

The m -step solvable Grothendieck conjecture for genus 0 curves over finitely generated fields

2nd Kyoto-Hefei Workshop on Arithmetic Geometry

Naganori Yamaguchi

RIMS Kyoto University, Japan

August 19 2020

reference:

The m -step solvable Grothendieck conjecture for genus 0 curves over finitely generated fields. Naganori Yamaguchi, master thesis, Kyoto University, 2020.

1 Introduction

2 Reconstruction of decomposition groups at cusps

3 The m -step solvable GC for genus 0 hyperbolic curves over fields fin. gen. over the prime field

The Grothendieck's anabelian conjecture (GC)

3/26

In this talk, a curve over a field k is defined as a one-dimensional scheme geometrically connected, separated and of finite type over k .

Definition

Let X be a smooth proper curve over k and U an non-empty open subscheme of X . Set $S := X - U$. Let $g(U)$ be the genus of X and $r(U) := |S(\bar{k})|$. We say that U is hyperbolic if $2 - 2g(U) - r(U) < 0$.

For curves, the main anabelian question is the reconstruction of the isom class from fundamental groups. Exactly:

The Grothendieck's anabelian conjecture (cf. [Mochizuki]¹)

Let k be a sub- p -adic field (e.g. field fin. gen. over \mathbb{Q}), and U, U' hyperbolic curves over k . Then the following holds.

$$\pi_1(U) \cong_{G_k} \pi_1(U') \implies U \cong_k U'$$

¹The local pro- p anabelian geometry of curves. Invent. Math., 138(2):319–423, 1999.

What is m -step solvable GC?

4/26

- Let G be a profinite group. Set $G^{[0]} := G$, $G^{[m]} := \overline{[G^{[m-1]}, G^{[m-1]}]}$ ($m \in \mathbb{N}$.) We call $G^m := G/G^{[m]}$ the maximal m -step solvable quotient of G .
- $\pi_1^{(m)}(U) := \pi_1(U)/\pi_1(U_{k^{\text{sep}}})^{[m]}$. This satisfies:

$$1 \rightarrow \pi_1(U_{k^{\text{sep}}})^m \rightarrow \pi_1^{(m)}(U) \rightarrow G_k \rightarrow 1 \quad (\text{exact}).$$

The m -step solvable Grothendieck conjecture

Let U, U' be hyperbolic curves over k . Then the following holds.

$$\pi_1^{(m)}(U) \cong_{G_k} \pi_1^{(m)}(U') \implies U \cong_k U'$$

- [Nakamura]² $m = 2$, k : a number field (+conditions), $(g, r) = (0, 4)$
- [Mochizuki] $m \geq 5$, k : a sub- p -adic field, (g, r) : general

It is desirable to prove the m -step solvable GC for as small m as possible ($m = 2$ is smallest expected).

²Rigidity of the arithmetic fundamental group of a punctured projective line. J. Reine Angew. Math., 405:117–130, 1990.

In this talk, we prove a result on the m -step solvable GC. To be more specific:

Main result

- k : a field finitely generated over the prime field, $p := \text{ch}(k) \geq 0$.
- U, U' : genus 0 hyperbolic curves over k .
- $m \geq 3$.
- If $p > 0$, we assume a non-isotrivial condition of U (more about that later).

Then the m -step solvable GC (with suitable modification when $p > 0$) holds.

- §2: We explain the reconstruction of decomposition groups at cusps, which is the main ingredient of the proof of the main result.
- §3 We give the exact statement of the main result and explain the outline of the proof in detail.
- Many of the proofs and definitions refer to [Nakamura2]³.

³Galois rigidity of the étale fundamental groups of punctured projective lines. J. Reine Angew. Math., 411:205–216, 1990.

1 Introduction

2 Reconstruction of decomposition groups at cusps

3 The m -step solvable GC for genus 0 hyperbolic curves over fields fin. gen. over the prime field

Center-freeness of free pro- C groups

7/26

Fix a non-empty non-trivial class of finite groups C which is closed under taking quotients, subgroups and extensions. We set $\mathbb{Z}_C := \hat{\mathbb{Z}}^C$.

Proposition 2.1.

Let \mathcal{F} be a free pro- C group and $X \subset \mathcal{F}$ a set of free generators. If $m \geq 2$ and $|X| \geq 2$, then for any $n \in \mathbb{Z} - \{0\}$ and $x \in X$, the following holds.

$$Z_{\mathcal{F}^m}(x^n) = \overline{\langle x \rangle}$$

Here, $Z_{\mathcal{F}^m}(x^n)$ is the centralizer of x^n in \mathcal{F}^m . In particular, \mathcal{F}^m is center-free.

