Galois action on pro-p fundamental groups of punctured CM elliptic curves

VaNTAGe

Shun Ishii (Keio university)

May 20, 2025

Introduction

Notation

- K : number field.
- $\bar{K}$: algebraic closure of K. We fix an embedding $\bar{K} \hookrightarrow \mathbb{C}$.
- X : (smooth) curve over K. We mostly consider the case where X : **hyperbolic**,

  i.e. the Riemann surface $X(\mathbb{C})$ is uniformized by the upper half plane $\mathbb{H}$.

  $\Leftrightarrow$ the top. fundamental group $\pi_1^{\mathrm{top}}(X(\mathbb{C}))$ is **not** abelian.

Example.

X	$\mathbb{P}^1 - \{0, 1, \infty\}$	$E - O$	proj. curve of genus $g \geq 2$
$\pi_1^{\mathrm{top}}(X(\mathbb{C}))$	F_2: free group of rank 2	F_2	S_g: surface group

- $X_{\bar{K}} := X \times_K \bar{K}$.
- $\pi_1(X)$: étale fundamental group of X, and

  $\pi_1(X_{\bar{K}})$: **geometric** étale fundamental group of X.

Outer Galois representation

Fact.

1. Descent+GAGA:

$$\pi_1(X_{\bar{K}}) \cong \pi_1(X_{\mathbb{C}}) \cong \widehat{\pi_1^{\mathrm{top}}(X(\mathbb{C}))} \quad \text{(prof. completion of } \pi_1^{\mathrm{top}}\text{)}.$$

2. Etale homotopy exact sequence: $X_{\bar{K}} \to X \to \mathrm{Spec}(K)$ induces

$$1 \to \pi_1(X_{\bar{K}}) \to \pi_1(X) \to G_K := \mathrm{Gal}(\bar{K}/K) \to 1.$$

Let $\pi_1(X_{\bar{K}})^{(p)}$ be the maximal pro-p quotient of $\pi_1(X_{\bar{K}})$.

Definition (outer Galois representation).

By the homotopy exact sequence, we obtain

$$\rho_X \colon G_K \to \mathrm{Out}(\pi_1(X_{\bar{K}})) := \mathrm{Aut}(\pi_1(X_{\bar{K}}))/\mathrm{Inn}(\pi_1(X_{\bar{K}}))$$

called **the outer Galois representation** associated to X, and

$$\rho_{X,p} \colon G_K \to \mathrm{Out}(\pi_1(X_{\bar{K}})^{(p)})$$

the pro-p outer Galois representation associated to X.

Outer Galois representation

■ When X is **not** hyperbolic, then ρ_X is as follows:

X	$\mathbb{P}^1$ or $\mathbb{A}^1$	$\mathbb{G}_m$	E: elliptic curve
$\pi_1(X_{\bar{K}})$	trivial	$\widehat{\mathbb{Z}}$	$\prod_p T_p(E)$
ρ_X	trivial	cyclotomic character	Gal. rep. associated to $\prod_p T_p(E)$

■ When X is hyperbolic, ρ_X is extensively studied in the context of anabelian geometry.

For example, we have:

Theorem (Belyi-Voevodsky-Matsumoto-Hoshi-Mochizuki)

If X is hyperbolic, then ρ_X is **injective**.

This theorem is proved when $X = \mathbb{P}^1 - \{0, 1, \infty\}$ by Belyi, $X = E - O$ by Voevodsky, X: affine by Matsumoto and finally X: general by Hoshi-Mochizuki.

Pro-p outer Galois representation

On the other hand, we have some arithmetic constraints on $\rho_{X,p}$:

Lemma.

1. $\mathrm{Out}(\pi_1(X_{\bar{K}})^{(p)})$ has an open pro-p subgroup.

   Hence so is $\mathrm{im}(\rho_{X,p})$ (and $\ker(\rho_{X,p})$ is huge!).

2. If v is a place of K above $\ell \neq p$ at which X has good reduction, then $\rho_{X,p}$ is unramified at v, i.e. the image of an inertia subgroup at v is trivial.

