A p-adic analytic approach to the absolute Grothendieck conjecture

Takahiro Murotani

RIMS

July 1, 2021

Arithmetic fundamental groups

K: a field of characteristic 0

$\overline{K}$: an algebraic closure of K

U: a geometrically connected scheme of finite type over K

$U_{\overline{K}} := U \times_{\operatorname{Spec} K} \operatorname{Spec} \overline{K}$

ξ: a geometric point of U

$\pi_1(U)(\simeq \pi_1(U, \xi))$: the arithmetic fundamental group of U

Arithmetic fundamental groups

K: a field of characteristic 0

$\overline{K}$: an algebraic closure of K

U: a geometrically connected scheme of finite type over K

$U_{\overline{K}} := U \times_{\operatorname{Spec} K} \operatorname{Spec} \overline{K}$

ξ: a geometric point of U

$\pi_1(U) (\simeq \pi_1(U, \xi))$: the arithmetic fundamental group of U

The Galois correspondence

There is a 1-1 correspondence:

$$\begin{array}{c} \mathcal{H} \subset \pi_1(U)\text{: an open subgroup} \\ \Big\updownarrow \text{1-1} \\ U_{\mathcal{H}}\text{: a connected finite étale covering of } U \end{array}$$

The homotopy exact sequence

$\pi_1(U_{\overline{K}})$: the geometric fundamental group of U
$G_K := \mathrm{Gal}(\overline{K}/K)$: the absolute Galois group of K

The homotopy exact sequence

$\pi_1(U_{\overline{K}})$: the geometric fundamental group of U
$G_K := \mathrm{Gal}(\overline{K}/K)$: the absolute Galois group of K

The homotopy exact sequence

We have the following exact sequence:

$$1 \to \pi_1(U_{\overline{K}}) \to \pi_1(U) \to G_K \to 1. \qquad (*)$$

Hyperbolic curves

Suppose that U is a **nonsingular curve** over K.

Hyperbolic curves

Suppose that U is a **nonsingular curve** over K.

$X = U^{\mathrm{cpt}}$: the smooth compactification of U
$g := g(X)$: the genus of X
$n := \sharp(X \setminus U)(\overline{K})$

Hyperbolic curves

Suppose that U is a **nonsingular curve** over K.

$X = U^{\mathrm{cpt}}$: the smooth compactification of U

$g := g(X)$: the genus of X

$n := \sharp(X \setminus U)(\overline{K})$

Definition of hyperbolic curves

U : a *hyperbolic curve* (over K) $\overset{\mathrm{def}}{\Longleftrightarrow} 2g + n - 2 > 0.$

In the following, let U be a **hyperbolic curve** over K.

The Galois-theoretic interpretation of $(*)$

K_U: the function field of U
$\widetilde{K_U}$: the maximal algebraic extension of K_U unramified on U

The Galois-theoretic interpretation of $(*)$

K_U: the function field of U

$\widetilde{K_U}$: the maximal algebraic extension of K_U unramified on U

The Galois-theoretic interpretation of $(*)$

The following two exact sequences are canonically identified:

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(U_{\overline{K}}) \arrow[r] & \pi_1(U) \arrow[r] \arrow[d, Leftrightarrow, "\text{canonically identified}"] & G_K \arrow[r] & 1, \quad (*) \\
1 \arrow[r] & \mathrm{Gal}(\widetilde{K_U}/K_U \cdot \overline{K}) \arrow[r] & \mathrm{Gal}(\widetilde{K_U}/K_U) \arrow[r] & \mathrm{Gal}(K_U \cdot \overline{K}/K_U) \arrow[r] & 1.
\end{tikzcd}$$

Decomposition groups

$\widetilde{X}$: the integral closure of X in $\widetilde{K_U}$

Decomposition groups

$\widetilde{X}$: the integral closure of X in $\widetilde{K_U}$

Definition of decomposition groups

For each closed point $\widetilde{x} \in \widetilde{X}$,

$$D_{\widetilde{x}} := \{\gamma \in \pi_1(U) \,|\, \gamma(\widetilde{x}) = \widetilde{x}\}.$$

We refer to $D_{\widetilde{x}}$ as the *decomposition group* of $\widetilde{x}$.

The relative Grothendieck conjecture

Is it possible to recover U group-theoretically from $\pi_1(U) \twoheadrightarrow G_K$?
i.e.,

$$(\pi_1(U) \twoheadrightarrow G_K) \underset{\text{recoverable}}{\overset{?}{\rightsquigarrow}} U.$$

The relative Grothendieck conjecture

Is it possible to recover U group-theoretically from $\pi_1(U) \twoheadrightarrow G_K$?
i.e.,

$$(\pi_1(U) \twoheadrightarrow G_K) \underset{\text{recoverable}}{\overset{?}{\rightsquigarrow}} U.$$

Known affirmative results

- $K/\mathbb{Q}$: finitely generated, $g = 0$ [Nakamura, 1990]
- $K/\mathbb{Q}$: finitely generated, $n \neq 0$ [Tamagawa, 1997]
- K: sub-p-adic
  (i.e. $K \simeq$ a subfield of a finitely generated extension of $\mathbb{Q}_p$)
  [Mochizuki, 1999]

The absolute Grothendieck conjecture

The absolute Grothendieck conjecture

Is it possible to recover U group-theoretically, solely from $\pi_1(U)$ (not $\pi_1(U) \twoheadrightarrow G_K$)?
i.e.,

$$\pi_1(U) \overset{?}{\rightsquigarrow} U.$$

The absolute Grothendieck conjecture

The absolute Grothendieck conjecture

Is it possible to recover U group-theoretically, solely from $\pi_1(U)$ (not $\pi_1(U) \twoheadrightarrow G_K$)?
i.e.,

$$\pi_1(U) \overset{?}{\rightsquigarrow} U.$$

Known affirmative results

- $[K : \mathbb{Q}] < \infty$ [Mochizuki, 2004]
- $p \geq 5$, $K/\mathbb{Q}_p$: unramified and finite, U: a "canonical lifting" [Mochizuki, 2003]
- $[K : \mathbb{Q}_p] < \infty$, U: "of Belyi type" [Mochizuki, 2007]

