Elliptic Curve 2

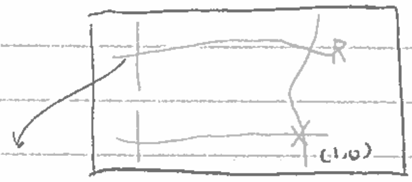
Haiyang Wang

23rd/oct/18 Tue.

Example. G : $x^2 - dy^2 = 1$ $\quad K \supseteq O_K \supseteq (\pi)$ $\pi | d$, $d \in O_K$

- affine group scheme over K: Spec $K[x,y]/(x^2-dy^2-1)$. (Char $k \neq 2$)
- model over O_K Spec $O_K[x,y]/(x^2-dy^2-1)$ ✳
- reduction over $\bar{k} = O_K/(\pi)$: Spec $\bar{k}[x,y]/(x^2-\bar{d}y^2-1)$

$\bar{d} = d \bmod (\pi)$



(closure of the pt R)

O_K point $x, y \in O_K$

$$\begin{tikzcd} ✳ \arrow[d] \\ \mathrm{Spec}(O_K) \end{tikzcd}$$

Rk. The reduction depends on our choice of equation. The reduction type is sensitive to the field K.

G_L/L $\quad K(\sqrt{d}) = L$, Over L, we could change coordinate to get an equation for G_L/L of the form $xy-1=0$.

$\quad |$ deg 1 or 2

G/K $\quad K$

$(\pi') \subseteq O_L \subseteq L$

$(\pi) \subseteq O_K \subseteq K$

Over O_L, we could look at the new model. Spec $O_L[x,y]/(xy-1)$

Both fibers (over (π) & (π')) gives the multiplicative group

($\mathbb{G}_{m_L}/L'$, and $\mathbb{G}_{m_{k_L}}/k'$).

☆ Over L, the new model seem better than the model over K.

This is a general phenomena: increasing the field in an appropriate way to get a better reduction (Semi-stable reduction)

$O_L[x,y]/(xy-1)$ $\qquad$ $O_L[x,y]/(x^2-dy^2-1)$

Two models with the same generic fiber over L ($\mathbb{G}_{m_L}/L$)

$x^2 - du^2 = (x-\sqrt{d}u)(x+\sqrt{d}u)$

$(\pi) \to$ Local ring

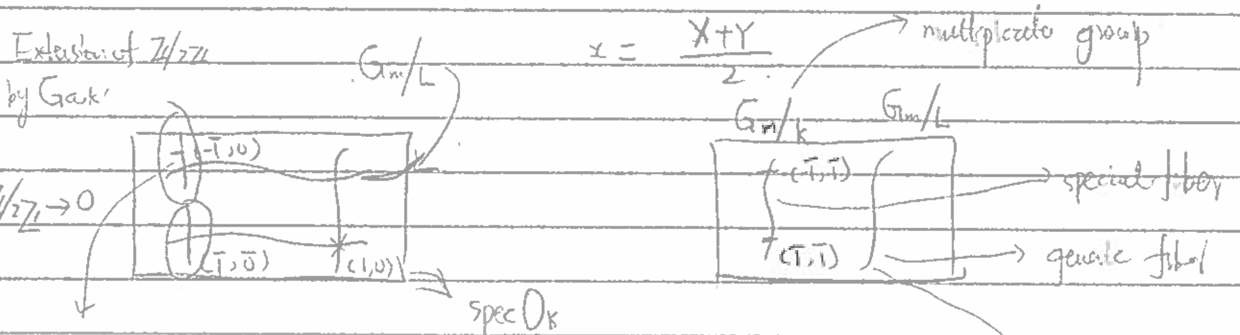
$$\operatorname{Spec} \mathcal{O}_L[x,y]/(x^2-dy^2-1) \longrightarrow \operatorname{Spec} \mathcal{O}_L[x,y]/(xy-1).$$

induced by: $X \longrightarrow x-\sqrt{d}y$ on the rings

$Y \longrightarrow x+\sqrt{d}y$

Inverse change of variable, $y = \dfrac{Y-X}{2\sqrt{d}}$

$x = \dfrac{X+Y}{2}$



$$0 \to G_a \xrightarrow{i} g \to \mathbb{Z}/2\mathbb{Z} \to 0$$

Two affine lines. (No map from affine line to multiplicative gp)

$$\mathcal{O}_L[x,y]/(xy-1) \longrightarrow \mathcal{O}_L[x,y]/(x^2-dy^2-1)$$

mod(π') $\quad k'[x,y]/(xy-1) \longrightarrow k'[x,y]/(x^2-1)$

$k' = \mathcal{O}_L/(\pi')$

$X \longrightarrow x$

$Y \longrightarrow x$

$XY=1 \longmapsto x^2=1$

$$\begin{tikzcd}\operatorname{Spec} \mathcal{O}_L[x,y]/(xy-1) \arrow[d] \\ \text{two direction.}\end{tikzcd}$$

$m = (x-x_0,\ x-y_0)$ maximal ideal

$(x \pm 1,\ x-y_0)$

$\updownarrow$

$(\pm 1,\ y_0)$

$(1, y_0)$ preimage $\quad (X-1,\ Y-1)$

$(-1, y_0)$ preimage. $\quad (X+1,\ Y+1)$

Morphisms of group scheme.
codim one $\longmapsto$ a pt

★ Torsion of multiplicative group G_m/k char$(k) \neq 2$ 2/2 ker[ℓ] : $[\ell]^{-1}$ of the identity

$\updownarrow$

maximal $\sqrt{(x-1)}$ ideal

defined by the ideal $(x^\ell - 1)$

μ_ℓ / k : $\mathrm{Spec}(k[x]/(x^\ell - 1))$ $x^\ell - 1$: x is a unit

but if k contain the ℓ^{th} roots of 1, $(\mathrm{char}\, k) \nmid \ell$)

μ_ℓ is isomor to the const group $\mathbb{Z}/\ell\mathbb{Z}$

✱ (L-fun of Elliptic Curves)

✱ ① Recall the Zeta fcn:

$$\zeta(s) \quad \prod_{p\ \text{prime}} \frac{1}{(1 - \frac{1}{p^s})}$$

② For ring A

$$\downarrow \quad \zeta_A(s) = \prod_{M \in \mathrm{Max}(A)} \frac{1}{1 - \frac{1}{\|M\|^s}}$$

such that

$\forall M \in \mathrm{Max}(A)$

$|A/M| =: \|M\| < \infty$

③ For any curve $X/\mathbb{Q}$, pick equations for it that have coefficients in $\mathbb{Z}$ and consider the ring

$$A := \mathbb{Z}[\cdots]/(\text{equations})$$

If it is an elliptic curve, we can pick an W.E. with coeff in $\mathbb{Z}$, and $A = \mathbb{Z}[x, y]/\text{W.E.}$

Then we can consider $\zeta_A(s)$.

✱ Consider $\mathbb{Z} \longrightarrow A$ give $\rightarrow$ giving by W.E. mod p

Spec A

2/3

Note that

$$\zeta_A(s) = \prod_{p \text{ prime}} \Big(\underbrace{\prod_{m \ni p} \Big(\frac{1}{1-\frac{1}{\|m\|^s}} \Big)}_{\text{this is the Zeta fcn for the fiber.}} \Big)$$

all pts in the fiber over p

☆ projectify Spec A so that each fiber has a pt at ∞

when the fibers are non-singular, it is an elliptic curve

$$\begin{tikzcd}
\text{fiber} & \mathcal{X}_p \arrow[l] \arrow[r, phantom, "\subseteq"] \arrow[d] & \mathcal{X} \arrow[r, phantom, "\supseteq"] \arrow[d] & \operatorname{spec}(A) \arrow[dl] \\
& \operatorname{Spec}\mathbb{Z}/p\mathbb{Z} \arrow[r] & \operatorname{Spec}\mathbb{Z} &
\end{tikzcd}$$

For each p where $\mathcal{X}_p$ is an elliptic curve over $\mathbb{F}_p$:

the term $\displaystyle\prod_{m \ni p} \Big(\frac{1}{1-\frac{1}{\|m\|^s}} \Big)$ in $\zeta_{\mathcal{X}}(s)$ (with ∞ added)

is just the Zeta-fcn of $\mathcal{X}_p$ with $T = p^{-s}$

Recall, $$Z(\mathcal{X}_p, T) = \frac{1 - a_pT + pT^2}{(1-T)(1-pT)}$$

☆ Start with $E|\mathbb{Q}$, choose a model $\mathcal{X}/\operatorname{spec}\mathbb{Z}$, given by W.E./$\mathbb{Z}$, get $\Delta(\text{W.E.}) \in \mathbb{Z}$, so except of $p \mid \Delta(\text{W.E.})$, the fiber $\mathcal{X}_p$ is an elliptic curve over $\mathbb{F}_p$.