Sketch.

(1)

$$\ker\left[\mathrm{Out}(\pi_1(X_{\bar{K}})^{(p)}) \to \mathrm{Aut}(\pi_1(X_{\bar{K}})^{\mathrm{ab}} \otimes \mathbb{F}_p)\right]$$

is a pro-p open subgroup. (2) follows from the specialization isomorphism for π_1.

Are there more constraints? or, can we determine the field $\bar{K}^{\ker(\rho_{X,p})}$ completely?

Previous result

Sharifi solves this question for $X = \mathbb{P}^1_{\mathbb{Q}} - \{0, 1, \infty\}$ under certain assumptions. Recall

$$\rho_{\mathbb{P}^1 - \{0,1,\infty\},p} \colon G_{\mathbb{Q}} \to \mathrm{Out}(\pi_1(\mathbb{P}^1_{\bar{\mathbb{Q}}} - \{0, 1, \infty\})^{(p)}).$$

In this case, let us write

- 山 $:= \bar{\mathbb{Q}}^{\ker(\rho_{\mathbb{P}^1 - \{0,1,\infty\},p})}$, and
- 天 $:=$ the **maximal** pro-p extension of $\mathbb{Q}(\mu_p)$ unramified outside p.

We have 山 $\subset$ 天 (cf. previous lemma).

Theorem (Sharifi, Hain-Matsumoto and Brown).

1. (Sharifi) Assume:
   - $p > 2$ is regular, and
   - Deligne's conjecture (the Deligne-Ihara conjecture) holds for p.

   Then we have 山 $=$ 天.
2. (Hain-Matsumoto and Brown) Deligne's conjecture holds for every p.

Main result: Setting

Main result.

Analogues of Sharifi's result for once-punctured CM elliptic curves.

More precisely, let

- $p \geq 5$: prime.
- K: imaginary quadratic field of class number one,
- E/K: elliptic curve with $O_K = \mathrm{End}_K(E)$,
- $X := E - O$: associated once-punctured elliptic curve,
- $\rho_{X,p}\colon G_K \to \mathrm{Out}(\pi_1(X_{\bar{K}})^{(p)})$: pro-$p$ outer Galois representation,
- $\rho_{E,p}\colon G_K \to \mathrm{Out}(\pi_1(E_{\bar{K}})^{(p)}) = \mathrm{GL}(T_p(E))$: p-adic Galois representation of E.

The main result is based on the following consequence of CM-theory:

We have

$$\bar{K}^{\ker(\rho_{E,p})} = K(E[p]) \cdot K(p^{\infty}),$$

where $K(p^{\infty})$ denotes the ray class field of K of conductor p^{∞}.

Main result: Statement

Theorem (I.).

We follow the notation from the previous slide. Assume:

1. The prime $p > 3$ splits in K as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$,
2. the class number of the ray class field $K(p)$ of conductor p does not divide p,
3. there is a unique prime of $K(\mathfrak{p}^2)$ above $\bar{\mathfrak{p}}$, and
4. an analogue of Deligne's conjecture holds.

Then we have

$$\bar{K}^{\ker(\rho_{X,p})} = K(E[p]) \cdot (\text{the maximal pro-}p\text{ extension of } K(p) \text{ unramified outside } p).$$

This gives a non-abelian variant of the classical equality $\bar{K}^{\ker(\rho_{E,p})} = K(E[p]) \cdot K(p^\infty)$.

note: $\subset$ always holds.

1. $p > 3$ splits in K as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$,
2. the class number $K(p)$ does not divide p,
3. there is a unique prime of $K(\mathfrak{p}^2)$ above $\bar{\mathfrak{p}}$, and
4. an analogue of Deligne's conjecture holds.

$\Rightarrow \bar{K}^{\ker(\rho_{X,p})} = K(E[p]) \cdot$ (the max. pro-p extension of $K(p)$ unramified outside p) (†)

Remark.

a. Examples of (K, p) satisfying (1)-(3):

K	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}(\sqrt{-19})$
p	$5, 13, 17$	7	7

b. We expect that (†) still holds when p does not split in K.

