 \arrow[d] & \mathbb{P}^1 \times \mathbb{P}^1 \arrow[d] & (x_3, x_4) \arrow[d, mapsto] \\
(x_1 x_2 : x_1 + x_2 : 1) & \mathbb{P}^2 \arrow[r, dashed, "g"'] & \mathbb{P}^2 & (x_3 x_4 ; x_3 + x_4 ; 1)
\end{tikzcd}$$
$(v : u : t)$ $\quad (g_2 : g_1 : g_0)$

morphism of degree 2, that is $\deg g_i = 2$, g_i homogeneous in $\cancel{t}, u, v$

Note that $G^{-1}(P+Q, P-Q) = \{(P+T, Q+T) : T \in E[2]\}$ is of size 4.

So now work with the diagram:

$$\begin{tikzcd} E\times E \arrow[r, "G"] \arrow[d, "\sigma"'] & E\times E \arrow[d, "\sigma"] \\ \mathbb{P}^2 \arrow[r, "g"] & \mathbb{P}^2 \end{tikzcd}$$

$$(1) = h(\sigma\circ G(P,Q)) = h(g\circ\sigma(P,Q)) = (2).$$

$$(1) = h((x_3x_4 : x_3+x_4 : 1)) = h(x_3) + h(x_4) + O(1)$$

(by using 5.9, $f = (x_3x_4 : x_3+x_4 : 1)$, $d=2$: $2^{-d}H(x_3)H(x_4) \leq H(f) \leq 2^{d-1}H(x_3)H(x_4)$)

$$(2) = h(g(x_2x_1 : x_1+x_2 : 1)) = 2h((x_1x_2 : x_1+x_2 : 1)) + O(1).$$

So $h(x_3)+h(x_4) = 2h(x_1) + 2h(x_2) + O(1)$.

Now if $f \in \bar{k}(x)$,

$$\begin{tikzcd} E \arrow[r, "f"] \arrow[d, "x"'] & \mathbb{P}^1 \\ \mathbb{P}^1 \arrow[ur, "\rho"'] & \end{tikzcd}$$

So $f = \rho\circ x$

We get $h_f(P) = \frac{\deg f}{2} h_x(P) + O(1)$ $(*)$ because $h_f(P) = h(f(P)) = h(\rho\circ x(P)) \overset{5.6}{=} \deg(\rho)\cdot h(x(P))$. //

"$\frac{\deg f}{2}$" $=\deg x$

And then

$$h_x(P+Q) + h_x(P-Q) = h_x(P) + h_x(Q) + O(1)$$

$$\Downarrow (*)$$

$$h_f(P+Q) + h_f(P-Q) = h_f(P) + h_f(Q) + O(1)$$

Theorem 6.7: (Mordell-Weil Th).

E/K an elliptic curve over a number field K. Then $E(K)$ is finitely-generated.

$$E(K) = E(K)_{tors} \times \mathbb{Z}^r$$

Pf: Enough to prove that the height function exists. $h : E(K) \to \mathbb{R}$. ((1),(2),(3))

(1): $h(P+Q) \leq 2h(P) + C_1$ $C_1 = C_1(E,Q)$

(2): $h([m]P) \geq m^2 h(P) - C_2$ $C_2 = C_2(E,m)$

(3): $\forall C_3$, $\{P \in E(K) : h(P) \leq C_3\}$ is finite. $\Leftarrow$ done.

Condition (1) follows immediately from Thm 6.2., since $h_X(P-Q)\geq 0$ and $h_X(Q)=O(1)$ (for fixed Q!).

Condition (2) is true for $m=\overset{\text{trivial}}{0,1},2 \leftarrow$ Thm 6.2. But it is true actually for all m! By induction,

$$h_X([m+1]P)+h_X([m-1]P)=2h_X([m]P)+2h_X(P)+O(1).$$

So

$$h_X([m+1]P)=\left[-(m-1)^2+2m^2+2\right]h_X(P)+O(1)=(m+1)^2h_X(P)+O(1).$$

<u>Flowchart of the proof.</u>

$$\left.\begin{matrix}5.6\\5.9\end{matrix}\right\}\to 6.2\to 3.1$$
$$5.11\to 3.1$$
$$\left.\begin{matrix}3.1\\1.1\end{matrix}\right\}\to 6.7$$

<u>Def 9.1</u>: The canonical height, or Neron-Tate height of a point P.

$$\frac{1}{\deg f}\lim_{N\to\infty}4^{-N}h_f([2^N]P)=:\hat{h}(P)$$

<u>exists</u> and is <u>independent of f</u>.

<u>Thm 9.3</u>:

(a) $\hat{h}(P+Q)+\hat{h}(P-Q)=2\hat{h}(P)+2\hat{h}(Q)$

(b) $m^2\hat{h}(P)=\hat{h}([m]P)$

(c) $\langle P,Q\rangle:=\hat{h}(P+Q)-\hat{h}(P)-\hat{h}(Q)$ is a bilinear form (so $\hat{h}$ is a quadratic form)

(d) $\hat{h}(P)\geq 0$ with equality iff P is a torsion point.

(e) $(\deg f)\cdot\hat{h}=h_f+O(1)$.

In the proof of the Weak MW-theorem, we used

$$E(K) \times G_{\bar{K}/K} \to E[m]$$
$$(P,\sigma) \mapsto Q^{\sigma} - Q \quad \text{where } [m]Q = P.$$

In non-degenerate form,

$$E(K)/mE(K) \times G_{L/K} \longrightarrow E[m] \quad \text{where } L = K(Q : mQ \in E(K)).$$

But the computation of $E(\mathbb{Q})/2E(\mathbb{Q})$ (as in Homework) used

$$E'(\mathbb{Q})/\phi E(\mathbb{Q}) \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2} \quad \text{where } E: y^2 = x^3+ax^2+bx,\ \phi: E \to E',\ \ker\phi = \{O,(0,0)\}.$$

$$E'(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$
$$(u,v) \longmapsto u\mathbb{Q}^{*2}$$

The isogeny $\phi: E \to E'$ gives rise to

$$\begin{tikzcd} k(E) \arrow[d, dash, "2"] \\ \phi^* k(E') \end{tikzcd} \qquad \begin{tikzcd} (x,y) \arrow[dr, dash] & & (x',y') \arrow[dl, dash] \\ & (u,v) & \end{tikzcd}$$

and $(x,y),(x',y') \in \underline{E(\mathbb{Q})} \Rightarrow u \in \mathbb{Q}^{*2}$.

Now assume $E[2] \subseteq E(\mathbb{Q})$, i.e.