$$\zeta_{\mathcal{X}}(s) = \prod_{p \nmid \Delta} \frac{1 - a_p p^{-s} + p \cdot p^{-2s}}{(1-p^{-s})(1-p\cdot p^{-s})} \cdot \prod_{p \mid \Delta} (*)$$

Zeta fcn of sth at $T = p^{-s}$ exclude

$$= \frac{\prod_{p\nmid\Delta}(1 - a_p p^{-s} + p^{1-2s})}{\quad} \quad (**)$$

☆ L fcn of $E/\mathbb{Q}$

$$L(E/\mathbb{Q}, s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s}) \prod_{p \nmid \Delta} \text{some good choice}$$

$\uparrow$ minimal discriminant

$\swarrow$ prescribed by the red E mod p

☆ Shimura–Taniyama–Weil: $E/\mathbb{Q}$ is related to some $X_0(N)$

$\exists\ X_0(N_E) \twoheadrightarrow E$

correct choice for $L(E/\mathbb{Q}, s)$, pull back to a differential form on $X_0(N_E)$

25th/ oct/ 18 Thr

Say $A = \left[\begin{array}{l} k[t] \\ \mathbb{Z} \end{array}\right.$ ff(A) = K

E/k Elliptic curve, W.E. $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ $a_i \in k$

$E/k \subseteq \mathbb{P}^2_k/k$.

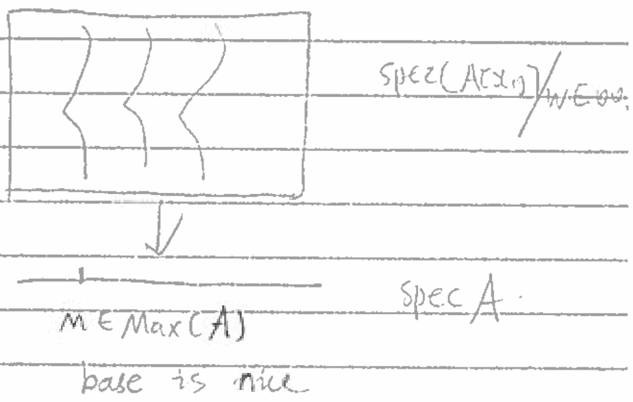
Use some change of variables,

$$\begin{cases} x' = \lambda^2 x \\ y' = \lambda^3 y \end{cases} \quad \lambda \in A \setminus \{0\}$$

We have W.E. E/A for E/K, $a_i \in A$..

☆ Consider

$$\begin{tikzcd} A[x,y]/(\text{W.E. over } A) \arrow[dd, bend right] \\ A \arrow[u] \\ \mathrm{Spec}\,(A[x,y]/\text{W.E. over } A) \arrow[d] \\ \mathrm{spec}\,A \end{tikzcd}$$



family of curves parametrized by spec A

1 parametrized family $\dim(A) = 1$
regular base for

$M \in \mathrm{Max}(A)$., The fiber above M is a (smooth) elliptic curve

if $\underbrace{\Delta(\text{WE over } A)}_{\in A} = \Delta(a_1, \dots, a_6) \not\subset M$

(Then Modulo M, $\bar{\Delta}(\bar{a}_1, \dots, \bar{a}_6) \neq \bar{0}$)

so the $\overline{\text{W.E.}}/(A/M)$ define an elliptic curve

☆ $A = \mathbb{C}[t]$, $\mathrm{Max}[A] = \mathbb{C}$.

$M \in \mathrm{Max}(A) \longleftrightarrow a \in \mathbb{C}$

$$\begin{tikzcd} X \arrow[d] \arrow[r, phantom, "\supseteq"] & X_D \arrow[d] \arrow[r, phantom, "\supseteq"] & X_a \arrow[d] \\ \mathbb{C} \arrow[r, phantom, "\supseteq"] & D \arrow[r, phantom, "\ni"] & a \end{tikzcd}$$

Take D small enough, so that

$$\begin{tikzcd} X_D \setminus X_a \arrow[d, "\longleftarrow \text{has only smooth fibers}"] \\ D \setminus \{a\} \end{tikzcd}$$

☆ In Algebraic Geometry, all open sets in spec (A) are dense (non-empty)

☆ In arith G, we proceed as follows:

$$\begin{tikzcd} M \in Max(A) & A \arrow[r] & A_M \arrow[dr, bend right] & \text{localize at } M. \\ & & & A_M/_{MA_M} \cong A/M \end{tikzcd}$$

$$\begin{tikzcd} X_M \arrow[r] \arrow[d] & X_{spec} \arrow[r] \arrow[d] \arrow[dr, phantom, "\boxed{X}"] & X \arrow[d] \\ Spec(A/M) \arrow[r] & Spec(A_M) \arrow[r] & Spec(A) \end{tikzcd}$$

first substitute for D centered at M.

A Dedekind $\Rightarrow$ A_M is a local p.i.d (DVR).

Thm Ded D with only finitely many maximal ideal is DVR

Notation O_K local pid with $ff(O_K) = k$.

$$\begin{matrix} O_K \\ \cup \\ (\pi) \end{matrix}$$

$\hookrightarrow$ maximal ideal

$O_K/(\pi) = k \Rightarrow$ Residue field

if $a \in \mathcal{O}_K$ $\text{ord}_\pi(a)$ is def as $a = (\text{unit})\,\pi^{\text{ord}_\pi(a)}$.
For convenience $\text{ord}_\pi(0) = \infty$

$$\mathcal{O}_K = \{ c \in k^* \mid v(c) \geq 0 \}$$

$$(\pi) = M_K = \{ c \in k^* \mid v(c) > 0 \}$$

☆ $D' \subseteq D$

$D' \longrightarrow$ smaller nbhd

$\longrightarrow \text{Spec}\, R \longrightarrow \text{Spec}\, \mathcal{O}_K$

with $\mathcal{O}_K \longrightarrow R$.
Two standard choices of R.

Completion ① $R = \hat{\mathcal{O}}_K$ = Completion of $\mathcal{O}_K$ at (π)

key:
$$\begin{tikzcd}
\mathcal{O}_K \arrow[r] & \hat{\mathcal{O}}_K \\
(\pi) \arrow[u, phantom, "\cup" description] & \pi\hat{\mathcal{O}}_K \arrow[u, phantom, "\cup" description]
\end{tikzcd}$$
$\pi\hat{\mathcal{O}}_K$ = maximal ideal in $\hat{\mathcal{O}}_K$

and $\mathcal{O}_K/(\pi) \xrightarrow{\sim} \hat{\mathcal{O}}_K/\pi\hat{\mathcal{O}}_K$

Strict henselization ②
$$\begin{tikzcd}
\mathcal{O}_K \arrow[r, hook] & R \\
(\pi) \arrow[u, phantom, "\cup" description] & (\pi R) \arrow[u, phantom, "\cup" description] \\
\mathcal{O}_K/(\pi) \arrow[r, hook] \arrow[d, equal] & R/\pi R \arrow[d, phantom, "\cong" description] \arrow[r, dash] & k^{sep} \\
R & R
\end{tikzcd}$$
(πR) is the maximal ideal of R

☆ k^{sep} is a separable closure of k.
If k is perfect (e.g.) k is finite)
then $k^{sep} = \bar{k}$

Get $\Delta(WE/O_K) = \Delta(a_1 \ldots a_6) \in O_K$

So $ord_\pi(\Delta) \geq 0$

Def. A minimal WE/O_K for E/K, is a WE/O_K for E/K s.t. $ord_\pi(\Delta(a_1 \ldots a_6))$ is minimal among all WE/O_K for E/K

! ☆ A minimal WE/O_K is not unique.