Example: (†) holds when $(K, p) = (\mathbb{Q}(\sqrt{-3}), 3)$ **without assuming (1)-(4)**.

c. Condition (3) $\Leftrightarrow$ If we write $\bar{\mathfrak{p}} = (\bar{\pi})$, then $\bar{\pi}$ generates $(O_K/\mathfrak{p}^2)^\times / O_K^\times$.

Example: When $K = \mathbb{Q}(\sqrt{-1})$, then

$$\frac{|\{p < 10^6 \mid p \text{ satisfies (1) and (3)}\}|}{|\{p < 10^6 \mid p \text{ satisfies (1)}\}|} = \frac{13705}{39175} = 0.3498\ldots$$

Deligne-Ihara's conjecture and its variant

Weight filtration on Galois groups

Write $\Pi := \pi_1(\mathbb{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\})^{(p)}$ and let $\{\Pi(m)\}_{m>0}$ be its descending central series:

$$\Pi(1) := \Pi \supset \Pi(2) := [\Pi(1), \Pi(1)] \supset \cdots \supset \Pi(m+1) := [\Pi, \Pi(m)] \supset \cdots .$$

Definition-Lemma.

1. We define **the weight filtration** $\{F^m G_{\mathbb{Q}}\}_{m>0}$ on $G_{\mathbb{Q}}$ by

$$F^m G_{\mathbb{Q}} := \ker\left[G_{\mathbb{Q}} \xrightarrow{\rho_{\mathbb{P}^1 - \{0,1,\infty\},p}} \mathrm{Out}(\Pi) \to \mathrm{Out}(\Pi/\Pi(m+1))\right].$$

   This is descending, central and $\bigcap_{m>0} F^m G_{\mathbb{Q}} = \ker(\rho_{\mathbb{P}^1 - \{0,1,\infty\},p})$.

2. Let

$$gr^m G_{\mathbb{Q}} := F^m G_{\mathbb{Q}} / F^{m+1} G_{\mathbb{Q}} \quad \text{and} \quad \mathfrak{g}_{0,3} := \bigoplus_{m>0} gr^m G_{\mathbb{Q}}.$$

   Then $gr^m G_{\mathbb{Q}}$ is a finite direct sum of $\mathbb{Z}_p(m)$ for each $m > 0$,

   and $\mathfrak{g}_{0,3}$ is naturally a graded Lie algebra over $\mathbb{Z}_p$.

Hence we obtain a graded Lie algebra $\mathfrak{g}_{0,3}$, which is a direct sum of Tate twists.

Deligne-Ihara's conjecture (proved by Hain-Matsumoto and Brown)

The Lie algebra $\mathfrak{g}_{0,3} \otimes \mathbb{Q}_p$ is freely generated by certain elements $\sigma_3, \sigma_5, \sigma_7, \ldots$ in each odd degree > 1.

Remark.

More precisely, Hain and Matsumoto proved the generation portion of the conjecture. Then Brown proved a certain motivic version of Belyi's injectivity theorem (formulated in terms of the category of mixed Tate motives over $\mathbb{Z}$), which implies the freeness portion.

Soulé characters

Each element σ_m is defined by the property that the image of σ_m under

the m-th Soulé character

$$\kappa_m : gr^m G_{\mathbb{Q}} \to \mathbb{Z}_p(m)$$

generates $\kappa_m(gr^m G_{\mathbb{Q}}) \neq 0$.

We do not explain Soulé characters here, but some important features are as follows:

Properties.

- They arise from the Galois action on the pro-p **metabelian** quotient of π_1.
- κ_m is nontrivial for every odd $m \geq 3$ (which is a highly nontrivial result).
- κ_m (from $F^1 G_{\mathbb{Q}}$) is surjective for every odd $m \geq 3 \Leftrightarrow$ Vandiver's conjecture holds.

Sharifi's result

Theorem (Sharifi, Hain-Matsumoto and Brown).

