RIMS-2002

Purely Mono-anabelian Reconstruction of Number Fields I: Solvably Closed Case

By

Reiya TACHIHARA and Shota TSUJIMURA

September 2026

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

Purely Mono-anabelian Reconstruction of Number Fields I: Solvably Closed Case

Reiya Tachihara and Shota Tsujimura

September 3, 2026

Abstract

The classical Neukirch–Uchida theorem, established in the 1970s, asserts that number fields may be "reconstructed" from the Galois groups of their solvably closed Galois extensions, in the sense of the full faithfulness of a suitable functor obtained by forming Galois groups. This type of reconstruction is referred to as a *bi-anabelian* reconstruction in modern anabelian geometry. On the other hand, more recently, Hoshi established a group-theoretic reconstruction algorithm for a number field whose input data is the underlying topological group of the Galois group of a solvably closed Galois extension of the number field. This type of reconstruction is referred to as a *mono-anabelian* reconstruction in modern anabelian geometry. While mono-anabelian results are stronger than their bi-anabelian counterparts at the level of statements, the verification of Hoshi's algorithm depends on the corresponding bi-anabelian result, i.e., the Neukirch–Uchida theorem. In the present paper, we establish another such reconstruction algorithm, neither the construction nor the verification of which relies on the corresponding bi-anabelian result; we propose to refer to this type of reconstruction as a *purely mono-anabelian* reconstruction. In particular, we give an alternative proof of the Neukirch–Uchida theorem for number fields. Finally, as a first step toward the subsequent work in the present series of papers, we observe that the techniques of the present paper may be applied, in a mostly straightforward fashion, to yield a certain purely mono-anabelian reconstruction algorithm in the "finite-step solvable" setting as well.

2020 Mathematics Subject Classification. Primary 11R32; Secondary 11R34, 11S20, 11S25.

Key words and phrases. algebraic number theory, anabelian geometry, mono-anabelian geometry, reconstruction, Neukirch–Uchida theorem, number field, Galois cohomology, Kummer theory, solvably closed Galois extension, cyclotomic synchronization.

Contents

Introduction

In anabelian geometry, we often discuss the "reconstructibility" of geometric objects from their fundamental groups. The term "reconstruction", however, does not have a single fixed meaning; its definition depends on the context. Ever since the conjectures of Grothendieck that gave birth to this research area (cf. [Letter]), the term has commonly been used to mean the full faithfulness of a suitable functor obtained by forming fundamental groups; reconstruction in this sense is called a *bi-anabelian* reconstruction in modern anabelian geometry. In the case where the geometric objects are the spectra of fields, so that the fundamental groups in question are Galois groups, a basic example of a bi-anabelian result is the classical Neukirch–Uchida theorem, established in the 1970s:

Theorem 1 (Neukirch–Uchida)**.** *For* $\square \in \{\circ, \bullet\}$*, let* $E_\square$ *be a solvably closed Galois extension of a number field* $F_\square$*. Write* $\mathrm{Isom}(E_\circ/F_\circ, E_\bullet/F_\bullet)$ *for the set of field isomorphisms* $\sigma\colon E_\circ \xrightarrow{\cong} E_\bullet$ *that satisfy* $\sigma(F_\circ) = F_\bullet$*, and* $\mathrm{Isom}\big(\mathrm{Gal}(E_\circ/F_\circ), \mathrm{Gal}(E_\bullet/F_\bullet)\big)$ *for the set of isomorphisms* $\mathrm{Gal}(E_\circ/F_\circ) \xrightarrow{\cong} \mathrm{Gal}(E_\bullet/F_\bullet)$ *of profinite groups. Then the map*

$$\mathrm{Isom}(E_\circ/F_\circ, E_\bullet/F_\bullet) \longrightarrow \mathrm{Isom}\big(\mathrm{Gal}(E_\circ/F_\circ), \mathrm{Gal}(E_\bullet/F_\bullet)\big);\ \sigma \longmapsto (\tau \mapsto \sigma\tau\sigma^{-1})$$

is bijective (cf. [Uchida3]).

Remark. Theorem 1 remains valid if "a number field" is replaced by "a function field of a curve over a finite field" (cf. [Uchida2]); in the present paper, however, we shall be concerned exclusively with the case of number fields.

Besides the sense described above, the term "reconstruction" is also used in another, more intrinsic sense, due to Mochizuki (cf. [AbsTopI], Introduction), which reflects the ordinary meaning of the word more directly: to reconstruct a geometric object from its fundamental group is to establish a group-theoretic reconstruction algorithm whose input data is the underlying topological group of the fundamental group and whose output data is (an object canonically isomorphic to) the geometric object in question. Reconstruction in this sense is called a *mono-anabelian* reconstruction in modern anabelian geometry. Strictly speaking, the terminology "group-theoretic" should be replaced by "topological-group-theoretic", but this abuse of terminology is standard; it means that the

output of the algorithm depends only on the abstract topological group structure of the input. In particular, a group-theoretic algorithm should be (at least) isomorphism-functorial in the input topological group (i.e., with respect to isomorphisms of topological groups, which are not necessarily compatible with other additional structures).

A mono-anabelian result is stronger than the corresponding bi-anabelian result, in the sense that the latter may be deduced formally from the former (cf. the proof of Corollary 4.7 below); moreover, this comparison appears to be strict, in the sense that a bi-anabelian result does not, in general, yield the corresponding mono-anabelian result (cf. the comment (C1) below; also the question Q.4 below). On the other hand, there exist many bi-anabelian results in the literature whose proofs essentially give rise to group-theoretic reconstruction algorithms; for instance, the Neukirch–Uchida theorem for function fields of curves over finite fields is such a result (cf. [Sawada]). The Neukirch–Uchida theorem for number fields, however, is not such a result: the original proofs, due to Uchida (cf. [Uchida1]; [Uchida3]), do not give a group-theoretic reconstruction algorithm for a number field (as pointed out in the discussion of the terms "mono-anabelian"/"bi-anabelian" in the Introduction of [AbsTopIII]). (For a comparison between the number field case and the function field case, cf. Remark 4.4.3 below.) Therefore, it is natural to pose the following question:

> **Q.1**: Can we establish, for a number field, a mono-anabelian reconstruction algorithm whose input data is the underlying topological group of the Galois group of a solvably closed Galois extension of the number field?

In [MnNF] and [MnNF2], this question was answered affirmatively by Hoshi:

Theorem 2 (Hoshi)**.** *There exists a mono-anabelian reconstruction algorithm for the action* $\mathrm{Gal}(E/F) \curvearrowright E$*, whose input data is the abstract profinite group* $\mathrm{Gal}(E/F)$ *and whose output data is a field which is canonically isomorphic to the field* E *together with the action of* $\mathrm{Gal}(E/F)$ *on it, where* E *is a solvably closed Galois extension of a number field* F *(cf. [MnNF2], Theorem 3.9; also [MnNF], Theorem A).*

Remark. The above algorithm is obtained by first establishing a reconstruction algorithm for the base field "F", then applying it to each (normal) open subgroup of (the underlying topological group of) "$\mathrm{Gal}(E/F)$", and finally taking the inductive limit of the resulting fields; the action $\mathrm{Gal}(E/F) \curvearrowright E$ is induced by the conjugation action.

This result, together with its proof (i.e., the verification of the algorithm), substantially deepens our understanding of the anabelian phenomenon under consideration. However, the verification of Hoshi's algorithm depends on the Neukirch–Uchida theorem for number fields; in particular, the deduction of the bi-anabelian Neukirch–Uchida theorem from Hoshi's mono-anabelian result is circular, so that it does not give an alternative proof of the theorem. In light of this observation, in the present paper, we propose the notion of

purely mono-anabelian geometry

which explores the following question:

> **Q.2**: Can we establish, for a geometric object, a group-theoretic reconstruction algorithm whose input data is the underlying topological group of a fundamental group of the geometric object, and which is such that neither the construction nor the verification of the algorithm relies on the corresponding (or any) bi-anabelian result?