☆ Homogenize the WE : define a smooth plane curve in $\mathbb{P}^2_K$

$$\begin{tikzcd}
\mathbb{P}^2_k \arrow[rr, hook, "\text{closed immer}"] \arrow[dd] & & \mathbb{P}^2_{O_K} \arrow[rr, hook, "\text{open immer}"] \arrow[dd] & & \mathbb{P}^2_K \arrow[dd] & & \dim 2 \\
& \overline{\mathcal{E}} \arrow[ul, hook] \arrow[dl] \arrow[d] \arrow[dddl, bend right] & & \mathcal{E} \arrow[ul, hook] \arrow[dl] \arrow[urrr] \arrow[ddr, bend left] & & E \arrow[ul, hook] \arrow[dl] \arrow[dddr, bend left] & (\mathcal{E},\ \text{base dim } 1 \\
\mathrm{Spec}\, k \arrow[rr, hook, "\text{closed}"] & \ & \mathrm{Spec}\, O_K \arrow[rr, hook, "\text{open}"'] & & \mathrm{Spec}\, K & & \text{fiber dim } 1 \Rightarrow 2) \\
& \text{def by } \overline{WE}/k & & & \text{def by } WE/O_K & & \\
\text{special fiber} & & & & & & \text{generic fiber}
\end{tikzcd}$$

W.E $y^2 + \bar{a}_1 xy + \bar{a}_3 y = x^3 + \bar{a}_2 x^2 + \bar{a}_4 x + \bar{a}_6$

In Silverman no middle part
$$\begin{tikzcd}
\mathbb{P}^2_{O_K} \arrow[d] \\
\mathrm{Spec}\, O_K
\end{tikzcd}$$

☆ For all $\mathcal{E}/O_K$, carry from a WE/O_K of E/K

Then all have the same generic fiber E/K

in other words, all $\mathcal{E}/O_K$ are models of E/K
scheme over O_K
(equation)

but the special fibers $\overline{\mathcal{E}}/k$ can be different.

Thm. The models $\mathcal{E}/O_K$ obtained from minimal WE/O_K for E/K are all isomorphic over O_K, More precisely, you pass

$$\begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases}$$ change of variable that preserve the W-E.

$\boxed{r, s, t \in K,\ u \text{ invertible}}$. $u \in K^*$ in general

Here we have $u \in O_K^*$, $r, s, t \in O_K$

The Σ in the middle ~~case~~, it's canonical. they are all isomorphic.

Def. Fix $O_K \subset K$ and E/K. The reduction of E modulo π is the following curve $\bar{E}/k$.

Let WE/O_K be a minimal W.E. for E/K over O_K

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

Then $\bar{E}/k$ is the plane curve,

$$zy^2 + \bar{a}_1xyz + \bar{a}_3yz^2 = x^3 + \bar{a}_2x^2z + \bar{a}_4xz^2 + \bar{a}_6z^3$$

$\underset{\Uparrow k}{\bar{a}_i} = a_i \bmod \pi,$

we have a natural reduction map

$$\begin{tikzcd} \mathbb{P}^2(K) \arrow[r, "red"] & \mathbb{P}^2(k) \\ E(K) \arrow[u, phantom, "\cup"] \arrow[r] & \bar{E}(k) \arrow[u, phantom, "\cup"] \end{tikzcd}$$

key: The curve $\bar{E}/k$ is well-def up to isomorphism over k:

Take 2 W.E $(WE)_1/O_K$, $(WE)_2/O_K$. For E/K that are both minimal. By the Thm, $\exists$ $\begin{cases} x = u^2x' + r & u \in O_K^* \\ y = u^3y' + u^2sx' + t & r, s, t \in O_K \end{cases}$

reduce mod π: Since $u \in O_K^*$, we get an iso, between the reduction of $(WE)_1$ and red of $(WE)_2$

Def. E/K is a good reduction mod π, if $\bar{E}/k$ is an elliptic curve.

So take a minimal Weierstrass WE/O_K for E/K

7/12

★ We will also use the following terminology.

Sometimes, bad reduction ⟺ not good ☹

precised

good reduction } semi-stable reduction

Multiplicative reduction

additive reduction

★ Suppose $\bar\Delta = \bar 0$, $(\mathrm{ord}_\pi(\Delta) > 0)$,

Then $\overline{WE}/k$ def a curve with a singular pt over $\bar k$

Since $(0:1:0)$ is never singular,

the singular pt is $(a,b) \in \bar k^2$,

Translate to put the point at $(0,0)$. (everything in $\bar k$)

After the translation, $\overline{WE}/k$ looks like:

$y^2 + \bar a_1 xy + \bar a_3 y = x^3 + \bar a_2 x^2 + a_4 x \longrightarrow (\bar a_i \in \bar k)$

with $\bar a_6 = 0$ ($(0,0)$ on the curve)

with $(0,0)$ singular $\Rightarrow \bar a_3 = \bar a_4 = 0$

★ So, $y^2 + \underbrace{\bar a_1 xy - \bar a_2 x^2} = x^3$

Two case

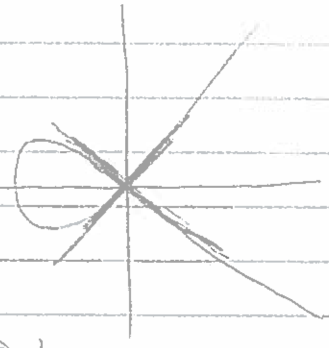
↓

homogeneous of deg 2,

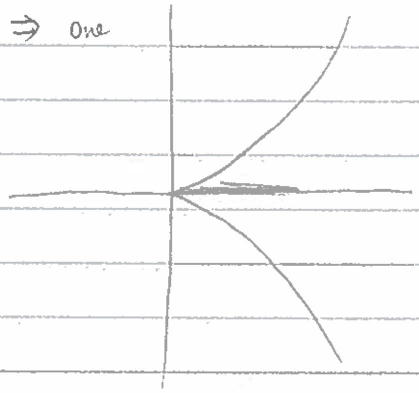
↓

if factors into $l_1 \cdot l_2 \Rightarrow$ two tangent line

~ ~ $l_1^2 \Rightarrow$ one tangent line



multiplicative red



additive red

① $L = (y-\alpha x)(y-\beta x)$ with $\alpha \neq \beta$ (Mult)

② $L = (y-\alpha x)^2$ (Add)

30th/Oct/18 Tue.

⚠ In Silverman's, all fields $\boxed{k}$ k are perfect.

E/k, $k = \mathbb{F}_p[t]$ is a natural thing

k perfect is reasonable assumption. (Residue field) (In fact, the difficulty occur only when $char(k) = 2$ or 3)

Rk Let WE/k be a W. E.

☆ ① if the plane curve defined by $WE = 0$ is singular in $\mathbb{P}^2(\bar{k})$, then it has at most one singular point : say $P_0 = (a,b) \in \bar{k}^2$

[when $char(k) = 2$ or 3, it is possible for the pt to be defined on a purely insep extension of k.

- $char(k) = 2$, $y^2 = x^3 + t$, $k = \mathbb{F}_2[t]$

  $P_0 = (0, \sqrt{t})$ is singular

- $char(k) = 3$, $y^2 = x^3 + t$ $k = \mathbb{F}_3[t]$

  $P_0 = (\sqrt[3]{t}, 0)$ is singular

② If $P = (a,b) \in \bar{k}^2$, then $[k(a,b) : k] \leq 3$

In particular, if $char(k) \geq 5$, then $k(a,b)$ must be separable

(We do not need k perfect)

③ Separable + Uniqueness $\Rightarrow (a,b) \in k^2$

$$\begin{tikzcd}
k(a,b) \arrow[r, hook, "\sigma"] \arrow[d, dash] & \bar{k} \\
k &
\end{tikzcd}$$

Then $WE(a,b) = 0 \Leftrightarrow \sigma(WE(a,b)) = 0 \Leftrightarrow WE(\sigma(a), \sigma(b)) = 0$

☆ Upshot $(\sigma(a), \sigma(b))$ on the curve and it's singular, $\Rightarrow (a,b) = (\sigma(a), \sigma(b))$

Separable $\Rightarrow$ send a to it's conjugate

$$\begin{tikzcd}
\forall \sigma : k(a,b) \arrow[rr] & & \bar{k} \\
& k \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Since the extension is separable, we know $(a,b) \in k^2$

☆ Same proof show that if k perfect, then the singular pt in k^2.

☆

Reduction. $O_K \subset k$ O_K DVR

Start with a WE/O_K

$y^2 + \cdots = x^3 + \cdots$ $a_i \in O_K$

Red. Red mod π

$\overline{W}/k$

$y^2 + \overline{a}_1 xy + \cdots = x^3 + \cdots$ $\overline{a}_i \in k$.

