Entanglement of Galois Representations of CM Elliptic Curves

(following Campagna & Pengo 2020, v2 2006.00883)

CRAAG II

Tyler Genao

7/16/2021

Q.E.D

1. Review non-CM case (Serre)
2. Recount the theory of CM
3. Learn about entanglement in division fields of CM elliptic curves, and sketch a proof
4. If time permits, share more results.

- The adelic open image theorem -

* Throughout, let F be a # field *

- Let $G_F := \mathrm{Gal}(\bar{F}/F)$ be the absolute Galois group of F.

- Given an elliptic curve E/F, G_F acts on E in a natural way:

- $\forall P \in E$, $\forall \sigma \in G_{\mathbb{F}}$, if $P = (x, y)$ then

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

- For integer $N \geq 1$, $G_{\mathbb{F}}$ also takes N-torsion to N-torsion. This gives us a group action of $G_{\mathbb{F}}$ on $E[N]$:

$$\rho_{E,N}: G_F \to \mathrm{Aut}(E[N]) \cong GL_2(\mathbb{Z}/N\mathbb{Z}).$$

This is called the mod-N Galois representation of E/F.

- The kernel of $\rho_{E,N}$ is of the form $G_{\overline{F}/F(E[N])}$ where $F(E[N])$ denotes the N-division field.

Some properties of $F(E[N])$:

- Equal to $F(x, y \mid (x,y) \in E[N])$
- Finite Galois extension of F
- $[F(E[N]) : F] = \#\rho_{E,N}(G_F)$.

Example of division fields

$$E_{/\mathbb{Q}}: y^2 = x^3 + x.$$

$$E[2] = \{ O, \ (0,0), \ (\pm i, 0) \}$$

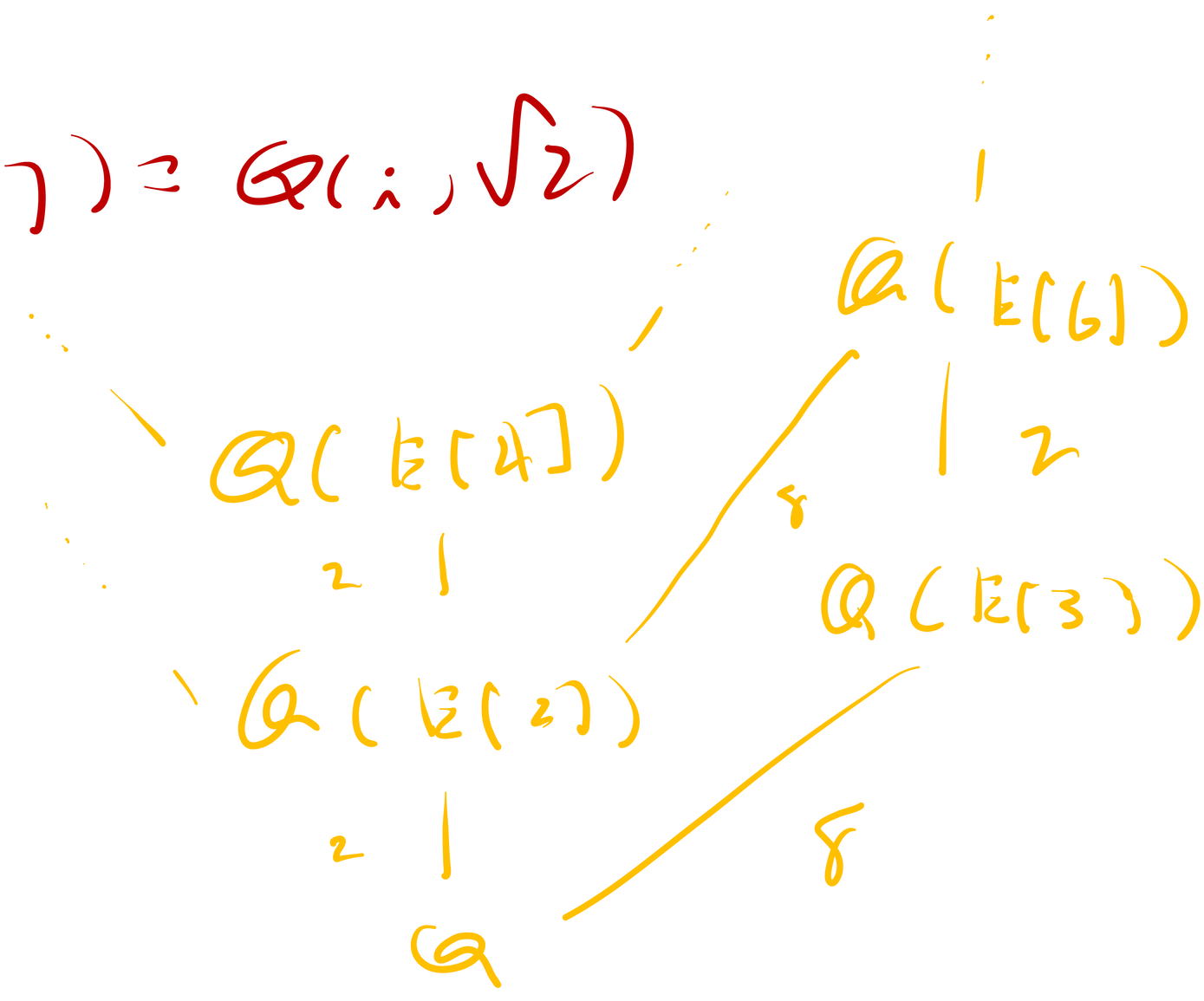
$$E[4] = E[2] \cup \{ (1, \pm\sqrt{2}), (1, \pm i\sqrt{2}),$$

