Mono-anabelian Reconstruction of Solvably Closed Galois Extensions of Number Fields

Yuichiro Hoshi

June 2022

Abstract. — A theorem of Uchida asserts that every continuous isomorphism between the Galois groups of solvably closed Galois extensions of number fields arises from a unique isomorphism between the solvably closed Galois extensions. In particular, the isomorphism class of a solvably closed Galois extension of a number field is completely determined by the isomorphism class of the associated Galois group. On the other hand, neither the statement of this theorem nor the proof of this theorem yields an "explicit reconstruction" of the given solvably closed Galois extension. In the present paper, we establish a functorial "group-theoretic" algorithm for reconstructing, from the Galois group of a solvably closed Galois extension of a number field, the given solvably closed Galois extension equipped with the natural Galois action.

Contents

Introduction

Let us first recall the following result, i.e., a theorem of Uchida [cf. [8, Theorem]]:

For $\square \in \{\circ, \bullet\}$, let $F_\square$ be a number field and $\widetilde{F}_\square$ a Galois extension of $F_\square$ that is *solvably closed*, i.e., does not admit any nontrivial finite abelian extension; write $Q_\square \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\widetilde{F}_\square/F_\square)$. Moreover, write

$$\mathrm{Isom}(\widetilde{F}_\bullet/F_\bullet, \widetilde{F}_\circ/F_\circ)$$

for the set of isomorphisms $\widetilde{F}_\bullet \xrightarrow{\sim} \widetilde{F}_\circ$ of fields that restrict to isomorphisms $F_\bullet \xrightarrow{\sim} F_\circ$ of subfields and

$$\mathrm{Isom}(Q_\circ, Q_\bullet)$$

2020 Mathematics Subject Classification. — 11R32.
Key words and phrases. — mono-anabelian geometry, mono-anabelian reconstruction, number field, solvably closed, profinite group of GSC-type.

for the set of continuous isomorphisms $Q_\circ \xrightarrow{\sim} Q_\bullet$. Then the natural map

$$\mathrm{Isom}(\widetilde{F}_\bullet/F_\bullet, \widetilde{F}_\circ/F_\circ) \longrightarrow \mathrm{Isom}(Q_\circ, Q_\bullet)$$

is *bijective.*

That is to say, every continuous isomorphism between the Galois groups of solvably closed Galois extensions of number fields arises from a unique isomorphism between the given solvably closed Galois extensions. In particular, it follows from the [surjectivity portion of the] above result that the isomorphism class of a solvably closed Galois extension of a number field is completely determined by the isomorphism class of the associated Galois group.

On the other hand, let us observe that neither the statement of the above result nor the proof of the above result yields an "explicit reconstruction" of the given solvably closed Galois extension. That is to say, the above result does not tell us how to reconstruct explicitly the given solvably closed Galois extension. Put another way, the above result yields only a *bi-anabelian reconstruction*, i.e., in the sense of [6, Introduction] [cf. also [6, Remark 1.9.8]], of solvably closed Galois extensions of number fields. In the present paper, we discuss a *mono-anabelian reconstruction*, i.e., in the sense of [6, Introduction] [cf. also [6, Remark 1.9.8]], of solvably closed Galois extensions of number fields. In particular, we concentrate on the task of establishing "group-theoretic software" [i.e., "group-theoretic algorithms"] related to the Galois groups of solvably closed Galois extensions of number fields.

We shall say that a field of characteristic zero is *absolutely Galois* if the field is Galois over the [unique] minimal subfield of the field. We shall say that a profinite group is *of GSC-type* (respectively, *of AGSC-type*) if the profinite group is isomorphic to the Galois group of a solvably closed Galois extension (respectively, an absolutely Galois solvably closed extension) of a number field [cf. [2, Definition 3.2]]. In [2], the author of the present paper has established a *mono-anabelian reconstruction* of *absolutely Galois* solvably closed extensions of number fields. More concretely, in [2], the author of the present paper has established a *functorial "group-theoretic" algorithm* [cf. [6, Remark 1.9.8] for more on the meaning the terminology "group-theoretic"] for constructing, from a profinite group *of AGSC-type*, a suitable *absolutely Galois solvably closed* field equipped with an action of the profinite group. The purpose of the present paper is to *generalize* this reconstruction result to the case of profinite groups *of GSC-type*. The main result of the present paper may be summarized as follows [cf. Definition 3.8 and Theorem 3.9]:

Summary. *There exists a **functorial*** [*cf. Remark* 3.9.1] ***"group-theoretic" algorithm***

$$G \qquad \mapsto \qquad \big(G \curvearrowright \widetilde{F}(G)\big)$$

*for constructing, from a profinite group G **of GSC-type**, a **solvably closed** field $\widetilde{F}(G)$ equipped with an action of G such that the subfield $\widetilde{F}(G)^G \subseteq \widetilde{F}(G)$ of $\widetilde{F}(G)$ of G-invariants is a **number field**, and, moreover, the action of G on $\widetilde{F}(G)$ determines a continuous **isomorphism***

$$G \xrightarrow{\sim} \mathrm{Gal}\big(\widetilde{F}(G)/\widetilde{F}(G)^G\big).$$

We thus conclude from this reconstruction result that a profinite group isomorphic to the Galois group of a solvably closed Galois extension of a number field admits a ring-theoretic basepoint [i.e., a "ring-theoretic interpretation" or a "ring-theoretic label"] *group-theoretically* constructed from the given profinite group. Note that the above result of Uchida plays a crucial role in the establishment of our reconstruction result. In particular, the proof of the reconstruction result given in the present paper does *not yield an alternative proof* of the above result of Uchida.

Acknowledgments

The author would like to thank the *referee* for carefully reading the manuscript and giving some helpful comments. This research was supported by JSPS KAKENHI Grant Number 21K03162 and by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

0. Notational Conventions

Monoids. — If M is a monoid, then we shall write $M^{\circledast} \stackrel{\mathrm{def}}{=} M \cup \{*_M \stackrel{\mathrm{def}}{=} M\}$; we regard $M^{\circledast}$ as a monoid, that contains M as a submonoid, by setting $*_M \cdot *_M \stackrel{\mathrm{def}}{=} *_M$, $a \cdot *_M \stackrel{\mathrm{def}}{=} *_M$, and $*_M \cdot a \stackrel{\mathrm{def}}{=} *_M$ for every $a \in M$.

Modules. — If M is a module, then we shall write

$$M^{\wedge} \stackrel{\mathrm{def}}{=} \varprojlim_{n} M/nM$$

— where the projective limit is taken over the positive integers n.

Profinite Groups. — Let G be a profinite group. Then we shall say that G is *slim* if the centralizer in G of an arbitrary open subgroup of G is trivial. If $H \subseteq G$ is a closed subgroup of G, then we shall write $C_G(H) \subseteq G$ for the *commensurator* of H in G, i.e., the subgroup of G consisting of the elements $g \in G$ such that the intersection $H \cap gHg^{-1} \cap g^{-1}Hg$ is of finite index in H; we shall say that H is *commensurably terminal* in G if the equality $H = C_G(H)$ holds. If n is an integer, and M is a topological G-module, then we shall write $H^n(G, M)$ for the n-th continuous group cohomology of G with coefficients in M and

$${}_{\infty}H^n(G, M) \stackrel{\mathrm{def}}{=} \varinjlim_{H \subseteq G} H^n(H, M)$$

— where the injective limit is taken over the open subgroups $H \subseteq G$ of G.

Fields. — Let K be a field of characteristic zero. Then we shall say that

- the field K is an *NF* [where "NF" is to be understood as an abbreviation for "Number Field"] if K is finite over the [unique] minimal subfield of K,
- the field K is *absolutely Galois* if K is Galois over the [unique] minimal subfield of K, and
- the field K is *solvably closed* if there is no nontrivial finite abelian extension of K.

We shall write $K^{\times}$ for the multiplicative module of nonzero elements of K and $K_{\times} \stackrel{\mathrm{def}}{=} K^{\times} \cup \{0\}$ for the underlying multiplicative monoid of K. [So we have a natural isomorphism $(K^{\times})^{\circledast} \xrightarrow{\sim} K_{\times}$ of monoids that maps $*_{K^{\times}} \in (K^{\times})^{\circledast}$ to $0 \in K_{\times}$.] If, moreover, the field K

is solvably closed, then we shall write $\Lambda(K)$ for the *cyclotome* associated to K, i.e.,

$$\Lambda(K) \stackrel{\text{def}}{=} \varprojlim_{n} \boldsymbol{\mu}_n(K)$$

— where the projective limit is taken over the positive integers n, and we write $\boldsymbol{\mu}_n(K) \subseteq K^{\times}$ for the multiplicative submodule of n-th roots of unity in K. Thus, one verifies immediately that the cyclotome has a natural structure of profinite, hence also topological, module and is isomorphic, as an abstract topological module, to the profinite completion of an infinite cyclic module.

