

# Reconstruction of one-punctured elliptic curves in positive characteristic by their geometric fundamental groups

Akira Sarashina

RIMS, Kyoto University

2019/03/12

# Anabelian Geometry

$k$  : a finitely generated extension field of prime fields

$U$  : a scheme  $/k$

$U$  is “anabelian”  $\Rightarrow$

the geometry of  $U$  can be recovered from  $\pi_1(U)$

If  $U$  is a smooth geometrically connected curve  $/k$ ,

$U$  is “anabelian”  $\stackrel{?}{\Leftrightarrow} U$  is hyperbolic  $\stackrel{\text{def}}{\Leftrightarrow} 2 - 2g - n < 0$

## Grothendieck conjecture for (hyperbolic) curves

$k$  : (finitely generated field  $/\mathbb{Q}$ ,  $g = 0$ )  $\rightarrow$  OK (Nakamura)

$k$  : (finite field,  $n > 0$ ) or  
(finitely generated field  $/\mathbb{Q}$ ,  $n > 0$ )  $\rightarrow$  OK (Tamagawa)

$k$  : (finite field) or  
(sub- $p$ -adic ( $k \hookrightarrow \exists L$  : fin. gen.  $/\mathbb{Q}_p$ ))  $\rightarrow$  OK (Mochizuki)

$k$  : alg. cl. field of positive characteristic  $\rightarrow$  today

$(k$  : alg. cl. field of characteristic 0  $\Rightarrow \pi_1(U) \simeq \Pi_{g,n}$ )

# Main result

## Theorem (Tamagawa)

$p, p'$ : prime numbers

$U = (\mathbb{P}^1 \setminus S) / \overline{\mathbb{F}_p}, \#S > 0$

$U'$ : a (smooth connected) curve /  $\overline{\mathbb{F}_{p'}}$

Then,

$$\pi_1(U) \simeq \pi_1(U') \Rightarrow U \simeq_{sch} U'$$

## Theorem (S.)

$p$ : an odd prime number

$p'$ : a prime number

$U = (E \setminus S) / \overline{\mathbb{F}_p}, \#S = 1 \quad (\exists E : \text{an elliptic curve} / \overline{\mathbb{F}_p})$

$U'$ : a (smooth connected) curve /  $\overline{\mathbb{F}_{p'}}$

Then,

$$\pi_1(U) \simeq \pi_1(U') \Rightarrow U \simeq_{sch} U'$$

[0]

- 1 Reconstruction of various invariants (Tamagawa)
- 2 Linear relations of the images in  $\mathbb{P}^1$
- 3 Combination of two additive structures

[0]

- 1 Reconstruction of various invariants (Tamagawa)
- 2 Linear relations of the images in  $\mathbb{P}^1$
- 3 Combination of two additive structures

# Notation

$k$  : an algebraically closed field of positive characteristic

$p$  : the characteristic of  $k$

$U$  : a smooth connected curve  $/k$

$X$  : the smooth compactification of  $U$

$g = g_U$  : the genus of  $X$

$S_U = X \setminus U$ ,  $n = n_U = \#(S_U)$

$\pi_1(U)$  : the étale fundamental group of  $U$

$\pi_1^{\text{tame}}(U)$  : the tame fundamental group of  $U$

$G^{ab}$  : the abelianization of a profinite group  $G$

$G^p$  : the maximal pro- $p$  quotient of a profinite group  $G$

$$(\lim_{H \triangleleft_{op} G, p \nmid [G:H]} G/H)$$

$G^{p'}$  : the maximal prime-to- $p$  quotient of a profinite group  $G$

$$(\lim_{H \triangleleft_{op} G, p \nmid [G:H]} G/H)$$

$r = r_U$  : the  $p$ -rank of the Jacobian variety of  $X$

(hence  $0 \leq r \leq g$ )

$$\pi_1(U) \rightsquigarrow p \text{ (if } (g, n) \neq (0, 0))$$

$$\text{Let } \epsilon = \begin{cases} 0 & (n = 0) \\ 1 & (n > 0) \end{cases}$$

Theorem (Corollary of G.A.G.A. theorems)