$$\left(\alpha, \pm\sqrt{\alpha^3+\alpha}\right), \left(\alpha, \pm\sqrt{\alpha^{-3}+\alpha^{-1}}\right),$$

$$\left(\alpha, \pm i\sqrt{\alpha^3+\alpha}\right), \left(\alpha, \pm i\sqrt{\alpha^{-3}+\alpha^{-1}}\right) \}$$

... where $\alpha^4 + 6\alpha^2 + 1 = 0$. (e.g., $\alpha = \sqrt{-3+2\sqrt{2}}$.)

- $\mathbb{Q}(E[2]) = \mathbb{Q}(i)$
- $\mathbb{Q}(E[4]) = \mathbb{Q}(i, \sqrt{2})$



For prime $p \in \mathbb{Z}^+$, the action of G_F

on the p-adic Tate module, $T_p(E) := \varprojlim_{n \geq 1} E[p^n]$

gives <u>p-adic representation</u>,

$$\rho_{E,p^\infty} : G_F \to \mathrm{Aut}(T_p(E))$$

$$\cong GL_2(\mathbb{Z}_p)$$

↑ p-adic integers

Finally, the action of G_F on $T(E) := \varprojlim_p T_p(E)$

gives <u>adelic</u> representation,

$$\hat{\rho}_E : G_F \to \mathrm{Aut}(T(E))$$

$$\cong \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

$\hat{\mathbb{Z}}$ profinite completion

- Attached to an elliptic curve E/F is its endomorphism ring

$$\mathrm{End}(E) := \{ \text{isogenies } \phi : E \to E \}.$$

- We always have $\mathbb{Z} \subseteq \mathrm{End}(E)$. But they might not be equal...

... If $\mathbb{Z} \neq \mathrm{End}(E)$, then $\mathrm{End}(E)$ is (isomorphic to) an order in an imaginary quadratic field.

• Then say that E has complex multiplication, or CM.

Ex: $E_i : y^2 = x^3 - x$ has an extra endomorph.:

$[i] : E \to E$, $[i](x,y) := (-x, iy)$. "multiplication by i."

1972, Serre's "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques"

If E/F has no CM, then $\hat{\rho}_E(G_F)$ has finite index in $GL_2(\hat{\mathbb{Z}})$.