1. Characterization of Minimal Solvably Closed Fields

In the present §1, we give a certain characterization of the minimal solvably closed subfield of a given solvably closed field [cf. Lemma 1.4 below]. In the present §1, let F be an *NF* and $\widetilde{F}$ a Galois extension of F that is *solvably closed*. We shall write

- $Q_F \stackrel{\text{def}}{=} \mathrm{Gal}(\widetilde{F}/F)$ for the Galois group of the Galois extension $\widetilde{F}/F$,
- $\mathcal{V}_{\widetilde{F}} \twoheadrightarrow \mathcal{V}_F$ for the respective sets of nonarchimedean primes of $\widetilde{F}$, F,
- $\mathcal{V}_F^{d=1} \subseteq \mathcal{V}_F$ for the subset consisting of nonarchimedean primes of F of degree one,
- $\mathbb{I}_F^{\text{fin}}$ for the group of finite idèles of F,
- $F_{\text{prm}} \subseteq F$ for the [unique] minimal subfield of F [i.e., the unique subfield of F *of PmF-type* — cf. [2, Definition 2.1]], and
- $F_{\text{prm}}^{\text{slv}} \subseteq \widetilde{F}$ for the [unique] maximal prosolvable extension of F_{prm} in $\widetilde{F}$. [Note that since $\widetilde{F}$ is solvably closed, one verifies easily that $F_{\text{prm}}^{\text{slv}}$ is a solvable closure of F_{prm}.]

Moreover, for each $v \in \mathcal{V}_F$, we shall write

- F_v for the completion of F at v.

Observe that, for $\widetilde{v} \in \mathcal{V}_{\widetilde{F}}$, if one writes $\widetilde{v}|_F \in \mathcal{V}_F$ for the restriction of $\widetilde{v}$ to F, then since $\widetilde{F}$ is solvably closed, it follows immediately from [5, Proposition 2.3, (iii)] [i.e., the Grunwald-Wang theorem — cf., e.g., [7, Theorem 9.2.8]] that the pair $(\widetilde{F}, \widetilde{v})$ determines an algebraic closure of $F_{\widetilde{v}|_F}$, together with a natural inclusion from $\widetilde{F}$ into the algebraic closure. For each $\widetilde{v} \in \mathcal{V}_{\widetilde{F}}$, we shall write

- $\widetilde{F}_{\widetilde{v}}$ $(\supseteq \widetilde{F})$ for the algebraic closure of $F_{\widetilde{v}|_F}$ determined by the pair $(\widetilde{F}, \widetilde{v})$.

Definition 1.1. — We shall write

$$\mathcal{H}^{\times}(F) \subseteq \mathbb{I}_F^{\text{fin}} \quad \Big(\subseteq \prod_{v \in \mathcal{V}_F} F_v^{\times} \Big)$$

for the *Kummer container* associated to F [cf. [2, Definition 3.9]], i.e., the module obtained by forming the fiber product of the diagram of the natural inclusions of modules

$$\begin{tikzcd} & \mathbb{I}_F^{\mathrm{fin}} \arrow[d, hook] \\ (F^\times)^\wedge \arrow[r, hook] & \prod_{v \in \mathcal{V}_F} (F_v^\times)^\wedge. \end{tikzcd}$$

Moreover, we shall write

$$\mathcal{H}_\times(F) \stackrel{\mathrm{def}}{=} \mathcal{H}^\times(F)^{\circledast}$$

[cf. [2, Definition 3.9]]. Thus, the natural inclusion $F^\times \hookrightarrow \mathbb{I}_F^{\mathrm{fin}}$ and the natural homomorphism $F^\times \to (F^\times)^\wedge$ determine an injective homomorphism $F^\times \hookrightarrow \mathcal{H}^\times(F)$, hence also an injective homomorphism $F_\times \hookrightarrow \mathcal{H}_\times(F)$. Let us regard $F^\times$, $F_\times$ as submonoids of $\mathcal{H}^\times(F)$, $\mathcal{H}_\times(F)$ by means of these injective homomorphisms, respectively:

$$\begin{tikzcd} F^\times \arrow[r, hook] \arrow[d, hook] & F_\times \arrow[d, hook] \\ \mathcal{H}^\times(F) \arrow[r, hook] & \mathcal{H}_\times(F). \end{tikzcd}$$

Lemma 1.2. — *Let a be an element of $\mathcal{H}^\times(F)$ and N a positive integer. If the N-th power $a^N \in \mathcal{H}^\times(F)$ is* ***contained*** *in the submodule $F^\times \subseteq \mathcal{H}^\times(F)$, then $a \in \mathcal{H}^\times(F)$ is* ***contained*** *in the submodule $F^\times \subseteq \mathcal{H}^\times(F)$.*

Proof. — Since [one verifies easily that] the natural homomorphism $F^\times \to (F^\times)^\wedge$ *factors* as the composite of the natural inclusion $F^\times \hookrightarrow \mathcal{H}^\times(F)$ and an *injective* homomorphism $\mathcal{H}^\times(F) \hookrightarrow (F^\times)^\wedge$, to verify Lemma 1.2, it suffices to verify the *triviality* of the torsion submodule of the cokernel of the natural homomorphism $F^\times \to (F^\times)^\wedge$. On the other hand, this *triviality* follows from [1, Lemma 5.29, (ii)]. This completes the proof of Lemma 1.2. $\square$

Definition 1.3. — Let F' be an intermediate field of the extension $\widetilde{F}/F$ finite over F. [So F' is an NF.] Then, for each positive integer n, we shall define two subsets

$$\mathcal{G}(F', n) \subseteq \mathcal{F}(F', n) \subseteq F'_\times \quad \big(\subseteq \mathcal{H}_\times(F')\big)$$

of $F'_\times$ as follows:

- We shall write $\mathcal{G}(F', 1) \stackrel{\mathrm{def}}{=} \mathcal{F}(F', 1) \stackrel{\mathrm{def}}{=} (F_{\mathrm{prm}})_\times$ $(\subseteq F'_\times)$.

- If $n \geq 2$, then we shall write $\mathcal{G}(F', n) \subseteq F'_\times$ for the subset of $F'_\times$ consisting of the elements $a \in \mathcal{H}_\times(F')$ that satisfy the following condition: There exists a positive integer N such that the N-th power $a^N \in \mathcal{H}_\times(F')$ is contained in the subset $\mathcal{F}(F', n-1) \subseteq \mathcal{H}_\times(F')$. [Observe that it follows from Lemma 1.2 that the inclusion $\mathcal{F}(F', n-1) \subseteq F'_\times$ implies the inclusion $\mathcal{G}(F', n) \subseteq F'_\times$.]

- If $n \geq 2$, then we shall write $\mathcal{F}(F', n) \subseteq F'_\times$ for the [underlying set of the] subfield of F' generated by $\mathcal{G}(F', n) \subseteq F'_\times$.

Moreover, we shall write

$$\mathcal{F}(F', \infty) \stackrel{\text{def}}{=} \bigcup_{n} \mathcal{F}(F', n) \subseteq F'_{\times}$$

— where the union is taken over the positive integers n.

Lemma 1.4. — *The* ***equality****, i.e., in* $\widetilde{F}_{\times}$,

$$\bigcup_{F'} \mathcal{F}(F', \infty) = (F^{\text{slv}}_{\text{prm}})_{\times}$$

— where the union is taken over the intermediate fields F' of the extension $\widetilde{F}/F$ finite over F — holds.

Proof. — Let us first verify the inclusion

$$\bigcup_{F'} \mathcal{F}(F', \infty) \subseteq (F^{\text{slv}}_{\text{prm}})_{\times}.$$

Now observe that one verifies immediately [cf. also the definition of the subset "$\mathcal{F}(F', 1)$"] that, to verify this inclusion, it suffices to verify the following assertion:

> Claim 1.4.A. — For each intermediate field F' of $\widetilde{F}/F$ finite over F and each integer $n \geq 2$, the inclusion $\mathcal{F}(F', n-1) \subseteq (F^{\text{slv}}_{\text{prm}})_{\times}$ implies the inclusion $\mathcal{G}(F', n) \subseteq (F^{\text{slv}}_{\text{prm}})_{\times}$.

