Serre's Adelic Open Image Theorem

(the non-CM case)

SeZoum

Tyler Genao

4/30/2021

Overview

(1) Review basics & go over what's left

(2) Sketch the proof of the main theorem

(3) Go over some key ideas behind proofs,

such as tame inertia & its characters

Galois representations of elliptic curves

- E/F an elliptic curve over a # field
- $G_F := \mathrm{Gal}(\overline{F}/F)$ acts on the torsion subgroup $E[\mathrm{tors}]$, via e.g.

$$(x, y)^\sigma := (x^\sigma, y^\sigma).$$

- For all $N \in \mathbb{Z}^+$, $G_F \circlearrowright E[N]$
- Thus we have the mod-N representation

$$\rho_{E,N}: G_F \to \mathrm{Aut}(E[N])$$

- $E[N]$ is a rank two $\mathbb{Z}/N\mathbb{Z}$-modules, so choosing a basis ...

... we get

$$\rho_{E,N} : G_{\mathbb{Q}} \to GL_2(N)$$

where $GL_2(N) := GL_2(\mathbb{Z}/N\mathbb{Z})$.

- For prime $\ell \in \mathbb{Z}^+$, the ℓ-adic Tate module

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

- $T_\ell(E)$ is a rank two $\mathbb{Z}_\ell$-module, and G_F extends to act on $T_\ell(E)$, so...

... one has the ℓ-adic representation

$$\rho_{E,\ell^\infty} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_\ell)$$

Packing the ℓ-adic Tate modules together, we get the adelic Tate module

$$T(E) := \prod_{\ell} T_\ell(E) \cong \varprojlim E[N].$$

$G_f \circlearrowright T(E)$ gives the adelic

representation

$$\rho_E : G_f \to GL_2(\hat{\mathbb{Z}}).$$

Question: what do we know about

$\rho_E(G_F)$?

- "Easier" question: What do we know about each $\rho_{E,\omega}(G_F)$?

Main theorem of Serre's "Abelian ℓ-adic representations and elliptic curves":

Let E/F be a non-CM elliptic curve defined over a # field.

Then ρ_{E,ℓ^∞} has open image in $GL_2(\mathbb{Z}_\ell)$.

(Equivalently, has finite index.)

In the same book, he does more:

Notation:

$$G := \rho_E(G_F)$$

$$G_{\lambda^\infty} := \rho_{E,\lambda^\infty}(G_F)$$

$$G_\lambda := \rho_{E,\lambda}(G_F).$$

Proposition (IV-19):

For $E/\mathbb{Q}$ with no CM, TFAE:

* $GL_2(\mathbb{N}) := GL_2(\mathbb{Z}/N\mathbb{Z})$

(1) G is open in $GL_2\hat{\mathbb{Z}}$

(2) $G_{\ell^\infty} = GL_2(\mathbb{Z}_\ell)$ for almost all ℓ

(3) $G_\ell = GL_2(\ell)$ " " " "

(4) $G_\ell \supseteq SL_2(\ell)$ " " " "

- Using the theory of Tate curves, Serre shows that if $E/\mathbb{Q}_p$ has non-integral j-invariant then $G_p \cong GL_2(\mathbb{Z}_p)$ for $p \gg 0$. ("large enough p")

i.e. If $E/\mathbb{Q}_p$ has non-integral j-invariant then $G \subseteq GL_2(\hat{\mathbb{Z}})$ is open.

Main theorem of Serre's "Galois properties of points of finite order on elliptic curves":

If $E/\mathbb{Q}$ does not have CM, then

$\rho_E(G_{\mathbb{Q}})$ is open in $GL_2(\hat{\mathbb{Z}})$.

The main theorem is equivalent to:

for all $\ell \gg 0$, one has

$$\rho_{E,\ell}(G_F) = GL_2(\ell).$$

(so the ℓ-division field $F(E[\ell])/F$ is as large as possible.)

The Proof

To show that $\rho_E(G_F)$ is open in $GL_2(\hat{\mathbb{Z}})$, it is equivalent to show that for $\ell >> 0$

$$G_\ell \subseteq SL_2(\ell)$$

where $G_\ell := \rho_{E,\ell}(G_F)$.

Subgroups of $GL_2(\mathbb{R})$

* Numbering follows P.L. Clarks translation, see sezoom site

- Proposition 16: For a subgroup $G \subseteq GL_2(\mathbb{R})$ with $|\mathbb{R}| \# G$, one has G irreducible iff $G \supseteq SL_2(\mathbb{R})$.