Proof

(Step 1) $Z_{\mathcal{F}^m}(x^n) \subset \overline{\langle x \rangle} \cdot \mathcal{F}^{[m-1]} / \mathcal{F}^{[m]}$

(Step 2) $\mathbb{Z}_C[[\mathcal{F}^1]] \ni x^n - 1$ is a non-zero-divisor.

(Step 3) $x^n - 1$ is a non-zero-divisor $\Leftrightarrow Z_{\mathcal{F}^2}(x^n) = \overline{\langle x \rangle}$

(In this step, we use pro- C Branchfield-Lyndon theory.)

(Step 4) The induction on $m \geq 2$. □

Separatedness of decomposition groups at cusps

We introduce the following notation.

- Define $\bar{\Pi}$ as the maximal pro- C quotient of $\pi_1(U_{k^{\text{sep}}})$.
- $\Pi^{(m)} := \pi_1(U)/\text{Ker}(\pi_1(U_{k^{\text{sep}}}) \rightarrow \bar{\Pi}^m)$. This satisfies:

$$1 \rightarrow \bar{\Pi}^m \rightarrow \Pi^{(m)} \rightarrow G_k \rightarrow 1. \quad (\text{exact})$$

- $\tilde{U}^m \rightarrow U_{k^{\text{sep}}}$, $\tilde{X}^m \rightarrow X_{k^{\text{sep}}}$: the covers corresponding to $\bar{\Pi}^m$.
- I_y (resp. D_y): the stabilizer of $y \in \tilde{X}^m - \tilde{U}^m$ w.r.t $\bar{\Pi}^m \curvearrowright \tilde{X}^m - \tilde{U}^m$ (resp. $\Pi^{(m)} \curvearrowright \tilde{X}^m - \tilde{U}^m$).

Corollary 2.2.

- U : a hyperbolic curve over k with $r(U) \geq 2$.
- $\mathbb{Z}/p\mathbb{Z} \notin C$
- $m \geq 2$

For all distinct pairs $y, y' \in \tilde{X}^m - \tilde{U}^m$, the following hold.

- (1) $I_y = N_{\bar{\Pi}^m}(I_y)$ and $D_y = N_{\Pi^{(m)}}(I_y)$.
- (2) I_y and $I_{y'}$ are not commensurable. In particular, $D_y \neq D_{y'}$.

Main result of §2

9/26

We consider the following assumptions.

Setting of §2

- k : a field finitely generated over the prime field, $p := \text{ch}(k)$
- U : a hyperbolic curve over k with $r(U) \geq 3$.
- $\mathbb{Z}/p\mathbb{Z} \notin C$

Under the assumption, we show:

Main result of §2

The decomposition groups at cusps of $\Pi^{(m)}(U)$ can be recovered group-theoretically from $\Pi^{(m+2)}(U) \rightarrow G_k$.

Flow of the proof

To prove, we define the maximal cyclic subgroups of cyclotomic type (CSCT), and show that the inertia groups can be characterized as the images of CSCT.

The maximal cyclic subgroup of cyclotomic type (CSCT)

10/26

Definition

Let $J <^{\text{cl}} \overline{\Pi}^m$. If J satisfies the following conditions, then J is called the maximal cyclic subgroup of cyclotomic type (CSCT).

- (i) $J \cong \mathbb{Z}_C$
- (ii) $J \simeq \overline{J} (:= \text{the image } J \text{ by } \overline{\Pi}^m \rightarrow \overline{\Pi}^{\text{ab}})$ and $\overline{\Pi}^{\text{ab}} / \overline{J}$ is torsion-free.
- (iii) $\text{pr}_{U/k}(N_{\Pi(m)}(J)) <^{\text{op}} G_k$.
- (iv) The following diagram is commutative.

$$\begin{array}{ccc}
 N_{\Pi(m)}(J) & \xrightarrow{\text{conjugate}} & \text{Aut}(J) \\
 \text{pr}_{U/k} \downarrow & & \parallel \\
 G_k & \xrightarrow{\chi_{\text{cycl}}} & \mathbb{Z}_C^\times
 \end{array}$$

Reconstruction of the inertia groups

11/26

Proposition 2.3.

For any $I <^{\text{cl}} \overline{\Pi}^m$, the following conditions are equivalent.