The absolute Grothendieck conjecture

The absolute Grothendieck conjecture

Is it possible to recover U group-theoretically, solely from $\pi_1(U)$ (not $\pi_1(U) \twoheadrightarrow G_K$)?
i.e.,

$$\pi_1(U) \overset{?}{\rightsquigarrow} U.$$

Known affirmative results

- $[K : \mathbb{Q}] < \infty$ [Mochizuki, 2004]
- $p \geq 5$, $K/\mathbb{Q}_p$: unramified and finite, U: a "canonical lifting" [Mochizuki, 2003]
- $[K : \mathbb{Q}_p] < \infty$, U: "of Belyi type" [Mochizuki, 2007]

However, when $[K : \mathbb{Q}_p] < \infty$, the absolute Grothendieck conjecture is **unsolved in general**.

The theorem of Neukirch-Uchida

The theorem of Neukirch-Uchida

The theorem of Neukirch-Uchida

For $i = 1, 2$,
K_i: an algebraic number field
G_{K_i}: the absolute Galois group of K_i
Then

$$G_{K_1} \simeq G_{K_2} \Longleftrightarrow K_1 \simeq K_2.$$

The theorem of Neukirch-Uchida

The theorem of Neukirch-Uchida

For $i = 1, 2$,
K_i: an algebraic number field
G_{K_i}: the absolute Galois group of K_i
Then

$$G_{K_1} \simeq G_{K_2} \Longleftrightarrow K_1 \simeq K_2.$$

When K is an algebraic number field, this theorem reduces the **absolute** Grothendieck conjecture to the **relative** case.

The theorem of Neukirch-Uchida

The theorem of Neukirch-Uchida

For $i = 1, 2$,
K_i: an algebraic number field
G_{K_i}: the absolute Galois group of K_i
Then

$$G_{K_1} \simeq G_{K_2} \Longleftrightarrow K_1 \simeq K_2.$$

When K is an algebraic number field, this theorem reduces the **absolute** Grothendieck conjecture to the **relative** case.

However, when K is a p-adic local field,
the analogue of the theorem of Neukirch-Uchida **fails to hold**.

The theorem of Neukirch-Uchida

The theorem of Neukirch-Uchida

For $i = 1, 2$,
K_i: an algebraic number field
G_{K_i}: the absolute Galois group of K_i
Then

$$G_{K_1} \simeq G_{K_2} \Longleftrightarrow K_1 \simeq K_2.$$

When K is an algebraic number field, this theorem reduces the **absolute** Grothendieck conjecture to the **relative** case.

However, when K is a p-adic local field, the analogue of the theorem of Neukirch-Uchida **fails to hold**.

In the following, we concentrate on the **absolute p-adic** Grothendieck conjecture.

Notation

In the following,

$K/\mathbb{Q}_p$: a finite extension

k: the residue field of K

$q = q(K) := \sharp k$

Notation

In the following,

$K/\mathbb{Q}_p$: a finite extension

k: the residue field of K

$q = q(K) := \sharp k$

Moreover,

For each open subgroup $\mathcal{H} \subset \pi_1(U)$,

$U_{\mathcal{H}}$: the étale covering of U corresponding to $\mathcal{H}$

$X_{\mathcal{H}} := (U_{\mathcal{H}})^{\mathrm{cpt}}$: the smooth compactification of $U_{\mathcal{H}}$

$K_{\mathcal{H}}$: the integral closure of K in $U_{\mathcal{H}}$

$q_{\mathcal{H}} := q(K_{\mathcal{H}})$

The absolute p-adic Grothendieck conjecture

An approach to the absolute Grothendieck conjecture

The absolute p-adic Grothendieck conjecture

$\Uparrow$ [Mochizuki, 2013]

Group-theoretic characterization of decomposition groups
i.e., $\pi_1(U) \rightsquigarrow D_{\widetilde{x}}$ ($\widetilde{x} \in \widetilde{X}$: closed point)

An approach to the absolute Grothendieck conjecture

The absolute p-adic Grothendieck conjecture

$\Uparrow$ [Mochizuki, 2013]

Group-theoretic characterization of decomposition groups
i.e., $\pi_1(U) \rightsquigarrow D_{\widetilde{x}}$ ($\widetilde{x} \in \widetilde{X}$: closed point)

$\Uparrow$ [Tamagawa, 1997]

Group-theoretic determination of
whether or not U and its coverings admit rational points (†)
i.e., $\pi_1(U) \rightsquigarrow X_{\mathcal{H}}(K_{\mathcal{H}}) = \emptyset$ or not ($\forall \mathcal{H} \underset{\text{open}}{\subset} \pi_1(U)$)

An approach to the absolute Grothendieck conjecture

The absolute p-adic Grothendieck conjecture

$\Uparrow$ [Mochizuki, 2013]

Group-theoretic characterization of decomposition groups
i.e., $\pi_1(U) \rightsquigarrow D_{\widetilde{x}}$ ($\widetilde{x} \in \widetilde{X}$: closed point)

$\Uparrow$ [Tamagawa, 1997]

Group-theoretic determination of
whether or not U and its coverings admit rational points
i.e., $\pi_1(U) \rightsquigarrow X_{\mathcal{H}}(K_{\mathcal{H}}) = \emptyset$ or not $(\forall \mathcal{H} \underset{\text{open}}{\subset} \pi_1(U))$ (†)

In the following, we concentrate on (†).

Serre's i-invariant

Theorem (Serre)

Y: a nonempty and compact analytic manifold over K
Then Y is the disjoint union of a finite number of (closed) balls and the number of balls is well defined $\mod (q-1)$.

Serre's i-invariant

Theorem (Serre)

Y: a nonempty and compact analytic manifold over K
Then Y is the disjoint union of a finite number of (closed) balls and the number of balls is well defined $\mod (q-1)$.