$$\begin{aligned} \pi_1^{(-)}(U)^{ab} \\ \simeq \begin{cases} (\hat{\mathbb{Z}}^{p'})^{\oplus 2g+n-\epsilon} \times \mathbb{Z}_p^{\oplus r} & (n = 0 \text{ or } (-) = \textit{tame}) \\ (\hat{\mathbb{Z}}^{p'})^{\oplus 2g+n-\epsilon} \times \prod_{j \in J} \mathbb{Z}_p & (n > 0 \text{ and } (-) = \textit{unrestricted}) \end{cases} \end{aligned}$$

here,  $\#J = \#k$

$l$  : prime number

$p = l \Leftrightarrow \pi_1(U)^{ab, l'}$  is a free  $\hat{\mathbb{Z}}^{l'}$ -module

$\therefore \pi_1(U) \rightsquigarrow p$



$$\pi_1(U) \rightsquigarrow \chi = 2 - 2g - n$$

$$\left( \pi_1(U)^{ab} \simeq \begin{cases} (\hat{\mathbb{Z}}^{p'})^{\oplus 2g} \times \mathbb{Z}_p^{\oplus r} & (n = 0) \\ (\hat{\mathbb{Z}}^{p'})^{\oplus 2g+n-1} \times \prod_{i \in I} \mathbb{Z}_p, \#I = \#k & (n > 0) \end{cases} \right)$$

Then,  $\epsilon = 0 \Leftrightarrow n = 0 \Leftrightarrow \pi_1(U)^{ab}$  is finitely generated  $\hat{\mathbb{Z}}$ -module

$$\therefore \pi_1(U) \rightsquigarrow \epsilon$$

$$\chi = 2 - \epsilon - \text{rank}_{\hat{\mathbb{Z}}^{p'}}(\pi_1(U)^{ab, p'})$$

$$\therefore \pi_1(U) \rightsquigarrow \chi$$

$$\pi_1(U) \rightsquigarrow r$$

By Hurwitz's formula,

$$\ker(\pi_1(U) \rightarrow \pi_1^{\text{tame}}(U)) \subset H \Leftrightarrow \chi_H = (\pi_1(U) : H)\chi$$

$$\therefore \pi_1(U) \rightsquigarrow \pi_1^{\text{tame}}(U)$$

$$r = \text{rank}_{\mathbb{Z}_p}(\pi_1^{\text{tame}}(U)^{ab,p})$$

$$\therefore \pi_1(U) \rightsquigarrow r$$

$$(\pi_1^{\text{tame}}(U)^{ab} \simeq (\hat{\mathbb{Z}}^{p'})^{\oplus 2g+n-\epsilon} \times \mathbb{Z}_p^{\oplus r})$$

$$\pi_1(U) \rightsquigarrow (g, n)$$

$$(\pi_1(U) \rightsquigarrow \epsilon)$$

$$\underline{n = 0}$$

$$g = \frac{1}{2}(2 - \chi)$$

$$\therefore \pi_1(U) \rightsquigarrow (g, n)$$

$$\pi_1(U) \rightsquigarrow (g, n)$$

$$n > 0$$

### Theorem (Deuring-Shafarevich formula)

Let  $H \triangleleft_{op} \pi_1(U)$  such that  $[\pi_1(U) : H] = p^m$ .

Then,  $r_H - 1 + n_H = (\pi_1(U) : H)(r - 1 + n)$

Clearly,  $n_H \geq n$  holds.

Thus,  $n \geq \frac{1}{p-1} \max_{H \triangleleft_{op} \pi_1(U), [\pi_1(U) : H] = p} (r_H - 1 - p(r - 1))$  holds.

Using Riemann-Roch theorem, we can prove the existence of an étale covering  $U_H \rightarrow U$  such that  $n_H = n$ .

Thus,  $n = \frac{1}{p-1} \max_{H \triangleleft_{op} \pi_1(U), [\pi_1(U) : H] = p} (r_H - 1 - p(r - 1))$  holds.