Purely mono-anabelian geometry is important in that it further deepens our understanding of the phenomenon; this may be seen concretely in the evident fact that an affirmative answer to Q.2 yields a non-circular proof of the corresponding bi-anabelian result. Specifically, in our situation, i.e., in the number field case, Q.2 becomes the following question:

> **Q.3**: Can we establish, for a number field, a mono-anabelian reconstruction algorithm whose input data is the underlying topological group of the Galois group of a solvably closed Galois extension of the number field, and which is pure in the sense that neither the construction nor the verification of the algorithm relies on the corresponding (or any) bi-anabelian result?

In the present paper, we give an affirmative answer to this question, which yields an alternative proof of the Neukirch–Uchida theorem for number fields. Our main result is as follows.

Theorem A (Purely mono-anabelian reconstruction of number fields)**.** *There exists a purely mono-anabelian reconstruction algorithm for the action* $\mathrm{Gal}(E/F) \curvearrowright E$*, whose input data is the abstract profinite group* $\mathrm{Gal}(E/F)$ *and whose output data is a field which is canonically isomorphic to the field* E *together with the action of* $\mathrm{Gal}(E/F)$ *on it, where* E *is a solvably closed Galois extension of a number field* F *(cf. Theorem 4.5 below; Theorem 4.6 below). Here, the use of the modifier "purely" indicates that neither the construction nor the verification of the algorithm relies on the corresponding (or any) bi-anabelian result (cf. Remark 4.6.1 below for more details on the phrase "or any"). In particular, one obtains an alternative proof of the classical Neukirch–Uchida theorem for number fields (cf. Theorem 1; Corollary 4.7 below).*

Remark. The Remark following Theorem 2 applies to Theorem A as well.

The notions of bi-anabelian and purely mono-anabelian reconstruction introduced above are the two extremes of a finer scale, whose intermediate levels make it possible to say precisely in what sense a mono-anabelian algorithm may still depend on a bi-anabelian result. Making this scale explicit allows one to locate the previous results — in particular, Theorem 2 — relative to Theorem A, and leads to a natural and intriguing question (cf. Q.4 below). For concreteness, we shall discuss the reconstruction of a number field from the Galois group G of a suitable Galois extension of the number field.

(L1) *Bi-anabelian results*: results to the effect that every isomorphism between the Galois groups under consideration arises from a (unique) isomorphism of the corresponding fields — e.g., the classical Neukirch–Uchida theorem (cf. also Remark 4.6.2 below).

(L2) *Pseudo mono-anabelian results* ("pseudo mono-anabelian" is a term introduced in [AbsTopIII], Remark 3.7.5, in the context of the reconstruction of function fields of hyperbolic orbicurves): Suppose that, in addition to a bi-anabelian result as in (L1), one is given a group-theoretic construction, from G, of a "container", i.e., roughly speaking, an object constructed group-theoretically from G that admits a natural embedding of the field under consideration whenever G arises from a field — e.g., a first Galois cohomology module of a group-theoretically constructed copy of "$\widehat{\mathbb{Z}}(1)$" (cf. the Kummer map), or the direct product of the abelianizations of the group-theoretically reconstructed (non-archimedean) decomposition subgroups (cf. the reciprocity maps). Then one obtains a "mono-anabelian-shaped" reconstruction, as follows: fix a reference model for each isomorphism class of the Galois groups under consideration; then transport the subset of the container of the reference model constituted by the field of the reference model to the container of G, via some isomorphism between G and the Galois group of the reference model. Here, the well-definedness of this transport, i.e., the independence of the resulting subset of the choices of the reference model and the isomorphism, is precisely what is guaranteed by the bi-anabelian result. Thus, symbolically: (L1) + (group-theoretic construction of a container) = (L2).

(L3) *Impurely mono-anabelian results*, or, alternatively, *bi-dependent mono-anabelian results* (cf. [MnNF]; [MnNF2]; [MS]): the reconstruction algorithm itself is "intrinsic" — i.e., constructed group-theoretically without any use of reference models or choices of isomorphisms — but the verification of the algorithm (including the well-definedness of its constituent steps) relies on the bi-anabelian result of (L1).

(L4) *Purely mono-anabelian results* (i.e., the results of the present paper): the reconstruction algorithm is intrinsic, and, moreover, neither the construction nor the verification of the algorithm relies on the corresponding (or any) bi-anabelian result (cf. Remark 4.6.1 below for more details on the phrase "or any"); in particular, the corresponding bi-anabelian result is obtained as a formal consequence (cf. Corollary 4.7 below).

Thus, roughly speaking, we have a hierarchy

$$\text{(L1)} \ < \ \text{(L1)} + \text{(container)} \ = \ \text{(L2)} \ < \ \text{(L3)} \ < \ \text{(L4)}.$$

Here, we make four comments on this hierarchy:

(C1) (on the inequality (L1) < (L2)) The group-theoretic construction of a container in (L2) is by no means automatic. For instance, in a setting where the decomposition subgroups degenerate (e.g., suitable "pro-Σ" settings — cf. [Shimizu2]), local class field theory is no longer available to reconstruct the full multiplicative group, and the relevant cohomology modules may shrink; in such a setting, even the construction of a container — hence even a pseudo mono-anabelian reconstruction as in (L2) — is non-trivial. In particular, a bi-anabelian result does not, by itself, yield even a pseudo mono-anabelian reconstruction.

(C2) (on the inequality (L2) < (L3)) Both a result as in (L2) and a result as in (L3) may be summarized as "establishing an algorithm for reconstructing

a number field by means of the corresponding bi-anabelian result". At this level of description, (L2) and (L3) appear to be of the same logical strength. The significance of (L3), however, lies rather in the intrinsic nature of the algorithm, which reflects a deeper understanding of the phenomenon. In fact, it is precisely this intrinsic nature of the portions of Hoshi's algorithm reviewed in §2 and §3 below that the present paper builds upon.

(C3) (on the gradation within (L2)) Let us consider the situation where, in the setting of solvably closed extensions of number fields, one assumes (L1) and wishes to obtain (L2), i.e., to construct a "container". Suppose, moreover, that one takes as the container the direct product of the abelianizations of the non-archimedean decomposition subgroups (cf. the reciprocity maps). In this case, the natural way to construct the container group-theoretically is simply to apply Neukirch's (purely mono-anabelian) reconstruction — i.e., characterization — of the decomposition subgroups (cf. Theorem 3.4 below). Alternatively, a cruder way is to exploit the assumption (L1) and to transport the decomposition subgroups themselves from a reference model via an isomorphism. Both ways yield an algorithm belonging to (L2), rather than to (L3), as long as (L1) is used in the subsequent argument; nevertheless, the use of Neukirch's characterization is plainly "closer to (L3)" than the latter transport argument. Thus there is a gradation even within (L2). A similar gradation may also be seen within (L3).

Here, we also remark that, in the case of the present example, the transport argument is not only far from (L3) but also circular: as far as the authors know, every existing proof of (L1) (i.e., the classical Neukirch–Uchida theorem) makes use of Neukirch's characterization, so that one would be using the reconstruction of the decomposition subgroups in order to reconstruct the decomposition subgroups.

(C4) (on the notion of mono-anabelian results) Throughout the above discussion, we have implicitly regarded a mono-anabelian result as consisting of two components: an algorithm and its verification. Here, two algorithms are to be regarded as distinct unless their constructions (i.e., the underlying sets and the structures) coincide. In particular, results may differ either in the algorithm — e.g., in the choice of containers (cf. the two examples of containers in (L2)) — or, for one and the same algorithm, in the nature of the verification (cf. the distinction between (L3) and (L4)). Accordingly, we fix all the constructions involved in the present paper (such as the construction of the cohomology of profinite groups) and regard distinct constructions as distinct; we do not attempt to formalize a general notion of "equivalence" of algorithms. Finally, we note that these distinctions are by no means pedantic: for instance, the improvements to be obtained in the subsequent work [TT2] will be achieved by modifying the algorithms of §5 of the present paper — while leaving their outputs unchanged up to canonical isomorphism — so that the modified algorithms apply to substantially more demanding reconstruction tasks, e.g., reconstruction from weaker input data.

In light of the above discussion, it is natural to pose the following question

(cf. also Remark 4.7.1 below):

> **Q.4**: For any bi-anabelian result, can we establish a purely mono-anabelian reconstruction algorithm that gives a proof of the original bi-anabelian result? (In the vocabulary of the above hierarchy: can a result as in (L1) always be lifted to one as in (L4)?)