Definition of i-invariants

For Y as above,

$$i_K(Y) := (\text{the "number of balls"}) \in \mathbb{Z}/(q-1)\mathbb{Z}.$$

We refer to $i_K(Y)$ as the *i-invariant* of Y over K.
Moreover, we set

$$i_K(\emptyset) \equiv 0 \mod (q-1).$$

Examples of i-invariants

$\mathcal{O}_K$: the ring of integers of K
$\mathfrak{M}_K$: the maximal ideal of $\mathcal{O}_K$

Examples of i-invariants

$\mathcal{O}_K$: the ring of integers of K
$\mathfrak{M}_K$: the maximal ideal of $\mathcal{O}_K$

Example

For $m \in \mathbb{Z}_{\geq 0}$,

$$i_K(\mathfrak{M}_K^m) \equiv 1 \mod (q-1),$$

where $\mathfrak{M}_K^0 := \mathcal{O}_K$.
Moreover,

$$i_K(\mathfrak{M}_K^m \setminus \mathfrak{M}_K^{m+1}) \equiv 0 \mod (q-1).$$

Hyperbolic curves and i-invariants

If X is a **proper hyperbolic curve** over K $(g \geq 2)$,
$X(K)$ has a natural structure of compact analytic manifold over K.
($X(K)$: the set of K-rational points of X)

Hyperbolic curves and i-invariants

If X is a **proper hyperbolic curve** over K $(g \geq 2)$,
$X(K)$ has a natural structure of compact analytic manifold over K.
($X(K)$: the set of K-rational points of X)

$$\boxed{i_K(X(K)) \not\equiv 0 \mod (q-1)}$$

$$\Downarrow \qquad \not\Uparrow$$

$$\boxed{X(K) \neq \emptyset}$$

Hyperbolic curves and i-invariants

If X is a **proper hyperbolic curve** over K $(g \geq 2)$,
$X(K)$ has a natural structure of compact analytic manifold over K.
($X(K)$: the set of K-rational points of X)

$$i_K(X(K)) \not\equiv 0 \mod (q-1)$$

$$\Downarrow \qquad \not\Uparrow$$

$$X(K) \neq \emptyset$$

So, in some sense, the i-invariants are **"weaker"** data than the data of whether $X(K) = \emptyset$ or not.

Hyperbolic curves and i-invariants

If X is a **proper hyperbolic curve** over K $(g \geq 2)$,
$X(K)$ has a natural structure of compact analytic manifold over K.
($X(K)$: the set of K-rational points of X)

$$\boxed{i_K(X(K)) \not\equiv 0 \mod (q-1)}$$

$$\Downarrow \qquad \cancel{\Uparrow}$$

$$\boxed{X(K) \neq \emptyset}$$

So, in some sense, the i-invariants are **"weaker"** data than the data of whether $X(K) = \emptyset$ or not.

$\Longrightarrow$ The group-theoretic recovery of the former data is **easier** than that of the latter?

i-invariants and the absolute Grothendieck conjecture

In terms of the i-invariants, the absolute p-adic Grothendieck conjecture is reduced to the following two problems:

i-invariants and the absolute Grothendieck conjecture

In terms of the i-invariants, the absolute p-adic Grothendieck conjecture is reduced to the following two problems:

(A) May the decomposition groups be recovered from the data of the i-invariants of the sets of rational points of the hyperbolic curve and its coverings?

i.e., $i_{K_{\mathcal{H}}}(X_{\mathcal{H}}(K_{\mathcal{H}}))(\forall \mathcal{H} \underset{\text{open}}{\subset} \pi_1(U)) \overset{?}{\rightsquigarrow} D_{\widetilde{x}}\,(\widetilde{x} \in \widetilde{X} :$ closed point$)$

i-invariants and the absolute Grothendieck conjecture

In terms of the i-invariants, the absolute p-adic Grothendieck conjecture is reduced to the following two problems:

(A) May the decomposition groups be recovered from the data of the i-invariants of the sets of rational points of the hyperbolic curve and its coverings?

i.e., $i_{K_{\mathcal{H}}}(X_{\mathcal{H}}(K_{\mathcal{H}}))(\forall \mathcal{H} \underset{\text{open}}{\subset} \pi_1(U)) \overset{?}{\rightsquigarrow} D_{\widetilde{x}}(\widetilde{x} \in \widetilde{X}:$ closed point$)$

(B) May the i-invariants of the set of rational points of the hyperbolic curve be recovered group-theoretically from the arithmetic fundamental group of the curve?

i.e., $\pi_1(U) \overset{?}{\rightsquigarrow} i_K(X(K))$

i-invariants and the absolute Grothendieck conjecture

In terms of the i-invariants, the absolute p-adic Grothendieck conjecture is reduced to the following two problems:

(A) May the decomposition groups be recovered from the data of the i-invariants of the sets of rational points of the hyperbolic curve and its coverings?

i.e., $i_{K_{\mathcal{H}}}(X_{\mathcal{H}}(K_{\mathcal{H}}))(\forall \mathcal{H} \underset{\text{open}}{\subset} \pi_1(U)) \overset{?}{\rightsquigarrow} D_{\widetilde{x}}\,(\widetilde{x} \in \widetilde{X}:$ closed point$)$

(B) May the i-invariants of the set of rational points of the hyperbolic curve be recovered group-theoretically from the arithmetic fundamental group of the curve?

i.e., $\pi_1(U) \overset{?}{\rightsquigarrow} i_K(X(K))$

Today, we give

- a complete affirmative answer to (A);
- a partial affirmative answer to (B).

An affirmative answer to (A)

The following theorem gives an affirmative answer to (A):

Theorem A (M)

Suppose:

- X is a proper hyperbolic curve over K;
- $q \neq 2$;
- $m \in \mathbb{Z}_{>1}$ is a divisor of $q-1$.

Then the following 5 conditions are equivalent:

(i) $X(K) \neq \emptyset$.

(ii) $\exists X' \to X$: a finite étale covering s.t. $X'(K) \neq \emptyset$.

(iii) $\exists X' \to X$: a finite étale covering s.t. $i_K(X'(K)) \not\equiv 0 \mod (q-1)$.