$\therefore \pi_1(U) \rightsquigarrow (g, n)$

$$\pi_1(U) \rightsquigarrow \pi_1(X)$$

By Hurwitz's formula,

$$\ker(\pi_1(U) \rightarrow \pi_1(X)) \subset H \Leftrightarrow 2g_H - 2 = (\pi_1(U) : H)(2g - 2)$$

$$\therefore \pi_1(U) \rightsquigarrow \pi_1(X)$$

## $\pi_1(U) \rightsquigarrow S_U$ (only construction)

$K$  : the function field of  $U$

$\tilde{K}$  : the maximal Galois extension of  $K$  in  $K^{sep}$  that is unr. over  $U$

$\tilde{X}$  : the normalization of  $X$  in  $\tilde{K}$

$\tilde{S}_U$  : the inverse image of  $S_U$  under  $\tilde{X} \rightarrow X$

$Sub(G)$  : the set of closed subgroups of  $G$

$I_{\tilde{P}} \in Sub(\pi_1(U))$  : the inertia subgroup associated to  $\tilde{P} \in \tilde{S}_U$

By using the discussion of the tame case and representation theory of finite groups, we can prove that  $\tilde{S}_U \rightarrow Sub(\pi_1(U))$  ( $\tilde{P} \mapsto I_{\tilde{P}}$ ) is injective and  $\pi_1(U) \rightsquigarrow Im(\tilde{S}_U \rightarrow Sub(\pi_1(U)))$ .

We can identify  $S_U$  with  $\tilde{S}_U/\pi_1(U)$ .

## Summary of this section

$$\pi_1(U) \rightsquigarrow p, g, n, \pi_1(X), S_U$$

In the situation of the main result, we see that  $U$  and  $U'$  are defined over  $\overline{\mathbb{F}_p}$  and  $(g_U, n_U) = (g_{U'}, n_{U'})$ .

$$\begin{array}{ccc} H & \xleftrightarrow{\sim} & H' \\ \downarrow op & & \downarrow op \\ \pi_1(U) & \xleftrightarrow{\sim} & \pi_1(U') \end{array} \quad \longleftrightarrow \quad \begin{array}{cc} U_H & U'_{H'} \\ \downarrow f \acute{e} t & \downarrow f \acute{e} t \\ U & U' \end{array}$$

$$\Rightarrow S_{U_H} \simeq S_{U'_{H'}}$$

[0]

- 1 Reconstruction of various invariants (Tamagawa)
- 2 Linear relations of the images in  $\mathbb{P}^1$
- 3 Combination of two additive structures



## Notation and assumptions

In this section, we assume that  $X$  is a hyperelliptic curve and  $p \neq 2$ .

$x : X \rightarrow \mathbb{P}^1$  : a finite morphism of degree 2  
with ramified points  $\lambda_0, \lambda_\infty, \lambda_1, \dots, \lambda_{2g}$

We also assume that  $x^{-1}(x(S_U)) = S_U$ ,  $\lambda_0, \lambda_\infty, \lambda_1, \dots, \lambda_{2g} \in S_U$   
and  $\{\lambda_0, \lambda_\infty, \lambda_1, \dots, \lambda_{2g}\} \neq S_U$ .

$$\begin{aligned}\varphi &: \pi_1(U) \rightarrow \pi_1(\mathbb{P}^1 \setminus x(S_U)) \\ \psi &: \pi_1(\mathbb{P}^1 \setminus x(S_U)) \rightarrow \pi_1(\mathbb{P}^1 \setminus x(S_U))^{ab, p'} \\ L_U &= \ker(\psi \circ \varphi)\end{aligned}$$

$$(\pi_1(U), L_U) \rightsquigarrow x(S_U)$$

For each  $\mu \in S_U$  and  $P \in x(S_U)$ , we fix  $\tilde{\mu} \in \tilde{S}_U$  above  $\mu$  and  $\tilde{P} \in \tilde{S}_U$  above  $P$  respectively.

