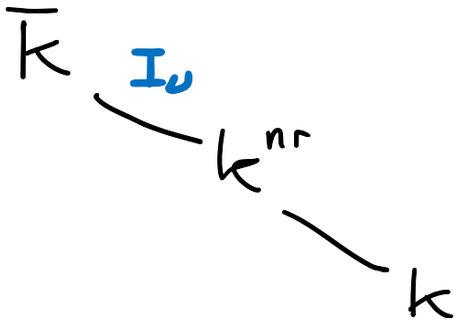
Elliptic Curves over Local Fields

• The action of Inertia

K local field, complete wrt v.

$\bar{K}$ algebraic closure

K^{nr} maximal unramified ext'n of K in $\bar{K}$



$G_K = \mathrm{Gal}(\bar{K}/K) = D(\mathcal{M}_{\bar{K}}/\mathcal{M}_K)$ decomposition group

$I_v = \mathrm{Gal}(\bar{K}/K^{nr}) = I(\mathcal{M}_{\bar{K}}/\mathcal{M}_K)$ the inertia subgp.

$\sigma \in G_K$ s.t. $\sigma(\alpha) \equiv \alpha \bmod \mathcal{M}_{\bar{K}}$ for all $\alpha \in R_{\bar{K}}$ $\Rightarrow \tilde{\sigma} = \mathrm{id}$ on $\bar{k}$

$$1 \longrightarrow \underset{\| \; I_v}{\mathrm{Gal}(\bar{K}/K^{nr})} \longrightarrow \mathrm{Gal}(\bar{K}/K) \longrightarrow \underset{\| \; \mathrm{Gal}(\bar{k}/k)}{\mathrm{Gal}(K^{nr}/K)} \longrightarrow 1$$

Def. Σ (G_K) is unramified at v if I_v acts trivially on Σ.

Prop. Let E/K be an ell. curve, s.t. $\tilde{E}/k$ is non-singular. (GOOD REDUCTION!)

(a) Let $m \geq 1$ s.t. $\gcd(m, \mathrm{char}(k)) = 1$.
Then $E[m]$ is unramified at v.

(b) Let $\ell \neq \mathrm{char}(k)$, then $T_\ell(E)$ is unramified at v.

Q: Converse? THE CRITERION OF NÉRON-OGG-SHAFAREVICH.

Thm. E/K ell. curve. TFAE:

(a) E has good reduction over K

(b) $E[m]$ is unramified at v for all integers $m \geq 1$ rel. prime to $\mathrm{char}(k) = p$

(c) The Tate module $T_\ell(E)$ is unramif. at v for some (all) primes ℓ rel. prime to p.

(d) $E[m]$ is unramif. at v for only many integers $m \geq 1$ rel. pr. to p.

Good And Bad Reduction

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

min'l model

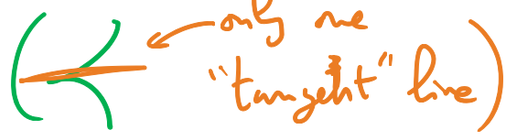
Def.

(a) E has good (or stable) reduction over K if $\tilde{E}$ is non-singular.

(b) E has multiplicative (or semi-stable) reduction over K if $\tilde{E}$ has a node  two "tangent" lines at sing.

(b.1) If the slopes are in k then, it is split mult.

(b.2) If the slopes are not in k, it is non-split mult.

(c) E has additive redn (or unstable) if $\tilde{E}$ has a cusp  only one "tangent" line

Prop. (III.1.4, III.2.5) (HOMEWORK!)

Let E/K be given by a min'l Weier. eq'n $y^2+a_1xy+\cdots = x^3+\cdots$.
Let Δ_E be the disc., and $c_{4,E}$ be as usual.

(a) E has good red'n $\iff v(\Delta)=0$ (i.e., $\Delta \in R^\times$)
In this case $\tilde{E}/k$ is an ell. curve.