On the other hand, Claim 1.4.A follows immediately from the definition of the subset "$\mathcal{G}(F', n)$".

Next, we verify the inclusion

$$\bigcup_{F'} \mathcal{F}(F', \infty) \supseteq (F^{\text{slv}}_{\text{prm}})_{\times}.$$

Now observe that one verifies immediately that, to verify this inclusion, it suffices to verify the following assertion:

> Claim 1.4.B. — For each subfield $E \subseteq F^{\text{slv}}_{\text{prm}}$ of $F^{\text{slv}}_{\text{prm}}$ finite and *Galois* over F_{prm}, there exists an intermediate field F' of $\widetilde{F}/F$ finite over F such that the inclusion $E \subseteq \mathcal{F}(F', \infty)$ holds.

To this end, let $E \subseteq F^{\text{slv}}_{\text{prm}}$ be a subfield of $F^{\text{slv}}_{\text{prm}}$ finite and *Galois* over F_{prm}. Then it follows from [2, Lemma 5.6, (iii)] — i.e., in the case where we take the "$(F, \widetilde{F}, E)$" of [2, Lemma 5.6, (iii)] to be $(F_{\text{prm}}, F^{\text{slv}}_{\text{prm}}, E)$ — that, to verify Claim 1.4.B, we may assume without loss of generality, by replacing E by a suitable finite extension of E in $F^{\text{slv}}_{\text{prm}}$ Galois over F_{prm}, that there exists a finite sequence of finite extensions of F_{prm} contained in E

$$F_{\text{prm}} = F_1 \subseteq F_2 \subseteq \ldots \subseteq F_{n-1} \subseteq F_n = E$$

such that, for each $i \in \{2, \ldots, n\}$, the extension F_i/F_{i-1} is *Galois*, and, moreover, one of the following two conditions is satisfied:

(1) The field F_i is obtained by adjoining a *root of unity* in $\widetilde{F}$ to F_{i-1}.

(2) If one writes d_i for the degree of the finite extension F_i/F_{i-1}, then d_i is a *prime number*, and, moreover, the field F_{i-1} contains a *primitive d_i-th root of unity*.

In particular, one verifies immediately [cf. also the definition of the subset "$\mathcal{F}(F', 1)$"] that, to verify Claim 1.4.B, it suffices to verify the following assertion:

> Claim 1.4.C. — For each $i \in \{2, \ldots, n\}$, if one writes $F' \subseteq \widetilde{F}$ for the subfield of $\widetilde{F}$ generated by E and F, then the inclusion $F_{i-1} \subseteq \mathcal{F}(F', i-1)$ implies the inclusion $F_i \subseteq \mathcal{F}(F', i)$.

On the other hand, Claim 1.4.C follows immediately from *Kummer theory*, together with above conditions (1), (2). This completes the proof of Lemma 1.4. $\square$

2. Reconstruction of Minimal Solvably Closed Fields

In the present §2, we establish a *functorial "group-theoretic" algorithm* for reconstructing, from the Galois group of a solvably closed Galois extension of an NF, the minimal solvably closed subfield of the given solvably closed extension [cf. Definition 2.6 below and Proposition 2.7 below]. In the present §2, let G be a profinite group *of GSC-type*, i.e., a profinite group isomorphic to the Galois group of a solvably closed Galois extension of an NF [cf. [2, Definition 3.2]]. Thus, by applying some functorial "group-theoretic" algorithms established in [2, §3] to G, one obtains

- sets $\widetilde{\mathcal{V}}(G) \twoheadrightarrow \mathcal{V}(G) \supseteq \mathcal{V}^{d=1}(G)$ [cf. [2, Proposition 3.5, (1), (2)]] and
- a monoid $\mathcal{H}_\times(G)$ [cf. [2, Proposition 3.11]].

Moreover, for each $D \in \widetilde{\mathcal{V}}(G)$ that maps to $\mathfrak{D} \in \mathcal{V}(G)$, by applying some functorial "group-theoretic" algorithms established in [2, §1] and [2, §3] to D and $\mathfrak{D}$, one obtains

- a prime number $p(D)$ [cf. [2, Theorem 1.4, (1)]],
- a positive integer $d(D)$ [cf. [2, Theorem 1.4, (2)]], and
- monoids $k_\times(\mathfrak{D}) \xrightarrow{\sim} k_\times(D) \subseteq \overline{k}_\times(D)$ [cf. [2, Theorem 1.4, (8), (9)], [2, Proposition 3.7, (2)]].

Definition 2.1. — Let $\mathfrak{D}$ be an element of $\mathcal{V}^{d=1}(G)$.

(i) For each $D \in \mathfrak{D}$, since $d(D) = 1$, we have a topological field $k(D)$ and a natural identification $k(D)_\times = k_\times(D)$ [cf. [3, Definition 5.2]; also Remark 2.1.1 below]. Then it follows from [2, Proposition 3.7, (i)] and [3, Theorem 5.4, (i)] that the topological field structures of the various topological fields $k(D)$ — where D ranges over the elements of $\mathfrak{D}$ — and the inclusion of monoids of [2, Proposition 3.7, (2)]

$$k_\times(\mathfrak{D}) \subseteq \prod_{D \in \mathfrak{D}} k_\times(D)$$

determine

- a *topological field structure* on the monoid $k_\times(\mathfrak{D})$, whose resulting topological field we denote by

$$k(\mathfrak{D}),$$

- a natural identification $k(\mathfrak{D})_\times = k_\times(\mathfrak{D})$, and
- an inclusion of topological rings

$$k(\mathfrak{D}) \subseteq \prod_{D \in \mathfrak{D}} k(D).$$

(ii) We shall write

$$F_{\mathrm{prm}}(\mathfrak{D}) \subseteq k(\mathfrak{D})$$

for the [unique] minimal subfield of $k(\mathfrak{D})$. Note that since the topological field $k(\mathfrak{D})$ is of characteristic zero [cf. [3, Remark 5.2.1]], the field $F_{\mathrm{prm}}(\mathfrak{D})$ is of PmF-type.

(iii) Let $\mathfrak{E}$ be an element of $\mathcal{V}^{d=1}(G)$. Then we shall write

$$\iota^{\mathrm{prm}}_{\mathfrak{D},\mathfrak{E}} \colon F_{\mathrm{prm}}(\mathfrak{D}) \xrightarrow{\sim} F_{\mathrm{prm}}(\mathfrak{E})$$

for the unique [cf. (ii)] isomorphism of fields.

Remark 2.1.1. — In light of the importance of the topological field "$k(D)$" that appears in Definition 2.1, (i), we pause to give a brief review of the reconstruction algorithm of this field structure on the monoid $k_\times(D)$ in the case where $d(D) = 1$ as follows: Write $(\Lambda(D)^{(p(D))})^{\mathrm{pf}}$ for the topological D-module that "corresponds" to the topological Galois module "$\mathbb{Q}_{p(D)}(1)$" [cf. [2, Theorem 1.4, (9), (iv)], [3, Definition 4.5, (i)]]. Then since we are working with the assumption that $d(D) = 1$, by considering the character on D that "corresponds" to the $p(D)$-adic cyclotomic character, we may construct an isomorphism of the monoid $k_\times(D)$ with the underlying multiplicative monoid $\mathrm{End}((\Lambda(D)^{(p(D))})^{\mathrm{pf}})_\times$ of the topological field $\mathrm{End}((\Lambda(D)^{(p(D))})^{\mathrm{pf}})$ [isomorphic to the topological field "$\mathbb{Q}_{p(D)}$"] obtained by forming the algebra of endomorphisms of the topological module $(\Lambda(D)^{(p(D))})^{\mathrm{pf}}$. In particular, by transporting the additive structure of the field $\mathrm{End}((\Lambda(D)^{(p(D))})^{\mathrm{pf}})$, we obtain a field structure on the monoid $k_\times(D)$.