The authors suspect that Q.4 has a negative answer in general, but do not know how to justify this suspicion; the comment (C1) above — to the effect that even the construction of a container may fail — may be regarded as evidence in this direction. We also note that even a precise formulation of Q.4 is a non-trivial task: it would require, in particular, precise general meta-mathematical notions of a "reconstruction algorithm", of its "verification", and of the "reliance" of the latter on a given bi-anabelian result (cf. the comment (C4) above).

Returning to the results of the present paper, we now discuss the main ingredients of the proof of Theorem A. For simplicity, we concentrate on the reconstruction algorithm for the base number field "F" (cf. the Remark following Theorem A). Let us introduce some notations here. We shall write $\mathcal{O}_F$ for the ring of integers of F; $\mathcal{V}_F$ for the set of non-archimedean primes of F; $F_{\mathfrak{p}}$ for the completion of F at $\mathfrak{p} \in \mathcal{V}_F$; $\mathcal{O}_{F_{\mathfrak{p}}}$ for the ring of integers of $F_{\mathfrak{p}}$; $\mathcal{V}_F^{d=1} \subset \mathcal{V}_F$ for the subset consisting of $\mathfrak{p} \in \mathcal{V}_F$ such that the natural homomorphism $\mathbb{Q}_p \hookrightarrow F_{\mathfrak{p}}$ is an isomorphism, where we write p for the residue characteristic of $\mathfrak{p}$. For an abelian group M, we shall write $\widehat{M}$ for the projective limit $\varprojlim_{n \geq 1} M/nM$, where the index set $\mathbb{Z}_{\geq 1}$ is equipped with the non-archimedean order, i.e., the order defined by divisibility, and the transition morphisms $M/nM \twoheadrightarrow M/n'M$, where n' divides n, are the natural projections. We shall refer to $\widehat{M}$ as the *Kummer completion* of M; this notion plays a central role throughout the present paper (cf. Definition 1.1 below; also Lemma 1.3 below for its relation to Kummer theory of fields). It is easily verified that $\widehat{\mathcal{O}_F^{\times}}$ and $F^{\times}$ naturally inject into $\widehat{F^{\times}}$ (cf. Lemma 1.4 below; Remark 1.1.7 below).

Our starting point is Kummer theory: once a cyclotome, i.e., a copy of "$\widehat{\mathbb{Z}}(1)$", has been reconstructed group-theoretically from $\mathrm{Gal}(E/F)$, the Kummer completion $\widehat{F^{\times}}$ may also be reconstructed group-theoretically as $H^1\big(\mathrm{Gal}(E/F), \widehat{\mathbb{Z}}(1)\big)$ (cf. Lemma 1.3 below; the assumption that E is solvably closed). Thus, naively, the problem of reconstructing the field F may be divided into the following three problems: the problem of reconstructing the cyclotome "$\widehat{\mathbb{Z}}(1)$"; the problem of *decompleting* $\widehat{F^{\times}}$, i.e., of isolating the subgroup $F^{\times} \subset \widehat{F^{\times}}$; and the problem of recovering the additive structure on $F = F^{\times} \cup \{0\}$. In what follows, we shall write $G \stackrel{\text{def}}{=} \mathrm{Gal}(E/F)$ to emphasize that the input data $\mathrm{Gal}(E/F)$ of the algorithm should be regarded as an abstract profinite group (i.e., rather than as a profinite group acting on a field). Roughly speaking, our purely mono-anabelian reconstruction of F proceeds in the following three steps:

(1) We reconstruct the *global cyclotome* $G \curvearrowright \Lambda^{\mathrm{gl}}(G)$, i.e., a cyclotome directly related to our global Galois group $G = \mathrm{Gal}(E/F)$, hence also the abelian group $H^1\big(G, \Lambda^{\mathrm{gl}}(G)\big)$, which is canonically isomorphic to the Kummer completion $\widehat{F^{\times}}$. Here, the adjective "global" reflects the fact that, for each non-archimedean decomposition subgroup $D \subset G$, we also

have a local analogue $D \curvearrowright \Lambda^{\mathrm{loc}}(D)$, which we shall refer to as the *local cyclotome*; these local cyclotomes are related, by construction, to the global one via the *local-global cyclotomic synchronization isomorphisms* $\Lambda^{\mathrm{gl}}(G) \xrightarrow{\cong} \Lambda^{\mathrm{loc}}(D)$.

(2) We reconstruct the subgroup

$$\mathcal{H}^{\times}(F) \stackrel{\mathrm{def}}{=} F^{\times} \cdot \widehat{\mathcal{O}_F^{\times}} \subset \widehat{F^{\times}}$$

(where we note that the actual definition of $\mathcal{H}^{\times}(F)$ is slightly different from, but essentially equivalent to, this definition — cf. Lemma 1.8 below); that is to say, we solve the decompletion problem "up to units". Also, we reconstruct the ring $\mathcal{R}(F) \stackrel{\mathrm{def}}{=} \prod_{\mathfrak{p} \in \mathcal{V}_F^{d=1}} F_{\mathfrak{p}}$, as well as the natural injective (cf. Lemma 1.9 below) homomorphism $\mathcal{H}^{\times}(F) \hookrightarrow \mathcal{R}(F)$ of multiplicative monoids. We shall refer to $\mathcal{H}^{\times}(F)$ as the *Kummer container* of F and to $\mathcal{R}(F)$ as the *ring container* of F; both containers play crucial roles in our algorithm, although the notation "$\mathcal{R}(F)$" and the terminology "ring container" are used only in the present Introduction. We note also that, strictly speaking, $\mathcal{R}(F)$ corresponds not to the ring "$\mathcal{R}(G)$" employed in the present paper (cf. Theorem 4.5, (1), below) — whose index set is, roughly speaking, a set of primes of E rather than of F — but rather to a certain "diagonal" subring of it; this difference is, however, inessential (cf. the discussion at the beginning of §4 below).

(3) We characterize the subset $F^{\times}$ inside the Kummer container $\mathcal{H}^{\times}(F)$; the additive structure on the resulting $F = F^{\times} \cup \{0\}$ is then obtained simply by observing that F is a subring of the ring container $\mathcal{R}(F)$.

Thus, Step (1) solves the first of the three problems discussed above; Step (2) gives a partial solution to the second; and Step (3) completes the solution to the second and, simultaneously, solves the third.

Steps (1) and (2) are entirely due to Hoshi (cf. [MnNF]; [MnNF2]); both steps are founded on Neukirch's group-theoretic characterization of the set $\mathbb{V}(G) \subset 2^G$ of the non-archimedean decomposition subgroups of $G = \mathrm{Gal}(E/F)$ (cf. Theorem 3.4 below; also the comment (C3) above); indeed, it is by way of the decomposition subgroups that the local theory reviewed in §2 below enters the discussion. In the following discussion, we will briefly review the contents of Steps (1) and (2), together with the local theory underlying them (cf. §2 and §3 below for more details), and then discuss the essential ideas of Step (3).

In the local theory, for each non-archimedean decomposition subgroup D of $G = \mathrm{Gal}(E/F)$ whose conjugacy class corresponds to $\mathfrak{p} \in \mathcal{V}_F$ (cf. Remark 3.5.1 below), we reconstruct the subgroups $\mathcal{O}^{\times}(D) \subset k^{\times}(D) \subset D^{\mathrm{ab}}$ which correspond to the images of $\mathcal{O}_{F_{\mathfrak{p}}}^{\times}$ and $F_{\mathfrak{p}}^{\times}$ via the local reciprocity map, as well as the local cyclotome $\Lambda^{\mathrm{loc}}(D)$. Moreover, if $\mathfrak{p} \in \mathcal{V}_F^{d=1}$ (a condition which may be verified group-theoretically from D), we also reconstruct the field structure on "$k^{\times}(D) \cup \{0\}$"; here, we note in advance that this essentially completes the reconstruction of the ring container appearing in Step (2). We also make a historical remark here: most of the local theory involved in the present paper was essentially classically well-known to experts, while the reconstruction of the ring structure in the case of $\mathbb{Q}_p$ is due to Hoshi (cf. [MLFTop], Definition 5.2; also Lemma 2.7 below).

