Elliptic Curves over Local Fields

K local field, complete wrt. a discrete valuation v

R ring of integers of K $= \{x \in K : v(x) \geq 0\}$

$R^\times$ unit gp of R $= \{x \in K : v(x) = 0\}$

$\mathfrak{m}$ max'l ideal of R $= \{x \in K : v(x) > 0\}$

π a uniformizer for R, $\mathfrak{m} = \pi R$.

$k = R/\mathfrak{m}$ the residue field, $p = \mathrm{char}(k)$

$a \in \mathbb{Z}$

$a = m p^n$, $\gcd(m,p) = 1$

ex $K = \mathbb{Q}_p$, $v = v_p$ s.t. $v_p(a) = v_p(m \cdot p^n) = n$

$R = \mathbb{Z}_p$, $R^\times = \mathbb{Z}_p - p\mathbb{Z}_p = \{\alpha \in \mathbb{Z}_p : \alpha \not\equiv 0 \bmod p\}$

$\mathfrak{m} = p\mathbb{Z}_p$, $\pi = p$

$k = \mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$

$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in K$

the change of variables: preserves Weier. forms

$$\begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases}$$

and

$\Delta_{E'} = u^{12}\Delta_E$

$c_{4,E'} = u^4 \cdot c_{4,E}$

In particular:

$$E : y^2 + a_1xy + a_3y = x^3 + \dots \longleftrightarrow E' : y'^2 + a_1'x'y' + a_3'y' = x'^3 + \dots$$

$$(x,y) \longleftrightarrow (u^{-2}x, u^{-3}y)$$

$$a_i \longleftrightarrow a_i' = u^i a_i$$

$$\Delta_E \longleftrightarrow \Delta_{E'} = u^{-12}\Delta_E$$

$$c_{4,E} \longleftrightarrow c_{4,E'} = u^{-4}c_{4,E}$$

a local field!!

Def A Weiers. eq'n over K is called minimal (at v) if

- $a_i \in R$
- $v(\Delta)$ is smallest among Weier. models w/ $a_i \in R$.

ex $E: y^2+xy+y = x^3+x^2+22x-9 \;/\mathbb{Q} \subseteq \mathbb{Q}_p$

$\Delta_E = -2^{15}\cdot 5^2$, $c_{4,E} = -5\cdot 211$

$\Rightarrow E/\mathbb{Q}_p$ is minimal (for any $p \in \mathbb{Z}$)

Remark Although minimality is defined wrt $v(\Delta)$, the valuation of c_4 helps decide whether $v(\Delta)$ is as small as it can be subject to $a_i \in R$.

ex $E: y^2+6xy+864y = x^3+180x^2+14256x+559872$

$\Delta_E = -2^{12}\cdot 3^{12}\cdot 11\cdot 941$ (Magma: MinimalModel(E);)

$[u,r,s,t] = [6,-72,0,-216]$

$E': y^2+xy+4y = x^3-x^2+2x-1$ $\quad \Delta' = -11\cdot 941.$

$\cong E'': y^2+xy+3y = x^3+2x^2+4x+5$ $\quad \Delta'' = \Delta' = -11\cdot 94.$

Prop. (a) Every ell. curve E/K (local field) has a min'l Weier. eq'n.

(Not true over global fields in general!)

(b) ... unique up to a change of vars $\begin{cases} x = u^2x' + r \\ y = u^3y' + u^2sx' + t \end{cases} = *$ with $u \in R^\times$, $r,s,t \in R$.

(c) Conversely if one starts from a Weier. eq'n w/ $a_i \in R$ and $\begin{cases} x = \\ y = \end{cases}$ $(*)$ and we get a minimal model then $u,r,s,t \in R$.

Reduction Modulo π (mod $\mathfrak{m}$)

K, $R \xrightarrow{\sim} k = R/\mathfrak{m}$ natural reduction map

$r \longmapsto r \bmod \mathfrak{m}$

$(\mathbb{Z}_p \longrightarrow \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p/p\mathbb{Z}_p)$

$E: y^2 + a_1xy + a_3y = x^3 + \cdots \ /K \xrightarrow{\sim} \tilde{E}: y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \cdots \ /k$

(minimal model)