( $\tilde{X}$  = the normalization of  $\mathbb{P}^1$  in  $\tilde{K}$ )

By G.A.G.A. theorems, if  $x(\mu) = P$ ,

$$(\psi \circ \varphi)(l_{\tilde{\mu}}) = \begin{cases} \psi(l_{\tilde{P}}) & (x \text{ is unramified at } \lambda) \\ 2\psi(l_{\tilde{P}}) & (x \text{ is ramified at } \lambda) \end{cases}$$

Thus, for any  $\mu$  and  $\nu \in S_U$ ,

$$\mu \sim \nu \stackrel{\text{def}}{\Leftrightarrow} x(\mu) = x(\nu) \Leftrightarrow$$

$$(l_{\tilde{\mu}} L_U) / L_U = (\psi \circ \varphi)(l_{\tilde{\mu}}) = (\psi \circ \varphi)(l_{\tilde{\nu}}) = (l_{\tilde{\nu}} L_U) / L_U$$

We can identify  $x(S_U)$  with  $S_U / \sim$ .

$$\therefore (\pi_1(U), L_U) \rightsquigarrow x(S_U)$$

## Additive structure on $\mathbb{P}^1(k) \setminus \{P_\infty\}$ ass. to $P_0$ and $P_\infty$

Fix  $P_0$  and  $P_\infty \in \mathbb{P}^1(k)$  s.t.  $P_0 \neq P_\infty$ . Let  $\phi : \mathbb{P}^1 \simeq \mathbb{P}^1$  be a  $k$ -isomorphism such that  $\phi(P_0) = 0$  and  $\phi(P_\infty) = \infty$ .

Then the bijection  $\mathbb{P}^1(k) \setminus \{P_\infty\} \simeq \mathbb{P}^1(k) \setminus \{\infty\} = k$  does not depend on the choice of  $\phi$  up to scalar multiplication.

Then the additive str. on  $k$  induces one on  $\mathbb{P}^1(k) \setminus \{P_\infty\}$

Thus, we can define a linear relation of  $x(S_U) \setminus \{x(\lambda_\infty)\}$  ass. to  $x(\lambda_0)$  and  $x(\lambda_\infty)$

$$\sum_{P \in x(S_U) \setminus \{x(\lambda_\infty)\}, a_P \in \mathbb{F}_p} a_P P = 0$$

$$(\pi_1(U), L_U) \rightsquigarrow \sum_{P \in X(S_U) \setminus \{X(\lambda_\infty)\}, a_P \in \mathbb{F}_p} a_P P = 0 \text{ or not (sketch)}$$

Step 1(construct a suitable covering)

Let  $\tilde{a}_P \in \{0, 1, \dots, p-1\} \subset \mathbb{Z}$  s.t.  $\tilde{a}_P \bmod p = a_P$ ,  $s = \sum_P \tilde{a}_P$   
 and  $H \triangleleft_{op} \pi_1(U)$  the open normal subgroup of  $\pi_1(U)$

corresponding to the Kummer covering defined by

$$y^{p-1} = (x - P_0)^{s-1} \prod_{P \in X(S_U) \setminus \{P_0, P_\infty\}} (x - P)^{-\tilde{a}_P}$$

exponent of poly.  $\leftrightarrow$  ramification index  $\leftrightarrow$  index of inertia subgp.

$$\therefore (\pi_1(U), L_U) \rightsquigarrow H$$

$$(\pi_1(U), L_U) \rightsquigarrow \sum_{P \in X(S_U) \setminus \{x(\lambda_\infty)\}, a_P \in \mathbb{F}_p} a_P P = 0 \text{ or not (sketch)}$$

## Step 2

By Artin-Schreier theory,

$$\begin{aligned} \text{Hom}(\pi_1(X_H)^{ab}/p, \mathbb{F}_p) &= \text{Hom}_{\text{conti}}(\pi_1(X_H), \mathbb{F}_p) = H_{\text{et}}^1(X_H, \mathbb{F}_p) \\ &= H^1(X_H, \mathcal{O}_{X_H})[F - 1] \end{aligned}$$

Thus,  $(\pi_1(U), L_U) \rightsquigarrow (H^1(X_H, \mathcal{O}_{X_H})[F - 1] = 0 \text{ or not})$

By calculating the Frobenius map  $F$  and using the defining equation of  $X_H$ , we see that the vanishing of (a part of)  $H^1(X_H, \mathcal{O}_{X_H})[F - 1]$  is equivalent to the linear relation.