If we have a singular pt $\Rightarrow$ pt in k (in Silverman)

Assume char$(k) = 2$ or 3, & k perfect, So that any singular pt on $\overline{WE} = 0$ is on k.

Assume that $P_0 = (\overline{a}, \overline{b}) \in k^2$ is a singular pt.

☆ Let $(a, b) \in O_K^2$ be a lift of $(\overline{a}, \overline{b})$,

Make the translation

$$\begin{cases} X = x - a & \text{on } WE/O_K. \\ Y = y - b \end{cases}$$

to get a new WE/O_K

Recall $\begin{cases} x = \lambda^2 x' + Y \\ y = \lambda^3 y' + \lambda^2 s x' + t \end{cases}$

☆ Then, $\lambda^{12} \Delta' = \Delta$ (indep of Y, s, t)

$\lambda^4 c_4' = c_4$

$\lambda^6 c_6' = c_6$

In particular, both WE have the same C_4 after translation.

In particular $c_4 \in O_K$.

☆ Reduce the translated WE. now the singular pt is $(\overline{0}, \overline{0})$,

$y^2 + \overline{a}_1 xy = x^3 + \overline{a}_2 x^2$

or $y^2 + \overline{a}_1 xy - \overline{a}_2 x^2 = x^3$

Case1 $y^2 + \overline{a}_1 xy - \overline{a}_2 x^2$ has two dist roots

$(y - \alpha x)(y - \beta x)$ with $\alpha \neq \beta$

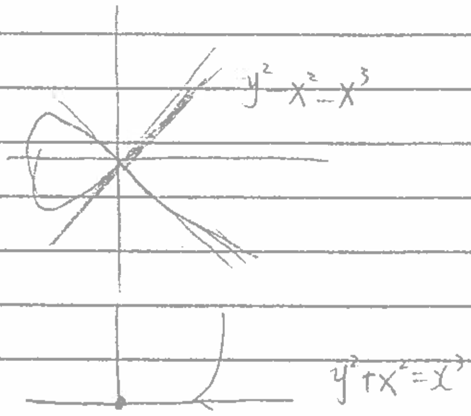
This holds $\Leftrightarrow$ $\overline{a}_1^2 + 4\overline{a}_2 \neq 0$

(Multiplicative red)

(Split Multi red if $\alpha, \beta \in k$)

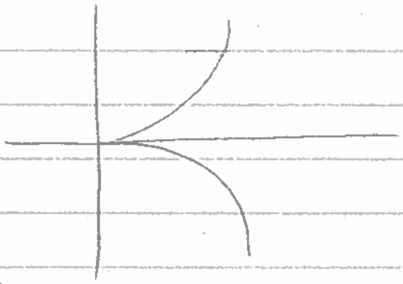
Example $y^2 + x^2 = x^3$

$y^2 - x^2 = x^3$ over $\mathbb{R}$



Case 2. Additive Red. one tangent line

$(y-\alpha x)^2 = x^3$



☆ Recall $c_4 = b_2^2 - 24 b_4$ $\qquad b_2 = a_1^2 + 4a_2$

$\bar{c}_4 = \bar{b}_2^2 - 24\bar{b}_4$ $\qquad b_4 = 2a_4 + a_1 a_3$

$= (\bar{a}_1^2 + 4\bar{a}_2')^2$

(because $(\bar{0}, \bar{0})$ sing, then $\bar{a}_4' = \bar{a}_3' = 0$)

Upshot $\bar{c}_4 \neq \bar{0} \Leftrightarrow 2$ dist tangent line.

Condition Given WE/O_K:

$v(\Delta) = 0$ $\Leftrightarrow$ good red

$v(\Delta) > 0$ and $v(c_4) = 0$ $\Leftrightarrow$ multiplicative red

$v(\Delta) > 0$, $v(c_4) > 0$ $\Leftrightarrow$ additive red

$\to$ (divisible by π)

(for the red of WE/O_K, there is a chan that by chang variable on WE/O_K, we can get into another case)

Rk. If $v(\Delta) < 0$, or $v(c_4) < 0$, then the given WE/O_K is minimal,

(i.e. its $\operatorname{ord}_\pi(\Delta)$ is minimal among all WE over O_K)

Pf: Spse its not minimal, then $\exists$ another $(WE)_0/O_K$,

with $\operatorname{ord}_\pi(\Delta_{WE_0}) < \operatorname{ord}_\pi(\Delta_{WE})$

Since $\Delta_{WE_0} = \lambda^{12}\Delta_{WE}$ for some $\lambda \in k^*$

then $\operatorname{ord}_\pi(\Delta_{WE_0}) - \operatorname{ord}_\pi(\Delta_{WE})$ is divisible by 12.

Hence if $\operatorname{ord}_\pi(\Delta_{WE}) < 12$, and $\operatorname{ord}_\pi(\Delta_{WE_0}) > 0$,

we must have $\operatorname{ord}_\pi(\Delta_{WE_0}) = \operatorname{ord}_\pi(\Delta_{WE})$

Same proof for $v(c_4) < 4$ ※

Rk. Good reduction or Multiple red are two types of semi-stable red.

Semi-stable Something remains constant but not everything.

☆ Have good red everywhere, except at $p \mid \Delta$, at these p, it's multiplicative red.

★ Consider a finite extension $\swarrow B \in L$

Choose $M \in \mathrm{Max}(B)$. Def $O_L : B_M$, then it's a DVR

☆ we can compare the two red types

- E/K over O_K
- E/L over O_L

Note: $O_L \supseteq (\pi_L)$ $\qquad \pi_K O_L = (\pi_L)^e$ for some $e \geq 2$.

$O_K \supseteq (\pi_K)$ $\qquad$ for $\alpha \in O_K$.

$$\mathrm{ord}_{\pi_L}(\alpha) = e\, \mathrm{ord}_{\pi_K}(\alpha) \quad (✪$$

Claim: If E/K has semi-stable red over O_K, then it has the same type semi-stable redu over O_L,

Pf: Choose a minimal equ over O_K,

Then the same equation over O_L is still minimal (not true in general if the reduction is additive) ($e\, \mathrm{ord}_{\pi_K}(\alpha)$ may be very large)

☆ If $\mathrm{ord}_{\pi_K}(\Delta_{WE}) = 0 \Rightarrow \mathrm{ord}_{\pi_L}(\Delta_{WE}) = 0$ (By ✪)

If $\mathrm{ord}_{\pi_K}(c_4(WE)) = 0 \Rightarrow \mathrm{ord}_{\pi_L}(c_4(WL)) = 0$

(

(Semi-stable red theory)
If E/K is an additive red over O_K, then there exist a finite separable extension L/K, s.t. E/L has semi-stable reduction over O_L, whatever the choice of $M \in \mathrm{Max}(B)$ as done above)
(Serre-Groth '60s') (True X' for abelian variety)]

1st/Nov/18 Thr

6th/NOV/18 Tue

$\mathcal{O}_K$ dvr $K = \mathrm{ff}(\mathcal{O}_K)$

$\mathcal{O}_K/(\pi_K) =: k$ $\mathrm{ord}_\pi = v$. (when char $\neq 2, 3$), k is alway perfect.

E.g. $y^2 = x(x-1)(x-\lambda)$ over $K := k(\lambda)$ (Legendre family of Elliptic curve)

char $(k) \neq 2$, $\Rightarrow$ a smooth curve

Geometrically, this is a family of curves over $\mathbb{P}^1_k$

Each pt in $\mathbb{P}^1_k$ corresponding to a dvR in K

we are going to look at the reduction of E/K over 3 different $\mathcal{O}_K$.

at 0: $\mathcal{O}_K = k[\lambda]_{(\lambda)}$

at 1: $\mathcal{O}_K = k[\lambda]_{(\lambda-1)}$

at ∞: $\mathcal{O}_K = k[\frac{1}{\lambda}]_{(\frac{1}{\lambda})}$

Exercise For any other dvr in $k(\lambda)$, E/K has good reduction at that place over $\mathcal{O}_K$

☆ at 0, modulo λ: $y^2 = x^2(x-1) \rightsquigarrow y^2 = x^3 - x^2$

$y^2 + x^2 = x^3$ (Multiplicative reduct.

split $\Leftrightarrow \sqrt{-1} \in k$.

at 1, modulo $\lambda-1$: $y^2 = x(x-1)^2 \rightsquigarrow y^2 = X^2(X+1)$

$y^2 - X^2 = X^3$

split multiplicative red.

