

# GLOBAL SOLVABLY CLOSED ANABELIAN GEOMETRY

SHINICHI MOCHIZUKI

February 2006

ABSTRACT. In this paper, we study the *pro- $\Sigma$  anabelian geometry of hyperbolic curves*, where  $\Sigma$  is a nonempty set of prime numbers, over Galois groups of “*solvably closed extensions*” of number fields — i.e., infinite extensions of number fields which have no nontrivial abelian extensions. The main results of this paper are, in essence, immediate corollaries of the following three ingredients: (a) classical results concerning the structure of Galois groups of number fields; (b) an anabelian result of Uchida concerning Galois groups of solvably closed extensions of number fields; (c) a previous result of the author concerning the *pro- $\Sigma$  anabelian geometry of hyperbolic curves over nonarchimedean local fields*.

## Contents:

- §1. Basic Properties
- §2. Anabelian Results
- §3. Some Examples

## Introduction

In this paper, we study various properties of *solvably closed Galois groups of number fields*, i.e., Galois groups of field extensions of number fields that admit no nontrivial abelian field extensions [cf. Definition 1.1, (i)]. In §1, we show that such Galois groups satisfy many of the properties of *absolute Galois groups* of number fields that are of importance in the context of *anabelian geometry*. In particular, this includes properties concerning *Galois cohomology*, *center-free-ness*, *decomposition groups* of valuations, and *topologically finitely generated closed normal subgroups*. In §2, after reviewing a fundamental result of Uchida [cf. [Uchida]] to the effect that solvably closed Galois groups of number fields are *anabelian*, we apply the various results obtained in §1 to give a new version of the main result of [Mzk2] concerning the *pro- $\Sigma$  anabelian geometry of hyperbolic curves*, where  $\Sigma$  is a nonempty set of prime numbers, in the context of solvably closed Galois groups of number fields. Finally, in §3, we observe that “*relatively small*” solvably closed Galois groups of number fields exist in “*substantial abundance*”. For instance, in the case of

---

2000 *Mathematical Subject Classification*. Primary 14H30; Secondary 11R99.

*punctured elliptic curves*, it is possible in many instances to obtain solvably closed Galois groups of number fields that are, on the one hand, “*large enough*” to be *compatible* with the outer action on the pro- $\Sigma$  geometric fundamental group of the punctured elliptic curve, but, on the other hand, “*small enough*” to be *linearly disjoint* from various field extensions arising from the *l-torsion points* of the elliptic curve, for a prime number  $l \notin \Sigma$ .

### Acknowledgements:

The author wishes like to thank *Akio Tamagawa* for bringing the results exposed in Theorems 1.5, 2.1 of the text to his attention.

## Section 1: Basic Properties

We begin by defining the notion of a *solvably closed Galois group of a number field* and showing that such Galois groups satisfy many properties that are well-known in the case of absolute Galois groups of number fields.

Let  $F$  be a *number field* [i.e., a finite extension of the field of rational numbers],  $\overline{F}$  an *algebraic closure* of  $F$ , and  $\tilde{F} \subseteq \overline{F}$  a [not necessarily finite!] *Galois extension* of  $F$ . Write  $G_F \stackrel{\text{def}}{=} \text{Gal}(\overline{F}/F)$ ,  $Q_F \stackrel{\text{def}}{=} \text{Gal}(\tilde{F}/F)$ . Thus, one may think of  $Q_F$  as a *quotient*  $G_F \twoheadrightarrow Q_F$  of  $G_F$ .

### Definition 1.1.

(i) We shall say that a field is *solvably closed* if it has no nontrivial abelian extensions. If  $\tilde{F}$  is solvably closed, then we shall say that  $\tilde{F}/F$  is a *solvably closed extension* and refer to  $Q_F$  as a *solvably closed Galois group* of the number field  $F$ .

(ii) If  $G$  is any *profinite group*, and  $p$  is a prime number, then we shall write

$$\text{cd}_p(G)$$

for the smallest positive integer  $i$  such that  $H^j(G, A) = 0$  for all continuous  $p$ -torsion  $G$ -modules  $A$  and all  $j > i$ , if such an integer  $i$  exists; if such an integer  $i$  does not exist, then we set  $\text{cd}_p(G) \stackrel{\text{def}}{=} \infty$  [cf. [NSW], Definition 3.3.1].

**Remark 1.1.1.** Observe that the Galois group  $Q_F$  is *solvably closed* if and only if, for any open subgroup  $H_Q \subseteq Q_F$ , whose inverse image in  $G_F$  we denote by  $H_G \subseteq G_F$ , the surjection induced on *maximal pro-solvable quotients*

$$H_G^{\text{sol}} \twoheadrightarrow H_Q^{\text{sol}}$$

by the quotient morphism  $H_G \twoheadrightarrow H_Q$  is an isomorphism.

**Remark 1.1.2.** Thus, if we denote by  $\tilde{F}^{\text{sol}} \subseteq \overline{F}$  the *maximal solvable [Galois] extension* of  $\tilde{F}$ , then one verifies immediately that  $\text{Gal}(\tilde{F}^{\text{sol}}/F)$  is a *solvably closed Galois group* of the number field  $F$ . In particular, [by taking  $\tilde{F} = F$ , it follows that] the *maximal pro-solvable quotient*  $G_F^{\text{sol}}$  of  $G_F$  is a *solvably closed Galois group* of the number field  $F$ .

**Remark 1.1.3.** One verifies immediately that any *open subgroup of a solvably closed Galois group of a number field* is again a solvably closed Galois group of a number field.