- (a) I is an inertia group.
- (b) There exists a CSCT J of $\overline{\Pi}^{m+2}$ whose image by $\overline{\Pi}^{m+2} \rightarrow \overline{\Pi}^m$ coincides with I .

Sketch of $(b) \Rightarrow (a)$

In this case, for all $H <^{\text{op}} \overline{\Pi}^{m+2}$ containing $\overline{\Pi}^{[m+1]}/\overline{\Pi}^{[m+2]}$, we reconstruct $\mathcal{I}_H = \langle \text{inertia groups} \rangle \subset H^{\text{ab}}$, and we show that the image of $J \cap H$ is contained in \mathcal{I}_H . □

The pro- ℓ setting

If C coincides with $\{\ell\text{-group}\}$, then $m + 2$ can be replaced with $m + 1$.

Proof of Main result of §2

12/26

Setting of §2

- k : a field finitely generated over the prime field, $p := \text{ch}(k)$
- U : a hyperbolic curve over k with $r(U) \geq 3$.
- $\mathbb{Z}/p\mathbb{Z} \notin C$

Main result of §2

The decomposition groups at cusps of $\Pi^{(m)}(U)$ can be recovered group-theoretically from $\Pi^{(m+2)}(U) \rightarrow G_k$.

Proof

We reconstructed the inertia groups of $\overline{\Pi}^m$, group-theoretically (Proposition 2.3). Since the decomposition groups at cusps are the normalizer of the inertia groups if $m \geq 2$ (Corollary 2.2), the assertion holds if $m \geq 2$. When $m = 1$, we must use the maximal nilpotent quotient of $\overline{\Pi}^m$. □

The pro- ℓ setting

If C coincides with $\{\ell\text{-group}\}$, then $m + 2$ can be replaced with $m + 1$ ($m \geq 2$).

1 Introduction

2 Reconstruction of decomposition groups at cusps

3 The m -step solvable GC for genus 0 hyperbolic curves over fields fin. gen. over the prime field

Assumption

In this section, we assume that:

Setting of §3

- (1) k : a field finitely generated over the prime field, $p := \text{ch}(k)$.
- (2) U, U' : **genus 0** hyperbolic curves over k .
- (3) C contains $\mathbb{Z}/\ell\mathbb{Z}$ for **all primes** $\ell \neq p$.

- By (2), we get $r(U) \geq 3$. Then we can use the results of §2.
- By (3), The group $\bar{\Pi}$ (cf. §2) coincides with the maximal prime to p quotient of the fundamental group. In other word, we have

$$\bar{\Pi} = \pi_1^{(p)'}(U_{k^{\text{sep}}}).$$

First, we introduce the following notation.

Definition

Let $p > 0$ and $k_0 := k \cap \bar{\mathbb{F}}_p$. A curve X over k is isotrivial if there exists a curve X_0 over \bar{k}_0 such that $X_0 \times_{\bar{k}_0} \bar{k} \cong X_{\bar{k}}$.

Setting of §3

- k : a field finitely generated over the prime field, $p := \text{ch}(k)$.
- U, U' : genus 0 hyperbolic curves over k .
- C contains $\mathbb{Z}/\ell\mathbb{Z}$ for all primes $\ell \neq p$.

The following theorem is the main result of this talk.

Main theorem

- $m \geq 3$
- If $p > 0$, we assume:

$$\forall R \subset (U_{\bar{k}})^{\text{cpt}} - U_{\bar{k}} \text{ with } |R| = 4, \quad (U_{\bar{k}})^{\text{cpt}} - R \text{ is non-isotrivial.}$$

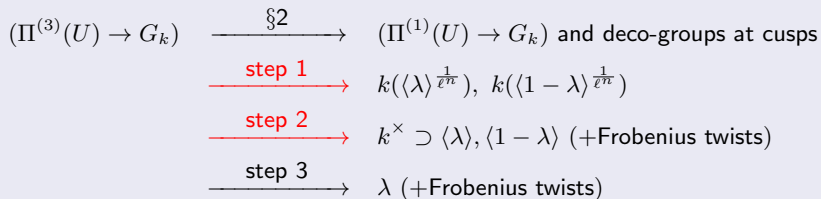
Then the following hold.

$$\Pi^{(m)}(U) \underset{G_k}{\cong} \Pi^{(m)}(U') \implies \begin{cases} U \underset{k}{\cong} U' & p = 0 \\ \exists n, n' \in \mathbb{N} \cup \{0\} \text{ s.t. } U(n) \underset{k}{\cong} U'(n') & p > 0 \end{cases}$$