Definition 2.2. — Let us recall the natural inclusion of monoids [cf. [2, Proposition 3.11, (ii)]]

$$\mathcal{H}_\times(G) \subseteq \prod_{\mathfrak{D} \in \mathcal{V}^{d=1}(G)} k_\times(\mathfrak{D}).$$

We shall write

$$(F_{\mathrm{prm}})_\times(G) \subseteq \mathcal{H}_\times(G)$$

for the subset of $\mathcal{H}_\times(G)$ consisting of the elements $a \in \mathcal{H}_\times(G)$ that satisfy the following condition: For each $\mathfrak{D}$, $\mathfrak{E} \in \mathcal{V}^{d=1}(G)$, if one writes $a_{\mathfrak{D}} \in k_\times(\mathfrak{D})$, $a_{\mathfrak{E}} \in k_\times(\mathfrak{E})$ for the images of $a \in \mathcal{H}_\times(G)$ in $k_\times(\mathfrak{D})$, $k_\times(\mathfrak{E})$, respectively, then $a_{\mathfrak{D}} \in F_{\mathrm{prm}}(\mathfrak{D})_\times$ ($\subseteq k_\times(\mathfrak{D})$), $a_{\mathfrak{E}} \in F_{\mathrm{prm}}(\mathfrak{E})_\times$ ($\subseteq k_\times(\mathfrak{E})$), and, moreover, the equality $\iota^{\mathrm{prm}}_{\mathfrak{D},\mathfrak{E}}(a_{\mathfrak{D}}) = a_{\mathfrak{E}}$ holds.

Proposition 2.3. — *Suppose that we are in the situation at the beginning of the preceding* §1. *Then the isomorphism of monoids of* [2, Proposition 3.11, (i)]

$$\mathcal{H}_\times(F) \xrightarrow{\sim} \mathcal{H}_\times(Q_F)$$

restricts to a ***bijective*** *map of subsets*

$$(F_{\mathrm{prm}})_{\times} \xrightarrow{\sim} (F_{\mathrm{prm}})_{\times}(Q_F).$$

Proof. — This assertion follows immediately from the various definitions involved. □

Definition 2.4. — Let us recall the natural inclusions [cf. [2, Proposition 3.11, (ii)]]

$$(F_{\mathrm{prm}})_{\times}(G) \subseteq \mathcal{H}_{\times}(G) \subseteq \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k_{\times}(\mathfrak{D}) = \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})_{\times}.$$

For each positive integer n, we shall define two subsets

$$\mathcal{G}(G,n) \subseteq \mathcal{H}_{\times}(G), \qquad \mathcal{F}(G,n) \subseteq \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})_{\times}$$

as follows:

- We shall write $\mathcal{G}(G,1) \stackrel{\mathrm{def}}{=} \mathcal{F}(G,1) \stackrel{\mathrm{def}}{=} (F_{\mathrm{prm}})_{\times}(G)$.
- If $n \geq 2$, then we shall write $\mathcal{G}(G,n) \subseteq \mathcal{H}_{\times}(G)$ for the subset of $\mathcal{H}_{\times}(G)$ consisting of the elements $a \in \mathcal{H}_{\times}(G)$ that satisfy the following condition: There exists a positive integer N such that the N-th power $a^N \in \mathcal{H}_{\times}(G)$ is contained in the subset $\mathcal{F}(G,n-1) \subseteq \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})_{\times}$.
- If $n \geq 2$, then we shall write $\mathcal{F}(G,n) \subseteq \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})_{\times}$ for the [underlying set of the] subring of $\prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})$ generated by $\mathcal{G}(G,n)$.

Moreover, we shall write

$$\mathcal{F}(G,\infty) \stackrel{\mathrm{def}}{=} \bigcup_{n} \mathcal{F}(G,n) \subseteq \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})_{\times}$$

— where the union is taken over the positive integers n.

Proposition 2.5. — *The following assertions hold:*

(i) *Suppose that we are in the situation at the beginning of the preceding* §1. *Then the isomorphism of monoids* [*cf.* [2, Proposition 3.5, (i), (ii)], [2, Proposition 3.7, (i)]]

$$\prod_{v\in\mathcal{V}_F^{d=1}} (F_v)_{\times} \xrightarrow{\sim} \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(Q_F)} k_{\times}(\mathfrak{D}) = \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(Q_F)} k(\mathfrak{D})_{\times}$$

restricts to a ***bijective*** *map of subsets*

$$\mathcal{F}(F,\infty) \xrightarrow{\sim} \mathcal{F}(Q_F,\infty).$$

(ii) *The subset* $\mathcal{F}(G,\infty) \subseteq \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})_{\times}$ *is* ***contained*** *in the subset* $\mathcal{H}_{\times}(G) \subseteq \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})_{\times}$*:*

$$\mathcal{F}(G,\infty) \subseteq \mathcal{H}_{\times}(G) \subseteq \prod_{\mathfrak{D}\in\mathcal{V}^{d=1}(G)} k(\mathfrak{D})_{\times}.$$

PROOF. — Assertion (i) follows immediately from Proposition 2.3, together with the various definitions involved [cf. also [2, Proposition 3.11, (i)]]. Assertion (ii) is a formal consequence of assertion (i) [cf. also [2, Proposition 3.11, (i)]]. $\square$

DEFINITION 2.6. — We shall write

$$F^{\mathrm{slv}}_{\mathrm{prm}}(G) \stackrel{\mathrm{def}}{=} \varinjlim_{H \subseteq G} \mathcal{F}(H, \infty) \subseteq \varinjlim_{H \subseteq G} \mathcal{H}_{\times}(H)$$

[cf. Proposition 2.5, (ii)] — where the injective limits are taken over the open subgroups $H \subseteq G$ of G [cf. also [2, Proposition 3.11, (iii)]] — for the ring obtained by forming the injective limit of the various rings $\mathcal{F}(H, \infty)$. Note that since [it is immediate that] the assignment "$G \mapsto F^{\mathrm{slv}}_{\mathrm{prm}}(G)$" is functorial with respect to isomorphisms of profinite groups, the action of G on G by conjugation induces an action of G on the ring $F^{\mathrm{slv}}_{\mathrm{prm}}(G)$.

PROPOSITION 2.7. — *The following assertions hold:*

(i) *Suppose that we are in the situation at the beginning of the preceding* §1. *Then the various isomorphisms* $\mathcal{H}_{\times}(F') \xrightarrow{\sim} \mathcal{H}_{\times}(\mathrm{Gal}(\widetilde{F}/F'))$ *of monoids* [*cf.* [2, Proposition 3.11, (i)]] — *where* F' *ranges over the intermediate fields of the extension* $\widetilde{F}/F$ *finite over* F — *determine a* Q_F***-equivariant isomorphism of rings***

$$F^{\mathrm{slv}}_{\mathrm{prm}} \xrightarrow{\sim} F^{\mathrm{slv}}_{\mathrm{prm}}(Q_F).$$

(ii) *The ring* $F^{\mathrm{slv}}_{\mathrm{prm}}(G)$ *is a* ***field*** *that is* ***absolutely Galois*** *and* ***solvably closed***. *In particular, the group of automorphisms of the field* $F^{\mathrm{slv}}_{\mathrm{prm}}(G)$ — *equipped with the* ***profinite topology*** *determined by the various subfields of* $F^{\mathrm{slv}}_{\mathrm{prm}}(G)$ *that are NF's* — *is a* ***profinite group of AGSC-type*** [*cf.* [2, Definition 3.2]].

PROOF. — Assertion (i) follows immediately from Lemma 1.4 and Proposition 2.5, (i), together with the various definitions involved. Assertion (ii) is a formal consequence of assertion (i). $\square$

3. MONO-ANABELIAN RECONSTRUCTION OF SOLVABLY CLOSED GALOIS EXTENSIONS

In the present §3, we finish establishing a *functorial "group-theoretic" reconstruction algorithm* for profinite groups *of GSC-type* [cf. Definition 3.8 below and Theorem 3.9 below]. In the present §3, we maintain the notational conventions introduced at the beginning of the preceding §2.

DEFINITION 3.1. — Let D be an element of $\widetilde{\mathcal{V}}(G)$.