**Proposition 1.2. (Galois Cohomology of Solvably Closed Galois Groups)**  
*Suppose that  $Q_F$  is a solvably closed Galois group of the number field  $F$ . Then:*

(i) *The natural surjection  $G_F \twoheadrightarrow Q_F$  induces an isomorphism*

$$H^i(Q_F, A) \xrightarrow{\sim} H^i(G_F, A)$$

for all continuous torsion  $Q_F$ -modules  $A$  and all integers  $i \geq 0$ . In particular, if  $F$  contains a **square root of  $-1$** , then  $\text{cd}_p(Q_F) = 2$  for all prime numbers  $p$ .

(ii) *Let  $p$  be a prime number; suppose that  $F$  contains a **primitive  $p$ -th root of unity**. Then for any automorphism  $\sigma$  of the field  $\tilde{F}$  that preserves and acts **nontrivially** on  $F \subseteq \tilde{F}$ , the automorphism induced by  $\sigma$  of the set of **one-dimensional  $\mathbb{F}_p$ -subspaces** of the  $\mathbb{F}_p$ -vector space*

$$H^2(Q_F, \mathbb{F}_p)$$

*is nontrivial.*

*Proof.* First, we consider assertion (i). Write  $J_F \stackrel{\text{def}}{=} \text{Ker}(G_F \twoheadrightarrow Q_F)$ . To show the desired isomorphism, it follows immediately from the Leray-Serre spectral sequence associated to the extension  $1 \rightarrow J_F \rightarrow G_F \rightarrow Q_F \rightarrow 1$  that it suffices to show that  $H^i(J_F, A) = 0$  for all  $i \geq 1$ . Since

$$H^i(J_F, A) \cong \varinjlim_{J_F \subseteq H \subseteq G_F} H^i(H, A)$$

[where  $H$  ranges over the open subgroups of  $G_F$  containing  $J_F$ ], we thus conclude the desired vanishing as follows: If  $i \geq 3$ , then the fact that  $H^i(H, A) = 0$  follows from the fact that  $\text{cd}_p(H) \leq 2$ , for  $H$  sufficiently small [i.e.,  $H$  that correspond to totally imaginary extensions of  $F$  — cf. [NSW], Proposition 8.3.17]. If  $i = 2$ , then we recall that by the well-known “*Hasse Principle for central simple algebras*” [cf., e.g., [NSW], Corollary 8.1.16; the discussion of [NSW], §7.1], it follows that we have an *exact sequence*

$$0 \rightarrow H^2(G_F, \mathbb{F}_p(1)) \rightarrow \bigoplus_v H^2(G_v, \mathbb{F}_p(1)) \rightarrow \mathbb{F}_p \rightarrow 0$$

where the “(1)” denotes a “*Tate twist*”;  $v$  ranges over the valuations of  $F$ ;  $G_v$  denotes the decomposition group of  $v$  in  $G_F$ , which is well-defined up to conjugation; and we recall in passing that the restriction to the various direct summands of the map to  $\mathbb{F}_p$  induces an *isomorphism*  $H^2(G_v, \mathbb{F}_p(1)) \cong \mathbb{F}_p$  for all nonarchimedean  $v$ . Thus, by applying the analogue for  $H$  of this exact sequence for  $G_F$ , together with the *Grunwald-Wang Theorem* [which assures the existence of global abelian field extensions with prescribed behavior at a finite number of valuations — cf., e.g., [NSW], Corollary 9.2.3], we conclude immediately that  $\varinjlim_H H^2(H, A) = 0$ . When  $i = 1$ , the fact that  $\varinjlim_H H^1(H, A)$  follows formally from the definition of a “*solvably closed*” Galois group [cf. Definition 1.1, (i)]. Now the statement concerning  $\text{cd}_p(Q_F)$  follows immediately from the isomorphism just verified, together with the fact that, if  $F$  contains a *square root of  $-1$*  [hence is *totally imaginary*], then  $\text{cd}_p(G_F) = 2$  [cf. [NSW], Proposition 8.3.17; the exact sequence just discussed concerning  $H^2(G_F, \mathbb{F}_p(1))$ ]. This completes the proof of assertion (i).

Finally, we observe that assertion (ii) follows immediately from the exact sequence just discussed concerning

$$H^2(G_F, \mathbb{F}_p(1)) \cong H^2(Q_F, \mathbb{F}_p(1)) \cong H^2(Q_F, \mathbb{F}_p)$$

[cf. assertion (i); our assumption that  $F$  contains a *primitive  $p$ -th root of unity*], together with *Tchebotarev’s density theorem* [cf., e.g., [Lang], Chapter VIII, §4, Theorem 10], which implies that if we write  $F_0 \subseteq F$  for the subfield fixed by  $\sigma$ , then there exist *two distinct* nonarchimedean valuations  $v_1, v_2$  of  $F_0$  that *split completely* in  $F$ . That is to say, if  $w_1, w_2$  are valuations of  $F$  lying over  $v_1, v_2$ , respectively, then there exists an element  $h \in H^2(Q_F, \mathbb{F}_p) \cong H^2(G_F, \mathbb{F}_p(1))$  [where we note that this isomorphism is *compatible* with the natural actions by  $\sigma$ , up to multiplication by an element of  $\mathbb{F}_p^\times$ ] which maps to a nonzero element of the direct sum in the above sequence whose unique nonzero components are the components labeled by  $v_1, v_2$ ; thus,  $\sigma(\mathbb{F}_p \cdot h) \neq \mathbb{F}_p \cdot h$ , as desired.  $\circ$

Before proceeding, we recall that a profinite group  $\Delta$  is *slim* if every open subgroup of  $\Delta$  has *trivial centralizer* in  $\Delta$  [cf. [Mzk1], Definition 0.1, (i)].