(iv) $\exists X' \to X$: a finite étale covering s.t. $i_K(X'(K)) \not\equiv 0 \mod m$.

(v) $\exists X' \to X$: a finite étale covering s.t. $i_K(X'(K)) \equiv$ (a power of p) $\mod (q-1)$.

Notation and assumption

For $i = 1, 2$,

p_i: a prime

$K_i/\mathbb{Q}_{p_i}$: a finite extension

$q_i := q(K_i)$

U_i: a hyperbolic curve over K_i

$X_i := U_i^{\mathrm{cpt}}$: the smooth compactification of U_i

Notation and assumption

For $i = 1, 2$,

p_i: a prime

$K_i/\mathbb{Q}_{p_i}$: a finite extension

$q_i := q(K_i)$

U_i: a hyperbolic curve over K_i

$X_i := U_i^{\mathrm{cpt}}$: the smooth compactification of U_i

Moreover, for each open subgroup $\mathcal{H}_i \subset \pi_1(U_i)$, we define

$$(U_i)_{\mathcal{H}_i},\ (X_i)_{\mathcal{H}_i}\,(= (U_i)_{\mathcal{H}_i}^{\mathrm{cpt}}),\ (K_i)_{\mathcal{H}_i},\ (q_i)_{\mathcal{H}_i}(:= q((K_i)_{\mathcal{H}_i}))$$

as above.

Notation and assumption

For $i = 1, 2,$

p_i: a prime

$K_i/\mathbb{Q}_{p_i}$: a finite extension

$q_i := q(K_i)$

U_i: a hyperbolic curve over K_i

$X_i := U_i^{\mathrm{cpt}}$: the smooth compactification of U_i

Moreover, for each open subgroup $\mathcal{H}_i \subset \pi_1(U_i)$, we define

$$(U_i)_{\mathcal{H}_i},\ (X_i)_{\mathcal{H}_i}\ (= (U_i)^{\mathrm{cpt}}_{\mathcal{H}_i}),\ (K_i)_{\mathcal{H}_i},\ (q_i)_{\mathcal{H}_i}(:= q((K_i)_{\mathcal{H}_i}))$$

as above.

Suppose that we are given an isomorphism $\alpha : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2)$.
Then we have $p_1 = p_2 =: p$, $q_1 = q_2 =: q$. [Mochizuki]

A group-theoretic consequence of Theorem A

The following theorem is a group-theoretic consequence of Theorem A:

Theorem A′ (M)

Suppose that

$\exists \mathcal{H}_0 \subset \pi_1(U_1)$: an open subgroup,

$\exists m \in \mathbb{Z}_{>1}$: a divisor of $(q_1)_{\mathcal{H}_0} - 1$,

$\forall \mathcal{H} \subset \pi_1(U_1)$: an open subgroup s.t. $\mathcal{H} \subset \mathcal{H}_0$,

$$i_{(K_1)_{\mathcal{H}}}((X_1)_{\mathcal{H}}((K_1)_{\mathcal{H}})) \equiv i_{(K_2)_{\alpha(\mathcal{H})}}((X_2)_{\alpha(\mathcal{H})}((K_2)_{\alpha(\mathcal{H})})) \mod m.$$

$$\cdots (\star)_{\mathcal{H},\, m}$$

Then $\alpha : \pi_1(U_1) \xrightarrow{\sim} \pi_1(U_2)$ preserves decomposition groups.
In particular, α arises from a unique isomorphism of schemes $U_1 \xrightarrow{\sim} U_2$.

A partial affirmative answer to (B)

The following theorem gives a partial affirmative answer to (B):

Theorem B (M)

Let $\mathcal{H} \subset \pi_1(U_1)$ be an open subgroup.
Suppose:

- p is odd (in particular, $2 \,|\, (q-1)$);
- $g((X_1)_{\mathcal{H}}) \geq 2$;
- $(X_1)_{\mathcal{H}}$ has log smooth reduction
  (i.e. has stable reduction after tame base extension).

Then $(\star)_{\mathcal{H},2}$ holds.

A partial affirmative answer to (B)

The following theorem gives a partial affirmative answer to (B):

Theorem B (M)

Let $\mathcal{H} \subset \pi_1(U_1)$ be an open subgroup.
Suppose:

- p is odd (in particular, $2 \mid (q-1)$);
- $g((X_1)_{\mathcal{H}}) \geq 2$;
- $(X_1)_{\mathcal{H}}$ has log smooth reduction
  (i.e. has stable reduction after tame base extension).

Then $(\star)_{\mathcal{H},2}$ holds.

Remark

If Theorem B is proved without assuming that $(X_1)_{\mathcal{H}}$ has log smooth reduction, the absolute p-adic Grothendieck conjecture holds for odd p.

Sketch of proof of Theorem A (1)

Theorem A (M)

Suppose:

- X is a proper hyperbolic curve over K;
- $q \neq 2$;
- $m \in \mathbb{Z}_{>1}$ is a divisor of $q-1$.

Then the following 5 conditions are equivalent:

(i) $X(K) \neq \emptyset$.

(ii) $\exists X' \to X$: a finite étale covering s.t. $X'(K) \neq \emptyset$.

(iii) $\exists X' \to X$: a finite étale covering s.t. $i_K(X'(K)) \not\equiv 0 \mod (q-1)$.

(iv) $\exists X' \to X$: a finite étale covering s.t. $i_K(X'(K)) \not\equiv 0 \mod m$.

(v) $\exists X' \to X$: a finite étale covering s.t. $i_K(X'(K)) \equiv$ (a power of p) $\mod (q-1)$.

Sketch of proof of Theorem A (2)

The implications (v) $\Longrightarrow$ (iv) $\Longrightarrow$ (iii) $\Longrightarrow$ (ii) $\Longrightarrow$ (i) are trivial.
We will show the implication (i)$\Longrightarrow$(v).

Sketch of proof of Theorem A (2)

The implications (v) $\Longrightarrow$ (iv) $\Longrightarrow$ (iii) $\Longrightarrow$ (ii) $\Longrightarrow$ (i) are trivial.
We will show the implication (i)$\Longrightarrow$(v).