$E: y^2 = (x-e_1)(x-e_2)(x-e_3)$ for $e_i \in \mathbb{Q}$. Each e_i gives a 2-isogeny.
($\ker\phi_i = \{O,(e_i,0)\}$.)

$$\begin{tikzcd} & E_1 \arrow[dr, "\hat{\phi}_1"] & \\ E \arrow[ur, "\phi_1"] \arrow[r, "\phi_2"] \arrow[dr, "\phi_3"'] & E_2 \arrow[r, "\hat{\phi}_2"] & E \\ & E_3 \arrow[ur, "\hat{\phi}_3"'] & \end{tikzcd} \qquad \begin{tikzcd} & k(E) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \phi_1^* k(E_1) \arrow[dr, dash] & \phi_2^* k(E_2) \arrow[d, dash] & \phi_3^* k(E_3) \arrow[dl, dash] \\ & [2]^* k(E) & \end{tikzcd}$$

and $k(E)/[2]^* k(E)$ is Galois, (by thm III 4.10)
with $\mathrm{Gal} = E[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Consider
$$E(\mathbb{Q}) \longrightarrow \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right)^3$$
$$(x,y) \longmapsto (\sigma_1, \sigma_2, \sigma_3) = (x-e_1, x-e_2, x-e_3)$$

Clearly, $\sigma_1\sigma_2\sigma_3 = y^2 \in \mathbb{Q}^{*2}$.

Also, $\sigma_i \in \mathbb{Q}^{*2} \Leftrightarrow (x,y) \in \hat{\varphi}_i E_i(\mathbb{Q}) \Leftrightarrow$

$$\begin{tikzcd}[column sep=small] (u,v) \arrow[dr] & & (u',v') \arrow[dl] & \in E_1(\mathbb{Q}) \\ & (x,y) & & \end{tikzcd}$$

So $(\sigma_1,\sigma_2,\sigma_3) = (1,1,1) \Leftrightarrow (x,y) \in E(\mathbb{Q})$ has four preimages in $E(\mathbb{Q})$ under $[2] \Leftrightarrow$

$\Leftrightarrow (x,y) \in 2E(\mathbb{Q})$.

($\Leftarrow$ need Galois extension.)

So we get an injection $\dfrac{E(\mathbb{Q})}{2E(\mathbb{Q})} \xhookrightarrow{\sigma = (\sigma_1,\sigma_2,\sigma_3)} \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right)^3$

We can regard at it as:

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \times E[2] \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$
$$(P, \quad T) \longmapsto f_T(P) \qquad \text{where } \operatorname{div} f_T = 2(T) - 2(O)$$
$$(\operatorname{div}(x-e_i) = 2(e_i,0) - 2O).$$

Let $E[m] \leq E(K)$. We will define a commutative diagram as follows:

$$\begin{tikzcd} \frac{E(K)}{mE(K)} \times E[m] \times G_{L/K} \arrow[r, "\text{Kummer on } E(K) \times id_{E[m]}"] \arrow[d, "\text{Take Pairing} \times id_{G_{L/K}}"'] & E[m] \times E[m] \arrow[d, "\text{Weil Pairing}"] \\ K^*/K^{*m} \times G_{L/K} \arrow[r, "\text{Kummer on } K^*"] & \mu_m \in \bar{K}^* \end{tikzcd}$$

- The Weil Pairing

$$E[m] \times E[m] \longrightarrow \mu_m \subset \bar{K}^*$$
$$(S,T) \longmapsto e_m(S,T)$$

$T \in E[m] \Rightarrow mT - mO = (f)$ for some $f \in K(E)$

Also, $(f \circ [m])(P) = 0 \Leftrightarrow f([m]P) = 0 \Leftrightarrow [m]P = T$

$(f \circ [m])(P) = \infty \Leftrightarrow f([m]P) = 0 \Leftrightarrow [m]P = O \Leftrightarrow P \in E[m]$.

Choose $T' \in E(\bar{K})$, with $[m]T' = T$.

Then, $(f \circ [m])_0 = m \cdot \sum_{R \in E[m]} T' + R$

$(f \circ [m])_\infty = m \cdot \sum_{R \in E[m]} R$

$$\Rightarrow (f \circ [m]) = m \underbrace{\left(\sum_{R \in E[m]} (T'+R) - \sum_{R \in E[m]} R \right)}_{(g) = \operatorname{div} g \text{ for some } g \in K(E).}$$

After scaling f by a constant, we may assume that $f \circ [m] = g^m$

Now define $e_m(S,T) := \dfrac{g(X+S)}{g(X)}$ for any $X \in E(K)$.

Note that:

$$g(X+S)^m = (f \circ [m])(X+S) = f([m]X + [m]S) = (f \circ [m])X = g(X)^m$$

Thus $e_m^X(S,T) \in \mu_m$.

There is at least an $a \in \mu_m$ s.t $g(X+S) - a\,g(X) = 0$ for infinitely many X.

So it is identically 0, so $g(X+S) = a\,g(X)$ $\forall X$.

So now, we can compute:

$$\begin{tikzcd}
E(K)\times E[m]\times G_{L|K} & E[m]\times E[m] \\
(P,\,T,\,\sigma) \arrow[r, mapsto] \arrow[d, "\substack{\mathrm{div}\, f_T \\ = mT - mO}"'] & (Q^\sigma - Q,\, T) \arrow[d, "\text{choose } X = Q"] \\
(f_T(P),\,\sigma) \arrow[r, mapsto] & \dfrac{\beta^\sigma}{\beta} \overset{?}{=} \dfrac{g_T(Q^\sigma)}{g_T(Q)} = \dfrac{g_T(Q)^\sigma}{g_T(Q)}
\end{tikzcd}$$

$f_T(P) = \alpha = \beta^m$, $\beta = \sqrt[m]{\alpha}$, in some extension of K.

The diagram commutes if $\beta^m = (g(Q))^m = f_T(\underbrace{[m]Q}_{=P}) = f_T(P)$

Notation

→ Weil pairing: $e_m(Q^\sigma - Q, T) = \dfrac{g_T(Q)^\sigma}{g_T(Q)}$ s.t. $\mathrm{div}\, f_T = mT - mO$, $f_T \circ [m] = g_T^m$

→ $\delta_E : E(K)/mE(K) \longrightarrow \{\text{maps } (\sigma \mapsto Q^\sigma - Q) \text{ for } \sigma \in G_{\bar K|K},\ mQ \in E(K)\}$.