**Corollary 1.3.** (Slimness) *Every solvably closed Galois group of a number field is slim.*

*Proof.* Suppose that  $Q_F$  is *solvably closed*. Let  $H_Q \subseteq Q_F$  be an *open subgroup*,  $\sigma \in Q_F$  an element of the *centralizer* of  $H_Q$ . Write  $F_H \subseteq \tilde{F}$  for the extension of  $F$  defined by  $H_Q$ . Since  $Q_F$  is *solvably closed*, by taking  $H_Q$  to be *sufficiently small*, we may assume that  $F_H$  contains a  $p$ -th root of unity, for some prime number  $p$ . Note that since  $\sigma$  *commutes* with  $H_Q$ , it follows that  $\sigma$  acts *trivially* on  $H^2(H_Q, \mathbb{F}_p)$ . Thus, by applying Proposition 1.2, (ii), to the action of  $\sigma$  on  $\tilde{F}/F_H$ , we conclude that  $\sigma$  acts trivially on  $F_H$ , i.e., that  $\sigma \in H_Q$ . On the other hand, since  $H_Q$  may be taken to be arbitrarily small, it thus follows that  $\sigma = 1$ , as desired.  $\circ$

The next two results, concerning *decomposition groups* and *topologically finitely generated closed normal subgroups*, respectively, are well-known in the case of *absolute Galois groups* [cf., e.g., [NSW], Corollary 12.1.3; [FJ], Proposition 16.11.6].

**Proposition 1.4. (Decomposition Groups)** *Suppose that  $Q_F$  is a solvably closed Galois group of the number field  $F$ . Let  $v, w$  be valuations of  $F$  such that  $v \neq w$ ; write  $G_v, G_w \subseteq Q_F$  for the corresponding decomposition groups [which are well-defined up to conjugation] in  $Q_F$  and  $F_v, F_w$  for the corresponding completions of  $F$ . Then:*

(i) *Suppose that  $F$  contains a square root of  $-1$ , and that  $v, w$  are nonarchimedean; let  $K$  be a finite extension of  $F_v$ . Then there exists a finite Galois extension of  $F$  contained in  $\tilde{F}$  whose restriction to  $F_v$  contains  $K$  and whose restriction to  $F_w$  is the trivial extension.*

(ii) *Suppose that  $v, w$  are archimedean; let  $K$  be a nontrivial finite extension of  $F_v$ . Then there exists a quadratic extension of  $F$  contained in  $\tilde{F}$  whose restriction to  $F_v$  contains  $K$  and whose restriction to  $F_w$  is the trivial extension.*

(iii) *The surjection  $G_F \rightarrow Q_F$  induces an isomorphism of  $G_v$  with the decomposition group of  $v$  in  $G_F$ . In particular, if  $v$  is nonarchimedean, then  $G_v$  is slim and torsion-free.*

$$(iv) \quad G_v \cap G_w = \{1\}.$$

(v) *Suppose that  $v$  is archimedean (respectively, nonarchimedean). Then the normalizer (respectively, commensurator) of  $G_v$  in  $Q_F$  is equal to  $G_v$ .*

*Proof.* First, we consider assertion (i). Since the absolute Galois group of  $F_v$  is *pro-solvable* [cf., e.g., [NSW], Chapter VII, §5], we may assume, by recursion, that  $K$  is an *abelian extension* of  $F_v$ . Since, moreover,  $F$  contains a square root of  $-1$ , it follows that we may apply the *Grunwald-Wang Theorem* [cf., e.g., [NSW], Corollary 9.2.3] to  $F$ . Now assertion (i) follows immediately by applying the Grunwald-Wang Theorem to  $F$ . Assertion (ii) follows by considering the quadratic extension of  $F$  determined by taking the square root of an element  $f \in F$  which is  $< 0$  at  $v$  and either  $> 0$  or nonreal at  $w$  [where we note that the *existence* of such an  $f$  follows immediately from the fact that the valuations  $v, w$  are *distinct*]. In the *nonarchimedean* case, assertion (iii) follows formally from assertion (i), together with the well-known facts that the absolute Galois group of a nonarchimedean local field is *slim* [cf., e.g., [Mzk1], Theorem 1.1.1, (ii)] and [of *finite cohomological dimension* — cf., e.g., [NSW], Corollary 7.2.5 — hence] *torsion-free*. In the *archimedean* case, assertion (iii) follows, for instance, by considering the extension of  $F$  obtained by adjoining a square root of  $-1$ . To verify assertion (iv), let us first observe that if at least one of  $v, w$  is *nonarchimedean*, then it follows from the *torsion-free-ness* portion of assertion (iii) that both  $v, w$  are *nonarchimedean* [cf. also the well-known fact that the absolute Galois group of an *archimedean* local field is finite, of order  $\leq 2!$ ], and, moreover, that [from the point of view of verifying assertion (iv)]

one may replace  $F$  by a finite abelian extension of  $F$  that satisfies the hypothesis of assertion (i). Now assertion (iv) follows immediately from assertions (i), (ii), (iii). Finally, assertion (v) follows formally from assertion (iv) [together with the *torsion-free-ness* portion of assertion (iii) in the *nonarchimedean* case].  $\circ$

**Theorem 1.5. (Topologically Finitely Generated Closed Normal Subgroups)** *Suppose that  $\tilde{F}$  is a Galois extension of the number field  $F$  such that for some prime number  $p$ ,  $\tilde{F}$  has no cyclic extensions of degree  $p$  [e.g., a solvably closed extension of  $F$ ]. Then every topologically finitely generated closed normal subgroup  $N \subseteq Q_F$  is trivial.*