J: the Jacobian of X
If $X(K) \neq \emptyset$, for $P_0 \in X(K)$,
$j = j_{P_0} : X \hookrightarrow J$, $P \mapsto [\mathscr{L}(P - P_0)]$: a closed immersion

Sketch of proof of Theorem A (2)

The implications (v) $\Longrightarrow$ (iv) $\Longrightarrow$ (iii) $\Longrightarrow$ (ii) $\Longrightarrow$ (i) are trivial.
We will show the implication (i)$\Longrightarrow$(v).

J: the Jacobian of X
If $X(K) \neq \emptyset$, for $P_0 \in X(K)$,
$j = j_{P_0} : X \hookrightarrow J$, $P \mapsto [\mathscr{L}(P - P_0)]$: a closed immersion

For $\nu \in \mathbb{Z}_{>0}$, we define an étale covering X_ν of X by:

$$\begin{tikzcd} X_\nu \arrow[r, hook] \arrow[d] \arrow[dr, phantom, "\Box"] & J \arrow[d, "\nu_J"] \\ X \arrow[r, hook, "j = j_{P_0}"'] & J \end{tikzcd}$$

where $\nu_J : J \to J$ denotes multiplication by ν on J.

Sketch of proof of Theorem A (3)

Fact (M)

(i) For $n \gg 0$ and an appropriate choice of P_0,

$$i_K(X(K) \cap p_J^n(J(K))) \equiv (\text{a power of } p) \mod (q-1).$$

(Note that $X(K) \overset{j_{P_0}}{\hookrightarrow} J(K)$.)

Sketch of proof of Theorem A (3)

Fact (M)

(i) For $n \gg 0$ and an appropriate choice of P_0,

$$i_K(X(K) \cap p_J^n(J(K))) \equiv (\text{a power of } p) \mod (q-1).$$

(Note that $X(K) \overset{j_{P_0}}{\hookrightarrow} J(K)$.)

(ii)

$$i_K(X_{p^n}(K)) \equiv i_K(X(K) \cap p_J^n(J(K))) \times \sharp J(K)[p^n] \mod (q-1).$$

Sketch of proof of Theorem A (3)

Fact (M)

(i) For $n \gg 0$ and an appropriate choice of P_0,

$$i_K(X(K) \cap p_J^n(J(K))) \equiv \text{(a power of } p\text{)} \mod (q-1).$$

(Note that $X(K) \overset{j_{P_0}}{\hookrightarrow} J(K)$.)

(ii)

$$i_K(X_{p^n}(K)) \equiv i_K(X(K) \cap p_J^n(J(K))) \times \sharp J(K)[p^n] \mod (q-1).$$

By Facts (i) and (ii), for $n \gg 0$ and an appropriate choice of P_0,

$$i_K(X_{p^n}(K)) \equiv \text{(a power of } p\text{)} \mod (q-1).$$

We may take $X' = X_{p^n}$.

Sketch of proof of Theorem B (1)

Theorem B (M)

Let $\mathcal{H} \subset \pi_1(U_1)$ be an open subgroup.
Suppose:

- p is odd (in particular, $2 \,|\, (q-1)$);
- $g((X_1)_{\mathcal{H}}) \geq 2$;
- $(X_1)_{\mathcal{H}}$ has log smooth reduction
  (i.e. has stable reduction after tame base extension).

Then $(\star)_{\mathcal{H},\,2}$ holds.

Sketch of proof of Theorem B (1)

Theorem B (M)

Let $\mathcal{H} \subset \pi_1(U_1)$ be an open subgroup.
Suppose:

- p is odd (in particular, $2 \,|\, (q-1)$);
- $g((X_1)_{\mathcal{H}}) \geq 2$;
- $(X_1)_{\mathcal{H}}$ has log smooth reduction
  (i.e. has stable reduction after tame base extension).

Then $(\star)_{\mathcal{H},\,2}$ holds.

By replacing U_1 by $(U_1)_{\mathcal{H}}$, we may assume that $\mathcal{H} = \pi_1(U_1)$.

Sketch of proof of Theorem B (2)

For $i = 1,\, 2$, by Deligne-Mumford,
$\exists L_i/K_i$: a finite Galois extension,
$X_i \times_{\operatorname{Spec} K_i} \operatorname{Spec} L_i$ has the stable model $\mathfrak{X}_i$.

Sketch of proof of Theorem B (2)

For $i = 1, 2$, by Deligne-Mumford,
$\exists L_i/K_i$: a finite Galois extension,
$X_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, L_i$ has the stable model $\mathfrak{X}_i$.
$\mathcal{O}_{L_i}$ the ring of integers of L_i
k_{L_i}: the residue field of L_i
$G_i := \mathrm{Gal}(L_i/K_i)$
$\overline{K_i}$: an algebraic closure of K_i

Sketch of proof of Theorem B (2)

For $i = 1, 2$, by Deligne-Mumford,
$\exists L_i/K_i$: a finite Galois extension,
$X_i \times_{\operatorname{Spec} K_i} \operatorname{Spec} L_i$ has the stable model $\mathfrak{X}_i$.
$\mathcal{O}_{L_i}$ the ring of integers of L_i
k_{L_i}: the residue field of L_i
$G_i := \operatorname{Gal}(L_i/K_i)$
$\overline{K_i}$: an algebraic closure of K_i

Fact [Mochizuki]

(i) Whether or not X_i has stable reduction is group-theoretic.

Sketch of proof of Theorem B (2)

For $i = 1, 2$, by Deligne-Mumford,
$\exists L_i/K_i$: a finite Galois extension,
$X_i \times_{\operatorname{Spec} K_i} \operatorname{Spec} L_i$ has the stable model $\mathfrak{X}_i$.
$\mathcal{O}_{L_i}$ the ring of integers of L_i
k_{L_i}: the residue field of L_i
$G_i := \operatorname{Gal}(L_i/K_i)$
$\overline{K_i}$: an algebraic closure of K_i

Fact [Mochizuki]

(i) Whether or not X_i has stable reduction is group-theoretic.