- But already almost all G_n are irreducible! See Theorem IV.2.2 of the book.

- So does $\rho \mid_{H} \cong \sigma$ for almost every ρ?

- What subgroups of $GL_2(\mathbb{Z})$ can $G_{\mathbb{Q}}$ be?

- $B(\lambda) := \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in GL_2(\lambda) \right\}$ Borel

- $Cs(\ell) := \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in GL_2(\lambda) \right\}$ split Cartan

- $Cns(\lambda) := \left\{ \begin{bmatrix} a & b\varepsilon \\ b & a \end{bmatrix} \in GL_2(\lambda) \right\}$ $\lambda \supsetneq \mathbb{F}_\ell$ non-split Cartan

(Regular representation of $\mathbb{F}_\ell(\varepsilon)^\times$ acting on itself by multiplication.

$* \varepsilon \in \mathbb{F}_\ell$, $\sqrt{\varepsilon} \notin \mathbb{F}_\ell$.

- Normalizers of the Cartan subgroups:

$$C_s^+(\ell) = C_s(\ell) \cup \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} C_s(\ell)$$

$$= \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix}, \begin{bmatrix} 0 & b \\ c & 0 \end{bmatrix} \in GL_2(\ell) \right\}.$$

$$C_{ns}^+(\ell) = C_{ns}(\ell) \cup \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} C_{ns}(\ell)$$

$$= \left\{ \begin{bmatrix} a & b\varepsilon \\ b & a \end{bmatrix}, \begin{bmatrix} a & b\varepsilon \\ -b & -a \end{bmatrix} \in GL_2(\ell) \right\}.$$

Essentially due to Dickson:

Let $\ell \in \overline{\mathbb{Z}}$ be prime, and $G \leq GL_2(\ell)$ a subgp.

① If $\ell \nmid |G|$ then up to conjugacy

(a) $G \supseteq SL_2(\ell)$ (irreducible)

(b) G is contained in the Borel (reducible).

② If $\ell \mid |G|$ then up to conjugacy

(a) G is contained in the normalizer of a Cartan

(b) The image of G in $PGL_2(\ell)$ is $\cong A_4, S_4$ or A_5.

$C := GL_2(\ell)/\mathbb{F}_\ell^\times$.

- no CM $\Rightarrow$ almost all G_ℓ are irreducible.

- So if $\rho_\ell \neq G_\ell$ for $\ell \gg 0$, then ✓.

- suppose for contradiction that $\rho_\ell \neq G_\ell$ for $\ell \gg 0$.

- So for ∞'ly many ℓ, G_ℓ is contained in either $C_s^+(\ell)$ or $C_{ns}^+(\ell)$, or $G_\ell/\mathbb{F}_\ell^\times \cong A_4$, S_4 or A_5.

Reductions

① Replace f with a finite extension for which E/f has semistable reduction, such as $f(E[12])$.

② $\ell >> 0$, so assume: (a) $\ell \geq 7$,

(b) ℓ unramified in f

(c) $\bar{\rho}_\ell$ is irreducible.

Inertia

- Let $w \mid \ell$ in $\overline{F}$. Let $v := w \cap F$.
- $I_w :=$ inertia group at w. $I_w \subseteq G_F$.
- $\rho_{E,\ell}(I_w) \subseteq G_\ell$.
- Corollaries 7, 9 and 13 describe the action of I_w on $E[\ell]$.

① E has good ordinary or multiplicative reduction at v: then

* up to conjugacy

$$\rho_{E,\lambda}(I_v) = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \in GL_2(\ell) \right\} \quad \underline{\text{or}} \quad \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in GL_2(\ell) \right\}$$

split semi-Cartan ↗ ↖ split Borel

② E has good supersingular reduction at v:

$$\rho_{E,\lambda}(I_v) = C_{ns}(\ell).$$

(Corollary 7.9; Prop. 13)

- We're assuming $\ell \nmid \#G_{ab}$, so split BorC

  case cannot happen.

- In any case above, $\rho_{\bar{k},\ell}(I_w)$ is <u>cyclic</u>

  of order $\ell-1$ or ℓ^2-1.

- $\therefore$ since $\ell+1 \geq 6$, $\overline{G} \not\cong A_4, S_4$ or A_5.

- Also, G_{ℓ^∞} is not contained in a split Cartan.

- So our classification leaves us in two cases:

  A. $G_\ell = Cns(\ell)$;

  B. G_ℓ is contained in the normalizer of a Cartan subgroup but not the Cartan subgroup itself.

- We will reduce to case A.