*Proof.* Although this fact only follows formally from the statement of [FJ], Proposition 16.11.6, in the case where  $\tilde{F}$  is algebraically closed, as was explained to the author by A. Tamagawa, the proof given in [FJ] generalizes immediately to the case of arbitrary  $\tilde{F}$  [i.e., as in the statement of Theorem 1.5]: Indeed, if we write  $L \subseteq \tilde{F}$  for the Galois [since  $N$  is normal] field extension of  $F$  determined by  $N$ , and assume that  $N$  is *nontrivial*, then it follows that there exists a *proper* normal open subgroup  $N_1 \subseteq N$  of  $N$ . Thus,  $N_1$  determines a finite Galois extension  $L_1/L$  of degree  $> 1$ . But, by [FJ], Theorem 13.9.1, (b) [i.e., “Weissauer’s extension theorem for Hilbertian fields”], this implies that  $L_1$  is *Hilbertian*, hence, by [repeated application of] [FJ], Theorem 16.11.2, that  $L_1$  admits Galois extensions with Galois group isomorphic to a product of an arbitrary finite number of copies of  $\mathbb{Z}/p\mathbb{Z}$ . By our assumption on  $\tilde{F}$ , it follows that such Galois extensions of  $L_1$  are contained in  $\tilde{F}$ , hence that  $N_1$  admits finite quotients isomorphic to a product of an arbitrary finite number of copies of  $\mathbb{Z}/p\mathbb{Z}$ . But this contradicts the assumption that  $N$  is *topologically finitely generated*.  $\circ$

## Section 2: Anabelian Results

Next, we consider the *anabelian geometry of hyperbolic curves*, in the context of *solvably closed Galois groups of number fields*.

The following result is due to K. Uchida [cf. the main theorem of [Uchida]]:

**Theorem 2.1. (Solvably Closed Galois Groups are Anabelian)** *For  $i = 1, 2$ , let  $\tilde{F}_i/F_i$  be a solvably closed extension of a number field  $F_i$ ; write  $Q_i \stackrel{\text{def}}{=} \text{Gal}(\tilde{F}_i/F_i)$ . Then passing to the induced morphism on Galois groups determines a bijection between the set of isomorphisms of topological groups*

$$Q_1 \xrightarrow{\sim} Q_2$$

*and the set of isomorphisms of fields  $\tilde{F}_1 \xrightarrow{\sim} \tilde{F}_2$  that map  $F_1$  onto  $F_2$ .*

Next, let us assume that we have been given a *hyperbolic curve* [cf., e.g., [Mzk1], §0, for a discussion of hyperbolic curves] over  $F$ . Let  $\Sigma$  be a *nonempty set of prime numbers*. Write

$$\Delta_X$$

for the *maximal pro- $\Sigma$  quotient* of the geometric fundamental group  $\pi_1(X \times_F \overline{F})$  of  $X$  [relative to some basepoint]. Here, we note in passing that  $\Sigma$  *may be recovered from*  $\Delta_X$  as the set of prime numbers that occur as factors of orders of finite quotients of  $\Delta_X$ . Thus, one has a *natural outer action*

$$G_F \rightarrow \text{Out}(\Delta_X)$$

of  $G_F$  on  $\Delta_X$ .

**Lemma 2.2.** (Slimness)  $\Delta_X$  is slim.

*Proof.* This follows immediately by considering Galois actions on abelianizations of open subgroups of  $\Delta_X$  — cf. the proof of [Mzk1], Lemma 1.3.1, in the case where  $\Sigma$  is the set of all prime numbers.  $\circ$

**Definition 2.3.** We shall say that the [not necessarily solvably closed!] extension  $\tilde{F}/F$ , or, alternatively, the Galois group  $Q_F$ , is  $\Sigma$ -compatible with  $X$  if the natural outer action

$$G_F \rightarrow \text{Out}(\Delta_X)$$

factors through the quotient  $G_F \twoheadrightarrow Q_F$ . Thus, if  $Q_F$  is  $\Sigma$ -compatible with  $X$ , then one obtains an *exact sequence of profinite groups*

$$1 \rightarrow \Delta_X \rightarrow \Pi_X \rightarrow Q_F \rightarrow 1$$

by taking  $\Pi_X \stackrel{\text{def}}{=} \text{Aut}(\Delta_X) \times_{\text{Out}(\Delta_X)} Q_F$  [cf. Lemma 2.2!].

**Proposition 2.4.** (Geometric Subgroups are Characteristic) For  $i = 1, 2$ , let  $\tilde{F}_i/F_i$  be a **solvably closed extension** of a number field  $F_i$ ;  $Q_i \stackrel{\text{def}}{=} \text{Gal}(\tilde{F}_i/F_i)$ ;  $\Sigma_i$  a *nonempty set of prime numbers*;  $X_i$  a **hyperbolic curve** over  $F_i$  with which  $Q_i$  is  $\Sigma_i$ -compatible;  $1 \rightarrow \Delta_{X_i} \rightarrow \Pi_{X_i} \rightarrow Q_i \rightarrow 1$  the resulting exact sequence of profinite groups [cf. Definition 2.3]. Then any **isomorphism of topological groups**

$$\Pi_{X_1} \xrightarrow{\sim} \Pi_{X_2}$$

maps  $\Delta_{X_1}$  isomorphically onto  $\Delta_{X_2}$ . In particular,  $\Sigma_1 = \Sigma_2$ .

*Proof.* We give *two proofs* of Proposition 2.4. The *first proof* consists of simply observing [cf. the proof of [Mzk1], Lemma 1.1.4, (i), via [Mzk1], Theorem 1.1.2] that the image of  $\Delta_{X_1}$  under the composite of the isomorphism  $\Pi_{X_1} \xrightarrow{\sim} \Pi_{X_2}$  with

the surjection  $\Pi_{X_2} \twoheadrightarrow Q_2$  forms a *topologically finitely generated closed normal subgroup* of  $Q_2$ , hence is *trivial*, by Theorem 1.5.

The *second proof* of Proposition 2.4 only uses Theorem 1.5 in the well-known case of an *absolute Galois group* of a number field. Moreover, when either  $\Sigma_1$  or  $\Sigma_2$  is *not* equal to the set of *all prime numbers*, then this second proof does not use Theorem 1.5 *at all*.