$P \longmapsto \tilde{P}$

$(x_0, y_0) \longmapsto (\tilde{x}_0, \tilde{y}_0)$

$[x_0, y_0, z_0] \longmapsto [\tilde{x}_0, \tilde{y}_0, \tilde{z}_0]$

$P \in E(K) \Rightarrow P = [x_0, y_0, z_0]$ $x_0, y_0, z_0 \in R$.

w/ one of $v(x_0), v(y_0), v(z_0)$ is 0.

ex $E : y^2 = x^3 - 2$, $\Delta_E = -1728 = -12^3 = -2^6 \cdot 3^3$

$\Rightarrow E/\mathbb{Q}_p$ minimal (for all p)

$p=5$

$\Delta_E \equiv -1728 \equiv -3 \equiv 2 \bmod 5$ $(\neq 0 \Rightarrow \tilde{E}/\mathbb{F}_5$ is smooth!)

$E \longrightarrow \tilde{E}$

$[x_0, y_0, z_0] \longmapsto [\tilde{x}_0, \tilde{y}_0, \tilde{z}_0] \bmod 5$

$P = (3,5) \longmapsto (3,0) \in \tilde{E}(\mathbb{F}_5)$

$2P = \left(\frac{129}{100}, -\frac{383}{1000}\right) \longmapsto$?

$2P = [1290, -383, 1000] \longmapsto [0,1,0] \in \tilde{E}(\mathbb{F}_5)$

"$\mathcal{O}$"

$\tilde{P} \in \tilde{E}[2]$

However!

P is of infinite order on E!

$$E/K \xrightarrow{\sim} \tilde{E}/k$$

WARNING: $\Delta \neq 0$ in K but $\Delta \equiv 0 \bmod \mathfrak{M}$

and therefore $\tilde{E}$ may be singular!

ex $\Delta = 7$ in $\mathbb{Q}_7$, $\Delta \equiv 0 \bmod 7\mathbb{Z}_7$.

Def $\tilde{E}_{ns}(k) = \{$ non-singular pts on $\tilde{E}\}$ Recall: $\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^+$ or $\bar{k}^*$

$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\}$ pts of non-sing. red'n.

$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\}$ kernel of $\sim$

Prop There is an exact sequence of abelian groups:

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \xrightarrow{\sim} \tilde{E}_{ns}(k) \longrightarrow 0.$$

Proof. On $(E(K), +)$, $(\tilde{E}_{ns}(k), +)$ addition is defined by intersections of lines with the curve in $\mathbb{P}^2$.

Since $\mathbb{P}^2(K) \xrightarrow{\sim} \mathbb{P}^2(k)$ takes lines to lines,

then $E_0(K)$ is a group and $E_0(K) \xrightarrow{\sim} \tilde{E}_{ns}(k)$ is a hom.

and $E_1(K)$ is its kernel.

We need $\sim$ is surjective.

$E_0(K) \xrightarrow{\sim} \tilde{E}_{ns}(k)$ is surjective: use Hensel's lemma.

Let $E: f(x,y) = 0$ (min'l Weiers. eq'n).

$\tilde{E}: \tilde{f}(x,y) = 0$. Let $\tilde{P} = (\alpha, \beta) \in \tilde{E}_{ns}(k)$

Since $\tilde{P}$ is non-singular either $\frac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0$ or $\frac{\partial \tilde{f}}{\partial y}(\tilde{P}) \neq 0$.

$\frac{\partial \tilde{f}}{\partial x}(\tilde{P}) \neq 0$ — true

Let $y_0 \in R$ s.t. $\tilde{y}_0 = \beta$.

Consider $p(x) = f(x, y_0)$:
- $p(x)$ has a root $\alpha \bmod M$ ($p(x, y_0) \equiv p(\alpha, \beta) \equiv 0 \bmod M$)
- $p'(\alpha) \not\equiv 0 \bmod M$

Hensel!

$\Rightarrow \exists\, x_0 \in R$ s.t. $x_0 \equiv \alpha \bmod M$ and $p(x_0) = 0$ in R

$\Rightarrow f(x_0, y_0) = 0$ in R and thus $P = (x_0, y_0) \in E(K) \longmapsto \tilde{P} = (\alpha, \beta) \in \tilde{E}_{ns}(k)$

$\Rightarrow \sim$ is surjective ▨

In general:

$$0 \to E_1(k) \longrightarrow E_0(k) \longrightarrow \tilde{E}_{ns}(k) \to 0$$

Note

If $\Delta_E \not\equiv 0 \bmod \mathcal{M}$ then $\tilde{E} = \tilde{E}_{ns}$, $\tilde{E}$ is non-singular and $E = E_0$.

$$\Rightarrow \quad 0 \to E_1(k) \longrightarrow E(k) \longrightarrow \tilde{E}(k) \to 0$$

Prop Let E/K be given by a min'l W. eq'n. Let $\hat{E}/R$ be the formal gp assoc. to E, and let $w(z) \in R[[z]]$ the power series of Ch IV. Then $\hat{E}(\mathcal{M}) \xrightarrow{f} E_1(k)$ is an isomorphism.