(i) Write G_0 for the profinite group of automorphisms of the field $F^{\mathrm{slv}}_{\mathrm{prm}}(G)$ [cf. Proposition 2.7, (ii)]. Then it follows from the Grunwald-Wang theorem [cf., e.g., [7, Theorem 9.2.8]], together with Proposition 2.7, (i), and [2, Proposition 3.5, (i)], that the composite

$$D \hookrightarrow G \longrightarrow G_0$$

of the natural inclusion $D \hookrightarrow G$ and the action $G \to G_0$ of G on $F^{\mathrm{slv}}_{\mathrm{prm}}(G)$ [cf. Definition 2.6] is injective. Moreover, it follows immediately from [5, Proposition 2.3, (v)] and a similar argument to the argument applied in the proof of [7, Theorem 12.1.9], together with Proposition 2.7, (i), and [2, Proposition 3.5, (i)], that if one writes $C \subseteq G_0$ for the commensurator of the image of D in G_0 by the above displayed composite, then

- the subgroup C of G_0 is an element of $\widetilde{\mathcal{V}}(G_0)$ [cf. Proposition 2.7, (ii), [2, Proposition 3.5, (1)]], and

- the above displayed composite $D \hookrightarrow G_0$ factors through a continuous open injective homomorphism $D \hookrightarrow C$.

Thus, we have a field $\overline{k}(C)$ and a natural identification $\overline{k}(C)_\times = \overline{k}_\times(C)$ [cf. Proposition 2.7, (ii), [2, Theorem 1.4, (9)], [2, Proposition 5.8, (3)]]. Moreover, the field structure of the field $\overline{k}(C)$ and the isomorphism $\overline{k}_\times(D) \xrightarrow{\sim} \overline{k}_\times(C)$ of monoids induced by the resulting continuous open injective homomorphism $D \hookrightarrow C$ [cf. [2, Theorem 1.4, (9)]] determine

- a *field structure* on the monoid $\overline{k}_\times(D)$, whose resulting field we denote by

$$\overline{k}(D),$$

and

- a natural identification $\overline{k}(D)_\times = \overline{k}_\times(D)$.

(ii) We shall write

$$k(D) \stackrel{\mathrm{def}}{=} \overline{k}(D)^D$$

for the subfield of $\overline{k}(D)$ of D-invariants. Thus, it follows from [2, Theorem 1.4, (iv)] that we have a natural identification $k(D)_\times = k_\times(D)$.

PROPOSITION 3.2. — *The following assertions hold:*

(i) *Suppose that we are in the situation at the beginning of* §1. *Let $\widetilde{v}$ be an element of $\mathcal{V}_{\widetilde{F}}$. Write $v \stackrel{\mathrm{def}}{=} \widetilde{v}|_F \in \mathcal{V}_F$ for the restriction of $\widetilde{v} \in \mathcal{V}_{\widetilde{F}}$ to F and $D_{\widetilde{v}} \in \widetilde{\mathcal{V}}(Q_F)$ for the image of $\widetilde{v} \in \mathcal{V}_{\widetilde{F}}$ by the bijective map of* [2, Proposition 3.5, (i)]. *Then the commutative diagram of monoids*

$$\begin{array}{ccc} (F_v)_\times & \hookrightarrow & (\widetilde{F}_{\widetilde{v}})_\times \\ \wr\downarrow & & \downarrow\wr \\ k_\times(D_{\widetilde{v}}) & \hookrightarrow & \overline{k}_\times(D_{\widetilde{v}}) \end{array}$$

— *where the horizontal arrows are the natural inclusions, the left-hand vertical arrow is the isomorphism of monoids of* [2, Theorem 1.4, (iii)], *and the right-hand vertical arrow is the isomorphism of monoids of* [2, Theorem 1.4, (iv)] — *determines a* ***commutative diagram of fields***

$$\begin{array}{ccc} F_v & \hookrightarrow & \widetilde{F}_{\widetilde{v}} \\ \wr\downarrow & & \downarrow\wr \\ k(D_{\widetilde{v}}) & \hookrightarrow & \overline{k}(D_{\widetilde{v}}) \end{array}$$

— *where the horizontal arrows are the natural inclusions, and the right-hand vertical arrow is* $D_{\widetilde{v}}$***-equivariant****.*

(ii) *Let D be an element of $\widetilde{\mathcal{V}}(G)$. Then the action of D on the field $\overline{k}(D)$ determines a continuous* ***isomorphism***

$$D \xrightarrow{\sim} \mathrm{Gal}\big(\overline{k}(D)/k(D)\big).$$

Proof. — Assertion (i) follows immediately from [2, Proposition 5.8], together with the various definitions involved. Assertion (ii) is a formal consequence of assertion (i). □

Definition 3.3. — Let D be an element of $\widetilde{\mathcal{V}}(G)$. Then we shall say that a collection

$$F[D] \subseteq \widetilde{F}[D] \subseteq \overline{k}(D)$$

of two subfields $F[D] \subseteq \widetilde{F}[D]$ of $\overline{k}(D)$ is *of standard type* if the following four conditions are satisfied:

(1) The field $F[D]$ is an NF.

(2) The field $\widetilde{F}[D]$ is Galois over $F[D]$ and solvably closed.

(3) For each element of D, the action of the element of D on $\overline{k}(D)$ preserves the subfield $\widetilde{F}[D] \subseteq \overline{k}(D)$ and induces the identity automorphism of the subfield $F[D] \subseteq \widetilde{F}[D]$.

(4) There exists a continuous isomorphism $\mathrm{Gal}(\widetilde{F}[D]/F[D]) \xrightarrow{\sim} G$ [cf. (2)] such that the composite of the resulting homomorphism $D \to \mathrm{Gal}(\widetilde{F}[D]/F[D])$ [cf. (3)] and the isomorphism $\mathrm{Gal}(\widetilde{F}[D]/F[D]) \xrightarrow{\sim} G$ coincides with the natural inclusion $D \hookrightarrow G$.

Proposition 3.4 (Uchida). — *For $\Box \in \{\circ, \bullet\}$, let $F_\Box$ be an* ***NF*** *and $\widetilde{F}_\Box$ a Galois extension of $F_\Box$ that is* ***solvably closed****; write $Q_\Box \overset{\mathrm{def}}{=} \mathrm{Gal}(\widetilde{F}_\Box/F_\Box)$. Moreover, write*

$$\mathrm{Isom}(\widetilde{F}_\bullet/F_\bullet, \widetilde{F}_\circ/F_\circ)$$

for the set of isomorphisms $\widetilde{F}_\bullet \xrightarrow{\sim} \widetilde{F}_\circ$ of fields that restrict to isomorphisms $F_\bullet \xrightarrow{\sim} F_\circ$ of subfields and

$$\mathrm{Isom}(Q_\circ, Q_\bullet)$$

for the set of continuous isomorphisms $Q_\circ \xrightarrow{\sim} Q_\bullet$. Then the natural map

$$\mathrm{Isom}(\widetilde{F}_\bullet/F_\bullet, \widetilde{F}_\circ/F_\circ) \longrightarrow \mathrm{Isom}(Q_\circ, Q_\bullet)$$

is ***bijective****.*

Proof. — This assertion follows from [8, Theorem]. □

Lemma 3.5. — *The following assertions hold:*

(i) *In the situation of Proposition 3.4, let $\widetilde{v}_\circ$, $\widetilde{v}_\bullet$ be elements of $\mathcal{V}_{\widetilde{F}_\circ}$, $\mathcal{V}_{\widetilde{F}_\bullet}$, respectively. Write $D_\circ \in \widetilde{\mathcal{V}}(Q_\circ)$, $D_\bullet \in \widetilde{\mathcal{V}}(Q_\bullet)$ for the respective images of $\widetilde{v}_\circ$, $\widetilde{v}_\bullet$ by the bijective map of* [2, Proposition 3.5, (i)]*. Let α, β be continuous isomorphisms $Q_\circ \xrightarrow{\sim} Q_\bullet$ such* *that the* ***equalities*** $\alpha(D_\circ) = \beta(D_\circ) = D_\bullet$ *hold, and, moreover, the resulting continuous isomorphism* $\alpha|_{D_\circ}: D_\circ \xrightarrow{\sim} D_\bullet$ ***coincides*** *with the resulting continuous isomorphism* $\beta|_{D_\circ}: D_\circ \xrightarrow{\sim} D_\bullet$. *Then the* ***equality*** $\alpha = \beta$ *holds.*

(ii) *A continuous isomorphism* $\mathrm{Gal}(\widetilde{F}[D]/F[D]) \xrightarrow{\sim} G$ *as in condition* (4) *of Definition* 3.3 *is* ***unique***.