For  $i = 1, 2$ , let  $H_i \subseteq \Pi_{X_i}$  be corresponding normal open subgroups; write  $H_i \twoheadrightarrow J_i$  for the quotients determined by the quotients  $\Pi_{X_i} \twoheadrightarrow Q_i$ . By taking the  $H_i$  to be *sufficiently small*, we may also assume that the number fields determined by the  $J_i$  contain *square roots of  $-1$* . Thus, by Proposition 1.2, (i), it follows that

$$\mathrm{cd}_p(H_i) = 2 + d(p, i)$$

where  $d(p, i)$  is equal to 1 or 2 [depending on whether  $X_i$  is *affine* or *proper*] if  $p \in \Sigma_i$  and  $d(p, i) = 0$  if  $p \notin \Sigma_i$ . Since  $H_1 \xrightarrow{\sim} H_2$ , we thus conclude that  $\Sigma_1 = \Sigma_2$ , and that  $X_1$  is affine if and only if  $X_2$  is. Now if  $\Sigma_1 = \Sigma_2$  is the set of *all prime numbers*, and  $X_1, X_2$  are *affine*, then it follows from *Matsumoto's injectivity theorem* [cf. [Mtm0], Theorem 2.1] that the field  $\tilde{F}_i$  is an *algebraic closure* of  $F_i$ ; thus, in this case, Proposition 2.4 follows from [Mzk1], Lemma 1.1.4, (i) [i.e., Theorem 1.5 for absolute Galois groups of number fields].

Next, let us suppose that there exists a *prime number*  $p$  such that  $p \notin \Sigma_1$ ,  $p \notin \Sigma_2$ . This implies that, for  $i = 1, 2$ , the natural homomorphism

$$H^2(J_i, \mathbb{F}_p) \rightarrow H^2(H_i, \mathbb{F}_p)$$

is an *isomorphism*, hence that  $\Delta_{X_i}$  acts *trivially* on  $H^2(H_i, \mathbb{F}_p)$ . Thus, the natural action of  $\Pi_{X_i}$  on  $H^2(H_i, \mathbb{F}_p)$  *factors* through the quotient  $\Pi_{X_i} \twoheadrightarrow Q_i/J_i$ . Now, by taking  $H_i$  to be *sufficiently small*, we may assume [since  $Q_i$  is *solvably closed*!] that the extension field of  $F_i$  determined by  $J_i$  contains a *primitive  $p$ -th root of unity*. Thus, by Proposition 1.2, (ii), we conclude that the action of  $Q_i/J_i$  on  $H^2(H_i, \mathbb{F}_p)$  is *faithful*. Since the isomorphism  $\Pi_{X_1} \xrightarrow{\sim} \Pi_{X_2}$  induces an isomorphism  $H_1 \xrightarrow{\sim} H_2$ , hence an isomorphism  $H^2(H_1, \mathbb{F}_p) \xrightarrow{\sim} H^2(H_2, \mathbb{F}_p)$  which is compatible with the respective actions of  $\Pi_{X_1}, \Pi_{X_2}$ , we thus conclude that the isomorphism  $\Pi_{X_1} \xrightarrow{\sim} \Pi_{X_2}$  preserves the kernels of the surjections  $\Pi_{X_i} \twoheadrightarrow Q_i/J_i$ , hence that the subgroup  $\Delta_{X_i} = \mathrm{Ker}(\Pi_{X_i} \twoheadrightarrow Q_i)$  may be recovered as the intersection of the kernels of the surjections  $\Pi_{X_i} \twoheadrightarrow Q_i/J_i$ , by letting the  $H_i$  range over all sufficiently small normal open subgroups of  $\Pi_{X_i}$ . This completes the proof of Proposition 2.4 in the case where there exists a *prime number*  $p$  such that  $p \notin \Sigma_1$ ,  $p \notin \Sigma_2$ .

Finally, we consider the case where  $X_1, X_2$  are *proper*. Let  $p$  be a prime number; suppose that the  $H_i$  have been taken to be *sufficiently small* so that the number fields determined by the  $J_i$  contain a *primitive  $p$ -th root of unity* and a *square root of  $-1$* . Then it follows from the Leray-Serre spectral sequence associated to the extension  $1 \rightarrow D_i \rightarrow H_i \rightarrow J_i \rightarrow 1$  [where we write  $D_i \stackrel{\mathrm{def}}{=} \mathrm{Ker}(H_i \twoheadrightarrow J_i)$ ] and Proposition 1.2, (i), that there is a *natural isomorphism*

$$H^4(H_i, \mathbb{F}_p) \cong H^2(J_i, \mathbb{F}_p) \otimes H^2(D_i, \mathbb{F}_p)$$



which is *compatible* with the natural action of  $\Pi_{X_i}$  on the various cohomology modules involved. Here, we note that [by the well-known structure of the cohomology of the geometric fundamental group of an algebraic curve]  $\Delta_{X_i} \subseteq \Pi_{X_i}$  acts *trivially* on  $H^2(D_i, \mathbb{F}_p)$ . Thus, Proposition 2.4 follows in the present case by applying Proposition 1.2, (ii), as in the argument given in the preceding paragraph.  $\circ$

**Theorem 2.5. (The Anabelian Geometry of Hyperbolic Curves over Solvably Closed Galois Groups)** *For  $i = 1, 2$ , let  $\tilde{F}_i/F_i$  be a solvably closed extension of a number field  $F_i$ ;  $Q_i \stackrel{\text{def}}{=} \text{Gal}(\tilde{F}_i/F_i)$ ;  $\Sigma_i$  a nonempty set of prime numbers;  $X_i$  a hyperbolic curve over  $F_i$  with which  $Q_i$  is  $\Sigma_i$ -compatible;  $1 \rightarrow \Delta_{X_i} \rightarrow \Pi_{X_i} \rightarrow Q_i \rightarrow 1$  the resulting exact sequence of profinite groups [cf. Definition 2.3];  $\tilde{X}_i \rightarrow X_i$  the pro-finite étale covering of  $X_i$  determined by  $\Pi_{X_i}$  [regarded as a quotient of the étale fundamental group of  $X_i$ ]. Then passing to the induced morphism on fundamental groups determines a bijection between the set of isomorphisms of topological groups*

$$\Pi_{X_1} \xrightarrow{\sim} \Pi_{X_2}$$

and the set of compatible pairs of isomorphisms of schemes  $\tilde{X}_1 \xrightarrow{\sim} \tilde{X}_2$ ,  $X_1 \xrightarrow{\sim} X_2$ .