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

$$0 \longmapsto \mathcal{O}.$$

Recall $\hat{\mathbb{G}}_a$ $\quad 0 \to \mathcal{M} \to R \to k \to 0$

$\hat{\mathbb{G}}_m$ $\quad 0 \to 1+\mathcal{M} \to R^\times \to k^* \to 0$

$\hat{E}$ $\quad 0 \to \hat{E}(\mathcal{M}) \to E(k) \to \tilde{E}(k) \to 0$??? (true if $\tilde{E}$ is smooth!)

$\hat{E}(\mathcal{M}) = E_1(k)$

$\hat{E}(\mathcal{M}) \xrightarrow{f} E_1(k)$, $f(z) = \left(\frac{z}{w(z)}, \frac{-1}{w(z)}\right)$

Proof ($E_1(k) \cong \hat{E}(\mathcal{M})$).

From def. of $w(z)$, the pt. $\left(\frac{z}{w(z)}, \frac{-1}{w(z)}\right) \in E$ (power series)

and $w(z) = z^3(1 + \dots) \in R[\![z]\!]$ so it converges for any $z \in \mathcal{M}$

$\Rightarrow f(z) \in E(k)$ for any $z \in \mathcal{M}$.

$f(z) = [z, -1, w(z)] \xrightarrow[\text{mod } \mathcal{M}]{\sim} [0, -1, 0] = [0, 1, 0] \to f(z) \in E_1(k)$.

Moreover! $\oplus$ on $\hat{E}(\mathcal{M})$ was defined to match add. on E

$\Rightarrow f$ is a gp hom.

- $\hat{E}(\mathcal{M}) \xrightarrow{f} E_1(k)$ is a gp. hom.

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

- Injective: $[z,-1,w(z)] = [0,1,0] \rightsquigarrow z=0 \Rightarrow \ker f = \{0\}$.

- Surjective: Let $(x,y) \in E_1(k)$, $[x,y,1] \xrightarrow{\sim} \mathcal{O}$

  $\Rightarrow \exists \alpha \in \mathcal{M} \quad [\alpha x, \alpha y, \alpha] = [0,1,0]$

  $\Rightarrow v(\alpha x) > v(\alpha y) \Rightarrow v(x) > v(y)$

  $\Rightarrow v(x) - v(y) > 0 \Rightarrow v\left(\frac{x}{y}\right) > 0. \Rightarrow \frac{x}{y} \in \mathcal{M}$