(see e.g. my SeZoom slides)

Alternatively stated,

"If E/F does not have CM, then all but finitely many ℓ-division fields are as large as possible over prime $\ell \in \mathbb{Z}^+$:

$$[F(E[\ell]):F] = \#GL_2(\mathbb{Z}/\ell\mathbb{Z}).$$"

- What about $F(E[\lambda])$ when E has CM?
- Fact: When E has CM, for all $N \geq 1$

$$\rho_{E,N} : G_F \to GL_2(\mathbb{Z}/N\mathbb{Z})$$

is abelian — so never surjects onto

$GL_2(\mathbb{Z}/N\mathbb{Z})$ for $N > 1$!

Galois representations of CM elliptic curves

- Let $E/\mathbb{C}$ have <u>complex multiplication</u>.
- $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $K/\mathbb{Q}$ (a rank two $\mathbb{Z}$-submodule of K with 1.)
- "E has CM by $\mathcal{O}$, i.e., is $\mathcal{O}$-CM."
- <u>Ex:</u> $E/\mathbb{Q}: y^2 = x^3 - x$ has CM by $\mathbb{Z}[i]$.

- Claim: $\exists$ "normalized" isomorphism

$$[\cdot] : \mathcal{O} \xrightarrow{\sim} \mathrm{End}(E)$$

- E is an $\mathcal{O}$-module by $[\cdot]$: $\forall \alpha \in \mathcal{O}$

$\forall P \in E$,

$$\alpha \cdot P := [\alpha](P).$$

- For an ideal $I \subseteq \mathcal{O}$, we can define I-torsion

$$E[I] := \{ P \in E : \forall \alpha \in I \quad \alpha \cdot P = \mathcal{O} \}.$$

* Assume that $K \subseteq F$. ← "rationally defined" cm. *

- The action of $\mathcal{O}$ on E commutes with the action of G_F on E:

$$\alpha \cdot (p^\sigma) = (\alpha \cdot p)^\sigma.$$

In other words, E is an $\mathcal{O}[G_F]$-module.

So for an ideal $I \subseteq \mathcal{O}$, we have the

mod-I Galois representation

$$\rho_{E,I} : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathcal{O}}(E[I])$$

Fact: if $I \subseteq \mathcal{O}$ is invertible, then

$$E[I] \cong_{\mathcal{O}} \mathcal{O}/I.$$

So $\mathrm{Aut}_{\mathcal{O}}(E[I]) \cong GL_1(\mathcal{O}/I) = (\mathcal{O}/I)^\times$, (unit group)

and our mod-I representation becomes

$$\rho_{E,I} : G_F \to (\mathcal{O}/I)^\times.$$

- Special case: $I = N\mathcal{O}$. Then

$$\rho_{E,N\mathcal{O}} = \rho_{E,N}.$$

So $\forall N \in \mathbb{Z}^+$, the image of the mod-$N$ Repn

$$\rho_{E,N} : G_F \to GL_2(\mathbb{Z}/N\mathbb{Z})$$

is contained in $(\mathbb{Z}/N\mathbb{Z})^\times \leq GL_2(\mathbb{Z}/N\mathbb{Z})$.

So it's <u>always abelian</u>, and thus never surjects onto $GL_2(\mathbb{Z}/N\mathbb{Z})$ if $N > 1$.

Entanglements

- Goal: understand the image $\hat{\rho}_E(G_F)$ as much as possible in the CM case.

- note that

$$\hat{\rho}_E(G_F) \cong \mathrm{Gal}(F(E[\mathrm{tors}])/F)$$

Can we "factorize" this by the p-adic representations?

We are guaranteed that the natural map

$$\mathrm{Gal}(F(E[\mathrm{lcm}(S)])/F) \to \prod_{p} \mathrm{Gal}(F(E[p^\infty])/F)$$

is injective, but not necessarily surjective -

analogous to fields being linearly disjoint.

Recall:

- Say extensions F_1/F, F_2/F are F-linearly disjoint if $F_1 \cap F_2 = F$.