* $C(\ell) := C_s(\ell)$ or $C_{ns}(\ell)$

- Suppose we're in case B:

$$G_\ell \subseteq C^+(\ell), \qquad G_\ell \not\subseteq C(\ell).$$

- $C(\ell)$ has index 2 in $C^+(\ell)$. $\therefore$ the composition

$$\varepsilon_\ell : G_F \xrightarrow{\rho_{E,\ell}} C^+(\ell) \twoheadrightarrow C^+(\ell)/C(\ell) \cong \mathbb{Z}/2\mathbb{Z}$$

is a quadratic character.

Fact: the fixed field $F_\ell := \overline{F}^{\ker \varepsilon_\ell}$

is a quadratic unramified extension of F.

- Hermite's theorem: there are finitely many unramified quadratic extensions of F.
- $\Rightarrow$ finitely many F_ℓ.

- One has

$$\varepsilon_\ell(G_{F_\ell}) = 1$$

and so

$$\rho_{E,\lambda}(G_{F_\ell}) \subseteq \ell(\ell).$$

- Replace F with compositum of all F_ℓ.
(ramification doesn't change & still a # field).

- Assume that for $l \gg 0$ one has

$$G_l = GL_2(\mathbb{Z}_l).$$

So G_l is abelian, $\therefore$ simultaneously diagonalizable over $\overline{\mathbb{F}}_l$.

- Write $G_l \otimes \overline{\mathbb{F}}_l \sim \begin{bmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{bmatrix}$.

$\chi_i : Gal(F^{ab}/F) \to \overline{\mathbb{F}}_l^\times$, $i = 1, 2$.

Theorem 6: If (ρ_ℓ) is a system of semi-simple ℓ-adic rep'ns satisfying certain properties, one has that the system comes from a system $\{\psi_\ell\}$ associated to a $\mathbb{Q}$-rational rep'n

$$\psi_0 : G_m \to GL_d. \quad \leftarrow \text{abelian!}$$

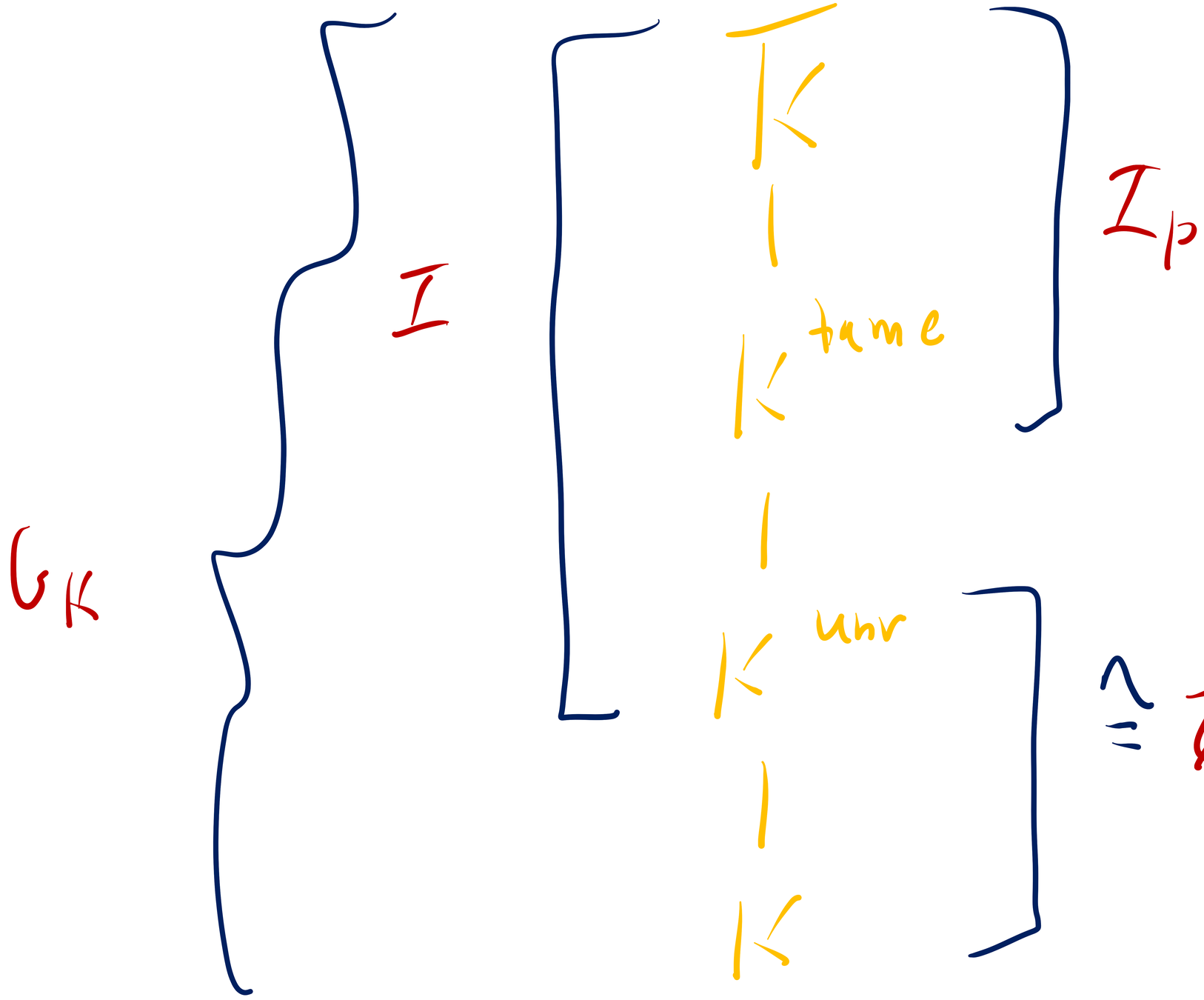
- Our system $(\rho_{k,\omega})$ is semi-simple and satisfies the properties of Theorem 6 above.