Proof. — First, we verify assertion (i). Write α^F, β^F for the respective isomorphisms $\widetilde{F}_\bullet \xrightarrow{\sim} \widetilde{F}_\circ$ of fields that correspond to α, β by the bijective map of Proposition 3.4. Then since $\alpha(D_\circ) = \beta(D_\circ) = D_\bullet$, one verifies easily that the isomorphisms α^F, β^F determine isomorphisms $(\widetilde{F}_\bullet)_{\widetilde{v}_\bullet} \xrightarrow{\sim} (\widetilde{F}_\circ)_{\widetilde{v}_\circ}$ of fields that restrict to isomorphisms $(F_\bullet)_{\widetilde{v}_\bullet|_{F_\bullet}} \xrightarrow{\sim} (F_\circ)_{\widetilde{v}_\circ|_{F_\circ}}$ of subfields, respectively. Write $\alpha^{F,v}$, $\beta^{F,v}$ for these isomorphisms $(\widetilde{F}_\bullet)_{\widetilde{v}_\bullet} \xrightarrow{\sim} (\widetilde{F}_\circ)_{\widetilde{v}_\circ}$, respectively; α^D, β^D for the continuous isomorphisms $D_\circ \xrightarrow{\sim} D_\bullet$ induced by the isomorphisms $\alpha^{F,v}, \beta^{F,v}: (\widetilde{F}_\bullet)_{\widetilde{v}_\bullet} \xrightarrow{\sim} (\widetilde{F}_\circ)_{\widetilde{v}_\circ}$, respectively. Now observe that it follows immediately from the various definitions involved that the *equalities* $\alpha|_{D_\circ} = \alpha^D$, $\beta|_{D_\circ} = \beta^D$ hold. Thus, it follows from our assumption that $\alpha^D = \beta^D$, which thus [cf., e.g., [4, Proposition 2.1]] implies that $\alpha^{F,v} = \beta^{F,v}$. In particular, one may conclude that $\alpha^F = \beta^F$, which thus implies that $\alpha = \beta$, as desired. This completes the proof of assertion (i).

Assertion (ii) is a formal consequence of assertion (i) [cf. also [2, Proposition 3.5, (i)]]. This completes the proof of Lemma 3.5. □

Lemma 3.6. — *The following assertions hold:*

(i) *Suppose that we are in the situation at the beginning of* §1. *Let* D *be an element of* $\widetilde{\mathcal{V}}(Q_F)$. *Write* $\widetilde{v}_D \in \mathcal{V}_{\widetilde{F}}$ *for the image of* $D \in \widetilde{\mathcal{V}}(Q_F)$ *by the bijective map of* [2, Proposition 3.5, (i)]. *Thus, it follows from Proposition* 3.2, (i), *that we have an isomorphism* $\widetilde{F}_{\widetilde{v}_D} \xrightarrow{\sim} \overline{k}(D)$ *of fields. Then the collection consisting of the two subfields of* $\overline{k}(D)$ *obtained by forming the images of the two subfields* $F \subseteq \widetilde{F}$ *of* $\widetilde{F}_{\widetilde{v}_D}$ *by the above isomorphism* $\widetilde{F}_{\widetilde{v}_D} \xrightarrow{\sim} \overline{k}(D)$ *is* ***of standard type*** [*i.e., with respect to the profinite group* Q_F *of GSC-type*].

(ii) *Let* D *be an element of* $\widetilde{\mathcal{V}}(G)$. *Then there* ***exists*** *a* ***unique*** *collection of two subfields of* $\overline{k}(D)$ ***of standard type***.

Proof. — Assertion (i) follows immediately from Proposition 3.2, (i), together with the various definitions involved. Next, we verify assertion (ii). The *existence* portion of assertion (ii) is a formal consequence of assertion (i) [cf. also Proposition 3.2, (i), [2, Proposition 3.5, (i)]]. To verify the *uniqueness* portion of assertion (ii), let

$$F[D]_\circ \subseteq \widetilde{F}[D]_\circ \subseteq \overline{k}(D), \qquad F[D]_\bullet \subseteq \widetilde{F}[D]_\bullet \subseteq \overline{k}(D)$$

be two collections *of standard type*. Now I claim the following assertion:

> Claim 3.6.A. — There exists a *D-equivariant* [cf. condition (3) of Definition 3.3] *isomorphism* of fields
>
> $$\iota_{\widetilde{F}}: \widetilde{F}[D]_\circ \xrightarrow{\sim} \widetilde{F}[D]_\bullet$$
>
> that restricts to an *isomorphism* $F[D]_\circ \xrightarrow{\sim} F[D]_\bullet$ of subfields.

To this end, let us observe that it follows immediately from Proposition 3.4, together with conditions (1), (2), (4) of Definition 3.3, that there exists an *isomorphism* $\iota_{\widetilde{F}}: \widetilde{F}[D]_\circ \xrightarrow{\sim}$

$\widetilde{F}[D]_\bullet$ of fields that restricts to an *isomorphism* $F[D]_\circ \overset{\sim}{\to} F[D]_\bullet$ of subfields such that the composite

$$G \xleftarrow{\sim} \mathrm{Gal}(\widetilde{F}[D]_\bullet/F[D]_\bullet) \xrightarrow{\sim} \mathrm{Gal}(\widetilde{F}[D]_\circ/F[D]_\circ) \xrightarrow{\sim} G$$

— where the first and third arrows are the respective unique [cf. Lemma 3.5, (ii)] isomorphisms of condition (4) of Definition 3.3, and the second arrow is the isomorphism obtained by conjugating by $\iota_{\widetilde{F}}$ — is the *identity automorphism* of G. Then one verifies immediately from condition (4) of Definition 3.3, together with the various definitions involved, that the isomorphism $\iota_{\widetilde{F}}$ is D*-equivariant*, as desired. This completes the proof of Claim 3.6.A.

For each $\square \in \{\circ, \bullet\}$, write

$$\iota_\square \colon \widetilde{F}[D]_\square^\times \longrightarrow {}_\infty H^1\Big(D, \Lambda\big(\overline{k}(D)\big)\Big)$$

for the homomorphism obtained by forming the composite

$$\widetilde{F}[D]_\square^\times = \varinjlim_H (\widetilde{F}[D]_\square^\times)^H \longrightarrow \varinjlim_H H^1\big(H, \Lambda(\widetilde{F}[D]_\square)\big)$$

$$= {}_\infty H^1\big(\mathrm{Gal}(\widetilde{F}[D]_\square/F[D]_\square), \Lambda(\widetilde{F}[D]_\square)\big) \xrightarrow{\sim} {}_\infty H^1\big(G, \Lambda(\widetilde{F}[D]_\square)\big) \longrightarrow {}_\infty H^1\Big(D, \Lambda\big(\overline{k}(D)\big)\Big)$$

— where the injective limits are taken over the open subgroups $H \subseteq \mathrm{Gal}(\widetilde{F}[D]_\square/F[D]_\square)$ of $\mathrm{Gal}(\widetilde{F}[D]_\square/F[D]_\square)$, we write $(\widetilde{F}[D]_\square^\times)^H \subseteq \widetilde{F}[D]_\square^\times$ for the submodule of $\widetilde{F}[D]_\square^\times$ of H-invariants, the first arrow is the homomorphism obtained by forming the injective limit of the various homomorphisms of [2, Lemma 3.10, (vi)], the second arrow is the isomorphism induced by the unique [cf. Lemma 3.5, (ii)] isomorphism of condition (4) of Definition 3.3, and the third arrow is the homomorphism induced by the natural inclusion $D \hookrightarrow G$ and the natural identifications $\Lambda(\widetilde{F}[D]_\square) = \Lambda(\overline{k}(D))$. Now I claim the following assertion:

> Claim 3.6.B. — To complete the verification of the *uniqueness* portion of assertion (ii), it suffices to verify the *commutativity* of the diagram of modules
>
> $$\begin{tikzcd} \widetilde{F}[D]_\circ^\times \arrow[dd, "\iota_{\widetilde{F}}|_{\widetilde{F}[D]_\circ^\times}"', "\wr"] \arrow[dr, "\iota_\circ"] & \\ & {}_\infty H^1\Big(D, \Lambda\big(\overline{k}(D)\big)\Big). \\ \widetilde{F}[D]_\bullet^\times \arrow[ur, "\iota_\bullet"'] & \end{tikzcd}$$

To this end, let us observe that it is immediate that, for each $\square \in \{\circ, \bullet\}$, the homomorphism $\iota_\square$ *factors* as the composite of the natural inclusion $\widetilde{F}[D]_\square^\times \hookrightarrow \overline{k}(D)^\times$ and the homomorphism

$$\overline{k}(D)^\times = \varinjlim_{H \subseteq D} \big(\overline{k}(D)^\times\big)^H \longrightarrow \varinjlim_{H \subseteq D} H^1\Big(H, \Lambda\big(\overline{k}(D)\big)\Big) = {}_\infty H^1\Big(D, \Lambda\big(\overline{k}(D)\big)\Big)$$

— where the injective limits are taken over the open subgroups $H \subseteq D$ of D, and we write $(\overline{k}(D)^\times)^H \subseteq \overline{k}(D)^\times$ for the submodule of $\overline{k}(D)^\times$ of H-invariants — obtained by forming the injective limit of the various homomorphisms of [2, Lemma 1.3, (x)] [cf. also Proposition 3.2, (ii)]. Thus, Claim 3.6.B follows from the *injectivity* proved in [2, Lemma 1.3, (x)]. This completes the proof of Claim 3.6.B.