- If also F_1, F_2 are Galois over F, then

$$Gal(F_1 \cdot F_2/F) \xrightarrow{\sim} Gal(F_1/F) \times Gal(F_2/F).$$

- A family $\{F_i\}_I$ of field extensions of F is linearly disjoint over F if the natural map

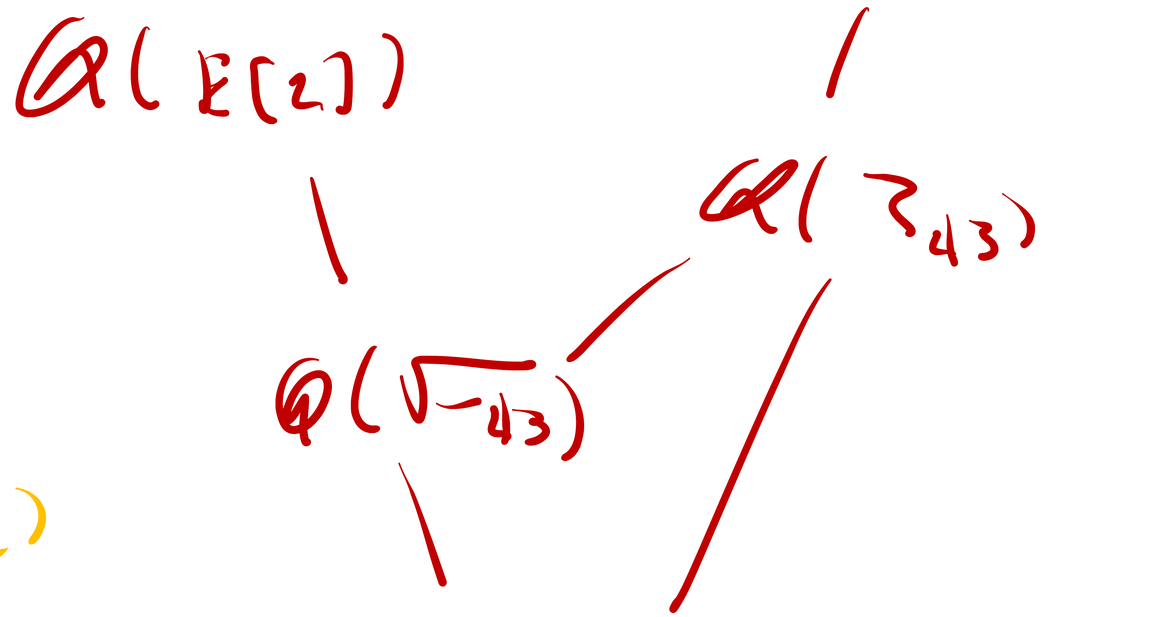
$$\mathrm{Gal}(\textstyle\prod_I F_i / F) \hookrightarrow \prod_I \mathrm{Gal}(F_i / F)$$

is surjective.

- If $\{F_i\}_I$ is not linearly disjoint over F, we say that it is <u>entangled</u> over F.

Entanglement Example:

$E: y^2+y = x^3+x^2$.



- $\rho_{E,2^\infty}: G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_2)$

and $\rho_{E,43^\infty}: G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_{43})$

surject, but $\rho_{E,86}: G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/86\mathbb{Z})$

does not. (see Álvaro's $\hat{\rho}_E(G_{\mathbb{Q}})$ talk)

Theorem (Campagna + Pengo, 2020)

Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Let F/K be a # field, and E/F an $\mathcal{O}$-CM elliptic curve. Define

$$b_E := f_{\mathcal{O}} \cdot \Delta_F \cdot |\mathcal{O}_F / \mathfrak{f}_E|$$ where

① $f_{\mathcal{O}}$ is the <u>conductor</u> of $\mathcal{O}$, i.e. $f_{\mathcal{O}} := [\mathcal{O}_K : \mathcal{O}]$.

② $\Delta_F := \Delta_{F/\mathbb{Q}}$ the <u>absolute discriminant</u> of F.

③ $\mathfrak{f}_E$ the <u>conductor ideal</u> of E over F.

... Let S be the set of prime divisors of b_E.

Let $f(E[s^\infty]) := \prod_{p \in S} f(E[p^\infty])$. Then

$$\{ f(E[s^\infty]) \} \cup \{ f(E[p^\infty]) \}_{p \notin S}$$

is f-linearly disjoint, i.e. the natural map

$$Gal(F(E[tors])/F) \hookrightarrow Gal(F_{S^\infty}/F) \times \prod_{p \notin S} Gal(F_{p^\infty}/F)$$

$$(L \mapsto \hat{\rho}_E(G_F))$$

is an isomorphism.