Let $X = \mathbb{P}^1_{\mathbb{Q}} \setminus \{0, 1, \infty\}$ and p an odd regular prime. Then we have

$$山(:= \bar{\mathbb{Q}}^{\ker(\rho_{X,p})}) = 天(:= \text{the maximal pro-}p\text{ extension of }\mathbb{Q}(\mu_p)\text{ unramified outside }p).$$

Strategy of proof.

(Technical part, we use the regularity here) Construct nice lifts $\sigma_3 \in F^3 G_{\mathbb{Q}}, \sigma_5 \in F^5 G_{\mathbb{Q}}, \ldots$ such that their images freely generate the Galois group $\mathrm{Gal}(天/\mathbb{Q}(\mu_{p^\infty}))$.

We compare the following two filtrations on the Galois group $\mathrm{Gal}(天/\mathbb{Q}(\mu_{p^\infty}))$:

1. Weight filtration F^m: Its intersection is $\mathrm{Gal}(天/山)$.
2. Universal filtration $\tilde{F}^m$: it is the **fastest** descending central filtration on $\mathrm{Gal}(天/\mathbb{Q}(\mu_{p^\infty}))$ satisfying $\sigma_m \in \tilde{F}^m \mathrm{Gal}(天/\mathbb{Q}(\mu_p))$ for every $m = 3, 5, \ldots$.
    - Its intersection is trivial, and
    - The associated graded Lie algebra $/\mathbb{Z}_p$ is freely generated by $\sigma_3, \sigma_5, \ldots$.

Then use Deligne-Ihara's conjecture to show that two filtrations coincide.

Our proof also follows this strategy: assuming that the graded Lie algebra associated to $X = E - O$ is nice, show that two filtrations on the concerned Galois group coincide.

However, this approach comes with a few difficulties:

1. What are analogues of Soulé characters and Deligne-Ihara's conjecture?

   $\to$ We answer this question in the following.

2. (omitted in this talk) In our situation, the structure of $gr^m G_K \otimes \mathbb{Q}_p$ (as a Galois module) becomes complicated and some parts of the previous strategy do not work.

   $\to$ To overcome this point, we introduce a two-variable refinement of the weight filtration

   $$F^{(m_1,m_2)}G_K \subset F^{m_1+m_2}G_K,$$

   and establish fundamental properties.

3. (omitted in this talk) We use arithmetic assumptions on p to control the structure of the Galois group of the maximal pro-p extension of $K(p)$ unramified outside p.

   $\to$ The group is generated by $[K(p) : K] + 2$ generators satisfying a single relation which can be described explicitly to some extent.

Weight filtration on Galois group from $E - O$, (1)

- K: imaginary quadratic field of class number one,
- $p \geq 5$: prime which splits in K as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$,
- E/K: elliptic curve with $O_K = \mathrm{End}_K(E)$,
- $X := E - O$: associated once-punctured elliptic curve,
- $\rho_{X,p} \colon G_K \to \mathrm{Out}(\Pi)$: pro-$p$ outer Galois representation, where $\Pi := \pi_1(X_{\bar{K}})^{(p)}$.

The weight filtration is defined in the same way as $\mathbb{P}^1 - \{0, 1, \infty\}$:

$$F^m G_K := \ker\left[G_K \xrightarrow{\rho_{X,p}} \mathrm{Out}(\Pi) \to \mathrm{Out}(\Pi/\Pi(m+1))\right],$$

$$gr^m G_K := F^m G_K / F^{m+1} G_K \quad \text{and}$$

$$\mathfrak{g}_X := \bigoplus_{m>0} gr^m G_K.$$

Weight filtration on Galois group from $E - O$, (2)

Since p splits, we have two characters

- $\chi_1 : G_K \to \mathrm{Aut}(T_{\mathfrak{p}}(E)) = \mathbb{Z}_p^\times$ and
- $\chi_2 : G_K \to \mathrm{Aut}(T_{\bar{\mathfrak{p}}}(E)) = \mathbb{Z}_p^\times$

corresponding the $\mathfrak{p}$-adic (resp. $\bar{\mathfrak{p}}$-adic) Tate module.