Note that α induces the following commutative diagram [Mochizuki]:

$$\begin{array}{ccccc}
\pi_1(U_1) & \twoheadrightarrow & \pi_1(X_1) & \twoheadrightarrow & \operatorname{Gal}(\overline{K_1}/K_1) \\
{\scriptstyle\alpha}\downarrow\wr & & {\scriptstyle\alpha_X}\downarrow\wr & & {\scriptstyle\alpha_K}\downarrow\wr \\
\pi_1(U_2) & \twoheadrightarrow & \pi_1(X_2) & \twoheadrightarrow & \operatorname{Gal}(\overline{K_2}/K_2)
\end{array}$$

Sketch of proof of Theorem B (2)

For $i = 1, 2$, by Deligne-Mumford,
$\exists L_i/K_i$: a finite Galois extension,
$X_i \times_{\mathrm{Spec}\, K_i} \mathrm{Spec}\, L_i$ has the stable model $\mathfrak{X}_i$.
$\mathcal{O}_{L_i}$ the ring of integers of L_i
k_{L_i}: the residue field of L_i
$G_i := \mathrm{Gal}(L_i/K_i)$
$\overline{K_i}$: an algebraic closure of K_i

Fact [Mochizuki]

(i) Whether or not X_i has stable reduction is group-theoretic.

Note that α induces the following commutative diagram [Mochizuki]:

$$\begin{tikzcd}
\pi_1(U_1) \arrow[r, two heads] \arrow[d, "\alpha"', "\wr"] & \pi_1(X_1) \arrow[r, two heads] \arrow[d, "\alpha_X"', "\wr"] & \mathrm{Gal}(\overline{K_1}/K_1) \arrow[d, "\alpha_K"', "\wr"] \\
\pi_1(U_2) \arrow[r, two heads] & \pi_1(X_2) \arrow[r, two heads] & \mathrm{Gal}(\overline{K_2}/K_2)
\end{tikzcd}$$

By Fact (i), we may assume that $\alpha_K^{-1}(\mathrm{Gal}(\overline{K_2}/L_2))=\mathrm{Gal}(\overline{K_1}/L_1)$.

Sketch of proof of Theorem B (3)

Fact

(ii) If X_i has log smooth reduction, we may assume that L_i/K_i is tamely ramified. [Saito]

Sketch of proof of Theorem B (3)

Fact

(ii) If X_i has log smooth reduction, we may assume that L_i/K_i is tamely ramified. [Saito]

(iii) L_1/K_1: tamely ramified $\Longleftrightarrow$ L_2/K_2: tamely ramified. [Mochizuki]

Sketch of proof of Theorem B (3)

Fact

(ii) If X_i has log smooth reduction, we may assume that L_i/K_i is tamely ramified. [Saito]

(iii) L_1/K_1: tamely ramified $\Longleftrightarrow$ L_2/K_2: tamely ramified. [Mochizuki]

(iv) The special fiber $(\mathfrak{X}_i)_{k_{L_i}} := \mathfrak{X}_i \times_{\mathrm{Spec}\, \mathcal{O}_{L_i}} \mathrm{Spec}\, k_{L_i}$ is group-theoretic. [Mochizuki]

Sketch of proof of Theorem B (3)

Fact

(ii) If X_i has log smooth reduction, we may assume that L_i/K_i is tamely ramified. [Saito]

(iii) L_1/K_1: tamely ramified $\Longleftrightarrow$ L_2/K_2: tamely ramified. [Mochizuki]

(iv) The special fiber $(\mathfrak{X}_i)_{k_{L_i}} := \mathfrak{X}_i \times_{\operatorname{Spec} \mathcal{O}_{L_i}} \operatorname{Spec} k_{L_i}$ is group-theoretic. [Mochizuki]

By assumption and Facts (ii) and (iii), we may assume that $L_i/K_i\,(i = 1,\, 2)$ is **tamely ramified**.

Sketch of proof of Theorem B (3)

Fact

(ii) If X_i has log smooth reduction, we may assume that L_i/K_i is tamely ramified. [Saito]

(iii) L_1/K_1: tamely ramified $\Longleftrightarrow$ L_2/K_2: tamely ramified. [Mochizuki]

(iv) The special fiber $(\mathfrak{X}_i)_{k_{L_i}} := \mathfrak{X}_i \times_{\mathrm{Spec}\,\mathcal{O}_{L_i}} \mathrm{Spec}\,k_{L_i}$ is group-theoretic. [Mochizuki]

By assumption and Facts (ii) and (iii), we may assume that $L_i/K_i\,(i = 1,\,2)$ is **tamely ramified**.
Moreover, α induces the following commutative diagram (cf. Fact (iv)):

$$\begin{array}{ccc} (\mathfrak{X}_1)_{k_{L_1}} & \curvearrowleft & G_1\,(= \mathrm{Gal}(L_1/K_1)) \\ \wr\downarrow & & \wr\downarrow \\ (\mathfrak{X}_2)_{k_{L_2}} & \curvearrowleft & G_2\,(= \mathrm{Gal}(L_2/K_2)) \end{array}$$

Sketch of proof of Theorem B (4)

$$
\begin{tikzcd}
X_i(L_i) & \mathfrak{X}_i(\mathcal{O}_{L_i}) \arrow[l, "\sim"'] \arrow[r, "\rho_i"] & (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i}) \\
X_i(L_i)^{G_i} = X_i(K_i) \arrow[u, hook] & \mathfrak{X}_i(\mathcal{O}_{L_i})^{G_i} \arrow[l, "\sim"'] \arrow[r, "\rho'_i"] \arrow[u, hook] & (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i})^{G_i} \ni P_i \arrow[u, hook]
\end{tikzcd}
$$