* we write $F_{p^\infty} := F(E[p^\infty])$, etc.

- To prove this, we need to show that the family $\{F_{s-s}\} \cup \{F_{p^n}\}_{p \neq s}$ is $\mathbb{F}$-linearly disjoint.

- Equivalent to showing: $\forall p \neq s$, $\forall n \in \mathbb{Z}^+$, $\forall m \in \mathbb{Z}^+$ coprime to p, one has

$$F_{p^n} \cap F_m = \mathbb{F}.$$

$F(E[p^n])$ $\supset$ $\subset$ $F(E[m])$

The division fields of CM elliptic curves are exceptionally behaved:

* prop. 3.2: For ideals $\mathfrak{z} \subseteq \mathcal{O}$ coprime to $f_{\mathcal{O}}$, i.e. invertible, one has that $f_{\mathfrak{z}}/f$ is unramified at primes of $f_{\mathfrak{z}}$ not dividing $I(\mathcal{O}_F \cdot \mathcal{O}_E)$.

**Prop. 3.3: Let E/F be θ-CM, $\theta \subseteq F$.

Let $\mathfrak{p} \subseteq \theta$ be a prime ideal coprime to

$b_E \theta$. Then for $F_{\mathfrak{p}^n} := F(E[\mathfrak{p}^n])$,

(1) $F_{\mathfrak{p}^n}/F$ is totally ramified above $\mathfrak{p}^n$,

(2) $F_{\mathfrak{p}^n}$ is "as large as possible":

the mod-$\mathfrak{p}^n$ representation surjects onto $(\theta/\mathfrak{p}^n)^\times$.

Then the proof of the main theorem is as follows: if

$$M \subseteq F_{p^n} \cap F_m$$

is a subextension $\neq F$, then using Prop. 3.3, there is a prime in M ramified over p. But since $M \subseteq F_m$, Néron-Ogg-Shafarevich (or Prop. 3.2) says M is unramified over p. $\rightarrow\leftarrow$

A comparison:

(1) $E/\mathbb{Q}$ non-CM: the ℓ-division fields

$$\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \cong GL_2(\mathbb{Z}/\ell\mathbb{Z})$$

for sufficiently large prime ℓ.

(2) $E/\mathbb{Q}$ CM: the p-division fields

$$\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \hookrightarrow GL_1(\mathcal{O}/p\mathcal{O})$$

for prime ideals $p \subseteq \mathcal{O}$ coprime to $b_E\mathcal{O}$.

Elliptic curves over local fields

Notation

- L local field
- $\mathfrak{m}$ maximal ideal
- k residue field of characteristic $p > 0$
- v its valuation.

Theorem (Silverman I, Ch. 7, Prop. 2.1, 3.1)

For an elliptic curve E/L with good reduction, $\exists$ short exact sequence from reduction,

$$* \quad 0 \to \hat{E}(m) \to E(L) \xrightarrow{\text{red.}} \tilde{E}(k) \to 0 \quad *$$

where $\hat{E}(m)(\text{tors}) = \hat{E}[p^\infty]$. Thus, for $N \in \mathbb{Z}^+$ coprime to p, we have an injection $\text{red}: E(L)[N] \hookrightarrow \tilde{E}(k)$.

- Digression -

- Let E/k be an elliptic curve over a finite field of characteristic $p > 0$.
- Then $E[p]$ is a rank ≤ 1 $\mathbb{F}_p$-module.

  Say E is

  (1) supersingular if rank zero

  (2) ordinary if rank one.

Returning to...

Lemma 2.1: Let E/L have good reduction.

Define $h := \begin{cases} 1 & \text{if } \tilde{E}/k \text{ is ordinary} \\ 2 & \text{if } \tilde{E}/k \text{ is supersingular.} \end{cases}$

Then for all $x \in \hat{E}(m)$ of order p^n,

one has $$V(x) \leq \frac{V(p)}{p^{h(n-1)} \cdot (p^h - 1)}.$$

Theorem 12, section 13.4 of "Elliptic Functions" Lang

For F a # field and E/F an $\mathcal{O}$-CM elliptic curve, let $\mathcal{P} \subseteq F$ be a prime of good reduction for E. Let $p \in \mathbb{Z}^+$ lie below $\mathcal{P}$. Then ...