→ $\delta_K : K^*/K^{*m} \longrightarrow \{\text{maps } (\sigma \mapsto \beta^\sigma \beta^{-1}) \text{ for } \sigma \in G_{\bar K|K},\ \beta^m \in K^*\}$

→ Tate-pairing: $b(P,T) = f_T(P) \in K^*/K^{*m}$

Thm (a) The diagram commutes: $\underbrace{e_m(\delta_E(P), T)}_{\text{a function of } \sigma \text{ (map } G_{\bar K|K} \to \mu_m)} = \underbrace{\delta_K(b(P,T))}_{\text{map } G_{\bar K|K} \to \mu_m}$ and b is bilinear

(b) The Tate pairing b $(P,T) \mapsto f_T(P)$ is non-degenerate on the left:

if $b(P,T) \in K^{*m}$ $\forall\, P \in E(K)$, then $T = O$.

Pf (a) is almost done. To prove b bilinear, can use the bilinearity of the other arrows.

(b) It is enough to show that the Weil pairing $e_m(S,T)$ is non-deg on the left.

Then, $\delta_K(b(P,T)) = 1\ \forall\, P \in E(K) \iff e_m(\delta_E(P), T) = 1\ \forall\, P \in E(K) \iff T = O$.

(and δ_K is an isomorphism).

To see that $e_m(S,T)=1\ \forall\ S\in E[m] \Rightarrow T=O$:

if $e_m(S,T)=1\ \forall S\in E[m] \iff \dfrac{g_T(X+S)}{g_T(X)}=1\ \ \forall S\in E[m]$.

we get that:

<u>Claim</u>: This implies that $g_T=h\circ[m]$, for some h.

~~Pf~~ This uses that:

$$\begin{array}{l} k(E) \\ \Big|\ \text{Galois of deg } m^2,\ \mathrm{Gal}\cong E[m] \quad \tau_T^* \leftarrow\!\shortmid\ T \\ [m]^*k(E) \end{array}$$

(see [Sil III 4.10b]) where τ_T is the translation-by-T-map.

For $\varphi\in k(E)$, $\tau_T^*\circ\varphi=\varphi\circ\tau_T$

So $g_T(X+S)=g_T(X) \iff \tau_S^* g_T=g_T \Rightarrow g_T$ is fixed by $\tau_S^*\in \mathrm{Gal}\left(k(E)/[m]^*k(E)\right)$

In our case, it is true $\forall S\in E[m]$, so $g_T\in[m]^*k(E)$,

so $g_T=h\circ[m]$ for some $h\in k(E)$.

So $g_T=h\circ[m]$, and $g_T^m=f_T\circ[m]$. ~~So $g_T^m=h$~~

So $f_T\circ[m]=(h\circ[m])^m=h^m\circ[m] \Rightarrow f_T=h^m$

So $\mathrm{div}\, h^m=\mathrm{div}\, f_T=mT-mO \Rightarrow \mathrm{div}\, h=T-O \overset{\text{R-R}}{\Rightarrow} h\in k \Rightarrow T=O$

<u>Prop</u> ((c) in Thm): $b: E(k)/mE(k) \times E[m] \to k^*/k^{*m}$ has as image $\subseteq k(S,m)$ (a subgroup of)

where $k(S,m):=\{b\in k^*/k^{*m} ; \mathrm{ord}_\mathfrak{p}(b)\equiv 0 \pmod m$ for all $\mathfrak{p}\notin S\}$

for $S=M_k^\infty \cup \{\mathfrak{p}\in M_k^0 : E$ bad reduction at $\mathfrak{p}\}\cup\{\mathfrak{p}\in M_k^0 : \mathfrak{p}\mid m\}$.

Pf Recall (VIII) that if $L = K(Q : mQ \in E(K))$, then L/K is unramified outside S.

Let $\beta^m = \delta_T(P) = g_T(Q)^m$. Then $\beta = g_T(Q) \in L = K(Q : mQ \in E(K))$.

$$\begin{array}{ll} \mathfrak{q} & K(\beta) \quad \beta^m - b = 0 \\ | & | \\ \mathfrak{p} & K \end{array}$$

For $\mathfrak{p} \notin S$, $k(\beta)/K$ is unramified at $\mathfrak{p}$.

$$\left.\begin{array}{l} \mathrm{ord}_{\mathfrak{q}}(b) \overset{\mathfrak{q}|\mathfrak{p} \text{ unramified}}{=} \mathrm{ord}_{\mathfrak{p}}(b) \\ \quad \| \\ \mathrm{ord}_{\mathfrak{q}}(\beta^m) = m\, \mathrm{ord}_{\mathfrak{q}}(\beta) \end{array}\right\} \Rightarrow m \mid \mathrm{ord}_{\mathfrak{p}}(b)$$

//

__Prop (a) in Thm__: All arrows can be defined explicitly. (But that is how we started it!)

Consider the s.e.s.

$$1 \to \mu_m \to \bar{K}^* \xrightarrow{\wedge m} \bar{K}^* \to 1$$
$$x \longmapsto x^m$$

$$1 \to E[m] \to E(\bar{K}) \xrightarrow{[m]} E(\bar{K}) \to 1$$

Assume that $E[K] \subseteq E(K)$. Then have an exact seq:

$$1 \to E[m] \to E(K) \xrightarrow{[m]} E(K) \qquad \text{(not surjective)}$$

Let $\delta_E : E(K) \longrightarrow \mathrm{Hom}(G_{\bar{K}|K}, E[m])$, $P \mapsto (\sigma \mapsto Q^\sigma - Q)$

It is a group homomorphism, and $\ker \delta_E = mE(K)$. So:

$$1 \to E[m] \to E(K) \xrightarrow{[m]} E(K) \xrightarrow{\delta_E} \mathrm{Hom}(G_{\bar{K}|K}, E[m]) \to \cdots$$ Long exact sequence.

We will also get (using δ_K), and __assuming__ $\mu_m \subseteq K^*$:

$$1 \to \mu_m \to K^* \xrightarrow{m} K^* \xrightarrow{\delta_K} \mathrm{Hom}(G_{\bar{K}|K}, \mu_m) \to 1$$ ← this one actually stops!

$$b \longmapsto (\sigma \mapsto \beta^\sigma \beta^{-1})$$

Cohomology in the category of G-modules.

profinite works fine.

Let G be a group (could be nonabelian, could be infinite).

Def A G-module A is an abelian group on which G acts.

Def A morphism (or a G-homomorphism) is a gp hom. $A \xrightarrow{f} B$ s.t. f commutes with the action of G.

Rk: when G is infinite, need to assume that the action of G on A is continuous.
(i.e. for each $a \in A$, the stabilizer of a is of finite index in G).
(A has the discrete topology, and G a topology ~~in which~~ generated by the normal subgroups of finite index). (profinite topology).

Def $H^0(G,A) := A^G$, the subgroup of G-invariant elements of A.

$H^1(G,A) := Z^1(G,A) / B^1(G,A)$

where $Z^1(G,A) := \{ \{\theta_\sigma\} : \overset{G}{\overset{\Psi}{\sigma}} \mapsto \overset{A}{\overset{\Psi}{a_\sigma}} \mid \sigma(a_\tau) = a_{\sigma\tau} - a_\sigma \}$ ← 1-cocycles.