Sketch of proof of Theorem B (4)

$$\begin{tikzcd}
X_i(L_i) & \mathfrak{X}_i(\mathcal{O}_{L_i}) \arrow[l, "\sim"'] \arrow[r, "\rho_i"] & (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i}) \\
X_i(L_i)^{G_i} = X_i(K_i) \arrow[u, hook] & \mathfrak{X}_i(\mathcal{O}_{L_i})^{G_i} \arrow[l, "\sim"'] \arrow[r, "\rho_i'"] \arrow[u, hook] & (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i})^{G_i} \ni P_i \arrow[u, hook]
\end{tikzcd}$$

$$G_i \curvearrowright \rho_i^{-1}(P_i)$$

$${\rho_i'}^{-1}(P_i) = \rho_i^{-1}(P_i)^{G_i}$$

Sketch of proof of Theorem B (4)

$$\begin{tikzcd}
X_i(L_i) & & \mathfrak{X}_i(\mathcal{O}_{L_i}) \arrow[ll, "\sim"'] \arrow[r, "\rho_i"] & (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i}) \\
X_i(L_i)^{G_i} = X_i(K_i) \arrow[u, hook] & & \mathfrak{X}_i(\mathcal{O}_{L_i})^{G_i} \arrow[ll, "\sim"'] \arrow[r, "\rho_i'"] \arrow[u, hook] & (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i})^{G_i} \ni P_i \arrow[u, hook]
\end{tikzcd}$$

$$G_i \curvearrowright \rho_i^{-1}(P_i)$$
$$\rho_i'^{-1}(P_i) = \rho_i^{-1}(P_i)^{G_i}$$

When L_i/K_i is tamely ramified, we may calculate $i_{K_i}(\rho_i'^{-1}(P_i))$:

P_i : a smooth point $\Longrightarrow i_{K_i}(\rho_i'^{-1}(P_i)) \equiv 1 \mod (q-1)$.

P_i : a node and $p \neq 2 \Longrightarrow i_{K_i}(\rho_i'^{-1}(P_i)) \equiv 0$ or $2 \mod (q-1)$.

Sketch of proof of Theorem B (4)

$$
\begin{tikzcd}
X_i(L_i) & \mathfrak{X}_i(\mathcal{O}_{L_i}) \arrow[l, "\sim"'] \arrow[r, "\rho_i"] & (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i}) \\
X_i(L_i)^{G_i} = X_i(K_i) \arrow[u, hook] & \mathfrak{X}_i(\mathcal{O}_{L_i})^{G_i} \arrow[l, "\sim"'] \arrow[r, "\rho'_i"] \arrow[u, hook] & (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i})^{G_i} \ni P_i \arrow[u, hook]
\end{tikzcd}
$$

$$G_i \curvearrowright \rho_i^{-1}(P_i)$$

$$\rho_i'^{-1}(P_i) = \rho_i^{-1}(P_i)^{G_i}$$

When L_i/K_i is tamely ramified, we may calculate $i_{K_i}(\rho_i'^{-1}(P_i))$:

$$P_i: \text{ a smooth point} \Longrightarrow i_{K_i}(\rho_i'^{-1}(P_i)) \equiv 1 \mod (q-1).$$

$$P_i: \text{ a node and } p \neq 2 \Longrightarrow i_{K_i}(\rho_i'^{-1}(P_i)) \equiv 0 \text{ or } 2 \mod (q-1).$$

$\Longrightarrow$ If $p \neq 2$,

$$i_{K_i}(X_i(K_i)) \equiv \sharp(\mathfrak{X}_i)^{\mathsf{sm}}_{k_{L_i}}(k_{L_i})^{G_i} \mod 2.$$

Sketch of proof of Theorem B (4)

$$\begin{CD}
X_i(L_i) @<{\sim}<< \mathfrak{X}_i(\mathcal{O}_{L_i}) @>{\rho_i}>> (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i}) \\
@AAA @AAA @AAA \\
X_i(L_i)^{G_i} = X_i(K_i) @<{\sim}<< \mathfrak{X}_i(\mathcal{O}_{L_i})^{G_i} @>{\rho_i'}>> (\mathfrak{X}_i)_{k_{L_i}}(k_{L_i})^{G_i} \ni {\color{red}P_i}
\end{CD}$$

$$G_i \curvearrowright \rho_i^{-1}(P_i)$$
$$\rho_i'^{-1}(P_i) = \rho_i^{-1}(P_i)^{G_i}$$

When L_i/K_i is tamely ramified, we may calculate $i_{K_i}(\rho_i'^{-1}(P_i))$:

$$P_i : \text{ a smooth point} \Longrightarrow i_{K_i}(\rho_i'^{-1}(P_i)) \equiv 1 \mod (q-1).$$

$$P_i : \text{ a node and } p \neq 2 \Longrightarrow i_{K_i}(\rho_i'^{-1}(P_i)) \equiv 0 \text{ or } 2 \mod (q-1).$$

$\Longrightarrow$ If $p \neq 2$,

$$i_{K_i}(X_i(K_i)) \equiv \sharp(\mathfrak{X}_i)^{\mathsf{sm}}_{k_{L_i}}(k_{L_i})^{G_i} \mod 2.$$

Theorem B follows from Fact (iv).

Sketch of proof of Theorem B (5)

Calculation of $i_{K_i}(\rho_i'^{-1}(P_i))$

For simplicity, we omit subscripts i and assume that P is a smooth point.

$$\begin{tikzcd}
X(L) & \mathfrak{X}(\mathcal{O}_L) \arrow[l, "\sim"'] \arrow[r, "\rho"] & \mathfrak{X}_{k_L}(k_L) \\
X(L)^G = X(K) \arrow[u, hook] & \mathfrak{X}(\mathcal{O}_L)^G \arrow[l, "\sim"'] \arrow[r, "\rho'"] \arrow[u, hook] & \mathfrak{X}_{k_L}(k_L)^G \ni P \arrow[u, hook]
\end{tikzcd}$$

Sketch of proof of Theorem B (5)

Calculation of $i_{K_i}(\rho_i'^{-1}(P_i))$

For simplicity, we omit subscripts i and assume that P is a smooth point.