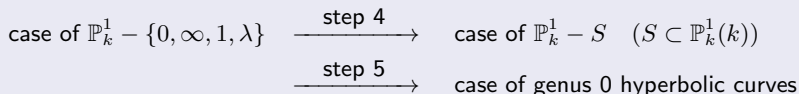
Here, $U(n), U'(n')$ are Frobenius twist of U, U'

Basic flow of the proof of Main theorem

16/26

Proof in the case of $U = \mathbb{P}_k^1 - \{0, \infty, 1, \lambda\}$ 

Proof in the case of genus 0 curves.



Rigidity invariant

Let x_1, x_2, x_3, x_4 be distinct elements of $k - \{0, 1\}$. We define the *rigidity invariant* of $\{x_1, x_2, x_3, x_4\}$ by

$$\kappa_n(x_1, x_2, x_3, x_4) := \left(\text{The fixed field of } \bigcup_H \bigcap_y p_{U/k}(H \cap D_y) \subset G_k \text{ in } k^{\text{sep}} \right).$$

Here, $y \in \tilde{X}^1 - \tilde{U}^1$ run through all closed points above x_3, x_4 , and H runs through the all open subgroups of $\Pi^{(1)}(\mathbb{P}_k^1 - \{x_1, x_2, x_3, x_4\})$ that satisfy the following conditions.

- (i) $\bar{H} := H \cap \bar{\Pi}^1$ contains all inertia groups at $\{x_3, x_4\}$.
- (ii) $\bar{\Pi}^1 / \bar{H} \cong \mathbb{Z}/n\mathbb{Z}$
- (iii) $p_{U/k}(H) = G_{k(\mu_n)}$
- (iv) $p_{U/k}^{-1}(G_{k(\mu_n)}) \triangleright H$

By definition, the rigidity invariant is defined by

$$\Pi^{(1)}(\mathbb{P}_k^1 - \{x_1, x_2, x_3, x_4\}) \rightarrow G_k \text{ and decomposition groups at cusps.}$$

Proof in the case of $U = \mathbb{P}_k^1 - \{0, \infty, 1, \lambda\}$

$$(\Pi^{(3)}(U) \rightarrow G_k) \xrightarrow{\text{step 1}} k(\langle \lambda \rangle^{\frac{1}{\ell^n}}), k(\langle 1 - \lambda \rangle^{\frac{1}{\ell^n}})$$

We can calculate rigidity invariant of $\{x_1, x_2, x_3, x_4\}$ by the following proposition.

Proposition 3.1.

$$\kappa_{\ell^n}(x_1, x_2, x_3, x_4) = k\left(\mu_{\ell^n}, \left(\frac{x_4 - x_1}{x_4 - x_2} \frac{x_3 - x_2}{x_3 - x_1}\right)^{\frac{1}{\ell^n}}\right) \quad (n \in \mathbb{N} \cup \{0\})$$

By the following calculation, we get $k(\langle \lambda \rangle^{\frac{1}{\ell^n}})$ and $k(\langle 1 - \lambda \rangle^{\frac{1}{\ell^n}})$ for all n .

- If $\{x_1, x_2, x_3, x_4\} = \{0, \infty, 1, \lambda\}$, then $\left(\frac{x_4 - x_1}{x_4 - x_2} \frac{x_3 - x_2}{x_3 - x_1}\right) = \lambda$
- If $\{x_1, x_2, x_3, x_4\} = \{\lambda, 0, \infty, 1\}$, then $\left(\frac{x_4 - x_1}{x_4 - x_2} \frac{x_3 - x_2}{x_3 - x_1}\right) = 1 - \lambda$

We can reconstruct $k^\times \supset \langle \lambda \rangle$ and $\langle 1 - \lambda \rangle$ (+Frobenius twists) from $\left\{ k(\langle \lambda \rangle^{\frac{1}{\ell^n}}) \right\}_{\ell, n}$ and $\left\{ k(\langle 1 - \lambda \rangle^{\frac{1}{\ell^n}}) \right\}_{\ell, n}$, respectively. Exactly, we can prove:

Proposition

Let $\lambda, \lambda' \in k^\times$. If $k(\langle \lambda \rangle^{\frac{1}{\ell^n}}) = k(\langle \lambda' \rangle^{\frac{1}{\ell^n}})$ for all ℓ different from p and all $n \in \mathbb{N} \cup \{0\}$, then the following hold.