$B^1(G,A) := \{ \{\theta_\sigma\} : \sigma \mapsto \sigma\alpha - \alpha$ for $\alpha \in A \}$.

Note that $B^1(G,A) \subseteq Z^1(G,A)$: ~~$\tau(\sigma\alpha - \alpha) = (\tau\sigma)(\alpha) - \tau\alpha = (\tau\sigma)\alpha - \alpha - (\tau\alpha - \alpha)$~~

$\sigma(\tau\alpha - \alpha) = (\sigma\tau)\alpha - \sigma\alpha = ((\sigma\tau)\alpha - \alpha) - (\sigma\alpha - \alpha)$ //

Two cycles $\{\theta_\sigma\}$, $\{\theta'_\sigma\}$ are said to be <u>cohomologous</u> if
$\exists\, \alpha$ s.t. $\theta'_\sigma - \theta_\sigma = \{\sigma\alpha - \alpha\}$ (i.e. $\theta'_\sigma - \theta_\sigma \in B^1(G,A)$).

(multiplicatively, $\theta'_\sigma = \alpha^{-1} \cdot \theta_\sigma \cdot \alpha^\sigma$).

(if $A^G = A$ (the action is trivial) then $B^1(G,A) = 0$, and $\underset{H^1(G,A)}{\overset{\shortparallel}{Z^1(G,A)}} = \mathrm{Hom}(G,A)$)

<u>Note</u>: $H^0(G,-)$ is a functor:

$$A \xrightarrow{f} B$$

becomes: $\underset{A^G}{\overset{\shortparallel}{H^0(G,A)}} \xrightarrow{f_0} H^0(G,B) = B^G$ and $f_0 = f|_{A^G}$

<u>Lemma</u>: $H^1(G,-)$ is a functor:

Pf/

$$H^1(G,A) \xrightarrow{f_1} H^1(G,B)$$
$$\{\theta_\sigma\} \longmapsto f\circ\{\theta_\sigma\}$$

Easy to verify that f_1 preserves cocycles and coboundaries.

<u>Theorem</u>: Let $0 \to A \to B \xrightarrow{\phi} C \to 0$ be a s.e.s of G-modules. Then there is a long exact sequence

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \xrightarrow{\delta} H^1(G,A) \to H^1(G,B) \to H^1(G,C) \to \cdots$$

where $\delta : H^0(G,C) \longrightarrow H^1(G,A)$ is defined as follows:

Let $c \in C^G = H^0(G,C)$. Then $c = \phi(b)$ for some $b \in B$.

Define $\{\theta_\sigma\} : \sigma \longmapsto \sigma b - b$

As $\phi(\sigma b - b) = \sigma\phi(b) - \phi(b) = \sigma c - c \overset{c \in C^G}{=} 0$, then $\sigma b - b \in \operatorname{im}(A)$.

Need to check that δ is well defined, and other things. ("exercise").

Special case: $G_{\bar{k}|k}$ acts on $E = E(\bar{k})$.

$$0 \to E[m] \to E \xrightarrow{[m]} E \to 0$$

gives a long exact sequence: (if we assume $E[m] \subseteq E(k)$).

$$0 \to E[m] \to E(k) \xrightarrow{[m]} E(k) \xrightarrow{\delta_E} \underbrace{H^1(G_{\bar{k}|k}, E[m])}_{= \, \mathrm{Hom}(G_{\bar{k}|k}, E[m])} \to H^1(G_{\bar{k}|k}, E) \xrightarrow{[m]} H^1(G_{\bar{k}|k}, E)$$

interpret as twists of E (§2) — interpret as homogeneous spaces.

And in fact, $\cancel{E(k) \times G_{\bar{k}|k} \to E[m], \ (P, \sigma) \mapsto}$

We have seen it:

$$\delta_E(P) = \langle P, - \rangle.$$

We can also start with $0 \to E[\phi] \to E \xrightarrow{\phi} E \to 0$ (a general isogeny)

gives a Kummer sequence: (using $0 \to H^0 \to H^0 \to \boxed{H^0 \to H^1 \to H^1} \to H^1 \to \dots$)

$$\begin{array}{ccccccccc}
0 \to & E(k)/\phi(E(k)) & \to & H^1(G_{\bar{k}|k}, E[\phi]) & \to & H^1(G_{\bar{k}|k}, E)[\phi] & \to 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 \to & 0 & \to & \prod_v H^1(G_{\bar{k}_v|k_v}, E[\phi]) & \to & \prod_v H^1(G_{\bar{k}_v|k_v}, E)[\phi] & \to 0
\end{array}$$

By the snake lemma, can obtain a new sequence:

$$\begin{array}{ccccccccc}
& 0 & & & & & \\
& \downarrow & & & & & \\
0 \to & E(k)/\phi E(k) & \to & \boxed{\mathrm{Sel}^{(\phi)}(E/k)} & \to & \boxed{Ш(E/k)[\phi]} & \to 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 \to & E(k)/\phi E(k) & \to & H^1(G_{\bar{k}|k}, E[\phi]) & \to & H^1(G_{\bar{k}|k}, E)[\phi] & \to 0 \\
& \downarrow & & \downarrow & & \downarrow & \\
0 \to & 0 & \to & \prod_v H^1(G_{\bar{k}_v|k_v}, E[\phi]) & \to & \prod_v H^1(G_{\bar{k}_v|k_v}, E)[\phi] & \to 0
\end{array}$$

Let C/K be a curve (smooth, proj).
Let D/K be a curve which is isomorphic to C over $\bar{K}$, $D \xrightarrow{\phi} C$ (ϕ defined over $\bar{K}$).

Define $\Theta: \underset{G_{\bar{K}|K}}{\sigma} \longmapsto \overset{\mathrm{Isom}(C)}{\phi^\sigma \circ \phi^{-1}}$

call Isom because ϕ need not be an isogeny.

Claim: Θ is a cocycle. $\left(\Theta \in Z^1(G_{\bar{K}/K}, \mathrm{Isom}(C))\right)$.

$\mathrm{Isom}(C) = \{\bar{K}\text{-isos of } C\}$.

Pf $\cancel{\tau(\phi^\sigma \circ \phi^{-1}) = (\phi^\sigma)^\tau \circ (\phi^\tau)^{-1} = \phi^{\tau\sigma}}$

$$\sigma(\Theta_\tau) = \sigma(\phi^\tau \circ \phi^{-1}) = (\phi^\tau)^\sigma \circ (\phi^\sigma)^{-1} = (\phi^{\sigma\tau}) \circ \phi^{-1} \circ \underbrace{\phi \circ (\phi^\sigma)^{-1}}_{= (\phi^\sigma \circ \phi^{-1})^{-1}} = \Theta_{\sigma\tau} \cdot \Theta_\sigma \quad //$$

Claim The class $\{\Theta_\sigma\} \in H^1(\ )$ depends only on D, not on ϕ.