$E_1(k) \xrightarrow{g} \hat{E}(\mathcal{M})$

$(x,y) \longmapsto -x/y$

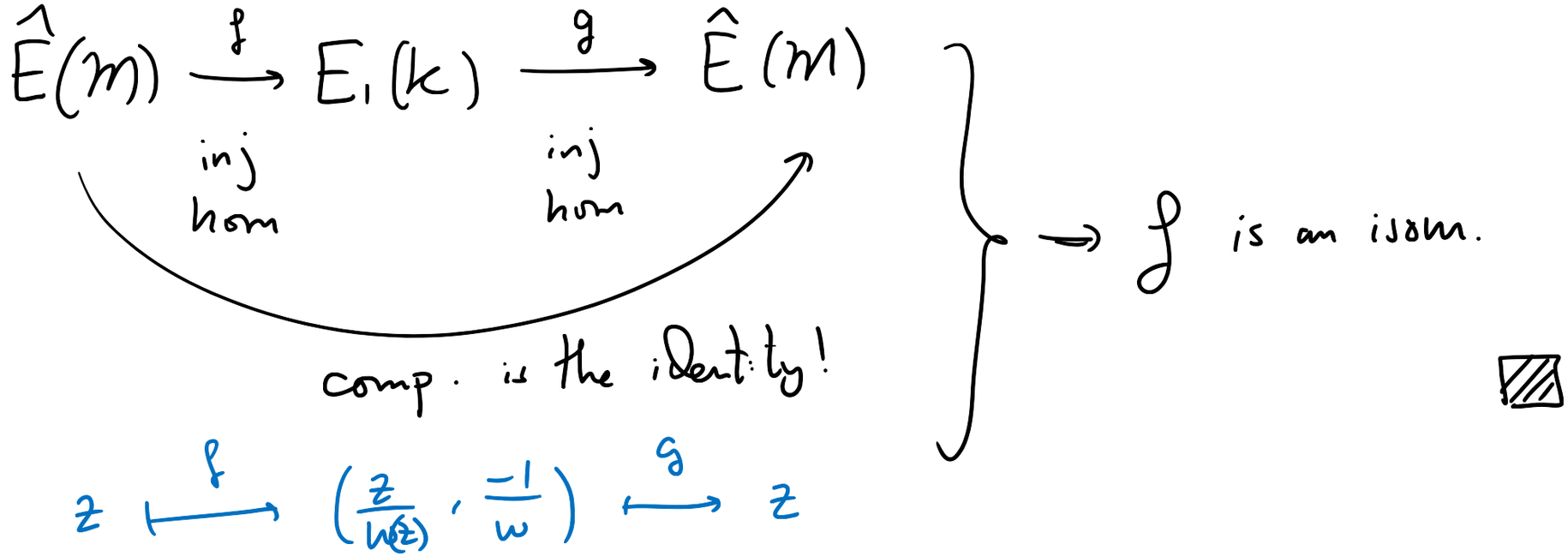
z''

and above shows if $(x,y) \in E_1(k)$ then $g(x,y) \in \hat{E}(\mathcal{M})$

g is
- also a hom.
- injective $\quad [x,1,z] \xrightarrow{g} -x = 0 \Rightarrow x = 0 \Rightarrow z = 0$

$\in \mathcal{M}$

$zy^2 + a_1 xyz + a_3 yz^2 = \ldots \Rightarrow z = a_6 z^3 + a_3 z^2$



$$z \xmapsto{f} \left(\frac{z}{h(z)}, \frac{-1}{w}\right) \xmapsto{g} z$$

Points of Finite Order

Prop Let E/K be an ell. curve and $m \geq 1$ an integer rel. prime to $p = \mathrm{char}(k)$. Then:

(a) The subgp $E_1(K)$ has no non-trivial points of order m.

(b) If the reduced curve $\tilde{E}/k$ is non-singular then the red'n map

$$E(K)[m] \longrightarrow \tilde{E}(k)$$

is injective.

ex $E/\mathbb{Q} : y^2 = x^3 + 3$. Find $E(\mathbb{Q})_{tors}$.

$\Delta_E = -3888 = -2^4 \cdot 3^5$. $\begin{cases} E/\mathbb{Q}_p \text{ is minimal for all primes } p. \\ \tilde{E}/\mathbb{F}_p \text{ is non-singular for } p \geq 5. \end{cases}$

$\boxed{p=5}$ $\tilde{E}(\mathbb{F}_5) = \{\tilde{\mathcal{O}}, (1,2), (1,3), (2,1), (2,4), (3,0)\}$

so $N_5 = \#\tilde{E}(\mathbb{F}_5) = 6$.

$E(\mathbb{Q}) \subseteq E(\mathbb{Q}_p)$

$\boxed{p=7}$ $N_7 = 13$.

PROP $\Rightarrow$ • If $q \neq 5,7$ then $\#E(\mathbb{Q})[q]$ divides 6 and 13 $\Rightarrow \#E(\mathbb{Q})[q] = 1$.
so no q-torsion over $\mathbb{Q}$.

• $q=5 \Rightarrow \#E(\mathbb{Q})[5]$ divides 13 but $\#E(\mathbb{Q})[5] = 1, 5, 25 \Rightarrow \#E(\mathbb{Q})[5] = 1$
so no 5-torsion over $\mathbb{Q}$.

• $q=7 \Rightarrow \#E(\mathbb{Q})[7]$ divides 6 $\Rightarrow \#E(\mathbb{Q})[7] = 1 \rightarrow$ so no 7-torsion over $\mathbb{Q}$.

$\Rightarrow E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$ However $(1,2) \in E(\mathbb{Q}) \Rightarrow E(\mathbb{Q})$ is infinite!