Since the cyclotome $\Lambda(\overline{k}(D))$ associated to $\overline{k}(D)$ is *isomorphic*, as an abstract topological module, to the profinite completion $\widehat{\mathbb{Z}}$ of the infinite cyclic module $\mathbb{Z}$, the automorphism

$$\Lambda\big(\overline{k}(D)\big) = \Lambda(\widetilde{F}[D]_\circ) \xrightarrow{\sim} \Lambda(\widetilde{F}[D]_\bullet) = \Lambda\big(\overline{k}(D)\big)$$

induced by the isomorphism $\iota_{\widetilde{F}}$ is given by multiplication by an element of $\widehat{\mathbb{Z}}^\times$, which we denote by $a \in \widehat{\mathbb{Z}}^\times$. Now I claim the following assertion:

> Claim 3.6.C. — To complete the verification of the *uniqueness* portion of assertion (ii), it suffices to verify that $a = 1$.

To this end, let us observe that it follows immediately from Claim 3.6.A that we have a commutative diagram of modules

$$\begin{tikzcd}
\widetilde{F}[D]_\circ^\times \arrow[r, "\iota_\circ"] \arrow[d, "\iota_{\widetilde{F}}|_{\widetilde{F}[D]_\circ^\times}"', "\wr"] & {}_\infty H^1\Big(D, \Lambda\big(\overline{k}(D)\big)\Big) \arrow[d, "\wr"] \\
\widetilde{F}[D]_\bullet^\times \arrow[r, "\iota_\bullet"'] & {}_\infty H^1\Big(D, \Lambda\big(\overline{k}(D)\big)\Big)
\end{tikzcd}$$

— where the right-hand vertical arrow is the automorphism given by multiplication by $a \in \widehat{\mathbb{Z}}^\times$. Thus, Claim 3.6.C follows from Claim 3.6.B. This completes the proof of Claim 3.6.C.

For each $\Box \in \{\circ, \bullet\}$, write $\widetilde{F}[D]_\Box^D$ for the subfield of $\widetilde{F}[D]_\Box$ of D-invariants. Then it follows immediately from Claim 3.6.A that we have a commutative diagram of modules

$$\begin{tikzcd}
(\widetilde{F}[D]_\circ^D)^\times \arrow[r, "\iota_\circ|_{(\widetilde{F}[D]_\circ^D)^\times}"] \arrow[d, "\iota_{\widetilde{F}}|_{(\widetilde{F}[D]_\circ^D)^\times}"', "\wr"] & H^1\Big(D, \Lambda\big(\overline{k}(D)\big)\Big) \arrow[d, "\wr"] \\
(\widetilde{F}[D]_\bullet^D)^\times \arrow[r, "\iota_\bullet|_{(\widetilde{F}[D]_\bullet^D)^\times}"'] & H^1\Big(D, \Lambda\big(\overline{k}(D)\big)\Big)
\end{tikzcd}$$

— where the right-hand vertical arrow is the automorphism given by multiplication by $a \in \widehat{\mathbb{Z}}^\times$. Thus, it follows immediately from Proposition 3.2, (ii) [cf. also [2, Lemma 1.5, (i)]], that we have a commutative diagram of modules

$$\begin{tikzcd}
(\widetilde{F}[D]_\circ^D)^\times \arrow[r] \arrow[d, "\iota_{\widetilde{F}}|_{(\widetilde{F}[D]_\circ^D)^\times}"', "\wr"] & \mathbb{Z} \arrow[r] & \widehat{\mathbb{Z}} \arrow[d, "\wr"] \\
(\widetilde{F}[D]_\bullet^D)^\times \arrow[r] & \mathbb{Z} \arrow[r] & \widehat{\mathbb{Z}}
\end{tikzcd}$$

— where the left-hand upper, lower horizontal arrows are the [necessarily *nontrivial*] valuations on $\widetilde{F}[D]_\circ^D$, $\widetilde{F}[D]_\bullet^D$ obtained by forming the restrictions of a $p(D)$-adic valuation on $k(D)$, respectively, the right-hand horizontal arrows $\mathbb{Z} \to \widehat{\mathbb{Z}}$ are the natural homomorphisms, and the right-hand vertical arrow is the automorphism given by multiplication by $a \in \widehat{\mathbb{Z}}^\times$. Thus, since $\iota_{\widetilde{F}}$ is an *isomorphism of fields* [which thus implies that $\iota_{\widetilde{F}}$ maps $p(D) \in \widetilde{F}[D]_\circ^D$ to $p(D) \in \widetilde{F}[D]_\bullet^D$], one may conclude that $a = 1$, which thus [cf.

Claim 3.6.C] implies the *uniqueness* portion of assertion (ii). This completes the proof of the *uniqueness* portion of assertion (ii), hence also of assertion (ii). □

Definition 3.7. — Let D, E be elements of $\widetilde{\mathcal{V}}(G)$ and

$$F[D] \subseteq \widetilde{F}[D] \subseteq \overline{k}(D), \qquad F[E] \subseteq \widetilde{F}[E] \subseteq \overline{k}(E)$$

respective unique [cf. Lemma 3.6, (ii)] collections of two subfields of $\overline{k}(D)$, $\overline{k}(E)$ of standard type [cf. Lemma 3.6, (ii)]. Then it follows immediately from Proposition 3.4, together with conditions (1), (2), (4) of Definition 3.3, that there exists an isomorphism $\widetilde{F}[D] \xrightarrow{\sim} \widetilde{F}[E]$ of fields that restricts to an isomorphism $F[D] \xrightarrow{\sim} F[E]$ of subfields such that the composite

$$G \xleftarrow{\sim} \mathrm{Gal}(\widetilde{F}[E]/F[E]) \xrightarrow{\sim} \mathrm{Gal}(\widetilde{F}[D]/F[D]) \xrightarrow{\sim} G$$

— where the first and third arrows are the respective unique [cf. Lemma 3.5, (ii)] isomorphisms of condition (4) of Definition 3.3, and the second arrow is the isomorphism obtained by conjugating by the isomorphism $\widetilde{F}[D] \xrightarrow{\sim} \widetilde{F}[E]$ — is the identity automorphism of G. Observe that it follows from Proposition 3.4 that such an isomorphism is unique. We shall write

$$\iota_{D,E} \colon \widetilde{F}[D] \xrightarrow{\sim} \widetilde{F}[E]$$

for the unique isomorphism as above.

Definition 3.8. — For each $D \in \widetilde{\mathcal{V}}(G)$, let $F[D] \subseteq \widetilde{F}[D] \subseteq \overline{k}(D)$ be a unique [cf. Lemma 3.6, (ii)] collection of two subfields of $\overline{k}(D)$ of standard type [cf. Lemma 3.6, (ii)]. Then we shall write

$$\widetilde{F}(G) \subseteq \prod_{D \in \widetilde{\mathcal{V}}(G)} \widetilde{F}[D]$$

for the subset of the ring $\prod_{D \in \widetilde{\mathcal{V}}(G)} \widetilde{F}[D]$ consisting of the elements $(a_D)_D$ such that, for each D_1, $D_2 \in \widetilde{\mathcal{V}}(G)$, the equality $\iota_{D_1,D_2}(a_{D_1}) = a_{D_2}$ holds. Note that since [it is immediate that] the assignment "$G \mapsto \widetilde{F}(G)$" is functorial with respect to isomorphisms of profinite groups, the action of G on G by conjugation induces an action of G on the set $\widetilde{F}(G)$. We shall write

$$F(G) \overset{\mathrm{def}}{=} \widetilde{F}(G)^G$$

for the subset of $\widetilde{F}(G)$ of G-invariants.