Lemma.

1. (Nakamura) We have $gr^m G_K = 0$ whenever m is odd and $gr^2 G_K = 0$.
2. As a $\mathrm{Gal}(K(E[p^\infty]/K))$-module, we have

$$gr^m G_K \otimes \mathbb{Q}_p \cong \bigoplus_{\substack{(m_1,m_2)\in\mathbb{Z}^2_{>0},\\ m_1+m_2=m}} \mathbb{Q}_p(m_1,m_2)^{r_{m_1,m_2}}$$

for some $r_{m_1,m_2} \geq 0$. Here, $\mathbb{Q}_p(m_1,m_2) := \mathbb{Q}_p(\chi_1^{m_1}\chi_2^{m_2})$.

Analogues of Soulé characters

For each even $m \geq 2$, Nakamura constructed a certain homomorphism

$$\kappa_{m+2,X} \colon gr^{m+2} G_K \to \mathrm{Sym}^m T_p(E) \otimes \mathbb{Z}_p(1),$$

from the Galois action on the metabelian π_1. It has nice properties and applications to anabelian geometry, but its nontriviality is **not** known except for very special m.

In our situation, RHS can be decomposed as

$$\mathrm{Sym}^m T_p(E) \otimes \mathbb{Z}_p(1) \cong \bigoplus_{\substack{(m_1,m_2) \in \mathbb{Z}_{\geq 0}^2 \\ m_1+m_2=m}} \mathbb{Z}_p(m_1+1, m_2+1),$$

hence we obtain characters

$$\{\kappa_{(m_1+1,m_2+1)} \colon gr^{m+2} G_K \to \mathbb{Z}_p(m_1+1, m_2+1)\}_{\substack{(m_1,m_2) \in \mathbb{Z}_{\geq 0}^2, \\ m_1+m_2=m}}$$

from $\kappa_{m,X}$.

Idea.

Use $\kappa_{(m_1+1,m_2+1)}$ as an analogue of Soulé characters.

Properties of characters

Recall:

Properties of Soulé characters.

- κ_m are nontrivial for every odd $m \geq 3$.
- κ_m (from $F^1 G_{\mathbb{Q}}$) is surjective for every odd $m \geq 3 \Leftrightarrow$ Vandiver's conjecture holds.

Similarly, we have:

Theorem (I.).

- $\kappa_{(m_1+1, m_2+1)} = 0$ if $m_1 \not\equiv m_2 \bmod |O_K^\times|$.
- If $m_1 \equiv m_2 \bmod |O_K^\times|$, then $\kappa_{(m_1+1, m_2+1)} \neq 0$ under a certain assumption.
- Moreover, if

  1. the class number $K(p)$ does not divide p, and
  2. there is a unique prime of $K(\mathfrak{p})$ above $\bar{\mathfrak{p}}$,

  then $\kappa_{(m_1+1, m_2+1)}$ (from $F^1 G_K$) is surjective except the case where $m_1 m_2 > 0$ and $(m_1, m_2) \equiv (0, 0) \bmod p-1$. The converse also holds.

Remark.

- Nakamura's homomorphism $\kappa_{m,X}$ can be defined for every once-punctured elliptic curves over number fields.
- However, our proof uses elliptic units and its relation to $\kappa_{(m_1+1,m_2+1)}$, which can be not generalized to non-CM cases.
- A certain assumption = The finiteness of the second cohomology group

  $$H^2_{\text{ét}}(O_K[1/p], \mathbb{Z}_p(m_1+1, m_2+1)).$$

  This is known to hold if $m_1 = m_2$ (Soulé) or $(m_1+1, m_2+1) = (0,0) \bmod p-1$. The finiteness also known to hold for every $(m_1, m_2) \in I$ when p is "regular" in the sense of Wingberg.
- This finiteness is a special case of a conjecture of Jannsen.