- (1) If $p = 0$, then $\langle \lambda \rangle = \langle \lambda' \rangle$.
- (2) If $p \neq 0$, there exists $\sigma \in \mathbb{Z}$ such that $\langle \lambda \rangle^{p^\sigma} = \langle \lambda' \rangle$. If, moreover, $\lambda \in k^\times$ is not a torsion element, then such σ is unique.

Remark

If k is an algebraic number field, step 1 and 2 are proved in [Nakamura1][Nakamura2]. The argument can be extended to the case of that k is a finitely generated field with arbitrary characteristic.

step 3 (characteristic 0 version)

20/26

Proof in the case of $U = \mathbb{P}_k^1 - \{0, \infty, 1, \lambda\}$

$$\begin{array}{ccc}
 (\Pi^{(3)}(U) \rightarrow G_k) & \xrightarrow{\text{step 2}} & k^\times \supset \langle \lambda \rangle, \langle 1 - \lambda \rangle \text{ (+Frobenius twists)} \\
 & \xrightarrow{\text{step 3}} & \lambda \text{ (+Frobenius twists)}
 \end{array}$$

Lemma 3.2. ($p = 0$)Let $\lambda, \lambda' \in k^\times - \{1\}$. If $\langle \lambda \rangle = \langle \lambda' \rangle$ and $\langle 1 - \lambda \rangle = \langle 1 - \lambda' \rangle$ in k^\times , then

$$\lambda = \lambda' \text{ or } \{\lambda, \lambda'\} = \{\rho, \rho^{-1}\} \quad (\rho : \text{primitive 6-th root of unity})$$

Proof

Suppose $\lambda \neq \lambda'$. If either $|\lambda| \neq 1$ or $|1 - \lambda| \neq 1$, we can get a contradiction by calculation. Then $\{\lambda, \lambda'\} = \{\rho, \rho^{-1}\}$. \square

step 3 (positive characteristic version)

21/26

Lemma 3.3. ($p > 0$)

Let $\lambda, \lambda' \in k^\times - \{1\}$ be non-torsion elements and $u, v \in \mathbb{Z}$. If $\langle \lambda \rangle^{p^u} = \langle \lambda' \rangle$ and $\langle 1 - \lambda \rangle^{p^v} = \langle 1 - \lambda' \rangle$ in \bar{k}^\times , then there exists a unique $n \in \mathbb{Z}$ such that $\lambda^{p^n} = \lambda'$.

The assumption of "non-torsion" is essentially important because there exists a counterexample of Lemma 3.3 if λ is a torsion element. For example, if $p = 7$,

$$\langle 3 \rangle = \langle 1 - 5 \rangle = \langle 5 \rangle = \langle 1 - 3 \rangle = \mathbb{F}_7^\times.$$

More generally:

Counterexample

Assume that $k = \mathbb{F}_p$. Because k^\times is a cyclic group having order $p - 1$, the cardinality of subgroups of k^\times equals to the cardinality of the divisor of $p - 1$. Taking enough large p , we can get this cardinalities $\leq \sqrt{p}$ (e.g. $p = 47$). Thus, Lemma 3.3 is false in this case.

Basic flow of the proof of Main theorem

22/26

Proof in the case of $U = \mathbb{P}_k^1 - \{0, \infty, 1, \lambda\}$

$$\begin{array}{lcl}
 (\Pi^{(3)}(U) \rightarrow G_k) & \xrightarrow{\S 2} & (\Pi^{(1)}(U) \rightarrow G_k) \text{ and deco-groups at cusps} \\
 & \xrightarrow{\text{step 1}} & k(\langle \lambda \rangle^{\frac{1}{\ell^n}}), k(\langle 1 - \lambda \rangle^{\frac{1}{\ell^n}}) \\
 & \xrightarrow{\text{step 2}} & k^\times \supset \langle \lambda \rangle, \langle 1 - \lambda \rangle \text{ (+Frobenius twists)} \\
 & \xrightarrow{\text{step 3}} & \lambda \text{ (+Frobenius twists)}
 \end{array}$$

Proof in the case of genus 0 curves.

$$\begin{array}{lcl}
 \text{case of } \mathbb{P}_k^1 - \{0, \infty, 1, \lambda\} & \xrightarrow{\text{step 4}} & \text{case of } \mathbb{P}_k^1 - S \quad (S \subset \mathbb{P}_k^1(k)) \\
 & \xrightarrow{\text{step 5}} & \text{case of genus 0 hyperbolic curves}
 \end{array}$$

Result: \mathbb{P}_k^1 minus 4 points in positive characteristic

23/26

We obtain the following proposition by the discussion so far.