- i.e. each $\rho_{k,\omega}$ is abelian, so does <u>not</u> have finite index in $GL_2(\mathbb{Z}_\ell)$...

... so by the l-adic open image theorem, E has CM! Contradiction. ∎

Fundamental Characters

Let K be a local field.



- I := inertia group
- I_p := wild inertia group
  - pro-p-group
  - Sylow p-subgroup of I
- $I_{tame} := I/I_p \cong \hat{\mathbb{Z}}(1)(K^{tame}/K^{unr})$.

- Prop. 5: if k has $\mathrm{char}(k) = p > 0$ and V/k is a finite dim'l vector space, then any semisimple

$$\rho : G_K \to \mathrm{Aut}(V)$$

has $I_p \subseteq \ker \rho$.

- So our action of inertia $I \curvearrowright V$ descends to $I^{tame} \curvearrowright V$.
- ρ is semi-simple, so can diagonalize $\rho(I^{tame})$ over $\overline{\mathbb{F}_\ell}$.
- Characters of $\rho(I^{tame})$ are well understood ...

- Let $d \geq 1$, $p \nmid d$. Let π uniformize K^{unr}.
- $K^d := K^{unr}(\pi^{1/d})$.
- K^d / K^{unr} is totally tamely ramified.
- $\exists$ isomorphism θ_d,

$\theta_d : Gal(K^d/K^{unr}) \xrightarrow{\sim} \mu_d$. ← d-th roots of 1 in $\overline{K}$.

- θ_d is a "cyclotomic"-like character:

$$\sigma(\pi^{1/d}) = \theta_d(\sigma) \cdot \pi^{1/d}.$$

$\theta_{p^{n-1}}$ is the fundamental character of level n. (so are its conjugates $\theta_{p^{n-1}}^{p^i}$, $1 \le i \le n-1$.)

$$K^{tame} = \bigcup K^d, \text{ so get}$$

$$\theta : \Sigma_{tame} \xrightarrow{\sim} \varprojlim_{pXd} M_d.$$

Fact: The Θ_d parametrize

$\mathrm{Hom}_{cts}(I_{tame}, \bar{k}^\times)$.

Formal groups

* Let $R, \mathfrak{m}$ be valuation ring & max. ideal of K.

- Let $f(X, Y)$ be a formal group law:

so $f(X,Y) \in R[[X,Y]]$ and

$$f(X,Y) = X + Y + \sum_{i,j \geq 1} c_{ij} X^i Y^j$$

• "plug in" $\mathfrak{m}$ into f.g.l., get new group structure $(\mathfrak{m}, \oplus_F)$.

• Get "multiplication-by-p":

$$[p](t) = pT + \sum_{i \geq 2} a_i T^i \in R[[T]].$$

- Say F has finite height h if

  $a_i \in m$ for all $i < p^h$, and

  $a_{p^h} \notin m$.

- Fact: $V := \ker(\lceil p \rfloor : \bar{m} \to \bar{m})$ is an

  $\mathbb{F}_p$-vector space of dimension h.

- V is a G_K-module.

Prop: $\exists$ structure on V of a 1-b

$\overline{\mathbb{F}}_p$ - vector space such that

① $I_p \circlearrowright V$ is trivial,

② $I_{tame} \circlearrowright V$ by the fundamental

character θ_{p^n-1}.