☆ at ∞, set $t = \frac{1}{\lambda}$

Now, $\mathcal{O}_K = k[t]_{(t)} \subseteq k(t) = k(\lambda)$

The WE we have is $y^2 = x(x-1)(x-\frac{1}{t})$

Consider $Y = t^3 y$, $X = t^2 x$, $\Rightarrow Y^2 = X(X-t^2)(X-t)$ WE/$\mathcal{O}_K$.

(Exercise) ☆ Is this a minimal WE over $\mathcal{O}_K$?

Determine the reduction of E/K over $\mathcal{O}_K$?

Exercise: Assume char$(k) \neq 2, 3$, General case $K \supseteq \mathcal{O}_K$

Suppose we have a W.E. over $\mathcal{O}_K$ for E/K.

This equation is minimal over $\mathcal{O}_K \Leftrightarrow$ either $v(\Delta) < 12$ or $v(C_4) < 4$. $\longrightarrow$ (char k = 0)

Rk. It is a thm that an elliptic curve over $k(\lambda)$ which has semi-stable reduction everywhere must have at least 4 places of bad reduction.

Rk. Consider $k(s) = k(t)[y]/(y^2-t)$ $s = "\sqrt{t}"$

$$\begin{tikzcd} k(s) \arrow[d, dash, "2"] \\ k(t) \end{tikzcd}$$

$y^2 = x(x-t^2)(x-t)$

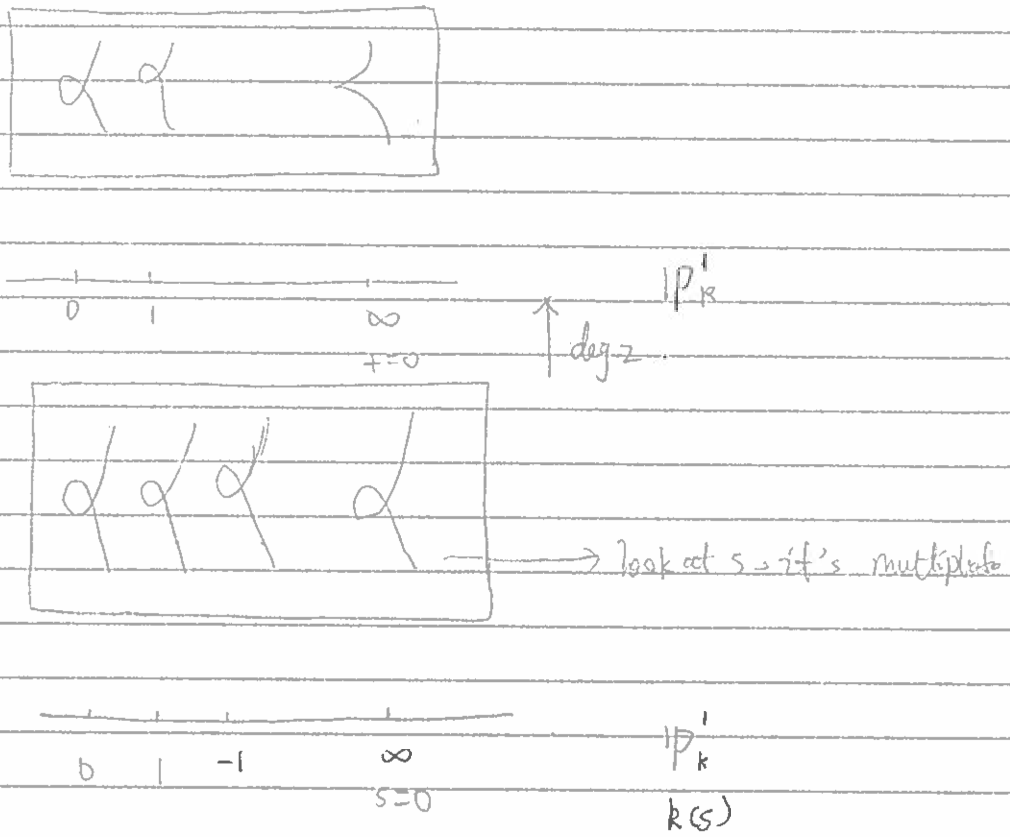
or $y^2 = x(x-s^4)(x-s^2)$ (

$\frac{y}{s^3} = Y$ $Y^2 = X(X-s^2)(X-1)$ (Multiplicative reduction)

$\frac{x}{s^2} = X$ This equation is minimal since it gives multiplicative reduction. $\hookrightarrow$ over $k[s]_{(s)}$

$\hookrightarrow$ over $k[s]_{(s)}$

Multiplicative reduction can not be transformed into



$\Rightarrow$ 4 places of bad reduction.

☆ Consider a W.E. for E/K with coeff in O_K.

WE/O_K : $y^2 + a_1xy + \cdots$ $a_i \in O_K$

$\Delta(WE/O_K) \in O_K$.

$$\begin{tikzcd}
\mathcal{X}_{WE} \arrow[rr, phantom, "\subset"] \arrow[dr] & & \mathbb{P}^2_{O_K} \arrow[dl] \\
& \operatorname{Spec} O_K &
\end{tikzcd}$$

Prop: Let WE_1/O_K & WE_2/O_K for M.W.E. for E/K,
s.t. $\operatorname{ord}_\pi(\Delta(WE_1)) = \operatorname{ord}_\pi(\Delta(WE_2))$
Then $\mathcal{X}_{WE_1}$ is isom to $\mathcal{X}_{WE_2}$ over $\operatorname{Spec} O_K$.
More precisely, the two W.E. are linked
by a change of variable

$x = \lambda^2 x' + r$
$y = \lambda^3 y' + \lambda^2 s x' + t$

If $\operatorname{ord}_\pi(\Delta(WE_1)) = \operatorname{ord}_\pi(\Delta(WE_2))$

$$\begin{cases} \lambda \in O_K^* \\ r, s, t \in O_K \end{cases}$$

☆ Then, the change of variables induce an isomorphism over O_K.

$$\left.\begin{aligned} x' &= (x - r)(\lambda^2)^{-1} \\ y' &= (\quad \dots \quad)(\lambda^3)^{-1} \end{aligned}\right\} \text{ in } O_K[x,y].$$

☆ Pf: Both WE_1 & WE_2 are over O_K,
For any change of variable,

$\lambda^{12}\Delta' = \Delta$

$\lambda^8 b_8' = \quad \dots \quad + 3r^4$

$\quad = \text{polyn}$ in r over O_K

$\lambda^6 b_6' = \text{poly}$ in r over O_K

$\quad = \quad \dots \quad + 3r^4$

$\lambda^2 a_2' = \text{poly}$ of deg 2 in s over O_K. (Once we know $r \in O_K$)

$\quad = \quad \dots \quad - s^2$

$\lambda^6 a_6' = \text{poly}$ of deg 2 in t over O_K (Once we know that $r, s \in O_K$)

$\quad = \quad \dots \quad - t^2$.

We have

$$\underbrace{12\operatorname{ord}_\pi(\lambda) + \operatorname{ord}_\pi(\Delta') = \operatorname{ord}_\pi(\Delta)}_{\text{equal by hypothesis}}$$

Pf that $\gamma \in O_K$.

$\gamma \in K$, and O_K is integrally closed in K, so $\gamma \in O_K$ if γ is integral over O_K.

Now that $\lambda \in O_K$, we get 2 relations for γ over O_K.

$$4\gamma^3 + \cdots = 0$$

$$3\gamma^4 + \cdots = 0$$

$$\Rightarrow (4\gamma^3 + \cdots)\gamma - (3)^4 + \cdots) = \gamma^4 + \cdots$$

This is the monic relation for γ over O_K $\Rightarrow$ $\gamma \in O_K$.

Same idea show that $s, t \in O_K$.

Upshot: A minimal WE/O_K produce a well-defined reduction type (In particular, if E/K has good reduction), we associate to it a unique well defined elliptic curve $\tilde{E}/k$.

(*) $\overline{j(E/K)} = j(\tilde{E}/k)$

Pf: Take minimal equ for E/k,

$$j(E/k) = \frac{c_4^3(WE)}{\Delta(WE)}$$

by hypothesis on minimal W.E., $\pi \nmid \Delta(W.E.)$ $\quad \Delta(W.E.) \in O_K^*$

So $j(E/k) \in O_K$

$\tilde{E}/k$ can be given by $\overline{WE} = 0$

therefore, $j(\tilde{E}/k) = \overline{j(E/k)}$.