Pf

$$\begin{tikzcd} D \arrow[r, "\phi"] \arrow[dr, "\phi'"'] & C \arrow[d, "\alpha"] \\ & C \end{tikzcd}$$

$\Rightarrow \Theta'_\sigma = \phi'^\sigma \circ \phi'^{-1} = (\alpha \circ \phi)^\sigma \circ (\alpha \circ \phi)^{-1} =$
$= \alpha^\sigma \circ \phi^\sigma \circ \phi^{-1} \circ \alpha^{-1} = \alpha^\sigma\, \Theta_\sigma \circ \alpha^{-1}$

So $\Theta' \sim \Theta$.

Claim: The cocycle Θ depends only on the K-isomorphism class of D.

Pf

$$\begin{tikzcd} D \arrow[r, "\phi"] & C \\ D' \arrow[u, "\lambda"] \arrow[ur, dashed, "\phi'"'] & \end{tikzcd}$$

where $\lambda: D' \xrightarrow{\sim} D$ is defined over $\underline{\underline{K}}$.

Now $\Theta'_\sigma = \phi'^\sigma \circ \phi'^{-1} = (\phi \circ \lambda)^\sigma \circ (\phi \circ \lambda)^{-1} = \phi^\sigma \circ \underbrace{\lambda^\sigma \circ \lambda^{-1}}_{\substack{\text{id} \\ \text{because } \lambda^\sigma = \lambda}} \circ \phi^{-1} = \Theta_\sigma$.

Def: A twist D/K of C/K is a K-isomorphism class of $D \simeq C$ over $\bar{K}$.

$\mathrm{Twist}(C/K) = \{D/K : D \simeq_{\bar{K}} C\}/\sim$ where $\sim$ is K-isomorphism.

<u>Theorem</u>: The natural map $\mathrm{Twist}(C/K) \longrightarrow H^1(G_{\bar{K}|K}, \mathrm{Isom}(C))$

$$[D/K] \longmapsto [\theta : \sigma \mapsto \phi^\sigma \circ \phi^{-1}]$$

$$(\phi : D \xrightarrow{\cong} C)$$

is a <u>bijection</u>.

pf/ It is well defined by all the previous claims.

<u>Injective</u>: Let D, D' be two twists with cohomologous 1-cocycles:

$$\begin{tikzcd} D \arrow[r, "\phi"] & C \arrow[d, "\alpha"] \\ D' \arrow[u, dashed, "\lambda"] \arrow[r, "\phi'"] & C \end{tikzcd}$$

s.t. $\exists \alpha \in \mathrm{Isom}(C)$ s.t.

$$\phi'^\sigma \circ \phi'^{-1} = \alpha^\sigma \circ \phi^\sigma \circ \phi^{-1} \circ \alpha^{-1}$$

$(\lambda := \phi^{-1} \circ \alpha^{-1} \circ \phi')$.

Need to show that λ is defined over K, i.e.

$$\forall \sigma, \ (\phi^{-1} \circ \alpha^{-1} \circ \phi')^\sigma = (\phi^{-1} \circ \alpha^{-1} \circ \phi')$$

//

<u>Surjective</u>: we need now to "create" a curve, so it will be more difficult.

Let $\bar{K}(C)$ be the function field of C over $\bar{K}$.

Look for a curve D/K s.t. $D \underset{\bar{K}}{\cong} C$ ($\Leftrightarrow \bar{K}(D) \cong \bar{K}(C)$). as fields. C, D smooth, proj. birationally equivalent.

we look then for a f.field $K(D)$ s.t.

$$\begin{cases} K(D) \otimes_K \bar{K} = \bar{K}(C) \\ D \longmapsto \{\theta_\sigma\} \quad (\text{for a given } \{\theta_\sigma\}) \end{cases}$$

Given $\{\theta_\sigma\} \in H^1(G_{\bar{K}|K}, \mathrm{Isom}(C))$, construct

$K(D)$ = fixed field of $\bar{K}(C)$ by a group G'.

Let $G' := \{\sigma' : \sigma \in G\}$ where $f^{\sigma'} := f^\sigma \circ \theta_\sigma$

$$\begin{tikzcd} C \arrow[r, "f^{\sigma'}"] \arrow[d, "\theta_\sigma"'] & \mathbb{P}^1 \\ C \arrow[ur, "f^\sigma"'] & \end{tikzcd}$$

(defined G' by how it acts on $\bar{K}(C)$).

(cont proof).

Need to check:

1) G' acts on $\bar{K}(C)$ (requires the cocycle condition).

2) G' acts continuously on $\bar{K}(C)$.

For $f \in \bar{K}(C)$, $\mathrm{Stab}(f)$ is of finite index in G':

$f = f^{\sigma'}$ when $\theta_\sigma = id$ and $f = f^{\sigma}$ (may not be necessary condition).

(2) ~~$G_{\bar{K}|K}$ acts continuously on~~ The cocycle $\theta_\sigma : G_{\bar{K}|K} \to \mathrm{Isom}(C)$ is continuous $\Rightarrow H = \{\sigma \in G_{\bar{K}|K} : \theta_\sigma = id\}$ is of finite index.

So $H' = \{\sigma \in G_{\bar{K}|K} : f^{\sigma} = f\}$ is of finite index.

But then $H \cap H'$ is of finite index in G by general group theory.

Claim: $\bar{K}(C)^{G'} \cap \bar{K} = K$ (want it so that D is defined over K).

Let $f \in \bar{K}$. Then $C \xrightarrow{f} \mathbb{P}^1$ is constant.

$f \in \bar{K}(C)^{G'} \Leftrightarrow f^{\sigma'} = f \quad \forall \sigma' \in G'$. (1)

Since f^{σ} is constant, $f^{\sigma'} = f^{\sigma} \; \forall \sigma$ (2)

$$\begin{tikzcd} C \arrow[r, "f^{\sigma'}"] \arrow[d, "\theta_\sigma"'] & \mathbb{P}^1 \\ C \arrow[ur, "f^{\sigma}"'] & \end{tikzcd}$$

So $f^{\sigma} \underset{(2)}{=} f^{\sigma'} \underset{(1)}{=} f$

Note. Not all twists C/K of an elliptic curve E/K are elliptic curves:

C/K ~~may~~ not have a K-rational point!.