*Proof.* By Proposition 2.4, any isomorphism  $\Pi_{X_1} \xrightarrow{\sim} \Pi_{X_2}$  induces an isomorphism  $Q_1 \xrightarrow{\sim} Q_2$ , hence, by Theorem 2.1, a compatible pair of isomorphisms of fields  $\tilde{F}_1 \xrightarrow{\sim} \tilde{F}_2$ ,  $F_1 \xrightarrow{\sim} F_2$ . Thus, we may apply ‘‘Theorem A’’ of [Mzk2] to the isomorphism  $\Pi_{X_1} \xrightarrow{\sim} \Pi_{X_2}$  to conclude that this isomorphism arises from a unique compatible pair of isomorphisms of schemes  $\tilde{X}_1 \xrightarrow{\sim} \tilde{X}_2$ ,  $X_1 \xrightarrow{\sim} X_2$ , as desired.  $\circ$

### Section 3: Some Examples

Finally, we conclude by observing that in various situations,  $\Sigma$ -compatible solvably closed extensions which are, moreover, ‘‘relatively small’’ [e.g., by comparison to the entire absolute Galois group of a number field] exist in substantial abundance.

**Proposition 3.1. (The Case of a Single Prime Number)** *Let  $\Sigma \stackrel{\text{def}}{=} \{r\}$ , where  $r$  is a prime number.*

(i) *Let  $\Delta$  be a topologically finitely generated pro- $r$  group. [Thus, since  $\Delta$  is topologically finitely generated, its topology admits a base of characteristic open subgroups, which determine a natural profinite topology on  $\text{Out}(\Delta)$ .] Write  $\Delta \twoheadrightarrow \Delta^{\text{ab}}$  for the abelianization of  $\Delta$ . Then the kernel of the natural morphism of profinite groups*

$$\text{Out}(\Delta) \rightarrow \text{Aut}(\Delta^{\text{ab}} \otimes \mathbb{F}_r)$$

is a **pro- $r$**  [hence, in particular, **pro-solvable!**] group.

(ii) Let  $X$  be a **hyperbolic curve** over  $F$ . Then there exists a finite Galois extension  $F_1$  over  $F$  such that the **maximal solvable extension** [which is **solvably closed** — cf. Remark 1.1.2]  $\tilde{F} \stackrel{\text{def}}{=} F_1^{\text{sol}}$  of  $F_1$  is  $\Sigma$ -**compatible** with  $X$ .

*Proof.* Assertion (i) follows immediately by considering the action of an outer automorphism in the kernel of  $\text{Out}(\Delta) \rightarrow \text{Aut}(\Delta^{\text{ab}} \otimes \mathbb{F}_r)$  on the *lower central series* of  $\Delta$ . Assertion (ii) follows formally from assertion (i) and the definitions.  $\circ$

**Proposition 3.2. (Basic Properties of Special Linear Groups)** Let  $l$  be a prime number. Write  $SL_2(\mathbb{F}_l)$  for the **special linear group** of 2 by 2 matrices with coefficients in  $\mathbb{F}_l$ ,  $PSL_2(\mathbb{F}_l) \stackrel{\text{def}}{=} SL_2(\mathbb{F}_l)/\{\pm 1\}$ .

(i) Suppose that  $l \geq 5$ . Then  $PSL_2(\mathbb{F}_l)$  is a **simple finite group**.

(ii) **No proper subgroup** of  $SL_2(\mathbb{F}_l)$  surjects onto  $PSL_2(\mathbb{F}_l)$ .

(iii)  $PSL_2(\mathbb{F}_2)$ ,  $PSL_2(\mathbb{F}_3)$ , as well as every proper subgroup of  $PSL_2(\mathbb{F}_l)$  [for arbitrary  $l$ ], is either **solvable** or isomorphic to  $PSL_2(\mathbb{F}_5)$ .

*Proof.* Assertions (i), (ii), (iii) are well-known — cf., e.g., [Serre], Chapter IV, §3.4, Lemmas 1, 2; [Carter], §1.2.  $\circ$