☆

$$\begin{tikzcd}
E/k \arrow[r, Rightarrow] & WE/O_K \arrow[r, squiggly] \arrow[d, squiggly] & \mathcal{X}_{WE} \subset \mathbb{P}^2_{O_K} \\
 & \text{minimal } WE/O_K \arrow[r, squiggly] \arrow[dr, squiggly] & \text{the reduction type} \\
 & & \mathcal{X}_{WE_{min}} \subset \mathbb{P}^2_{O_K}
\end{tikzcd}$$

☆ Analogy

$f(x) = 0$ (Number theory) $\qquad$ $f(x, y) = 0$ (Curve theory)

$$\begin{tikzcd} L \arrow[d, dash] & k[x]/(f(x)) \arrow[l] & & k[x,y]/f(x,y). \arrow[d, dash] \\ k & & & k \end{tikzcd}$$

Take $f(x) \in O_K[x]$

$O_K[x]/(f(x)) \subset k[x]/(f(x))$ $\qquad$ $O_K[x,y]/(f(x,y)) \rightarrow f(x,y) \in O_K[x,y]$

$\subseteq B$ integral closure.

Spec B our model for Spec L.

Good reduction: want spec$(B/(\pi))$ to be as nice as possible,

$B/(\pi)$ = product of fields, each is separable over $O_K/(\pi)$.

8th/Nov/18 Thr

☆ Analogy.

Number Theory

$$\begin{tikzcd} L \arrow[d, dash] & \mathrm{Spec}\, L \arrow[d] & \text{dim } 0 \\ k & \mathrm{Spec}\, k & \end{tikzcd}$$

— relative dim 0

$$\begin{tikzcd} ? \arrow[d, dash] \arrow[r, phantom, "\subseteq"] & L \arrow[d, dash] \\ O_K \arrow[r, phantom, "\subseteq"] & K \end{tikzcd}$$

~~$O_K[x]/(f(x))$~~

$L = k(\alpha)$, $f(\alpha) = 0$ $f(x) \in O_K[x]$

O_K ⟶ local pid

↓

Canonical choice : $B =$ Integral closure of O_K in L

(i) $\mathfrak{d}_{B/O_K}$, ideal in O_K

☆ (ii) L/K has a good reduction mod π $\Leftrightarrow$ $v(\mathfrak{d}_{B/O_K})$

In number Thy., we have the different:

Elliptic Curve : E dim 1.

$$\begin{tikzcd} E \arrow[d, dash] \\ \mathrm{Spec}\, k \end{tikzcd}$$

$$\begin{tikzcd} ? \arrow[d] & E \arrow[l] \arrow[d, dash] & & \mathcal{E} \arrow[d, dash] & E \arrow[l] \arrow[d, dash] \\ \mathrm{Spec}\, O_K & \mathrm{Spec}\, k \arrow[l, dash] & & \mathrm{Spec}\, O_K & \mathrm{Spec}\, k \arrow[l, dash] \end{tikzcd}$$

(given by a minimal WE over O_K (choice for this course)

(i) $\Delta \in O_K$

☆ (ii) E/k has good red mod π $\Leftrightarrow$ $v(\Delta) = 0$.

In number theory,

$\pi \mid \mathfrak{d}_{B/O_K} \Leftrightarrow \pi$ ramifies in B (*)

So π does not ramify in $B \Leftrightarrow L/K$ has good reduct.

$$\begin{tikzcd}
\operatorname{Spec} B/\pi B \arrow[r, hook] \arrow[d] & \operatorname{Spec} B \arrow[r, dash] \arrow[d] & \operatorname{Spec} L \arrow[d] \\
\operatorname{Spec} k \arrow[r, hook] & \operatorname{Spec} O_K \arrow[r, dash] & \operatorname{Spec} K
\end{tikzcd}$$

$k = O_K/(\pi)$.

$\pi B = M_1^{e_1} \cdots M_s^{e_s}$

$$\begin{tikzcd}
B/\pi B = B/M_1^{e_1} \times \cdots \times B/M_s^{e_s} \arrow[d, dash] \arrow[dr] & \\
O_K/\pi & \operatorname{Spec} B/M_1^{e_1} \text{ is a pt.}
\end{tikzcd}$$

⚠ $\pi B = M_1 \cdots M_s$ (i.e. $e_1 = \cdots = e_s = 1$). it's not sufficient to get (*).

☆ In general, π does not ramifies in B means:

$\pi B = M_1 \cdots M_s$ (distinct max ideal). and B/M_i is separable over $O_K/(\pi)$ $i = 1, \ldots, s$.

$B/\pi B$ = product of field & each is separable over $O_K/(\pi)$;

(algebra)

☆ Thm (Hermite - Minkowski)
Fix $d \geq 1$ and fix a finite set of primes $p_1, \dots, p_s$.
Then there are only finitely many $L/\mathbb{Q}$ of deg d s.t. L has good red at every prime p, $p \in \{p_1, \dots, p_s\}$

Thm (Shafarevic ~1962)
There exists only finitely many elliptic curve $E/\mathbb{Q}$, s.t. $E/\mathbb{Q}$ has good reduction at all prime p with $p \notin \{p_1, \dots, p_s\}$

Thm (Faltings 1983 Shafarevich conj.)
Same statement for curve $X/\mathbb{Q}$ of genus $g \geq 2$.

E.g. Fermat curve $x^p + y^p = z^p$ bad red only at p

curve $X_0(N)$, $X_1(N)$, $X(N)$ $\Bigg\}$ bad red only at prime p with $p | N$

☆ For Elliptic curve over $\mathbb{Q}$, we know where to find the ones with good red outside $\{p_1, \dots, p_s\}$

Exercise $K \supseteq O_K \twoheadrightarrow k$ char $k \neq 2, 3$.
Let WE/O_K be a W.F. for E/K over O_K,
Equation WE is minimal over O_K
$\Longleftrightarrow$ either $v(\Delta) < 12$
or $v(c_4) < 4$

☆ Given a WE/O_K for E/K, we can def a model in $\mathbb{P}^2/O_K$

$$\begin{tikzcd}
\mathbb{P}^2_k \arrow[r, leftrightarrow] & \mathbb{P}^2_{O_K} \arrow[rr, bend left] & \mathbb{P}^2_K \arrow[l, hook'] & {} \\
\tilde{\mathcal{E}}_{WE} \arrow[u, phantom, "\cup"] \arrow[r, hook] \arrow[d] & \mathcal{E}_{WE} \arrow[u, phantom, "\cup"] \arrow[d] & E \arrow[u, phantom, "\cup"] \arrow[l] \arrow[d] & \\
{} & {} & {} &
\end{tikzcd}$$

☆ We have a red map:

$$\begin{tikzcd} \mathbb{P}^2(k) \arrow[r, "red"] & \mathbb{P}^2(k) \\ E(k) \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\text{group homo.}"'] & \tilde{\mathcal{X}}_{WE}(k) \arrow[u, phantom, sloped, "\subseteq"] \end{tikzcd}$$

Best case: $\tilde{\mathcal{X}}_{WE}/k$ is an elliptic curve ($WE/\mathcal{O}_K$ was then minimal).

Thm: $E(k) \xrightarrow{red} \tilde{\mathcal{X}}_{WE}(k)$ is a group homo

Pf (sketch): In $E(k) \subseteq \mathbb{P}^2(k)$: 3 pt on a line add to a neutral element.

In $\tilde{\mathcal{X}}_{WE}(k) \subseteq \mathbb{P}^2(k)$ the same thing.

Take three pts on a line in $\mathbb{P}^2(k)$, reduce them, they still on a line.

☆ $\tilde{\mathcal{X}}_{WE}(k)$ is not an elliptic curve.