(b) E has mult. red'n $\iff v(\Delta)>0$, $v(c_4)=0$.
In this case $\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^*$

(c) E has add. red'n $\iff v(\Delta)>0$, $v(c_4)>0$
In this case $\tilde{E}_{ns}(\bar{k}) \cong (\bar{k},+)$

examples

(1) $E_1 : y^2 = x^3 + 35x + 5$, $\Delta = -2^4 \cdot 5^2 \cdot 71 \cdot 97$

$c_4 = -2^4 \cdot 3 \cdot 5 \cdot 7$.

- has good red'n at $p=7$ $\left(\tilde{E}_1 : y^2 = x^3 + 5 / \mathbb{F}_7\right)$
- At $p=5$ there is bad red'n, $\Delta \equiv c_4 \equiv 0 \bmod 5 \Rightarrow$ additive red'n.

$\tilde{E} : y^2 = x^3 / \mathbb{F}_5$ $\quad (y - 0\cdot x)^2 - x^3 = 0$

$y=0$ is the "tangent" line at $(0,0)$.

$f(x,y)=0$, $P=(x_0,y_0)$ singularity $\Rightarrow \left.\frac{\partial f}{\partial x}\right|_P = \left.\frac{\partial f}{\partial y}\right|_P = 0$

Taylor $\Rightarrow f(x,y) - f(x_0,y_0) = \left(y - y_0 - \alpha(x-x_0)\right)\cdot\left(y - y_0 - \beta(x-x_0)\right) - (x-x_0)^3$

"tangent" lines at sing.

example

$E_2 : y^2 = x^3 - x^2 + 35$, $\Delta = -2^4 \cdot 5 \cdot 7 \cdot 941$

$c_4 = 16$.

p=5 $y^2 + x^2 - 35 - x^3 = 0$

$y^2 + x^2 - x^3 \equiv 0 \mod 5$ (bad)

$(y-2x)(y+2x) - x^3 \equiv 0$ ⟶ split mult. red'n at 5.

p=7 $y^2 + x^2 - x^3 \equiv 0 \mod 7$ (bad)

DOES NOT FACTOR

$-1 \notin (\mathbb{F}_7^\times)^2$ ⟶ non-split mult. red'n at 7.

example $E/\mathbb{Q}: y^2 = x^3 + 7^3$ $\quad \Delta = -2^4 \cdot 3^3 \cdot 7^6$

$c_4 = 0$.

$\Rightarrow p = 7$ is **bad additive.**

Over $E/\mathbb{Q}(\sqrt{7})$: $E: y^2 = x^3 + (\sqrt{7})^6$ not minimal at 7

change vars: $y' = (\sqrt{7})^3 y$, $x' = (\sqrt{7})^2 x$

$\Rightarrow E': y'^2 = x'^3 + 1$ which has **good red'n** at the prime $(\sqrt{7})$ of $\mathbb{Q}(\sqrt{7})$ above 7.

$E'/\mathbb{Q}(\sqrt{7})$

$\rightsquigarrow$ additive red'n is "unstable"

Def. Let E/K be an ell. curve. E has potential good redn over K if there is a finite extn K'/K s.t. E has good redn over K'.

ex $E/\mathbb{Q}_7 : y^2 = x^3 + 7^3$ has pot. good redn (bad add.)
and good redn at $(\sqrt{7})$ of $\mathbb{Q}_7(\sqrt{7}) = K'$
K''

PROP. (Semi-stable redn thm.) E/K be an ell. curve.

(a) Let K'/K be an unramified extn. Then the redn type of E/K (good, mult., add) is the same as the redn type of E/K'.

(b) Let K'/K be any finite extn. If E has either good or mult. redn over K then it has the same type of redn over K'. (non-split mult may become split mult.)

(c) There exists a finite extn K'/K s.t. E/K' has either good or split mult. reduction.