In Step (1), we reconstruct the global cyclotome $\Lambda^{\mathrm{gl}}(G)$ by means of a consideration of the "finite idèles" $\mathbb{I}^{\mathrm{fin}}(G) \subset \prod_{D \in \mathbb{V}(G)} k^{\times}(D)$ (i.e., an analogue of the idèles obtained by ignoring the archimedean primes) and the "finite reciprocity map" $\mathbb{I}^{\mathrm{fin}}(G) \longrightarrow G^{\mathrm{ab}}$. In contrast to Step (2), Kummer theory plays no role in Step (1).

In Step (2), we reconstruct the Kummer container $\mathcal{H}^{\times}(F) \subset \widehat{F^{\times}}$ by pulling back the subgroup $\mathbb{I}^{\mathrm{fin}}(G) \hookrightarrow \prod_{D \in \mathbb{V}(G)} H^1\big(D, \Lambda^{\mathrm{loc}}(D)\big)$ via the natural homomorphism $H^1\big(G, \Lambda^{\mathrm{gl}}(G)\big) \hookrightarrow \prod_{D \in \mathbb{V}(G)} H^1\big(D, \Lambda^{\mathrm{loc}}(D)\big)$. Note that the local cyclotomes and the local-global synchronization isomorphisms both play indispensable roles here. Indeed, it is the local cyclotome $\Lambda^{\mathrm{loc}}(D)$ that makes available the local Kummer-theoretic inclusion $k^{\times}(D) \hookrightarrow H^1\big(D, \Lambda^{\mathrm{loc}}(D)\big)$, hence the former of the two homomorphisms above, while it is the synchronization isomorphisms that make available the latter (cf. Remark 3.8.1 below for a more detailed discussion). Finally, as already mentioned above, the reconstruction of the ring container $\mathcal{R}(F)$ is immediate from the local theory; it is precisely here that restricting our attention to the subset $\mathcal{V}_F^{d=1} \subset \mathcal{V}_F$ is essential. The natural injective homomorphism from the Kummer container to the ring container is also obtained automatically from the above constructions.

Now we explain the key ideas of Step (3), which constitutes the main novelty of the present paper. The fundamental heuristic here is that, from the viewpoint of the ring structure of F, Kummer completion appears to be a highly *transcendental* operation; that is to say, the new elements produced by the completion — i.e., the elements of $\widehat{F^{\times}} \setminus F^{\times}$ — should behave like "transcendental" elements. While $\widehat{F^{\times}}$ does not have an ambient ring structure, $\mathcal{H}^{\times}(F) \subset \widehat{F^{\times}}$ does admit one, namely, the ring container $\mathcal{R}(F)$ (cf. the injective homomorphism obtained in Step (2)). Thus the above heuristic leads to the following expectation, where we note the immediate but crucial fact that $\mathcal{R}(F)$ has a natural $\mathbb{Q}$-algebra structure:

> *$F^{\times}$ ought to consist precisely of those elements of the Kummer container that are algebraic over $\mathbb{Q}$.*

Unfortunately, the authors were unable to justify this expectation as stated (cf. also Remark 4.4.2 below). On the other hand, in the context of reconstruction, one is always free to impose further group-theoretically meaningful *necessary* conditions on the elements under consideration; the task is complete as soon as the accumulated necessary conditions become *sufficient*. Here, for simplicity, let us assume that F is Galois over $\mathbb{Q}$; then, in the present situation, we supplement the algebraicity condition with the requirements that the $\mathbb{Q}$-subalgebra of $\mathcal{R}(F)$ generated by the element in question be a field and that the resulting field admit an embedding into F (cf. Lemma 4.4 below). We note that the group-theoreticity of the latter condition is by no means trivial, since F is the very object under reconstruction; we obtain a group-theoretic characterization of this condition by way of a classical consequence of the Chebotarev density theorem (cf. Lemma 4.3 below). Note also that the ring container has thus played a double role: it supplies the ring-theoretic notions by means of which $F^{\times}$ is characterized, and it equips the resulting F with its field structure (cf. also Remark 4.4.1 below for more details, including a comparison with Hoshi's algorithm established in [MnNF2]).

Write $a \in \mathcal{H}^{\times}(F) \subset \mathcal{R}(F)$ for the element under consideration (i.e., an element satisfying the necessary conditions discussed above). Then the heart of the proof of the sufficiency (i.e., $a \in F \subset \mathcal{R}(F)$) lies in resolving the following discrepancy: the conditions assert only that the subfield generated by a is *abstractly* embeddable into F, while the desired conclusion is that the element a itself *lies in* F; that is to say, a is, so far, merely a *"candidate"* for a genuine element of F. Nevertheless, the candidate may be compared with genuine elements pointwise, i.e., at each prime in $\mathcal{V}_F^{d=1}$: at each such prime, the candidate a necessarily agrees (inside the local field "$\mathbb{Q}_p$") with one of the *finitely many genuine* elements constituted by the "$\mathbb{Q}$-conjugates" of a in F — i.e., the roots in F of the minimal polynomial of a over $\mathbb{Q}$, whose existence is precisely what the abstract embedding above guarantees (cf. the additional simplifying assumption that F is Galois over $\mathbb{Q}$). Thus, away from finitely many primes, $\mathcal{V}_F^{d=1}$ admits a finite partition, according to which of these genuine elements the candidate a agrees with. Finally, a classical theorem of Grunewald and Segal concerning congruence topologies on number fields (cf. [congtop], Theorem A; [TsjmGS], Theorem 0.1; Lemma 4.2 below) guarantees that at least one piece of this finite partition is "large" enough to promote the pointwise coincidence over it to an actual, global coincidence; in other words, *the candidate is, in fact, genuine* (cf. the proof of Lemma 4.4 below for details).

We conclude the present discussion by making explicit the mechanism that underlies Step (3): the gap between the desired object (i.e., "F") and a candidate object is overcome by means of a certain finite partition of the underlying set of "points" (i.e., $\mathcal{V}_F^{d=1}$), and this finite partition arises from a "core" object (i.e., "$\mathbb{Q}$"; concretely, the partition is indexed by the "$\mathbb{Q}$-conjugates" above); here, roughly speaking, by a "core" we mean a structure which is available independently of the particular object in question, and which may thus serve as a common standard of comparison (cf., e.g., [GeoAnbd] and [AbsTopIII] for more details on the notion of "core"). The authors expect that consideration of this kind — i.e., the use of a "core" to bridge such a gap — will prompt further development of anabelian geometry (cf. also Remark 4.4.3 below).

Finally, we discuss a "finite-step solvable" variant of Theorem A (cf. Theorem B below), which is obtained by applying almost the same argument as in the proof of Theorem A. However, this variant is already stronger than the finite-step solvable mono-anabelian results previously known in the literature (which will be discussed below); we take this as evidence of the fruitfulness of the purely mono-anabelian point of view of the present paper. Here, we note that the definitive treatment of the finite-step solvable variants — including a strengthening of Theorem B, by building on and substantially extending the techniques of the present paper — will be given in the subsequent work [TT2]; accordingly, in the present paper, we content ourselves with an outline of the proof of Theorem B (cf. the discussion at the beginning of §5 below).

In order to state Theorem B, we introduce several "finite-step solvable" notations. For a profinite group G, we define, inductively, $G[0] \stackrel{\text{def}}{=} G$ and $G[i] \stackrel{\text{def}}{=} \overline{[G[i-1], G[i-1]]}$, i.e., the closure of the commutator subgroup of $G[i-1]$, for $i \in \mathbb{Z}_{\geq 1}$. For $m \in \mathbb{Z}_{\geq 0}$, we shall refer to the quotient $G/G[m]$ as the *maximal m-step solvable quotient* of G. Similarly, for a field F and $m \in \mathbb{Z}_{\geq 0}$, we define, inductively, up to (not necessarily unique) F-isomorphism,

$F_0 \stackrel{\text{def}}{=} F$ and F_m to be the maximal abelian extension of F_{m-1}; we shall refer to F_m as a/the *maximal m-step solvable extension* of F. Thus, F_m may be realized, inside a fixed separable closure F^{sep} of F, as the subfield of F^{sep} corresponding to the closed subgroup $\text{Gal}(F^{\text{sep}}/F)[m] \subset \text{Gal}(F^{\text{sep}}/F)$; in particular, F_m/F is a Galois extension, and $\text{Gal}(F_m/F)$ is the maximal m-step solvable quotient of $\text{Gal}(F^{\text{sep}}/F)$. (For more details, see the discussion entitled "Fields and Field Extensions" in §0 below.) Then our second main result is as follows.