E has supersingular reduction at p iff p is inert or ramified in $K = \mathbb{Q} \otimes \mathbb{Q}$. Otherwise, $\tilde{E}$ is ordinary.

Proof sketch

**Prop. 3.3: Let E/F be θ-CM, $\theta \subseteq F$.

Let $\mathfrak{p} \subseteq \theta$ be a prime ideal coprime to

$b_E \theta$. Then for $F_{\mathfrak{p}^n} := F(E[\mathfrak{p}^n])$,

(1) $F_{\mathfrak{p}^n}/F$ is totally ramified above $\mathfrak{p}^n$,

(2) $F_{\mathfrak{p}^n}$ is "as large as possible":

the mod-$\mathfrak{p}^n$ representation surjects onto $(\theta/\mathfrak{p}^n)^\times$.

Proof

The proof of ① will immediately imply ②, since we'll show the following:

for all primes $\mathfrak{p} \subseteq \mathcal{O}_{\mathbb{P}^n}$ above p,

$$e(\mathfrak{p} \mid p\mathcal{O}_F) = \#(\mathcal{O}/\mathfrak{p}^n\mathcal{O})^\times.$$

(recall that $[F_{\mathbb{P}^n} : F] \mid \#(\mathcal{O}/\mathfrak{p}^n)^\times$.)

- So fix $\mathfrak{p} \subseteq \mathfrak{p}^n$ above p.
- Since $p \lambda \in \mathcal{O}_L$ we get
  - p invertible in $\mathcal{O}_L$
  - p unramified in L and thus $\mathcal{O}_L$
  - E has good reduction at $\mathfrak{p}$.

We have two cases of reduction to

consider:

① ordinary

② supersingular,

which correspond to when p is split

or inert in K, respectively.

- We'll look at the proof in the inert case.
- Thus $p\mathcal{O} = \mathfrak{p}$, and so our representation

$$\rho_{E,p^n} : \mathrm{Gal}(F_{p^n}/F) \hookrightarrow (\mathcal{O}_K/p\mathcal{O}_K)^\times$$

implies

$$[F_{p^n} : F] \mid p^{2(n-1)} \cdot (p^2-1).$$

* If $\Sigma \subseteq \mathcal{O}$ invertibles then $\mathcal{O}_K/\mathbb{Z} \cong \mathcal{O}_K/\Sigma$.

- Have fixed $\mathfrak{p} \subseteq \mathbb{F}_{p^n}$ above p.

- E has supersingular reduction at $\mathfrak{P}$, so

$$\widetilde{E}(k_{\mathfrak{p}})[p^\infty] = \{\mathcal{O}\}.$$

(here, $k_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$.)

- Thus, taking p-primary torsion of SES

$$0 \to \hat{E}(\mathfrak{m}_{\mathfrak{p}}) \to E((\mathbb{F}_{p^n})_{\mathfrak{p}}) \to \widetilde{E}(k_{\mathfrak{p}}) \to 0 \dots$$

↑ completion at $\mathfrak{p}$

... we get

$$\hat{E}(M_p)[p^\infty] = E((f_{p^n})_p)[p^\infty].$$

- From containment $F_{p^n} \subseteq (f_{p^n})_p$, we see that $\hat{E}(M_p)$ has an element x of order p^n.
- So Lemma 2.1 implies

$$v(x) \leq \frac{v(p)}{p^{h(n-1)} \cdot (p^h - 1)}.$$

- supersingular $\Rightarrow$ $h = 2$. since $v(p) = e(\mathcal{P}|_p)$,

we get

$$p^{2(n-1)} \cdot (p^2 - 1) \leq e(\mathcal{P}|_p),$$

but already

$$e(\mathcal{P}|_p) \leq [F_{p^n} : F] \leq \#(\mathcal{O}_K / p^n \mathcal{O}_K)^\times$$
$$= p^{2(n-1)}(p^2 - 1).$$

$\therefore$ $e(\mathfrak{P}|p) = \#(\mathcal{O}/\mathfrak{p}^n\mathcal{O})^\times = [f_{\mathfrak{p}^n} : \mathbb{F}]$,

and so $\mathfrak{P}$ is totally ramified over $\mathbb{F}$

& $\ell_{E,\mathfrak{p}^n}$ surjects onto $(\mathcal{O}/\mathfrak{p}^n\mathcal{O})^\times$.