Theorem 3.9. — *The following assertions hold:*

(i) *The subset $\widetilde{F}(G)$ of the ring $\prod_{D \in \widetilde{\mathcal{V}}(G)} \widetilde{F}[D]$ [cf. Definition* 3.8*] forms a* ***subring****. Moreover, the resulting ring is a* ***solvably closed field****.*

(ii) *The subset $F(G)$ of the field $\widetilde{F}(G)$ [cf.* (i)*] forms a* ***subfield****. Moreover, the resulting field is an* ***NF****.*

(iii) *The action of G on $\widetilde{F}(G)$ determines a continuous* ***isomorphism***

$$G \xrightarrow{\sim} \mathrm{Gal}\big(\widetilde{F}(G)/F(G)\big).$$

(iv) *Suppose that we are in the situation at the beginning of* §1*. Then the isomorphism of rings* [*cf. Proposition* 3.2*,* (i)*,* [2, Proposition 3.5, (i)]]

$$\prod_{\widetilde{v}\in\mathcal{V}_{\widetilde{F}}} \widetilde{F}_{\widetilde{v}} \xrightarrow{\sim} \prod_{D\in\widetilde{\mathcal{V}}(Q_F)} \overline{k}(D)$$

determines a ***commutative diagram of fields***

$$\begin{tikzcd} F \arrow[r, hook] \arrow[d, "\wr"'] & \widetilde{F} \arrow[d, "\wr"] \\ F(Q_F) \arrow[r, hook] & \widetilde{F}(Q_F) \end{tikzcd}$$

— where the horizontal arrows are the natural inclusions, and the right-hand vertical arrow is Q_F***-equivariant****.*

(v) *Let D be an element of $\widetilde{\mathcal{V}}(G)$. Then the natural inclusion $D \hookrightarrow G$ determines a* ***commutative diagram of fields***

$$\begin{tikzcd} F(G) \arrow[r, hook] \arrow[d, hook] & \widetilde{F}(G) \arrow[d, hook] \\ k(D) \arrow[r, hook] & \overline{k}(D) \end{tikzcd}$$

— where the horizontal arrows are the natural inclusions, and the right-hand vertical arrow is D***-equivariant****.*

Proof. — These assertions follow immediately from Proposition 3.2, (i), and Lemma 3.6, (i), (ii), together with the various definitions involved. □

Remark 3.9.1. — Let $G_\circ$, $G_\bullet$ be profinite groups *of GSC-type* and $\alpha\colon G_\circ \to G_\bullet$ a continuous *open* homomorphism.

(i) Suppose that α is *injective*. Then one verifies immediately that the homomorphism α determines a *commutative diagram of fields*

$$\begin{tikzcd} F(G_\bullet) \arrow[r, hook] \arrow[d, hook] & \widetilde{F}(G_\bullet) \arrow[d, "\wr"] \\ F(G_\circ) \arrow[r, hook] & \widetilde{F}(G_\circ) \end{tikzcd}$$

— where the horizontal arrows are the natural inclusions, and the right-hand vertical arrow is an isomorphism *compatible* with the respective actions of $G_\bullet$, $G_\circ$ relative to α.

(ii) Suppose that α is *surjective*, and that $\mathrm{Ker}(\alpha)$ has *no nontrivial finite abelian quotient*. Then one verifies immediately that the subfield $\widetilde{F}(G_\circ)^{\mathrm{Ker}(\alpha)}$ of $\widetilde{F}(G_\circ)$ of $\mathrm{Ker}(\alpha)$-invariants is *solvably closed*. Thus, it follows immediately from the construction of "$\widetilde{F}(-)$"

that the homomorphism α determines a *commutative diagram of fields*

$$\begin{tikzcd} F(G_\bullet) \arrow[r, hook] \arrow[d, "\wr"'] & \widetilde{F}(G_\bullet) \arrow[d, "\wr"] \\ F\big(G_\circ/\mathrm{Ker}(\alpha)\big) \arrow[r, hook] \arrow[d, "\wr"'] & \widetilde{F}\big(G_\circ/\mathrm{Ker}(\alpha)\big) \arrow[d, hook] \\ F(G_\circ) \arrow[r, hook] & \widetilde{F}(G_\circ) \end{tikzcd}$$

— where the horizontal arrows are the natural inclusions, the upper vertical arrows are the isomorphisms induced by the isomorphism $G_\circ/\mathrm{Ker}(\alpha) \xrightarrow{\sim} G_\bullet$ determined by α, and the right-hand upper vertical arrow is *compatible* with the respective actions of $G_\bullet$, $G_\circ$ relative to α.

(iii) Suppose that $\mathrm{Ker}(\alpha)$ has *no nontrivial finite abelian quotient.* Then it follows from (i), (ii) that the homomorphism α determines a *commutative diagram of fields*

$$\begin{tikzcd} F(G_\bullet) \arrow[r, hook] \arrow[d, hook] & \widetilde{F}(G_\bullet) \arrow[d, hook] \\ F(G_\circ) \arrow[r, hook] & \widetilde{F}(G_\circ) \end{tikzcd}$$

— where the horizontal arrows are the natural inclusions, and the right-hand vertical arrow is *compatible* with the respective actions of $G_\bullet$, $G_\circ$ relative to α. In particular, one may assert that the *"group-theoretic" algorithm*

$$G \qquad \mapsto \qquad \big(G \curvearrowright \widetilde{F}(G)\big)$$

established in the present paper is *functorial* with respect to *continuous open homomorphisms of profinite groups of GSC-type whose kernels have no nontrivial finite abelian quotients.*

Remark 3.9.2. — Note that, in the establishment of our reconstruction result, Uchida's theorem [i.e., Proposition 3.4] plays a crucial role [cf., e.g., the proof of Lemma 3.6, (ii)]. In particular, the proof of this reconstruction result does *not yield an alternative proof* of Uchida's theorem.

Remark 3.9.3. — We thus conclude from the reconstruction result obtained in the present paper that a profinite group *of GSC-type* admits a ring-theoretic basepoint [i.e., a "ring-theoretic interpretation" or a "ring-theoretic label"] *group-theoretically* constructed from the given profinite group.

References

[1] Y. Hoshi: Conditional results on the birational section conjecture over small number fields. *Automorphic forms and Galois representations. Vol. 2*, 187–230, London Math. Soc. Lecture Note Ser., **415**, *Cambridge Univ. Press, Cambridge*, 2014.

[2] Y. Hoshi: Mono-anabelian reconstruction of number fields. *On the examination and further development of inter-universal Teichmüller theory 2015*, 1–77, RIMS Kôkyûroku Bessatsu, **B76**, *Res. Inst. Math. Sci. (RIMS), Kyoto*, 2019.

[3] Y. Hoshi: Topics in the anabelian geometry of mixed-characteristic local fields. *Hiroshima Math. J.* **49** (2019), no. **3**, 323–398.

[4] Y. Hoshi: Introduction to mono-anabelian geometry. *Publications mathématiques de Besançon. Algèbre et théorie des nombres. 2021*, 5–44, Publ. Math. Besançon Algèbre Théorie Nr., 2021, *Presses Univ. Franche-Comté, Besançon*, 2022.

[5] S. Mochizuki: Global solvably closed anabelian geometry. *Math. J. Okayama Univ.* **48** (2006), 57–71.

[6] S. Mochizuki: Topics in absolute anabelian geometry III: global reconstruction algorithms. *J. Math. Sci. Univ. Tokyo* **22** (2015), no. **4**, 939–1156.

[7] J. Neukirch, A. Schmidt, and K. Wingberg: Cohomology of number fields. Second edition. Grundlehren der Mathematischen Wissenschaften, **323**. *Springer-Verlag, Berlin*, 2008.

[8] K. Uchida: Isomorphisms of Galois groups of solvably closed Galois extensions. *Tohoku Math. J. (2)* **31** (1979), no. **3**, 359–362.

(Yuichiro Hoshi) Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, JAPAN

Email address: `yuichiro@kurims.kyoto-u.ac.jp`