$$\begin{tikzcd}
X(L) & \mathfrak{X}(\mathcal{O}_L) \arrow[l, "\sim"'] \arrow[r, "\rho"] & \mathfrak{X}_{k_L}(k_L) \\
X(L)^G = X(K) \arrow[u, hook] & \mathfrak{X}(\mathcal{O}_L)^G \arrow[l, "\sim"'] \arrow[r, "\rho'"] \arrow[u, hook] & \mathfrak{X}_{k_L}(k_L)^G \ni P \arrow[u, hook]
\end{tikzcd}$$

We have $\hat{\mathcal{O}}_{\mathfrak{X},\,P} \simeq \mathcal{O}_L[[T]]$ and

$$\begin{aligned}
\rho^{-1}(P) &\simeq \mathrm{Hom}_{\mathrm{Spec}\,\mathcal{O}_L}(\mathrm{Spec}\,\mathcal{O}_L,\ \mathrm{Spec}\,\mathcal{O}_{\mathfrak{X},\,P}) \\
&\simeq \mathrm{Hom}_{\mathcal{O}_L}(\mathcal{O}_{\mathfrak{X},\,P},\ \mathcal{O}_L) \\
&\simeq \mathrm{Hom}_{\mathcal{O}_L}(\hat{\mathcal{O}}_{\mathfrak{X},\,P},\ \mathcal{O}_L) \simeq \mathfrak{M}_L.
\end{aligned}$$

$$(f : \hat{\mathcal{O}}_{\mathfrak{X},\,P} \simeq \mathcal{O}_L[[T]] \to \mathcal{O}_L) \mapsto f(T)$$

Sketch of proof of Theorem B (6)

Fact (M)

(v) For $\gamma \in G$, the action $G \curvearrowright \hat{\mathcal{O}}_{\mathfrak{X},\, P} \simeq \mathcal{O}_L[[T]]$ is given by:

$$a \in \mathcal{O}_L \subset \mathcal{O}_L[[T]] \Longrightarrow \gamma \cdot a = \gamma(a) \text{ (usual Galois action)}$$

$$T \in \mathcal{O}_L[[T]] \Longrightarrow \gamma \cdot T = \sum_{i=0}^{\infty} b_i T^i \, (b_i \in \mathcal{O}_L,\ b_0 \in \mathfrak{M}_L,\ b_1 \in \mathcal{O}_L^{\times})$$

Sketch of proof of Theorem B (6)

Fact (M)

(v) For $\gamma \in G$, the action $G \curvearrowright \hat{\mathcal{O}}_{\mathfrak{X},\,P} \simeq \mathcal{O}_L[[T]]$ is given by:

$$a \in \mathcal{O}_L \subset \mathcal{O}_L[[T]] \Longrightarrow \gamma \cdot a = \gamma(a) \text{ (usual Galois action)}$$

$$T \in \mathcal{O}_L[[T]] \Longrightarrow \gamma \cdot T = \sum_{i=0}^{\infty} b_i T^i \, (b_i \in \mathcal{O}_L,\, b_0 \in \mathfrak{M}_L,\, b_1 \in \mathcal{O}_L^{\times})$$

(vi) For $\gamma \in G$, the action $G \curvearrowright \rho^{-1}(P) \simeq \mathfrak{M}_L$ is given by:

$$[\gamma](x) := \gamma \cdot x = \sum_{i=0}^{\infty} \gamma(a_i x^i),$$

where $x \in \mathfrak{M}_L$ and $\gamma^{-1} \cdot T = \sum_{i=0}^{\infty} a_i T^i$.

Sketch of proof of Theorem B (7)

π_K: a uniformizer of K
K^{ur}: the maximal unramified extension of K in L
$\sigma \in G$: a generator of $\mathrm{Gal}(L/K^{\mathrm{ur}})$
$e := [L : K^{\mathrm{ur}}]$

Sketch of proof of Theorem B (7)

π_K: a uniformizer of K
K^{ur}: the maximal unramified extension of K in L
$\sigma \in G$: a generator of $\mathrm{Gal}(L/K^{\mathrm{ur}})$
$e := [L : K^{\mathrm{ur}}]$
Moreover, we take $\tau \in G$ such that:

$$\begin{tikzcd} G \arrow[r, two heads] & \mathrm{Gal}(K^{\mathrm{ur}}/K) \simeq \mathrm{Gal}(k_L/k) \\ \langle \tau \rangle \arrow[u, hook] \arrow[ur, two heads] & \end{tikzcd}$$

Then, $G = \langle \sigma, \tau \rangle$.

Sketch of proof of Theorem B (8)

The following theorem shows that we may take an isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},\,P} \simeq \mathcal{O}_L[[T]]$ such that the action of G is not so complicated:

Sketch of proof of Theorem B (8)

The following theorem shows that we may take an isomorphism $\hat{\mathcal{O}}_{\mathfrak{X},\,P} \simeq \mathcal{O}_L[[T]]$ such that the action of G is not so complicated:

Theorem (M)

$\exists T \in \hat{\mathcal{O}}_{\mathfrak{X},\,P}$ such that $\hat{\mathcal{O}}_{\mathfrak{X},\,P} \simeq \mathcal{O}_L[[T]]$ and

$$\begin{cases} \sigma^{-1} \cdot T &= \omega T, \\ \tau^{-1} \cdot T &= \dfrac{1}{u} T. \end{cases}$$

Here, $\omega \in \mathcal{O}_L^\times$ is an e-th root of unity and $u \in \mathcal{O}_L^\times$.
Moreover, $\exists x_0 \in \mathfrak{M}_L$ such that

$$\begin{cases} [\sigma](x_0) &= x_0, \\ [\tau](x_0) &= x_0. \end{cases}$$

Sketch of proof of Theorem B (9)

The theorem, together with easy calculation, shows that:

Sketch of proof of Theorem B (9)

The theorem, together with easy calculation, shows that:

Corollary

$$\rho'^{-1}(P) = \rho^{-1}(P)^G \simeq \mathcal{O}_K x_0.$$

In particular,

$$i_K(\rho'^{-1}(P)) \equiv 1 \mod (q-1).$$