Theorem B (A "4-step loss" finite-step solvable version of the purely mono-anabelian reconstruction of number fields)**.** *Let $m \in \mathbb{Z}_{\geq 1}$. Then there exists a purely mono-anabelian reconstruction algorithm for the action $\text{Gal}(F_m/F) \curvearrowright F_m$, whose input data is the abstract profinite group $\text{Gal}(F_{m+4}/F)$ and whose output data is a field which is canonically isomorphic to the field F_m together with the action of $\text{Gal}(F_m/F)$ on it, where F is a number field, F_{m+4} is a maximal $(m+4)$-step solvable extension of F, and F_m is the maximal m-step solvable extension of F inside F_{m+4} (cf. Theorem 5.6 below).*

Remark. By replacing the use of a "2-step loss" reconstruction algorithm for non-archimedean decomposition subgroups with the "1-step loss" refinement which the authors learned of through an announcement by Akio Tamagawa at a conference (cf. Remark 5.5.1 below), we may easily modify our algorithm of Theorem B to "3-step loss" (cf. Remark 5.6.2 below).

Here, we briefly compare Theorem B with the previous works. First, Theorem B may be regarded as a partial refinement of the bi-anabelian result of Saïdi and Tamagawa, which asserts, roughly speaking, that the isomorphism class of the field extension F_m/F is determined, in a functorial bi-anabelian fashion, by the abstract topological group $\text{Gal}(F_{m+3}/F)$ (resp. $\text{Gal}(F_{m+4}/F)$), where $m \in \mathbb{Z}_{\geq 2}$ (resp. $m \in \{0, 1\}$) and F is a number field (cf. [ST], Theorem 2). While Theorem B is less sharp than this result in that it does not cover the case $m = 0$ and requires a larger "step loss" (i.e., "4" as opposed to "3") when $m \geq 2$, it has the evident advantage of being (purely) mono-anabelian. On the other hand, we should emphasize that Theorem B relies on the reconstruction of the non-archimedean decomposition subgroups — an intermediate result of [ST] which is itself purely mono-anabelian.

Next, in the recent work [MS], Mao and Saïdi established a mono-anabelian reconstruction algorithm for "$\text{Gal}(F_m/F) \curvearrowright F_m$" from "$\text{Gal}(F_{m+9}/F)$", where $m \geq 3$, i.e., a "9-step loss" algorithm (cf. [MS], Theorem 1). However, as is emphasized in [MS], Introduction, their algorithm depends on the statement of the bi-anabelian result of [ST] in an essential way; in particular, their algorithm is not "purely" mono-anabelian in the sense of the present paper, and it does not yield an alternative proof of the bi-anabelian result of [ST]. Thus, Theorem B improves on the algorithm of [MS] both in the "step loss" and in the "purity". Finally, in [Mao], Mao established a purely mono-anabelian reconstruction algorithm for an abelian number field F from "$\text{Gal}(F_6/F)$" (cf. [Mao], Theorem 1.2; also [MS], Theorem 2, which treats, in a similar fashion, the case where F is an imaginary quadratic field or $\mathbb{Q}$); Theorem B may be regarded as a refinement of these results in the sense that it applies to arbitrary number fields and only requires the input "$\text{Gal}(F_5/F)$" (i.e., the case where $m = 1$). A more detailed comparison will be given in §5 below.

The present paper is organized as follows.

In §0, we fix the notations and conventions employed in the present paper.

In §1, we develop the general theory of Kummer completions and introduce the notion of the Kummer containers of a number field, which play central roles in the present paper.

In §2, we review various local "intermediate steps" of our reconstruction algorithm which were established by other researchers; §2 does not contain any new results. In particular, we review the reconstruction algorithm for the multiplicative group of a mixed characteristic local field, as well as the field structure on it in the case of $\mathbb{Q}_p$.

In §3, we continue to review previous results established by other researchers, switching our attention to the global ones; §3 does not contain any new results either. In particular, we review the reconstruction algorithm for the Kummer container.

In §4, in light of the various reconstruction algorithms reviewed in §2 and §3, we establish the first main result of the present paper, that is to say, the purely mono-anabelian reconstruction algorithm for number fields (cf. Theorem A above; Theorem 4.5 below; Theorem 4.6 below), together with an alternative, mono-anabelian proof of the classical Neukirch–Uchida theorem (cf. Corollary 4.7 below). The technical core of our approach is Lemma 4.2 below, which is a formal consequence of a classical result of Grunewald and Segal (cf. [congtop], Theorem A; [TsjmGS], Theorem 0.1).

Finally, in §5, as a first step toward the "finite-step solvable" variants of our algorithm to be developed in the subsequent work [TT2], we establish a purely mono-anabelian reconstruction algorithm for "$\mathrm{Gal}(F_m/F) \curvearrowright F_m$" from "$\mathrm{Gal}(F_{m+4}/F)$", where F is a number field and $m \in \mathbb{Z}_{\geq 1}$ (cf. Theorem B above; Theorem 5.6 below), and compare this result with the previous works.

0 Notations and Conventions

Numbers

We shall write $\mathbb{Z}_{\geq 0}$ for the set of non-negative rational integers. We shall write $\mathbb{Z}_{\geq 1}$ for the set of positive rational integers. We shall write $\mathbb{Z}$ for the set of rational integers. We shall write $\mathbb{Q}$ for the set of rational numbers. We shall write $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) for the p-adic completion of $\mathbb{Z}$ (resp. $\mathbb{Q}$). We shall write $\widehat{\mathbb{Z}}$ for the profinite completion of $\mathbb{Z}$ (cf. the discussion entitled "Topological Groups" below).

We shall refer to the order of integers defined by the usual "$\leq$", i.e., $x \leq y \iff y - x$ is non-negative (resp. defined by the division relation, i.e., $x \mid y \iff$ there exists an integer z such that $y = xz$) as the *archimedean* (resp. the *non-archimedean*) *order*.

Topological Groups

A topological group is referred to as a *profinite group* if it is isomorphic, as a topological group, to the projective limit of some projective system of discrete finite groups. In particular, the Galois group of a (not necessarily finite) Galois extension of fields is naturally regarded as a profinite group.

For a group G, we shall write $\hat{G}$ for the *profinite completion* of G, i.e., the profinite group obtained as the projective limit $\varprojlim_{[G:H]<\infty} G/H$, where H ranges over all normal subgroups of G of finite index. We warn the reader that this notation "$\hat{G}$" should be carefully distinguished from the notation "$\widehat{G}$" for the Kummer completion introduced in Definition 1.1 below, which is meaningful only in the case where G is abelian (cf. also Remark 1.1.3 and Remark 1.1.4 below for the relation between the two notions).

For a topological group G, we shall write G^{ab} for the abelianization of G, i.e., the quotient of G by the closure of the commutator subgroup of G. For a topological group G, we define, inductively, $G[0] \stackrel{\mathrm{def}}{=} G$ and $G[i] \stackrel{\mathrm{def}}{=} \overline{[G[i-1], G[i-1]]}$, i.e., the closure of the commutator subgroup of $G[i-1]$, for $i \in \mathbb{Z}_{\geq 1}$. Thus, each $G[i]$ is a characteristic (hence normal) closed subgroup of G, and $G[1]$ coincides with the kernel of the natural surjection $G \twoheadrightarrow G^{\mathrm{ab}}$. For $m \in \mathbb{Z}_{\geq 0}$, we shall refer to the quotient $G/G[m]$ as the *maximal m-step solvable quotient* of G. We shall say that G is *m-step solvable* if $G[m] = \{1\}$.

Monoids

If M is a monoid for whose binary operation we write multiplicatively, then we shall write $M^{\circledast} \stackrel{\mathrm{def}}{=} M \amalg \{0_M\}$, where 0_M is a formal symbol, and we extend the binary operation on M to $M^{\circledast}$ by setting $0_M \cdot a = a \cdot 0_M = 0_M$ for every $a \in M^{\circledast}$.

Rings and Modules

All rings that appear in the present paper are unital and commutative. For a ring A, we shall write $A^{\times}$ for the group of units of A. For an integral domain A, we shall write $\mathrm{Frac}\, A$ for the quotient field of A (e.g., $\mathbb{Q} = \mathrm{Frac}\, \mathbb{Z}$).