The twists C/K of an elliptic curve E/K that correspond to cocycles

$\theta \in H^1(G_{\bar{K}|K}, E) \subseteq H^1(G_{\bar{K}|K}, \mathrm{Isom}(E))$ are called the

homogeneous spaces for E/K.

Since $E = E(\bar{K})$ is abelian group, $H^1(G_{\bar{K}|K}, E)$ is a group inside a bigger set.

The set (group) of homogeneous spaces for E/K is denoted.

$WC(E/K)$: the <u>Weil-Chatelet</u> Group of E/K.

(originally, it was defined without cohomology).

We will define now $WC(E/K)$ independently, and later show that the two definitions coincide.

<u>Def</u>: A <u>homogeneous space</u> for E/K is a smooth curve C/K, together with a <u>simply transitive</u> group action of E on C defined over K.

$$\mu : C \times E \longrightarrow C \qquad \text{(a morphism defined over } K\text{)}$$
$$(p, P) \longmapsto \mu(p, P) = \text{"} p + P \text{"}$$

i.e.

(1) $p + O = p$

(2) $p + (P + Q) = (p + P) + Q$ simply (uniqueness) transitive (existence)

(3) $\forall_{p, q \in C}$, $\exists !\, P \in E$: $q = p + P$.

By (3), define $\nu : C \times C \longrightarrow E$
$$(q, p) \longmapsto P \quad \text{s.t.} \quad q = p + P. \quad (\text{write "} q - p \text{"})$$

We will later show that ν is also a morphism defined over K.

Let K be a field of <u>characteristic 0.</u>

<u>Prop</u>: For a homogeneous space C/K for E/K, choose $p_0 \in C$ (over $\bar{K}$) and let
$$\theta : E \longrightarrow C \qquad (\theta = \mu(p_0, -)).$$
$$P \longmapsto p_0 + P$$

a) θ is an isomorphism defined over $K(p_0)$

b) $p + P = \theta(\theta^{-1}(p) + P)$

c) $q - p = \theta^{-1}(q) - \theta^{-1}(p)$ on the elliptic curve!

d) $\nu : C \times C \longrightarrow E$ is a morphism defined over K.
$(q, p) \longmapsto q - p$

Pf (of prop):

(a) Let $\sigma \in G_{\bar{K}/K}$ s.t. $P_0^\sigma = P_0$. Then $\theta(P)^\sigma = (p_0 + P)^\sigma = p_0^\sigma + P^\sigma = p_0 + P^\sigma = \theta(P^\sigma)$
$\Rightarrow$ the coeff. of θ are invariant under $\sigma \Rightarrow \sigma$ defined on $K(P_0)$.
We know it is a morphism. To prove isomorphism, note that
θ is of degree 1?, ~~with~~ inverse the rational map $q = p_0 + P \longmapsto P = q - p_0$.

~~If we assume proved that $\nu: E\times C \to E$ is a morphism we will be~~ done.

(if char $K = 0$, we don't need ν: as θ is bijective on points, $\deg \theta = 1$. //

(b) $\theta(\theta^{-1}(p) + P) = p_0 + (\theta^{-1}(p) + P) = (p_0 + \theta^{-1}(p)) + P = p + P$ //

(c) $\theta^{-1}(q) - \theta^{-1}(p) \underset{\uparrow \text{ simply transitive}}{=} (p_0 + \theta^{-1}(q)) - (p_0 + \theta^{-1}(p)) = q - p$

(d) ν is a morphism by (c). Also,

$$(q-p)^\sigma = (\theta^{-1}(q) - \theta^{-1}(p))^\sigma = \theta^{-1}(q)^\sigma - \theta^{-1}(p)^\sigma = (p_0 + \theta^{-1}(q))^\sigma - (p_0 + \theta^{-1}(p))^\sigma =$$
$$= q^\sigma - p^\sigma \quad . \quad \Rightarrow \nu \text{ defined over } K$$ //

<u>Def</u> Two homogeneous spaces C/K, C'/K are <u>equivalent</u>,

$C/K \sim C'/K \iff \exists\, \theta : C \xrightarrow{\simeq} C'$ defined over K which is compatible with the action of E:

i.e.

$$\begin{array}{ccc} C\times E & \xrightarrow{\mu} & C \\ {\scriptstyle(\theta,\mathrm{id})}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\theta} \\ C'\times E & \xrightarrow{\mu'} & C \end{array}$$

(i.e. $\theta(p + P) = \theta(p) + P$.

The class of E/K is called the <u>trivial class</u>.

Def The Weil-Châtelet group $WC(E/k) := \{ [C/k] : C/k \text{ hom-spaces for } E/k \}$ (classes).

Prop: $C/k \sim E/k \iff C(k) \neq \emptyset$

Pf $\Rightarrow$] Let $\theta : E \xrightarrow{\simeq} C$ where θ defined over k.

Then $\theta(O) \in C(k)$ //

$\Leftarrow$] Fix $P_0 \in C(k)$, and let
$$\theta : E \longrightarrow C$$
$$P \longmapsto P_0 + P$$

θ is an isomorphism defined over $k(P_0) = K$!
Need to check that θ is compatible with μ:

$$\theta(Q+P) = P_0 + Q + P = (P_0+Q) + P = \theta(Q) + P$$ //

Recall that there's a bijection $\mathrm{Twists}(E/k) \leftrightarrow H^1(G_{\bar{k}/k}, \mathrm{Isom}(E))$.

Also, $H^1(G_{\bar{k}/k}, E(\bar{k})) \subseteq H^1(G_{\bar{k}/k}, \mathrm{Isom}(E))$.

Moreover, $WC(E) \subseteq \mathrm{Twists}(E/k)$.

$\to$ So, is $WC(E) \overset{?}{=} H^1(G_{\bar{k}/k}, \mathrm{Isom}(E))$??

YES !

Theorem: Let E/k be an elliptic curve. Then, the map

$$W.C.(E/k) \longrightarrow H^1(G_{\bar{k}/k}, E)$$
$$[C/k] \longmapsto \{ \sigma \mapsto P_0^\sigma - P_0 \} \quad \text{where } P_0 \in C \text{ (arbitrarily chosen)}$$

is well-defined, and is a bijection between the two sets.

Pf
1) $\sigma \mapsto P_0^\sigma - P_0$ is a cocycle.
2) The map is well-defined.

Let $C/k \sim C'/k$, say $\Theta : C \xrightarrow{\sim} C'$ and let $P_0' \in C'$ (include here the case $C = C'$, $P_0' \neq P_0$).

$$P_0^\sigma - P_0 = \Theta(P_0^\sigma) - \Theta(P_0) = \Theta(P_0)^\sigma - \Theta(P_0) = (P_0' + P)^\sigma - (P_0' + P) = (P_0'^\sigma - P_0') + (P^\sigma - P)$$

As $P^\sigma - P$ is a coboundary, the two are equivalent as cocycles.