If we want, we can assume the unique singular pt on $\tilde{\mathcal{X}}_{WE}(k)$ is $(0:0:1) \in \mathbb{P}^2(k)$

We still have a red map from

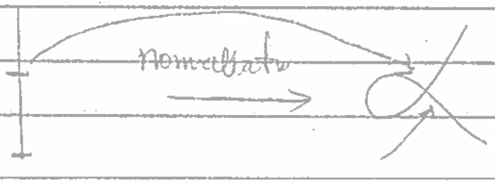
$$\begin{tikzcd} \mathbb{P}^2(k) \arrow[r] & \mathbb{P}^2(k) \\ E(k) \arrow[u, phantom, sloped, "\subseteq"] \arrow[r] & \tilde{\mathcal{X}}_{WE}(k) \arrow[u, phantom, sloped, "\subseteq"] \end{tikzcd}$$

☆ There is no gp structure on $\tilde{\mathcal{X}}_{WE}(k)$

☆ But,

Thm: $\tilde{\mathcal{X}}_{WE}(k) \setminus \{\text{sing pt}\}$ does have a group structure (Three pts add to there)

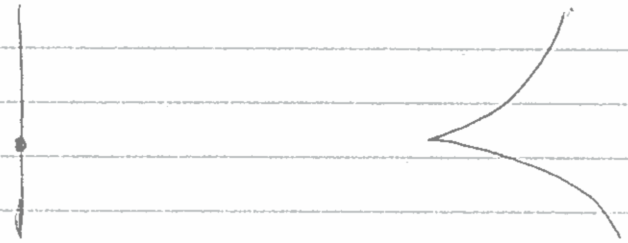
Rk.



$$\begin{tikzcd}
\mathbb{P}^1\setminus\{2\text{ pts}\} \arrow[r] \arrow[d] & \widetilde{\mathcal{X}}_{WE}(k)\setminus\{\text{singul pt}\} \\
\text{multiplicato gp } (\mathbb{A}^1-\{0\} &
\end{tikzcd}$$

$\boxed{\text{two rational pts}}$

$\mathbb{P}^1\setminus\{0,\infty\} \cong \mathbb{G}_m$, the multiplicate group



$$\mathbb{P}^1\setminus\{1\text{ pt}\} \longrightarrow \widetilde{\mathcal{X}}_{WE}(k)\setminus\{\text{sing pt}\}$$

$\mathbb{P}^1\setminus\{\infty\} = \mathbb{A}^1$ additive group $\mathbb{G}_a$

☆

$$\begin{tikzcd}
E(k) \arrow[r, "red"] & \widetilde{\mathcal{X}}_{WE}(k) \\
red^{-1}(\widetilde{\mathcal{X}}_{WE}(k)\setminus\{p_0\}) \arrow[u, phantom, sloped, "\subseteq"] \arrow[r] & \widetilde{\mathcal{X}}_{WE}(k)\setminus\underbrace{\{\text{sing pt}\}}_{p_0} \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

Thm This map is a group homor

★ Assume that WE/O_K is minimal (and we have bad red)

Then $E^\circ(k) := red^{-1}(\widetilde{\mathcal{X}}_{WE}(k)\setminus\{p_0\})$

$\cap\!|$

$E(k) \leftarrow$ subgp

$red^{-1}(\widetilde{\mathcal{X}}_{WE}(k)\setminus\{p_0\})$ is a subgp of $E(k)$

Thm (k is perfect) $E(k)/E^\circ(k)$ is a finite abelian gp such that

(1) If good red. no sing pt, then $F^\circ(k) = E(k)$

③ If E/k has additive red, then

$E(k)/E^{\circ}(k) \in \{(0), \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2\}$

If $k = \mathbb{Q}_p$ or a complete field k_v, w.r.t. a valuation v,
then $|E(k_v)/E^{\circ}(k_v)|$ is called the Tamagawa number c_v at v.

Ellipc curve $\simeq \mathbb{C}/\text{lattice}$ ⟶ lattice is the fundamental gp.

13th/Nov/18 Tue.

$K \supseteq \mathcal{O}_K \to k$ DVR.

E/K. WE/$\mathcal{O}_K$ for E/K. (For arbitrary W.E.) not minimal)

$$\begin{tikzcd}
\mathbb{P}^2_k \arrow[r, phantom, "\subseteq"] & \mathbb{P}^2_{\mathcal{O}_K} \arrow[r, phantom, "\subseteq"] & \mathbb{P}^2_K & \\
\mathcal{E}_k \arrow[u, hook] \arrow[r, hook] \arrow[d] & \mathcal{E} \arrow[u, phantom, sloped, "\subseteq"] \arrow[u, phantom, "\text{closed}"'] \arrow[r, phantom, "\supseteq"] \arrow[d] \arrow[rr, bend left, "\text{dim}=2"] & E \arrow[u, phantom, sloped, "\subseteq"] \arrow[u, phantom, "\text{open}"'] \arrow[d] \arrow[r] & \text{scheme.} \\
\operatorname{Spec} k & \operatorname{Spec} \mathcal{O}_K \arrow[r, phantom, "\supseteq"] & \operatorname{Spec} K &
\end{tikzcd}$$

red:

$$\begin{tikzcd}
\mathbb{P}^2(K) \arrow[r] & \mathbb{P}^2(k) \\
E(K) \arrow[u, phantom, sloped, "\subseteq"] \arrow[r] & \mathcal{E}_k(k) \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

Case1: Good red: $\mathcal{E}_k(k)$ has a group structure, and red is a group hom.

Case2: Bad red: $p_0 \in \mathcal{E}_k(k)$ is the singular point (k perfect).

Then $\mathcal{E}_k \setminus \{p_0\}$ has a group structure.

☆

$$\begin{tikzcd}
E(K) \arrow[r, squiggly, "?"] & ? \\
E^0(K) \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, "\text{red}", "\text{group homo}"'] \arrow[d] \arrow[dr] & \mathcal{E}_k(k) \setminus \{p_0\} \\
\text{subgroup of } E(K). & \text{preimage of } \mathcal{E}_k(k) \setminus \{p_0\}.
\end{tikzcd}$$

☆ We have $E^0(K) = E(K)$, $\Leftrightarrow$ no pts in $E(K)$ reduces to p_0.

regular / ~~singular~~ / smooth

$\begin{cases} \text{reg} = \text{smooth} & \text{dim } 1 \\ \text{reg} \neq \text{Smooth} & \text{dim} \geq 2 \end{cases}$

(regular pts [illegible])

prop. If P_0 is a regular pt of $\mathcal{E}$, then $E^{\circ}(K) = E(K)$.

Every local ring
not regular

prop. ⓐ $\mathcal{E}$ is a normal scheme. (i.e. noetherian, integral, $\forall p \in \mathcal{E}$, $\mathcal{O}_{\mathcal{E},p}$ is integrally closed

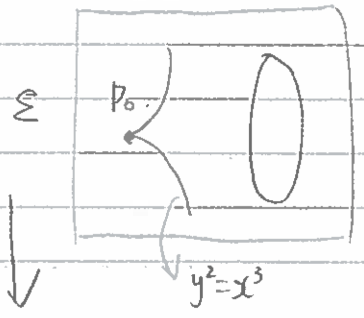
E.g. $\mathcal{X} = \mathrm{Spec}(A)$ A domain, noetherian,
$\mathcal{X}$ normal $\Leftrightarrow$ A integrally closed.

E.g. $\mathcal{O}_k[X,y]/_{NE}$ is integ closed ※

ⓑ If $p \in \mathcal{E}$ is a closed pt, (i.e. $p \in \mathcal{E}_k$)
and p is a regular pt in $\mathcal{E}_k$ then p is also a regular point of $\mathcal{E}$

Recall: If A is local noetherian dim n, with max ideal $\mathcal{M}$, then
- $\mathcal{M}$ can not be generated by fewer than n elemts
- A is called regular if $\mathcal{M}$ can be generated by n elemts.
- If $\dim A = 1$, and A is regular, then A is a $\underbrace{\text{local PID}}_{\text{DVR}}$

E.g. $y^2 = x^3 + T^5$. char(k) ≠ 2, 3.



$$\operatorname{Spec} \mathcal{O}_K[x,y]/y^2-(x^3+\pi^5) \subseteq \mathcal{E}$$

$$\cup\!\!\!\mid$$

$$p_0 \longleftrightarrow (x,y,\pi)$$

may not be minimal

$$\operatorname{Spec}(k[x,y]/y^2-x^3) \subseteq \mathcal{E}_k$$

$$\cup\!\!\!\mid$$

$$p_0 \longleftrightarrow (x,y)$$

$\hookrightarrow$ minimal system

can not be generated by fewer elemts.

$$(x,y)\left(k[x,y]/y^2-x^3\right)_{(x,y)}$$

$\downarrow$

localize at (x,y)

☆ when $y^2=x^3+\pi \Rightarrow (x,y,\pi)=(x,y)$. So p_0 is regu on $\mathcal{E}$

Exercise. Show that $(x,y,\pi)\left(\mathcal{O}_K[x,y]/(y^2-(x^3+\pi^5))\right)_{(x,y,\pi)}$ can not be generated by two elemts.