If M is an abelian group, then we shall write $M[n]$ for the kernel of the multiplication-by-n map $M \longrightarrow M$; we shall write $M_{\mathrm{tor}} \stackrel{\mathrm{def}}{=} \bigcup_{n \geq 1} M[n]$. Thus M_{tor} is the subgroup of M constituted by all torsion elements of M. This notation may conflict with the notation "$G[i]$" for the derived series of a topological group G introduced above; however, no confusion will actually arise in the present paper.

Fields and Field Extensions

A field (resp. a valuation field) F is referred to as a *number field* (resp. a *mixed characteristic local field*) if it is isomorphic to a finite extension of $\mathbb{Q}$ (resp. a finite extension of $\mathbb{Q}_p$ with the unique extension to F of the natural discrete valuation on $\mathbb{Q}_p$). The letters "E" and "F" (resp. "K" and "L") will typically denote algebraic extensions of number fields (resp. mixed characteristic local fields). Note, however, that "E" and "F" may also denote general fields.

A field F is referred to as *solvably closed* if there exists no non-trivial finite abelian extension of F (or, equivalently, if there exists no non-trivial finite Galois extension of F whose Galois group is solvable).

For a number field F, we write $\mathcal{O}_F$ for the ring of integers of F, i.e., the integral closure of $\mathbb{Z}$ in F. For a mixed characteristic local field K, we write $\mathcal{O}_K$ for the ring of integers of K, i.e., the valuation ring of K.

For a number field F, we write $\mathcal{V}_F$ for the set of non-archimedean primes of F; we write $F_{\mathfrak{p}}$ for the completion of F at $\mathfrak{p} \in \mathcal{V}_F$. (This notation will be generalized to infinite extensions of number fields in Definition 3.2 below.) Also, we write $\mathcal{V}_F^{d=1}$ for the subset of $\mathcal{V}_F$ consisting of non-archimedean primes that "split completely" over $\mathbb{Q}$; the precise meaning is as follows. Write p for the prime number that underlies $\mathfrak{p} \in \mathcal{V}_F$ (i.e., the residue characteristic of $F_{\mathfrak{p}}$). Then we have a natural (continuous) ring homomorphism $\mathbb{Q}_p \hookrightarrow F_{\mathfrak{p}}$. Under this notation, we define $\mathcal{V}_F^{d=1} \stackrel{\text{def}}{=} \{\mathfrak{p} \in \mathcal{V}_F \mid \mathbb{Q}_p \to F_{\mathfrak{p}} \text{ is an isom.}\}$. The fact that $\mathcal{V}_F^{d=1} \subset \mathcal{V}_F$ is of natural density 1, hence of Dirichlet density 1 (cf. the discussion preceding [Neukirch], Chapter VII, Theorem (13.2)) is of frequent use in the present paper.

Here, we note that the valuation on a mixed characteristic local field may be reconstructed from its underlying field — indeed, $\mathcal{O}_K^\times$ is the unique subgroup M of $K^\times$ such that $K^\times/M \cong \mathbb{Z}$ (cf. the well-known structure of $K^\times$), and $\mathcal{O}_K$ is the subring of K generated by $\mathcal{O}_K^\times$. In particular, an isomorphism between the underlying fields of two mixed characteristic local fields is automatically compatible with the valuations, so that we shall not distinguish between the two possible meanings of "$\cong$" for mixed characteristic local fields.

For a field F and $m \in \mathbb{Z}_{\geq 0}$, we inductively define, up to (not necessarily unique) F-isomorphism, $F_0 \stackrel{\text{def}}{=} F$ and F_m the maximal abelian extension of F_{m-1} (which is determined up to F_{m-1}-isomorphism). In particular, F_1 is the maximal abelian extension of F, and F_m may be realized, inside a fixed separable closure F^{sep} of F, as the subfield of F^{sep} corresponding to the closed subgroup $\text{Gal}(F^{\text{sep}}/F)[m] \subset \text{Gal}(F^{\text{sep}}/F)$. Since this is a characteristic, hence a normal subgroup of $\text{Gal}(F^{\text{sep}}/F)$, it follows that F_m/F is a Galois extension. We shall refer to F_m as a/the *maximal m-step solvable extension* of F. Although the isomorphism class of F_m (as an F-algebra) is determined by F, we do not have a canonical way of identifying two isomorphic copies of F_m. Thus we prefer to say "a" maximal m-step solvable extension of F (i.e., rather than "the" maximal m-step solvable extension of F). In particular, we prefer to say "a" maximal abelian extension of F (i.e., rather than "the" maximal abelian extension of F). On the other hand, if F_m is a maximal m-step solvable extension of F, then we have "the" maximal n-step solvable extension F_n of F inside F_m for $0 \leq n \leq m$.

1 Kummer Completions and the Kummer Containers

In the present section, we discuss some generalities on a construction which we call "Kummer completion". It is closely related to the Kummer theory of fields of characteristic 0 and thus plays a crucial role in our purely mono-anabelian reconstruction algorithm for number fields.

Definition 1.1. Let M be an abelian group. Then we shall write $\widehat{M} \stackrel{\text{def}}{=} \varprojlim_{n \geq 1} M/nM$, where the index set $\mathbb{Z}_{\geq 1}$ is equipped with the non-archimedean order (cf. the discussion entitled "Numbers" in §0), and the transition map $M/n'M \longrightarrow M/nM$, where n divides n', is given by the natural projection. We shall refer to $\widehat{M}$ as the *Kummer completion* of M. We shall regard $\widehat{M}$ as a $\widehat{\mathbb{Z}}$-module in the natural way.

Remark 1.1.1. For an abelian group M, we have a natural homomorphism $M \longrightarrow \widehat{M}$; the operation of taking the Kummer completion determines a functor from the category of abelian groups to the category of $\widehat{\mathbb{Z}}$-modules.

Remark 1.1.2. Let M be an abelian group and N an abelian subgroup of M. Then the following inclusion holds:

$$\mathrm{Ker}(N \longrightarrow \widehat{N}) = \bigcap_{n \geq 1} nN \subset \bigcap_{n \geq 1} nM = \mathrm{Ker}(M \longrightarrow \widehat{M}).$$

In particular, if the natural homomorphism $M \longrightarrow \widehat{M}$ is injective, then so is the natural homomorphism $N \longrightarrow \widehat{N}$. (Note, however, that the natural homomorphism $\widehat{N} \longrightarrow \widehat{M}$ is not necessarily injective.) This descent property is particularly important in the case where M is the multiplicative group of a field E, and N is the multiplicative group of some subfield of E.

Remark 1.1.3. The Kummer completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$ coincides with the usual $\widehat{\mathbb{Z}}$, i.e., the profinite completion of $\mathbb{Z}$. More generally, for every finitely generated abelian group M, the Kummer completion $\widehat{M}$ of M coincides with the profinite completion $\hat{M}$ of M (cf. the discussion entitled "Topological Groups" in §0), which is, in light of the finitely-generatedness of M, canonically isomorphic to $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M$. In particular, in this case, the natural map $M \longrightarrow \widehat{M}$ is injective (cf. the well-known fact that $\widehat{\mathbb{Z}}$ is faithfully flat over $\mathbb{Z}$, or one may prefer a more direct argument).