$\mathcal{L}$

(cont proof).

i) Injectivity:

Let $p_0^\sigma - p_0$ (for $p_0 \in C$) be cohomologous to $p_0'^\sigma - p_0'$ (for $p_0' \in C'$).

If $p_0^\sigma - p_0 = (p_0'^\sigma - p_0') + P_0^\sigma - P_0$, define

$$\theta : C \longrightarrow C'$$
$$p \longmapsto p_0' + (p - p_0) + P_0$$

and verify it.
(that it is Galois-invariant)

$$\begin{tikzcd} p_0 \; C \arrow[rr] \arrow[dr, "\sim"] & & C' \; p_0' \arrow[dl, "\sim"'] \\ & E \arrow[r, "\sim"', "+P_0"] & E \end{tikzcd}$$

$p \mapsto p - p_0$, $\quad q \mapsto q - p_0'$

ii) Surjectivity:

Given a cocycle, we know that there exists a twist that maps to it. But we want it to be actually in $WC(E)$.

Let $\theta \in H^1(G_{\bar{K}|K}, E)$. $\exists$ a twist C/K corresponding to θ.
$(\theta : \sigma \mapsto Q_\sigma) \rightsquigarrow$ let $\theta : \sigma \mapsto \tau_{-Q_\sigma} \in \mathrm{Isom}(E)$

We know $\tau_{-Q_\sigma} = \theta = \phi^\sigma \circ \phi^{-1}$ for $\phi : C \to E$, and want to give to C/K the structure of an homogeneous space.

Define

$$\mu : C \times E \longrightarrow C$$
$$(p, P) \longmapsto \phi^{-1}(\phi(p) \underset{\text{on } E}{+} P)$$

(so basically using the group law on E).

Clearly it is a morphism, from the diagram

$$\begin{tikzcd} C \times E \arrow[r, dashed] \arrow[d, "(\phi, id)", "\simeq"'] & C \arrow[d, "\phi", "\simeq"'] \\ E \times E \arrow[r, "+_E"] & E \end{tikzcd}$$

C/K becomes then a homogeneous space (check it).

Need also to verify that the cocycle corresponding to C/K as hom. space is θ.

Let $p_0 := \phi^{-1}(O) \in C$.

Then $\sigma \longmapsto p_0^\sigma - p_0 = \phi^{-1}(O)^\sigma - \phi^{-1}(O) = \cancel{\phi^\sigma(O) - \phi^{-1}(O)}$

$= (\phi^\sigma)^{-1}(O) - \phi^{-1}(O) = \phi^{-1}(O + Q_\sigma) - \phi^{-1}(O) = $ (prop 3.2) $=$

$$\begin{tikzcd} & C \arrow[dl, "\phi"'] \arrow[dr, "\phi^\sigma"] & \\ E \arrow[ur, bend left, "\phi^{-1}"] \arrow[rr] & & E \end{tikzcd}$$

$P \longmapsto P - Q_\sigma$

$= (O + Q_\sigma) - O = Q_\sigma$

Starting with the ex. seq. $0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$,

we get the L.E.S:

$$\cdots \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(G_{\bar{K}|K}, E[\phi]) \to H^1(G_{\bar{K}|K}, E) \xrightarrow{\phi} H^1(G_{\bar{K}|K}, E') \to \cdots$$

So also get:

$$0 \to E'(K)/\phi E(K) \to H^1(G_{\bar{K}|K}, E[\phi]) \to H^1(G_{\bar{K}|K}, E)[\phi] \to 0.$$

Let $v \in M_K$ be a valuation. We have the tower of fields:

$$\begin{tikzcd} & \bar{K}_v \arrow[d, dash, "G_v"] \\ \bar{K} \arrow[ur, dash] \arrow[d, dash, "G"'] & K_v \\ K \arrow[ur, dash] & \end{tikzcd}$$

where $G_v \hookrightarrow G$ is the decomposition group of v.

Note that we have a map

$$\begin{tikzcd} H^1(G_{\bar{K}|K}, E) \arrow[r, "\mathrm{Res}"] & H^1(G_{\bar{K}_v|K_v}, E) \arrow[d, leftrightarrow] \\ WC(E/K) \arrow[u] & WC(E/K_v) \end{tikzcd}$$

easy to compute!

__Define__ Ш(E/K) as the kernel of the following:

$$0 \to Ш(E,K) \to H^1(G_{\bar{K}|K}, E) \xrightarrow{\prod \mathrm{Res}} \prod_{v \in M_K} H^1(G_{\bar{K}_v|K_v}, E)$$

The Selmer group is

$$0 \to Sel^{(\phi)}(E/K) \to H^1(G_{\bar{K}|K}, E[\phi]) \xrightarrow{\prod \mathrm{Res}} \prod_v H^1(G_v, E)$$

We get the following (the top row is obtained by the snake lemma):

$$\begin{tikzcd}
0 \arrow[r] & E'(K)/\phi E(K) \arrow[r] \arrow[d] & Sel^{(\phi)}(E/K) \arrow[r] \arrow[d] & Ш(E/K)[\phi] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E'(K)/\phi E(K) \arrow[r] \arrow[d] & H^1(G_{\bar{K}/K}, E[\phi]) \arrow[r] & H^1(G_{\bar{K}/K}, E) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & 0 \arrow[r] & \prod_v WC(E/K_v) \arrow[r] & \prod_v WC(E/K_v) \arrow[r] & 0
\end{tikzcd}$$

__Remark:__ $Sel^{(\phi)}(E/K) \hookrightarrow H^1(G_{\bar{K}/K}, E[\phi]; S)$

where $H^1(G_{\bar{K}/K}, E[\phi]; S)$ ~~is~~ the group of cocycles that are unramified outside S (A cocycle $\theta \in H^1(G_{\bar{K}/K}, E[\phi])$ is unramified at v if it is trivial on I_v, the inertia group of v).

Can take $S = \{ M_K^\infty \cup \{\text{primes of bad reduction}\} \cup \{\text{primes dividing } \deg \phi\}\}$.

Then $H^1(G_{\bar{K}/K}, E[\phi]; S) \simeq H^1(G_{L/K}, E[\phi])$ where $L = \bar{K}^H$ for suitable L.

__Corollary:__ $Sel^{(\phi)}(E/K)$ is __finite__ (because $G_{L/K}$ is finite and $E[\phi]$ is also).

Example (taken from Silverman):

$E/\mathbb{Q} : y^2 = x(x-2)(x-10)$.

$\dfrac{E(\mathbb{Q})}{2E(\mathbb{Q})}$?