Proof of (c) $E/K \rightsquigarrow E/K'$ with good or split. mult. red'n.

($\mathrm{char}(k) \neq 2$)

$K(E[2])$ or a quad. extn of $K(E[2])$

- Extend K by a finite ext'n s.t. E can be given by a model

$$E: \; y^2 = x(x-1)(x-\lambda) \quad \text{(Legendre Normal Form)}$$

$$c_4 = 16\cdot(\lambda^2-\lambda+1), \quad \Delta = 16\cdot\lambda^2(\lambda-1)^2$$

- CASE 1. $(\lambda \in R, \lambda \not\equiv 0,1 \bmod \mathfrak{m}) \Rightarrow \Delta \in R^\times$ so good reduction ☺

- CASE 2. $(\lambda \in R, \lambda \equiv 0 \text{ or } 1 \bmod \mathfrak{m}) \Rightarrow \Delta \in \mathfrak{m}$, $c_4 \equiv 16 \bmod \mathfrak{m}$

  $\not\equiv 0$

  So red'n is multiplicative, after possibly a quad. ext'n, red'n is split mult.

- CASE 3. $(\lambda \notin R)$ Choose $r \geq 1$ s.t. $\pi^r\lambda \in R^\times$. Then change vars $\begin{cases} x = \pi^{-r}x' \\ y = \pi^{-\frac{3r}{2}}y' \end{cases}$

  $K' = K(\alpha,\beta)$

  change $K' = K(\sqrt{\pi})$, gives

$$E_{/K'}: (y')^2 = x'(x'-\pi^r)(x'-\pi^r\lambda) \Rightarrow \Delta' \in \mathfrak{m}, \; c_4' \in R^\times$$

so split mult. red'n. ▨

The Group E/E_0

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\} \overset{!}{\subseteq} E(K)$$

$E_1(K) = \ker\left(E_0(K) \longrightarrow \tilde{E}_{ns}(k)\right)$

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

$\hat{E}(\mathfrak{m})$ GOOD! $0 \to E_1(K) \to E(K) \to \tilde{E}(k) \to 0$

Thm (Kodaira, Néron) E/K ell. curve.

- If E/K has split mult. red'n then $E(K)/E_0(K)$ is a cyclic gp of order $v(\Delta) = -v(j)$.
- In <u>all</u> other cases $E(K)/E_0(K)$ is a finite group of order at most 4.

<u>KEY</u>: The existence of a Néron model. !!

Prop $K/\mathbb{Q}_p$ finite, E/K.

Then, $E(K)$ contains a subgp of finite index isomorphic to $(R,+)$.

Pf. $E(K)/E_0(K)$ is finite (by Kod./Ner thm) AND $E_0(k)/E_1(k) \cong \tilde{E}_{ns}(k)$

($E_0(k)/E_1(k)$: finite; $\tilde{E}_{ns}(k)$: finite. $k/\mathbb{F}_p$ finite!)

$$E_1(K) \subseteq E_0(K) \subseteq E(K)$$

$\hat{E}(\mathfrak{m})$ = $\hat{E}(\mathfrak{m})$ (finite index) (finite index) $\hat{E}(\mathfrak{m})$ =

Suffices to show $(R,+) \subseteq E_1(K)$ of finite index.

- Filtration: $\hat{E}(\mathfrak{m}) \supseteq \hat{E}(\mathfrak{m}^2) \supseteq \hat{E}(\mathfrak{m}^3) \supseteq \dots$

  and $\hat{E}(\mathfrak{m}^i)/\hat{E}(\mathfrak{m}^{i+1}) \cong \mathfrak{m}^i/\mathfrak{m}^{i+1}$ (finite gp!)

- And for large enough r: $\hat{E}(\mathfrak{m}^r) \xrightarrow[\cong]{\log_f} \mathfrak{m}^r = \pi^r R \cong (R,+)$ as ab gps. ▨