**Remark 3.2.1.** The proper subgroups  $H$  of  $SL_2(\mathbb{F}_l)$  may be analyzed as follows: If  $H$  is of order divisible by  $l$ , then  $H$  contains an *element of order  $l$*  — i.e., [since  $\mathbb{F}_l^\times$ ,  $\mathbb{F}_l^\times$  are of order prime to  $l$ ] a *unipotent matrix* — and so it is easy to show [using the fact that  $SL_2(\mathbb{F}_l)$  is generated by  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ ] that  $H$  is *solvable* [assuming that it is proper]. On the other hand, if the order of  $H$  is *prime to  $l$* , then  $H$  may be classified by applying the *Hurwitz formula* to the Galois covering  $\mathbb{P}_{\overline{\mathbb{F}_l}}^1 \rightarrow \mathbb{P}_{\overline{\mathbb{F}_l}}^1/H$  [arising from the natural action of  $SL_2$  on  $\mathbb{P}_{\overline{\mathbb{F}_l}}^1$ , where  $\overline{\mathbb{F}_l}$  is an algebraic closure of  $\mathbb{F}_l$ ], which gives rise to fairly *restrictive conditions* on the ramification indices of this covering. In particular, if  $H$  is *non-abelian*, then, by taking an appropriate isomorphism of  $\mathbb{P}_{\overline{\mathbb{F}_l}}^1/H$  with  $\mathbb{P}_{\overline{\mathbb{F}_l}}^1$ , one concludes that this covering is ramified over the three points “0”, “1”, and “ $\infty$ ” of  $\mathbb{P}_{\overline{\mathbb{F}_l}}^1$ , with ramification index 2 at “0”, ramification index  $\in \{2, 3\}$  at “1”, and ramification index  $\in \{3, 4, 5\}$  (respectively, arbitrary,  $\geq 2$ ) at “ $\infty$ ” if the ramification index at “1” is equal to 3 (respectively, 2). Now it is an elementary exercise to classify the possible groups  $H$  that may occur. For instance, by considering *modular curves*, it follows immediately that the case  $H = PSL_2(\mathbb{F}_5)$  corresponds to the case where the ramification indices are (2, 3, 5).

**Proposition 3.3. (Linear Disjointness I)** Let  $l > 5$  be a prime number;  $r$  a prime number  $\neq l$ ;  $\Sigma \stackrel{\text{def}}{=} \{r\}$ ;  $X$  a **once-punctured elliptic curve** over a

**number field**  $F$ . Suppose further that  $F$  contains an  **$l$ -th root of unity**, and that the resulting homomorphism

$$G_F \rightarrow SL_2(\mathbb{F}_l)$$

determined by the action of the absolute Galois group  $G_F$  of  $F$  on the  $l$ -torsion points of the elliptic curve  $E$  compactifying  $X$  is **surjective**. Then there exists a **solvably closed extension**  $\tilde{F}/F$  which is  $\Sigma$ -**compatible** with  $X$ , and, moreover, **linearly disjoint** [over  $F$ ] from the extension  $K$  of  $F$  determined by the kernel of the homomorphism  $G_F \rightarrow SL_2(\mathbb{F}_l)$ .

*Proof.* Write  $L \subseteq K$  for the extension of  $F$  determined by the kernel of the homomorphism  $G_F \rightarrow PSL_2(\mathbb{F}_l)$ . Then it follows immediately from Proposition 3.2, (ii), that any Galois extension of  $F$  is linearly disjoint from  $K$  if and only if it is linearly disjoint from  $L$ . Now observe that  $\text{Gal}(L/F) \cong PSL_2(\mathbb{F}_l)$  is *simple* [cf. Proposition 3.2, (i)] and *non-abelian*. Thus, by Proposition 3.1, (i), it suffices to show that the *finite* Galois extension  $R$  of  $F$  determined by the kernel of the homomorphism  $G_F \rightarrow GL_2(\mathbb{F}_r)$  arising from the Galois action on the  $r$ -torsion points of  $E$  is *linearly disjoint* from  $L$ . On the other hand, again since  $\text{Gal}(L/F)$  is *simple* and *non-abelian*, this linear disjointness property follows from the fact [cf. Proposition 3.2, (iii); our assumption that  $r \neq l > 5$ ] that no subquotient of  $GL_2(\mathbb{F}_r)$  [or, equivalently,  $PSL_2(\mathbb{F}_r)$ , since  $PSL_2(\mathbb{F}_l)$  is simple and nonabelian] is isomorphic to  $PSL_2(\mathbb{F}_l)$ . This completes the proof of Proposition 3.3.  $\circ$

**Proposition 3.4. (Linear Disjointness II)** *Let  $l > 5$  be a prime number;  $\Sigma$  a nonempty set of prime numbers such that  $l \notin \Sigma$ ;  $X$  a **once-punctured elliptic curve** over a **number field**  $F$  with **stable reduction** over the ring of integers  $\mathcal{O}_F$  of  $F$ ;  $F_\mu$  the extension of  $F$  obtained by adjoining an  **$l$ -th root of unity**. Suppose further that  $l \geq [F : \mathbb{Q}] + 2$ ; that  $[F_\mu : F]$  divides  $(l - 1)/2$  [which implies that the homomorphism*

$$G_F \rightarrow PGL_2(\mathbb{F}_l) \stackrel{\text{def}}{=} GL_2(\mathbb{F}_l)/\mathbb{F}_l^\times$$

*determined by the action of the absolute Galois group  $G_F$  of  $F$  on the  $l$ -torsion points of the elliptic curve  $E$  compactifying  $X$  **factors** through the image of  $PSL_2(\mathbb{F}_l)$  in  $PGL_2(\mathbb{F}_l)$ ]; that the resulting homomorphism  $G_F \rightarrow PSL_2(\mathbb{F}_l)$  is **surjective**; and that, for each prime  $\mathfrak{l}$  of  $F$  lying over  $l$  at which  $E$  has **bad** reduction, the following condition is satisfied:*

*Write  $F_{\mathfrak{l}}$  for the completion of  $F$  at  $\mathfrak{l}$ . Thus, the elliptic curve  $E \times_F F_{\mathfrak{l}}$  is a **Tate curve**, hence has a well-defined “ **$q$ -parameter**”  $q_{\mathfrak{l}}$  in the ring of integers  $\mathcal{O}_{F_{\mathfrak{l}}}$ . Then the valuation of  $q_{\mathfrak{l}}$  is **prime to  $l$** .*

*Then:*

(i) There exists an extension  $\tilde{F}/F$  which is  $\Sigma$ -**compatible** with  $X$ , and, moreover, **linearly disjoint** [over  $F$ ] from the extension  $K$  of  $F$  determined by the kernel of the homomorphism  $G_F \rightarrow PSL_2(\mathbb{F}_l)$ .