Want to set up the pairing $E(\mathbb{Q}) \times E[2] \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$

In this case, $E[2] = \{O, (0,0), (2,0), (10,0)\}$.

$$(P, (0,0)) \mapsto (x-0)$$
$$(P, (2,0)) \mapsto (x-2)$$
$$(P, (10,0)) \mapsto (x-10)$$

$P \in 2E(\mathbb{Q}) \iff x-0,\ x-2,\ x-10 \in \mathbb{Q}^{*2}$

The bad primes are 2 and 5 (and the ∞ primes).

So the image of the pairing in $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is contained ~~in K(S,~~

in $K(S,2) = \{ b \in K^*/K^{*2} : \mathrm{ord}_v(b) \equiv 0 \pmod 2 \text{ for } v \notin S \}$.

For $b_1, b_2 \in K(S,2) \times K(S,2)$, $\exists ?\ P = (x,y) \in E(\mathbb{Q})$ s.t.

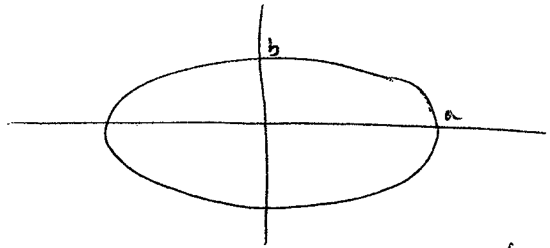
$$x = b_1 z_1^2$$
$$x - 2 = b_2 z_2^2$$

So get a system of equations

$$C = \begin{cases} y^2 = x(x-2)(x-10) \\ x = b_1 z_1^2 \\ x - 2 = b_2 z_2^2 \end{cases} \qquad x, y, z_1, z_2 \in \mathbb{Q}.$$

C is a twist of E, in fact!

• Elliptic curves over $\mathbb{C}$ (in 1 hour)



$$\left(\frac{x}{a}\right)^2+\left(\frac{y}{b}\right)^2=1.$$

Want to compute the arc-length of the ellipse:

$\oint \sqrt{dx^2+dy^2}$? we know $\frac{2x\,dx}{a^2}+\frac{2y\,dy}{b^2}=0 \Rightarrow \frac{dy}{dx}=-\frac{2xb^2}{2ya^2}$

||

$u=\frac{x}{a}$, $0\le k=1-\frac{b^2}{a^2}\le 1$

$$4\int_0^a \sqrt{1+\left(\frac{dy}{dx}\right)^2}\,dx = 4\int_0^a\sqrt{1+\left(\frac{2xb^2}{2ya^2}\right)^2}\,dx = 4a\int_0^1 \sqrt{\frac{1-k^2u^2}{1-u^2}}\,du$$

The integral

$\int_0^1 \sqrt{\frac{1-k^2u^2}{1-u^2}}\,du$ is called Jacobi's complete elliptic integral of the 2nd kind.

the integral

$\int_0^1 \frac{1}{\sqrt{(1-u^2)(1-k^2u^2)}}\,du$ is of first kind.

Obs: In the special case $k^2=0$ ($a^2=b^2$, the circle).

~~we have~~ $\oint$

If we fix t, and want an arc of length t, we should have

$$\boxed{t=\int_0^{\sin t}\frac{1}{\sqrt{1-y^2}}\,dy.}$$

So we can define the sine as the inverse of this integral; Also one can observe as well that sine is periodic. This is what happens in general.

Obs (Gauss $k^2=-1$, Abel for general k^2).

$$z = \int_0^{\mathrm{sin}(z;k)} \frac{1}{\sqrt{(1-u^2)(1-k^2u^2)}}\, du.$$

Then $\mathrm{sn}(z;k)$ is doubly-periodic; i.e. periodic in the two variables.

For $e_1, e_2, e_3 \in \mathbb{C}$ (distinct), define $\wp(z)$ such that

$$z = \frac{1}{2}\int_{\infty}^{\wp(z)} \frac{1}{\sqrt{(x-e_1)(x-e_2)(x-e_3)}}\, dx$$

Then $\wp(z)$ is an elliptic function, and $\exists\ g_2, g_3 \in \mathbb{C}$ s.t.

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

In other words, the field

$\mathbb{C}(\wp(z), \wp'(z))$ is the function field of the elliptic curve

$$y^2 = 4x^3 - g_2x - g_3$$

Def An elliptic function (relative to a lattice $\Lambda \subseteq \mathbb{C}$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$) is a meromorphic function $f(z)$ on z s.t. $f(z+\omega) = f(z)\ \forall \omega \in \Lambda, z \in \mathbb{C}$.

Def Define $\wp_\Lambda(z) := \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$.

It is called the Weierstrass-$\wp$ function WRT Λ.

Def $G_{2k}(\Lambda) := \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \omega^{-2k} \in \mathbb{C}$ is the Eisenstein series wrt Λ, of weight $2k$.

Theorem: $\wp_\Lambda(z)$ converges absolutely and uniformly on any compact subset of $\mathbb{C} \setminus \Lambda$.
Moreover, $\wp_\Lambda(z)$ is meromorphic, with poles of order 2 at $\omega \in \Lambda$ and no other poles.

Theorem: The field $\mathbb{C}(\Lambda)$ of all elliptic functions (wrt Λ) is

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

depend on Λ!

and $\wp'(z)^2 = 4\wp(z)^3 - \underbrace{60G_4}_{g_2}\wp(z) - \underbrace{140G_6}_{g_3}$

Prop:

$$\begin{aligned} \phi : \mathbb{C}/\Lambda &\longrightarrow E \subseteq \mathbb{P}^2(\mathbb{C}) \\ z &\longmapsto (\wp(z) : \wp'(z) : 1) \end{aligned}$$

is a complex analytic isomorphism of complex Lie groups.

comp. analytic varieties with a group structure.

Thm: There are bijections, given $\Lambda_1 \subseteq \Lambda_2$ lattices,

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\} \xleftrightarrow{1:1} \left\{ \begin{array}{l} \text{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \\ \text{with } \phi(0) = 0 \end{array} \right\}$$

$$\alpha \longmapsto \phi_\alpha : z \mapsto \alpha z$$

$$\updownarrow 1:1$$

$$\{\text{isogenies } \phi : E_1 \to E_2\}.$$

Theorem (Uniformization theorem): Given $A, B \in \mathbb{C}$ s.t. $A^3 - 27B^2 \neq 0$, there exists a lattice $\Lambda \subseteq \mathbb{C}$ s.t. $g_2(\Lambda) = A$, $g_3(\Lambda) = B$.

Corollary: Given $E/\mathbb{C}$, $\exists\, \Lambda \subset \mathbb{C}$ s.t. $\phi : \mathbb{C}/\Lambda \xrightarrow{\simeq} E$.

E.O.C.