Proposition 3.4. (characteristic $p > 0$ version)

- k : field finitely generated over \mathbb{F}_p
- $\lambda, \lambda' \in k - (k \cap \overline{\mathbb{F}_p})$.
- $U := \mathbb{P}_k^1 - \{0, 1, \infty, \lambda\}$, $U' := \mathbb{P}_k^1 - \{0, 1, \infty, \lambda'\}$

Then

$$\Pi^{(3)}(U) \cong_{G_k} \Pi^{(3)}(U') \implies \exists n, n' \in \mathbb{N} \cup \{0\} \text{ s.t. } U(n) \cong_k U'(n')$$

Remark (isotrivial cases)

If $\lambda \in k \cap \overline{\mathbb{F}_p}$ (in other words, λ is a torsion element of k^\times), Lemma 3.3 is not true. Hence, if $\lambda \in k \cap \overline{\mathbb{F}_p}$, Proposition cannot be proved by our method, the m -step solvable GC for isotrivial curves is still open.

Result: \mathbb{P}_k^1 minus 4 points in characteristic 0

24/26

We obtain the following proposition by the discussion so far.

Proposition 3.5. (characteristic 0 version)

- k : field finitely generated over \mathbb{Q}
- $\lambda, \lambda' \in k - \{0, 1\}$.
- $U := \mathbb{P}_k^1 - \{0, 1, \infty, \lambda\}$, $U' := \mathbb{P}_k^1 - \{0, 1, \infty, \lambda'\}$

Then

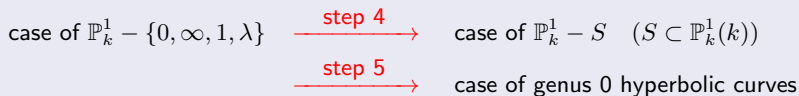
$$\Pi^{(3)}(U) \underset{G_k}{\cong} \Pi^{(3)}(U') \implies U \underset{k}{\cong} U'$$

Proof

If $\{\lambda, \lambda'\} \neq \{\rho, \rho^{-1}\}$, we reconstructed λ from $(\Pi^{(1)} \rightarrow G_k)$ and decomposition groups at cusps.

Thus, we have only to show that $\{\lambda, \lambda'\} \neq \{\rho, \rho^{-1}\}$. This step is very technical, but possible if we start from $(\Pi^{(3)} \rightarrow G_k)$. Indeed, $(\Pi^{(\text{pro-2}, 2)} \rightarrow G_k)$ and deco-groups at cusps are reconstructed from $(\Pi^{(3)} \rightarrow G_k)$. It is sufficient to show the claim. □

Proof in the case of genus 0 curves.

**Proof**

- (step 4): Reduce the case of $\mathbb{P}_k^1 - S$ ($|S| \geq 4$) to $\mathbb{P}_k^1 - \{4\text{pt}\}$ by dividing by the inertia groups. In this step, we have to assume the following assumption (cf. Lemma 3.3).

$$\forall R \subset S \text{ with } |R| = 4, \quad \mathbb{P}_k^1 - R \text{ is non-isotrivial.}$$

- (step 5): Reduce the case of genus 0 curves to $\mathbb{P}_k^1 - S$ by Galois descent. □

Setting of §3

- k : a field finitely generated over the prime field, $p := \text{ch}(k)$.
- U, U' : genus 0 hyperbolic curves over k .
- C contains $\mathbb{Z}/\ell\mathbb{Z}$ for all primes $\ell \neq p$.

So, we obtain the main result of this talk.

Main theorem

- $m \geq 3$
- If $p > 0$, we assume:

$$\forall R \subset (U_{\bar{k}})^{\text{cpt}} - U_{\bar{k}} \text{ with } |R| = 4, \quad (U_{\bar{k}})^{\text{cpt}} - R \text{ is non-isotrivial.}$$

Then the following hold.

$$\Pi^{(m)}(U) \underset{G_k}{\cong} \Pi^{(m)}(U') \implies \begin{cases} U \underset{k}{\cong} U' & p = 0 \\ \exists n, n' \in \mathbb{N} \cup \{0\} \text{ s.t. } U(n) \underset{k}{\cong} U'(n') & p > 0 \end{cases}$$