✓

Further results

Thm 1.1: given θ- cm E/F with

$F \supseteq K := \theta \otimes \alpha$, one has

$$\mathrm{Gal}(F(E[\mathfrak{p}^\infty])/F) \xrightarrow{\sim} \mathrm{Gal}(F(E[\mathfrak{p}^s])/F)$$

$$\| \qquad\qquad\qquad\qquad \times$$

$$\hat{\rho}_E(G_F) \qquad\qquad \prod_{\mathfrak{p}^{\chi s}} \mathrm{Gal}(F(E[\mathfrak{p}^s])/F)$$

where $s := \mathrm{support}(f_\theta \cdot \Delta_F \cdot |\theta/f_E|)$.

Question: what is the minimal $T \subseteq s$

such that

$$\{f(k[T^\infty])\} \cup \{f(k[x_p^{\pm\infty}])\}_{p \notin T}$$

is F-linearly disjoint?

- For an order $\mathcal{O}$ in imag. quad. K, let

$K_{\mathcal{O}}$ be the ring class field of $\mathcal{O}$.

- For any $\mathcal{O}$-CM ell. curve E, and has

$$K_{\mathcal{O}} = K(j(E)).$$

Analogous to the Hilbert class field $K(1)$ of K being generated by $j(E)$ for $\mathcal{O}_K$-CM E.

Recap:

- For E/F, the action of G_F on $E[tors]$ gives

$$\hat{\rho}_E : G_F \to GL_{\hat{\mathbb{Z}}}(\hat{\mathbb{Z}}).$$

- If E has $\mathcal{O}$-CM, then each $E[N]$ is a free rank one $\mathcal{O}/N\mathcal{O}$-module. Thus

$$\hat{\rho}_E : G_F \to GL_1(\hat{\mathcal{O}}) \cong \hat{\mathcal{O}}^\times.$$

Corollary 4.6 :

For θ - cm E/K_θ,

$$[\hat{\theta}^\times : \hat{\rho}_E(G_{K_\theta})] = \begin{cases} \#\theta^\times & \text{if } K_\theta(E[\text{tors}])/K \\ & \text{is abelian} \\ 1 & \text{else.} \end{cases}$$

Since we always have

max. abelian extension $\Rightarrow K^{ab} \subseteq K_0([E[tors]])$

we have that if $K_0([E[tors]])/K$ is nonabelian then the adelic index is 1, and thus no entanglement occurs.

Last question: When is

$K_\theta(\text{tors})/K$

(non) abelian?

Ex

If the class number $h_\theta = 1$, then

$$K_\theta = K.$$

Since $K_\theta(E(\mathfrak{f}))/K_\theta$ is always abelian,

we deduce that $\hat{\rho}_E : G_K \to \hat{\mathcal{O}}^\times$ is not

surjective if $\mathcal{O}$ is one of the 13 imag.

quad. orders of class number one.

Theorem 4.8: For any order $\mathcal{O}$ and $\mathcal{O}$-CM j-invariant j, there are $\mathcal{O}'$-ly many non-isomorphic E/K_0 with $j(E)=j$ and

$$K^{ab} = K_0(E[\text{tors}]),$$

and thus $[\hat{\theta}^\times : \hat{\rho}_E(G_{K_0})] = \#\mathcal{O}^\times$.

Theorem 4.9: if $h_\theta > 1$, then

for any θ-CM j-invariant j,

there are only many non-isomorphic

E/K_θ with $j(E) = j$ and

$$K^{ab} \subsetneq K_\theta(E[tors])$$

and thus $[\hat{\theta}^\times : \hat{\rho}_E(b_{K_\theta})] = 1$.

Thank You!