Remark 1.1.4. In the context of Remark 1.1.3, it is of interest to note that a similar coincidence does not necessarily hold for a more general abelian group, as the following counterexample shows. Let $M = \bigoplus_{i \in I} \mathbb{Z}$, where I is an infinite set (i.e., M is a free abelian group of infinite rank). Then we claim that we have the following natural commutative diagram, whose upper horizontal injective arrows are not surjective (hence not isomorphisms, as desired):

$$\begin{array}{ccccccc}
\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M & = & \bigoplus_{i \in I} \widehat{\mathbb{Z}} & \hookrightarrow & \widehat{M} & \hookrightarrow & \hat{M} \\
 & & & \searrow^{\not=} & \downarrow^{\not=} & \swarrow_{\not=} & \\
 & & & & \prod_{i \in I} \widehat{\mathbb{Z}}, & &
\end{array}$$

where we recall that we write $\hat{M}$ for the profinite completion of M. Indeed, it follows from the construction that $\widehat{M}$ may be regarded as a $\widehat{\mathbb{Z}}$-submodule of $\prod_{i \in I} \widehat{\mathbb{Z}}$ constituted by the elements $(a_i)_{i \in I}$ such that, for every $n \in \mathbb{Z}_{\geq 1}$, n divides a_i for all but finitely many $i \in I$; this explains the left-hand triangle of the above diagram. Also, one verifies immediately that the natural continuous homomorphism $\hat{M} \longrightarrow \prod_{i \in I} \widehat{\mathbb{Z}}$ of profinite groups is surjective; this surjectivity,

combined with the non-surjectivity of the middle vertical arrow, implies that the right-hand upper horizontal arrow is not surjective either. Finally, the verification of the non-injectivity of the right-hand slanted arrow is left to the interested reader, since we do not need it. (We note, however, that the explicit description of $\widehat{M}$ inside $\prod_{i \in I} \widehat{\mathbb{Z}}$ given above will be of use in the proof of Lemma 1.8 below.)

Remark 1.1.5. We shall say that an abelian group M is *Kummer complete* if the natural homomorphism $M \longrightarrow \widehat{M}$ is an isomorphism; this terminology will not be employed elsewhere in the present paper. Then it is of independent interest to note the fact that the Kummer completion $\widehat{M}$ of an abelian group M is itself Kummer complete; that is to say, the natural homomorphism $\widehat{M} \longrightarrow \widehat{\widehat{M}}$ is an isomorphism. Note that this fact yields another (somewhat indirect) verification of the existence of "counterexamples" as in Remark 1.1.4: since the operation $M \mapsto \widehat{M}$ is idempotent in the above sense, while the operation $M \mapsto \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M$ is not — cf., e.g., the natural surjection $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}} \longrightarrow\!\!\!\!\rightarrow \widehat{\mathbb{Z}}$, which is not injective — the natural homomorphism $\widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} M \longrightarrow \widehat{M}$ fails to be an isomorphism for some abelian group M (i.e., e.g., $M = \widehat{\mathbb{Z}}$). A similar remark applies to the comparison with the profinite completion (cf. Remark 4.1.1 below).

A sketch of the proof of the isomorphism $\widehat{M} \longrightarrow \widehat{\widehat{M}}$ is as follows; the details are left to the interested reader, since we do not need this isomorphism in the present paper. It follows immediately from the Chinese remainder theorem that $\widehat{M}$ is naturally isomorphic to $\prod_p M^{\wedge}_p$, where p ranges over prime numbers, and $M^{\wedge}_p$ denotes the p-adic completion $\varprojlim_{e \geq 1} M/p^e M$ of M. Then, since $M^{\wedge}_p$ itself is p-adically complete (a well-known, but non-trivial, fact; cf. [Stacks], Tag 05GG), and the multiplication-by-l map for a prime number $l \neq p$ is an automorphism of $M^{\wedge}_p$, we obtain the desired isomorphism $\widehat{M} \xrightarrow{\cong} \widehat{\widehat{M}}$.

Remark 1.1.6. If K is a mixed characteristic local field, then it follows from the well-known structure of $K^{\times}$ and $\mathcal{O}_K^{\times}$ that the natural homomorphism $K^{\times} \longrightarrow \widehat{K^{\times}}$ is injective and that $\mathcal{O}_K^{\times} \longrightarrow \widehat{\mathcal{O}_K^{\times}}$ is an isomorphism. In particular, the natural homomorphism $\widehat{\mathcal{O}_K^{\times}} \longrightarrow \widehat{K^{\times}}$ is also injective.

Remark 1.1.7. Let F be a number field. Then the natural homomorphism $F^{\times} \longrightarrow \widehat{F^{\times}}$ is injective. Indeed, consider the completion $F_{\mathfrak{p}}$ of F associated to some non-archimedean prime $\mathfrak{p} \in \mathcal{V}_F$; then the desired injectivity follows immediately from Remark 1.1.2 applied to "$(N \subset M)$" $= (F^{\times} \subset F_{\mathfrak{p}}^{\times})$ and Remark 1.1.6 applied to "K" $= F_{\mathfrak{p}}$.

Definition 1.2. Let F be a field and $n \in \mathbb{Z}_{\geq 1}$. Then we shall write $\mu(F)$ (resp. $\mu_n(F)$; $\Lambda(F)$) for the subgroup of $F^{\times}$ constituted by the roots of unity, i.e., $(F^{\times})_{\mathrm{tor}}$ (resp. the subgroup of $F^{\times}$ constituted by the n-th roots of unity, i.e., $F^{\times}[n] = \mu(F)[n]$; the projective limit $\varprojlim_{n \geq 1} \mu_n(F)$, where the index set $\mathbb{Z}_{\geq 1}$ is equipped with the non-archimedean order — cf. the discussion entitled "Numbers" in §0 — and the transition map $\mu_{n'}(F) \longrightarrow \mu_n(F)$, where n divides n', is given by the (n'/n)-th power map).

Lemma 1.3. *Let F be a field of characteristic 0 and E/F a Galois extension. Then the following assertions hold:*

(1) *For every* $n \in \mathbb{Z}_{\geq 1}$, *we have a canonical isomorphism of abelian groups* $\big(F^\times \cap (E^\times)^n\big)/(F^\times)^n \xrightarrow{\cong} H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big)$. *In particular, if* $F^\times \subset (E^\times)^n$ *(e.g., if* E *is an algebraic closure of* F*), then we have a canonical isomorphism* $F^\times/(F^\times)^n \xrightarrow{\cong} H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big)$.

(2) *By varying* $n \in \mathbb{Z}_{\geq 1}$ *in the assertion (1) and taking the projective limit, we obtain a canonical isomorphism of* $\widehat{\mathbb{Z}}$*-modules* $\varprojlim_{n\geq 1}\big(F^\times \cap (E^\times)^n\big)/(F^\times)^n \xrightarrow{\cong} H^1\big(\mathrm{Gal}(E/F), \Lambda(E)\big)$. *In particular, if* $F^\times \subset (E^\times)^n$ *for every* $n \in \mathbb{Z}_{\geq 1}$, *i.e.,* $F^\times$ *is divisible in* $E^\times$, *then we have a canonical isomorphism of* $\widehat{\mathbb{Z}}$*-modules* $\widehat{F^\times} \xrightarrow{\cong} H^1\big(\mathrm{Gal}(E/F), \Lambda(E)\big)$.

(3) *Let* F'/F *be a subextension of* E/F. *Then, for each* $n \in \mathbb{Z}_{\geq 1}$, *we have the following commutative diagram:*

$$\begin{array}{ccc} \big(F^\times \cap (E^\times)^n\big)/(F^\times)^n & \xrightarrow{\cong} & H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big) \\ {\scriptstyle natural}\downarrow & & \downarrow{\scriptstyle \mathrm{Res}} \\ \big((F')^\times \cap (E^\times)^n\big)/\big((F')^\times\big)^n & \xrightarrow{\cong} & H^1\big(\mathrm{Gal}(E/F'), \mu_n(E)\big), \end{array}$$

where the horizontal isomorphisms are those discussed in the assertion (1). In particular, by varying $n \in \mathbb{Z}_{\geq 1}$ *and taking the projective limit, we obtain the following commutative diagram:*

$$\begin{array}{ccc} \varprojlim_{n\geq 1}\big(F^\times \cap (E^\times)^n\big)/(F^\times)^n & \xrightarrow{\cong} & H^1\big(\mathrm{Gal}(E/F), \Lambda(E)\big) \\ {\scriptstyle natural}\downarrow & & \downarrow{\scriptstyle \mathrm{Res}} \\ \varprojlim_{n\geq 1}\big((F')^\times \cap (E^\times)^n\big)/\big((F')^\times\big)^n & \xrightarrow{\cong} & H^1\big(\mathrm{Gal}(E/F'), \Lambda(E)\big), \end{array}$$

where the horizontal isomorphisms are those discussed in the assertion (2). Moreover, if F'/F *is also Galois, then the lower horizontal isomorphisms in the above two diagrams are both compatible with the natural actions of* $\mathrm{Gal}(F'/F)$.