Now, we define

$$I := \{(m_1, m_2) \in \mathbb{Z}_{\geq 0}^2 \setminus \{(0,0)\} \mid m_1 \equiv m_2 \bmod |O_K^\times|\},$$

which is an analogue of $2\mathbb{Z}_{\geq 1}$ in the case of $\mathbb{P}^1 - \{0, 1, \infty\}$.

Assume that $\kappa_{(m_1,m_2)}$ is nontrivial[1] for every $(m_1, m_2) \in I$, and choose

$$\sigma_{(m_1+1,m_2+1)} \in \chi_1^{m_1}\chi_2^{m_2}\text{-isotypic component of } gr^{m_1+m_2+2}G_K \otimes \mathbb{Q}_p$$

such that its image under $\kappa_{(m_1+1,m_2+1)}$ is non-zero.

An analogue of Deligne-Ihara's conjecture for X

The graded Lie algebra $\mathfrak{g}_X \otimes \mathbb{Q}_p$ is freely generated by $\{\sigma_{(m_1+1,m_2+1)}\}_{(m_1,m_2)\in I}$.

[1] This is satisfied under assumptions of the main result.

Remark

1. If the conjecture holds, we have

$$\dim(gr^{m+2}G_K \otimes \mathbb{Q}_p) = A_{\frac{m}{2}+1},$$

for K such that $|O_K^\times| = 2$, where $(A_n)_{n\geq 1}$ is A072337 in OEIS.

$m+2$	4	6	8	10	12	$\cdots$
$A_{\frac{m}{2}+1}$	3	5	10	24	50	$\cdots$

It is expected that $\kappa_{4,X}$ and $\kappa_{6,X}$ induce isomorphisms

$$gr^4 G_K \otimes \mathbb{Q}_p \cong \mathrm{Sym}^2 V_p(E)(1) \quad \text{and}$$
$$gr^6 G_K \otimes \mathbb{Q}_p \cong \mathrm{Sym}^4 V_p(E)(1).$$

These holds if $\kappa_{(m_1+1,m_2+1)} \neq 0$ for every $(m_1, m_2) \in I$ with $m_1 + m_2 = 2$ or 4.

2. We proved the generation portion of the conjecture assuming the finiteness of H^2, using Hain-Matsumoto's approach (in preparation). In particular, we have

$$\dim gr^{m+2}G_K \otimes \mathbb{Q}_p \leq A_{\frac{m}{2}+1}.$$

Summary

- The Galois Lie algebra $\mathfrak{g}_X \otimes \mathbb{Q}_p$ has rich structure analogous to the genus 0 case.
- Assuming Deligne-Ihara-style conjectures, we can describe $\bar{K}^{\ker(\rho_{X,p})}$ explicitly.
- This deepens the parallel between $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and $E - O$.

<table>
<tr><th colspan="2">Field</th></tr>
<tr><td>$\mathbb{Q}$</td><td>K: imaginary quadratic</td></tr>
<tr><th colspan="2">Hyperbolic Curve</th></tr>
<tr><td>$\mathbb{P} - \{0, 1, \infty\} = \mathbb{G}_m - 1$</td><td>$X = E - O$</td></tr>
<tr><th colspan="2">Lie algebra</th></tr>
<tr><td>$\mathfrak{g} \otimes \mathbb{Q}_p = \mathrm{FreeLie}(\sigma_3, \sigma_5, \dots)$
(Hain-Matsumoto, Brown)</td><td>$\mathfrak{g}_X \otimes \mathbb{Q}_p \stackrel{?}{=} \mathrm{FreeLie}(\sigma_{1,3}, \sigma_{2,2}, \dots)$
(positive result on generation,
no result on freeness)</td></tr>
<tr><th colspan="2">Fixed Field</th></tr>
<tr><td>the maximal pro-p ext. of $\mathbb{Q}(\mu_p)$
unramified outside p,
if p is regular (Sharifi)</td><td>the maximal pro-p ext. of $K(p)$
unramified outside p and $K(E[p])$,
if p and the Lie algebra are nice (I.)</td></tr>
</table>

Thank you very much!