$\hookrightarrow$ localize at (x,y,π).

(i.e. p_0 is not regular)

$\boxed{\text{when } s=2,3,4,5}$

☆ Same for $s \geq 6$ but only that the [illegible] $/E$ is not [illegible]

to P_0, $y^2 = x^3 + \pi^2$, $P := (0, \pi)$
$\mathrm{red}(p) = (0,0) = P_0$.

So here $E^0(k) \neq E(k)$

when $s = 4$, $y^2 = x^3 + \pi^2$, let the point be $(0, \pi^2)$.

when $s = 5$, P_0 is singular, but $E^0(k) = E(k)$.

★ Rule of thumb: Singular pt on a scheme "hides" information.
★ For curves, say $X = \mathrm{Spec}\, B$ is singular, but integral

$$B \subseteq ff(B)$$

$$\rightsquigarrow$$

$$B \subseteq \underbrace{\text{integ closure of } B \text{ in } ff(B)}_{B'}$$

$$\begin{tikzcd} \mathrm{Spec}(B') \arrow[d] & \text{~~of~~ regular curve} \arrow[l] \\ \mathrm{Spec}(B) & \text{a finite morphism when } B \text{ is an affine } k\text{-algebra} \end{tikzcd}$$

O_K is Dedekind domain
O_K integr $\underbrace{\text{closure in } L}_{O_L}$ is finited generate O_K module

★ $\mathrm{Spec}(B') \setminus f^{-1}(S)$
$\downarrow$ is an isomor

$$\begin{tikzcd} \mathrm{Spec}(\mathcal{O}_L) \arrow[d] \\ \mathrm{Spec}(\mathcal{O}_K) \end{tikzcd}$$

prime ideal ramified in L

☆ We can hope to achieve understanding of the singu pt $P_0 \in \Sigma$ by doing a similar process of resolution of singularity

☆ There exists a scheme

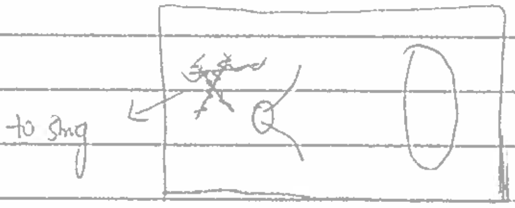
$$\begin{tikzcd} \Sigma' \setminus \{f^{-1}(P_0)\} \arrow[d, "f"', "\text{isomorphism}"] & \subseteq & \Sigma' \arrow[d, "f"] \\ \Sigma \setminus \{P_0\} & & \Sigma \end{tikzcd}$$

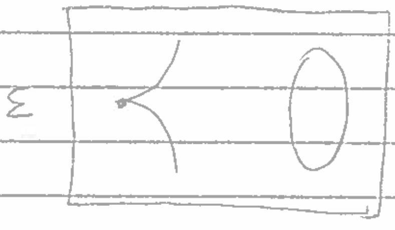
→ Σ' is regular everywhere

→ the fiber may not be finite

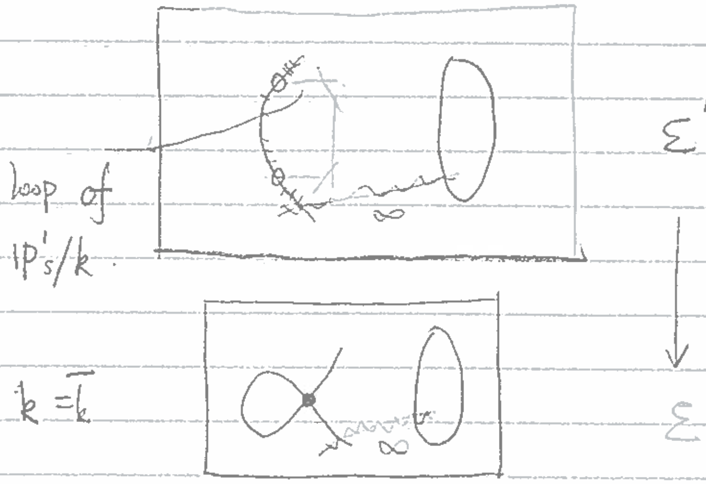
(could be a curve)

☆ $f^{-1}(P_0)$ is a union of finitely many projective curve on Σ'.





✱ The easier case: (Semi-stable reduction)



Exercise:

$$\begin{tikzcd}
\mathcal{X} \arrow[d, "\text{proper}"] \\
O_K
\end{tikzcd}$$

$\mathcal{X}$ regular

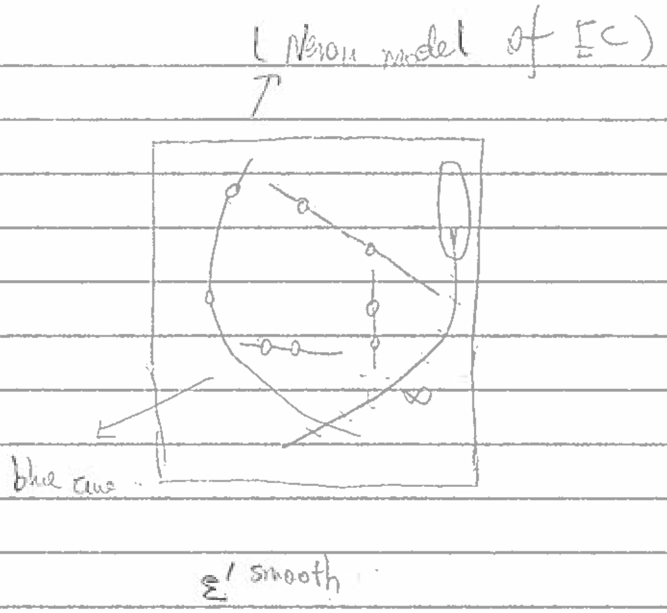
Generic fiber X/K. If $P \in X(K)$, then the reduction of p must be a regular pt of the special fibe $\mathcal{X}_k$.

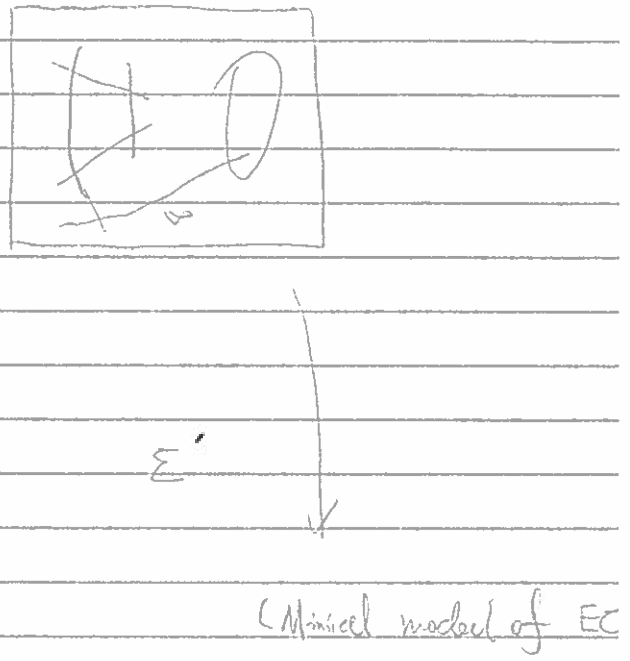
$xy - \pi^s$

$s > 1$: $(x, y, \pi) \curvearrowright$ blow-up at the maximal ideal, we have two $\mathbb{P}^1$

✱ Remove all singular pts in $\mathcal{E}_k'$

2/19





We have a group homo

$$\begin{tikzcd}
E(k) \arrow[r] & \mathcal{E}'^{smooth} \\
E^0(k) \arrow[r] \arrow[u, phantom, sloped, "\subseteq"] & \text{component of } \infty \arrow[u, phantom, sloped, "\subseteq"]
\end{tikzcd}$$

and $\mathcal{E}_k'^{smooth}$ has a group structure

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{E}_k(\bar{k})\setminus\{p_0\} \arrow[r] \arrow[d] & \mathcal{E}_k'^{smooth}(\bar{k}) \arrow[r] & \mathbb{Z}/\{\#\text{ of components in } \mathcal{E}_k'\} \arrow[r] & 0 \\
& \text{blue curve} & & &
\end{tikzcd}$$

($\mathcal{E}'^{smooth} \longrightarrow \operatorname{Spec} \mathcal{O}_K$ is a smooth morphism).