(ii) Write  $K_\mu$  for the extension of  $F$  determined by the kernel of the homomorphism  $G_F \rightarrow GL_2(\mathbb{F}_l)$  [arising from the Galois action on the  $l$ -torsion points of  $E$ ]. Thus,  $F_\mu \subseteq K_\mu$ ; write  $\tilde{F}_\mu \stackrel{\text{def}}{=} F_\mu \cdot \tilde{F}$  for the composite extension [over  $F$ ]. Then the maximal solvable extension  $\tilde{F}_\mu^{\text{sol}}$  of  $\tilde{F}_\mu$  forms a **solvably closed** extension of  $F_\mu$  which is  $\Sigma$ -**compatible** with  $X$  and, moreover, **linearly disjoint** over  $F_\mu$  from the extension  $K_\mu$  of  $F_\mu$ .

*Proof.* First, we consider assertion (i). Let  $\tilde{F}/F$  be the extension determined by the kernel of the homomorphism  $G_F \rightarrow \text{Out}(\Delta_X)$  [cf. Definition 2.3]. Let  $\mathfrak{l}$  be a prime of  $F$  lying over  $l$ . Since  $PSL_2(\mathbb{F}_l)$  is *simple* [cf. Proposition 3.2, (i)], to complete the proof of assertion (i), it suffices to show that the composite [i.e., over  $F$ ] field extension  $K \cdot \tilde{F}$  is *not equal* to  $\tilde{F}$ . Thus, suppose that  $K \cdot \tilde{F} = \tilde{F}$ . Since  $l \notin \Sigma$ , if  $E$  has *good reduction* at  $\mathfrak{l}$ , then it follows that  $\tilde{F}/F$  is *unramified* at  $\mathfrak{l}$ ; similarly, if  $E$  has *bad reduction* at  $\mathfrak{l}$ , then the fact that  $l \notin \Sigma$  implies that  $\tilde{F}/F$  is *tamely ramified* at  $\mathfrak{l}$ . On the other hand, if  $E$  has *good reduction* at  $\mathfrak{l}$ , then the fact that  $K \subseteq K \cdot \tilde{F} = \tilde{F}$  is unramified at  $\mathfrak{l}$  implies, by applying, for instance, results of Raynaud on the “*fully faithfulness of restriction to the generic fiber*” for *finite flat group schemes over moderately ramified discrete valuation rings* [cf. [Rayn], Corollaire 3.3.6, (1); our assumption that  $l \geq [F : \mathbb{Q}] + 2$ , which implies that the ring of integers  $\mathcal{O}_{F_\mathfrak{l}}$  is indeed “*moderately ramified*”], that, if we write  $\mathcal{E}$  for the stable model of the elliptic curve  $E$  over  $\mathcal{O}_{F_\mathfrak{l}}$  and  $\mathcal{E}[l]$  for the kernel of multiplication by  $l$  on  $\mathcal{E}$ , then  $\mathcal{E}[l]$  may be written as a direct product

$$\mathcal{E}[l] \cong \mathcal{G} \times \mathcal{G}$$

of two copies of some finite flat group scheme  $\mathcal{G}$  over  $\mathcal{O}_{F_\mathfrak{l}}$  [which implies, for instance, that the tangent space of  $\mathcal{E}[l]$ , hence also of  $\mathcal{E}$ , is *even-dimensional!*] — a contradiction. Finally, if  $E$  has *bad reduction* at  $\mathfrak{l}$ , then the fact that  $K \subseteq K \cdot \tilde{F} = \tilde{F}$  is tamely ramified at  $\mathfrak{l}$  contradicts our assumption concerning the “*valuation of the  $q$ -parameter*” [which implies that  $K$  is *wildly ramified* at  $\mathfrak{l}$ ]. This completes the proof of assertion (i).

To verify assertion (ii), let us first observe that by Proposition 3.2, (i) [cf. our assumption that  $l > 5$ ], (ii), and the *surjectivity* assumption in the statement of the present Proposition 3.4, we have  $\text{Gal}(K_\mu/F_\mu) \cong SL_2(\mathbb{F}_l)$ . Now, by applying Proposition 3.2, (ii), as in the proof of Proposition 3.3, assertion (ii) follows immediately from assertion (i), together with the *simplicity* [and *non-solvability*] of  $PSL_2(\mathbb{F}_l)$ .

○

**Bibliography**

- [Carter] R. W. Carter, *Simple groups of Lie type*, *Pure and Applied Mathematics* **28**, John Wiley & Sons (1972).
- [FJ] M. Fried and M. Jarden, *Field Arithmetic* (second edition), Springer-Verlag (2005).
- [Lang] S. Lang, *Algebraic number theory*, Addison-Wesley Publishing Co. (1970).
- [Mtmo] M. Matsumoto, Galois representations on profinite braid groups on curves, *J. Reine Angew. Math.* **474** (1996), pp. 169-219.
- [Mzk1] S. Mochizuki, The Absolute Anabelian Geometry of Hyperbolic Curves, *Galois Theory and Modular Forms*, Kluwer Academic Publishers (2003), pp. 77-122.
- [Mzk2] S. Mochizuki, The Local Pro- $p$  Anabelian Geometry of Curves, *Invent. Math.* **138** (1999), pp. 319-423.
- [NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields*, *Grundlehren der Mathematischen Wissenschaften* **323**, Springer-Verlag (2000).
- [Rayn] M. Raynaud, Schémas en groupes de type  $(p, \dots, p)$ , *Bull. Soc. Math. France* **102** (1974), pp. 241-280.
- [Serre] J.-P. Serre, *Abelian  $l$ -adic Representations and Elliptic Curves*, Benjamin (1968).
- [Uchida] K. Uchida, Isomorphisms of Galois groups of solvably closed Galois extensions, *Tôhoku Math. J.* **31** (1979), pp. 359-362.