$\therefore (\pi_1(U), L_U) \rightsquigarrow \sum_{P \in X(S_U) \setminus \{x(\lambda_\infty)\}, a_P \in \mathbb{F}_p} a_P P = 0 \text{ or not}$

## Summary of this section

$$(\pi_1(U), L_U) \rightsquigarrow x(S_U), \quad \sum_{P \in x(S_U) \setminus \{x(\lambda_\infty)\}, a_P \in \mathbb{F}_p} a_P P = 0$$

If we have the following diagram.

$$\begin{array}{ccc}
 L_{U_H} & \xleftrightarrow{\sim} & L_{U'_{H'}} \\
 \downarrow \text{hook} & & \downarrow \text{hook} \\
 H & \xleftrightarrow{\sim} & H' \\
 \downarrow \text{op} & & \downarrow \text{op} \\
 \pi_1(U) & \xleftrightarrow{\sim} & \pi_1(U')
 \end{array}
 \quad \longleftrightarrow \quad
 \begin{array}{ccc}
 \mathbb{P}^1 & & \mathbb{P}^1 \\
 \swarrow x & & \swarrow x' \\
 U_H & & U'_{H'} \\
 \downarrow f \text{ét} & & \downarrow f \text{ét} \\
 U & & U'
 \end{array}$$

We obtain  $\sigma : x(S_{U_H}) \simeq x'(S_{U'_{H'}})$  and see that

$$\begin{aligned}
 & \sum_{P \in x(S_U) \setminus \{x(\lambda_\infty)\}, a_P \in \mathbb{F}_p} a_P P = 0 \\
 \Leftrightarrow & \sum_{P \in x(S_U) \setminus \{x(\lambda_\infty)\}, a_P \in \mathbb{F}_p} a_P \sigma(P) = 0
 \end{aligned}$$

[0]

- 1 Reconstruction of various invariants (Tamagawa)
- 2 Linear relations of the images in  $\mathbb{P}^1$
- 3 Combination of two additive structures

## Notation and assumptions

In this section, we assume that  $k \simeq \overline{\mathbb{F}_p}$ ,  $g = 1$  and  $\#(X \setminus U) = 1$ .  
Let  $\{\mathcal{O}\} = X \setminus U$ .



$$\pi_1(X \setminus \{\mathcal{O}\}) \rightsquigarrow \pi_1(X \setminus X[m])$$

$$\begin{aligned} \pi_1(X \setminus X[m]) &\simeq \ker(\pi_1(X \setminus \{\mathcal{O}\}) \rightarrow \pi_1(X) \rightarrow \pi_1(X)/m) \\ \therefore \pi_1(X \setminus \{\mathcal{O}\}) &\rightsquigarrow \pi_1(X \setminus X[m]) \end{aligned}$$

$\pi_1(X \setminus \{\mathcal{O}\}) \rightsquigarrow X[m]$  with a group structure

We already know  $\pi_1(X \setminus \{\mathcal{O}\}) \rightsquigarrow \pi_1(X \setminus X[m]) \rightsquigarrow X[m]$

Fix  $\mathcal{P} \in X[m]$

The action of  $\pi_1(X \setminus \{\mathcal{O}\}) / \pi_1(X \setminus X[m]) (\simeq X[m])$  on  $X[m]$  defines the group structure on  $X[m]$  with identity  $\mathcal{P}$

$\therefore \pi_1(X \setminus \{\mathcal{O}\}) \rightsquigarrow X[m]$  with a group structure