- So natural action $\rho : G_F \to \mathrm{Aut}(V) \cong \mathbb{F}_{p^h}^\times$ is just $\rho = \theta_{p^h-1}$.

- $I_{\mathrm{tame}} \curvearrowright V \cong I_{\mathrm{tame}} \curvearrowright V \otimes \bar{k}$.

Corollary 6: $I_{\mathrm{tame}} \curvearrowright V \otimes \bar{k}$ is diagonalizable, and the action is given by the h fundamental characters $\theta_{p^h-1}^{p^i}$ at level h.

Reduction Types

& Inertia

Recap

- K complete disc. valued field, $\mathrm{char}\, K = 0$.
  Residue field k of pos. char. $p > 0$.
- E/K an ell. curve
- $G_K \curvearrowright E[p] \xrightarrow{\sim} \rho_{E,p} : G_K \to \mathrm{Gl}_2(p)$.
- $\det(\rho_{E,p}) = \chi_p$, mod-$p$ cyclo. char.

- We know

$$\det \rho_{k,p} = \chi_p$$

and as noted earlier (Prop. 9)

$$\chi_p|_{I_{tame}} = \theta_{p-1}^{e}$$

$e := e(K|\mathbb{Q}_p)$.

We can say more about I_w, $w|p$

in $\overline{K}$, by the reduction of E mod v,

where $v := w \cap K$ ---

Good ordinary reduction (height of $\hat{E}$ is 1):

- $\tilde{E} = E \bmod v$ is an elliptic curve.

- $E[p]$ is a 1-D vector space $/\mathbb{F}_p$.

- Short exact sequence

$$0 \to X_p \to E[p] \xrightarrow{\text{red.}} \tilde{E}[p] \to 0.$$

$E[p]$: rk 2 $/\mathbb{F}_p$

$\tilde{E}[p]$: rk Δ $/\mathbb{F}_p$

- $X_p := \ker\left(\mathrm{red} : E[p] \to \tilde{E}[p]\right)$

  - G_K-stable submodule.

  - I_p acts trivially on X_p and $\tilde{E}[p]$.

  $\therefore$ I tame acts on X_p and $\tilde{E}[p]$...

Proposition 12:

$$\rho_{E,p}(I_{tame}) = \left\{ \begin{bmatrix} \omega_{p-1}^{e} & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

Corollary 7: Two cases:

(A) I_p of $E[p]$ trivially

$\rightsquigarrow$ $\rho_{E,p}(I) = \left\langle \begin{bmatrix} \sigma_{p-1}^{e} & 0 \\ 0 & 1 \end{bmatrix} \right\rangle$.

↙ cyclic, order $\frac{p-1}{(p-1,e)}$

(B) I_p $\not\circlearrowleft$ $E[p]$ non-trivially (i.e. contains order p elt)

$\rightsquigarrow$ $\rho_{E,p}(I) = \left\langle \begin{bmatrix} \sigma_{p-1}^{e} & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{F}_p \right\rangle$.

↑ cyclic, order $\frac{p(p-1)}{(p-1,e)}$

good supersingular reduction (height of $\hat{E}$ is 2).

Proposition 13:

$\rho_{E,p}(I)$ equals $Cns(p)^e$, or

I_p of $E[p]$ nontrivially and $\rho_{E,p}(I)$ is Borel.

* (see Á. Lozano-Robledo's "On the field of definition of p-torsion points ...") ♭

Bad multiplicative reduction

(see Prop. 14)

- We've already shown via Tate curves that

$$\rho_{E,p}(G_K) \subseteq \left\{ \begin{bmatrix} * & * \\ & 1 \end{bmatrix} \right\}.$$

In fact, we get an identical situation to the case of good ordinary reduction:

Corollary 9

(a) The two characters for the semisimplification of I_{tame} on $E[p]$ are θ_{p-1}^e and 1.

(b) I_p on $E[p]$ trivially

$\rightsquigarrow \rho_{E,p}(I) = \langle \begin{bmatrix} \theta_{p-1}^e & 0 \\ 0 & 1 \end{bmatrix} \rangle$ cyclic, order $\frac{p-1}{(p-1,e)}$

(c) I_p on $E[p]$ nontrivially

$\rightsquigarrow \rho_{E,p}(I) = \langle \begin{bmatrix} \theta_{p-1}^e & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{F}_p \rangle$ order $\frac{p(p-1)}{(p-1,e)}$

Thank you!