## Lemma

$$\pi_1(X \setminus \{\mathcal{O}\}) \rightsquigarrow L_{X \setminus X[m]} (\subset \pi_1(X \setminus X[m]))$$

$$\begin{aligned} & (\pi_1(X \setminus X[m]), L_{X \setminus X[m]}) \\ & \rightsquigarrow x(X[m]), \text{ linear relations of } x(X[m]) \setminus \{x(\lambda_\infty)\} \end{aligned}$$

$$\begin{array}{ccc} X[m] & \xleftarrow{\sim} & X'[m] \\ \downarrow & & \downarrow \\ x(X[m]) & \xleftarrow{\sim} & x'(X'[m]) \end{array}$$

$$(\text{here, } \pi_1(X \setminus \{\mathcal{O}\}) \simeq \pi_1(X' \setminus \{\mathcal{O}'\}))$$

## Reconstruction of $\lambda$ invariants

Assume  $X$  (resp.  $X'$ ) is defined by  $y^2 = x(x-1)(x-\lambda)$   
 (resp.  $y^2 = x(x-1)(x-\lambda')$ ),  $\mathcal{O} = \infty$  (resp.  $\mathcal{O}' = \infty$ )  
 (and  $\pi_1(X \setminus \{\mathcal{O}\}) \simeq \pi_1(X' \setminus \{\mathcal{O}'\})$ ).

Let  $f$  (resp.  $f'$ )  $\in \mathbb{F}_p[T]$  be the minimal polynomial of  $\lambda$  (resp.  $\lambda'$ ).

By taking suitable  $m$ , we can assume that

$$(1, 0), (\lambda, 0), (\lambda^2, *_{\lambda^2}), \dots, (\lambda^{\deg(f)}, *_{\lambda^{\deg(f)}}) \in X[m]$$

$$\text{(here, } (*_{\nu})^2 = \nu(\nu-1)(\nu-\lambda))$$

and

$$X[m] \xleftarrow{\sim} X'[m]$$

$$(0, 0) \longleftrightarrow (0, 0)$$

$$(1, 0) \longleftrightarrow (1, 0)$$

$$(\lambda, 0) \longleftrightarrow (\lambda', 0)$$

$$\infty \longleftrightarrow \infty$$

## Reconstruction of $\lambda$ invariants

$$\pi_1(X \setminus \{\mathcal{O}\}) \rightsquigarrow \begin{cases} \sum_{P \in x(X[m]) \setminus \{x(\infty)\}, a_P \in \mathbb{F}_p} a_P P = 0 \\ \text{group structure of } X[m] \end{cases}$$

By the addition law of elliptic curves,

- $x((\lambda^i, *_{\lambda^i}) + (\lambda^i + 1, *_{\lambda^{i+1}})) + x((-\lambda^i, *_{-\lambda^i}) - \dots$   
 $= -8\lambda^{2i+1} + 4\lambda^{2i} + 4\lambda$
- $x((\lambda^i, *_{\lambda^i}) + (\lambda^i + 1, *_{\lambda^{i+1}})) + x((\lambda^i, *_{\lambda^i}) + (\lambda^i - 1, *_{\lambda^{i-1}})) - \dots$   
 $= 12\lambda^{2i} - 8\lambda^{i+1} - 8\lambda^i + 4\lambda$

$$x(X[m]) \longleftrightarrow x'(X'[m])$$

$$1 \longleftrightarrow 1$$

$$\lambda \longleftrightarrow \lambda'$$

$$\lambda^2 \longleftrightarrow \lambda'^2$$

$\vdots$

## Reconstruction of $\lambda$ invariants

We can regard  $f(\lambda)$  as a linear relation of  $1, \lambda, \lambda^2, \dots, \lambda^{\deg(f)} / \mathbb{F}_p$

$$\therefore f(\lambda) = 0 \Leftrightarrow f(\lambda') = 0$$

$$\therefore f = f'$$

There is an isom  $\alpha : \overline{\mathbb{F}_p} \simeq \overline{\mathbb{F}_p}$  s.t.  $\alpha(\lambda) = \lambda'$

$$\therefore X \setminus \{\mathcal{O}\} \simeq (X \setminus \{\mathcal{O}\}) \times_{\overline{\mathbb{F}_p}, \alpha} \overline{\mathbb{F}_p} = X' \setminus \{\mathcal{O}'\}$$



Thank you for your attention!