Proof. The assertion (1) follows immediately from the well-known Kummer theory, which we briefly review here. We have a short exact sequence of $\mathrm{Gal}(E/F)$-modules $1 \to \mu_n(E) \to E^\times \xrightarrow{(-)^n} (E^\times)^n \to 1$. By taking the cohomology exact sequence and applying "Hilbert 90", i.e., $H^1\big(\mathrm{Gal}(E/F), E^\times\big) = 0$, we obtain the desired result. The assertion (2) follows immediately from the assertion (1). The assertion (3) follows from the construction of the diagrams. This completes the proof of Lemma 1.3. □

Lemma 1.4. *Let* A *be an integrally closed domain (e.g., a Dedekind domain) and* $F = \mathrm{Frac}\, A$. *Then the natural homomorphism* $\widehat{A^\times} \longrightarrow \widehat{F^\times}$ *is injective.*

Proof. It suffices to show that the natural map $A^\times/(A^\times)^n \longrightarrow F^\times/(F^\times)^n$ is injective for every $n \geq 1$. Put another way, we want the inclusion $(F^\times)^n \cap A^\times \subset (A^\times)^n$. Let $a \in F^\times$. Suppose that $a^n \in A^\times$. Since A is integrally closed in F and $a^n \in A^\times \subset A$, it follows that $a \in A$. Now $a \in A$ and $a^n \in A^\times$ immediately imply that $a \in A^\times$, as desired. This completes the proof of Lemma 1.4. □

Corollary 1.5. *Let F be a number field and $H \subset F^\times$ a finitely generated subgroup. Then the natural homomorphism $\widehat{H} \longrightarrow \widehat{F^\times}$ is injective.*

Proof. For $\mathfrak{p} \in \mathcal{V}_F$, write $v_\mathfrak{p}$ for the normalized additive valuation $F \longrightarrow \mathbb{Z} \cup \{\infty\}$ determined by $\mathfrak{p}$. Also, for a finite subset $S \subset \mathcal{V}_F$, write $\mathcal{O}_{F,S}$ for the subring of *S-integers* of F, i.e., $\mathcal{O}_{F,S} \stackrel{\text{def}}{=} \{x \in F \mid \forall \mathfrak{p} \in \mathcal{V}_F \setminus S,\ v_\mathfrak{p}(x) \geq 0\}$; it is well-known that $\mathcal{O}_{F,S}$ is a Dedekind domain. Then it follows from the well-known "S-unit version of Dirichlet's unit theorem" (cf. [Neukirch], Chapter I, Corollary (11.7)) that $\mathcal{O}_{F,S}^\times$ is a finitely generated abelian group, and the desired injectivity in the special case where $H = \mathcal{O}_{F,S}^\times$ follows immediately from Lemma 1.4; in fact, only this special case will be of use in the present paper, and thus the reader may safely skip the remainder of the present proof.

For the general case, fix a finite system of generators $x_1, \ldots, x_k$ of H and write $S \stackrel{\text{def}}{=} \bigcup_{1 \leq i \leq k} \{\mathfrak{p} \in \mathcal{V}_F \mid v_\mathfrak{p}(x_i) \neq 0\}$. Note that S is finite and $H \subset \mathcal{O}_{F,S}^\times$. It follows immediately from Remark 1.1.3, together with the well-known fact that $\widehat{\mathbb{Z}}$ is flat over $\mathbb{Z}$, that the natural map $\widehat{H} \longrightarrow \widehat{\mathcal{O}_{F,S}^\times}$ is injective. Since the natural homomorphism $\widehat{H} \longrightarrow \widehat{F^\times}$ under consideration coincides with the composition of this injective homomorphism with the injective homomorphism $\widehat{\mathcal{O}_{F,S}^\times} \longrightarrow \widehat{F^\times}$ discussed above, we obtain the desired injectivity. This completes the proof of the general case of Corollary 1.5. $\square$

Remark 1.5.1. As mentioned in the proof, Corollary 1.5 is employed in the present paper only in the case where H is the group of "S-units"; that is to say, the injectivity of the natural map $\widehat{\mathcal{O}_{F,S}^\times} \longrightarrow \widehat{F^\times}$ is sufficient for the present paper. We included the more general result for the convenience of future reference.

Lemma 1.6. *Let F be a field of characteristic 0 and $F \longrightarrow E$ a finite extension of fields. Write $E \longrightarrow \widetilde{E}$ for a Galois closure of E over F. Suppose that, for every prime number l, $\mu_{l^\infty}(\widetilde{E}) \stackrel{\text{def}}{=} \bigcup_{n \geq 1} \mu_{l^n}(\widetilde{E})$ is finite. Then the following assertions hold:*

(1) The natural map $\widehat{F^\times} \longrightarrow \widehat{E^\times}$ is injective.

(2) Suppose further that the finite extension E/F is Galois, i.e., $E = \widetilde{E}$. Then the equality $\widehat{F^\times} = \widehat{E^\times}^{\mathrm{Gal}(E/F)}$ holds, where we identify $\widehat{F^\times}$ with its image in $\widehat{E^\times}$ in light of the assertion (1).

Proof. First, we verify the assertion (1). It suffices to show that the composition of the natural maps $\widehat{F^\times} \longrightarrow \widehat{E^\times} \longrightarrow \widehat{\widetilde{E}^\times}$, which coincides with the natural map $\widehat{F^\times} \longrightarrow \widehat{\widetilde{E}^\times}$, is injective. Thus we may assume without loss of generality that the finite extension E/F is Galois, i.e., $E = \widetilde{E}$. By Lemma 1.3, (3), for each $n \geq 1$, we have a natural commutative diagram

$$\begin{array}{ccc} F^\times/(F^\times)^n & \xrightarrow{\cong} & H^1\big(\mathrm{Gal}(\overline{E}/F), \mu_n(\overline{E})\big) \\ {\scriptstyle \text{natural}}\downarrow & & \downarrow{\scriptstyle \text{Res}} \\ E^\times/(E^\times)^n & \xrightarrow{\cong} & H^1\big(\mathrm{Gal}(\overline{E}/E), \mu_n(\overline{E})\big), \end{array}$$

where we fix an algebraic closure $E \hookrightarrow \overline{E}$. Thus it suffices to show that the projective limit, where we vary n, of the kernel of the right-hand vertical arrow is 0. On the other hand, this follows easily from the finiteness assumption on $\mu_{l^\infty}(E)$, as discussed below. We have the well-known inflation-restriction exact sequence (cf. [NSW], Proposition (1.6.7))

$$0 \longrightarrow H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big) \longrightarrow H^1\big(\mathrm{Gal}(\overline{E}/F), \mu_n(\overline{E})\big) \longrightarrow H^1\big(\mathrm{Gal}(\overline{E}/E), \mu_n(\overline{E})\big),$$

so it suffices to show that $\varprojlim_{n\geq 1} H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big) = 0$. Let $a \in \varprojlim_{n\geq 1} H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big)$, and write $a_m \in H^1\big(\mathrm{Gal}(E/F), \mu_m(E)\big)$ for the image of a via the natural map $\varprojlim_{n\geq 1} H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big) \longrightarrow H^1\big(\mathrm{Gal}(E/F), \mu_m(E)\big)$, where $m \in \mathbb{Z}_{\geq 1}$. It suffices to show that $a_m = 0$ for every positive integer m. Write $m = l_1^{c_1} \cdots l_k^{c_k}$ for the prime factorization of m, where $l_1, \ldots, l_k$ are prime numbers and $c_1, \ldots, c_k$ are positive integers; $d_i \stackrel{\text{def}}{=} \log_{l_i}\big(\#\mu_{l_i^\infty}(E)\big)$ (cf. the assumption that $\mu_{l_i^\infty}(E)$ is finite); $s \stackrel{\text{def}}{=} l_1^{d_1} \cdots l_k^{d_k}$. Then it is immediate that the s-th power map $\mu_{ms}(E) \stackrel{(-)^s}{\longrightarrow} \mu_m(E)$ is the trivial map. This implies that the natural map $H^1\big(\mathrm{Gal}(E/F), \mu_{ms}(E)\big) \longrightarrow H^1\big(\mathrm{Gal}(E/F), \mu_m(E)\big)$ is also the zero map. On the other hand, a_m is, by definition, equal to the image of a_{ms} via this natural map. Thus we conclude that $a_m = 0$, as desired. (Essentially, we have shown that $\Lambda(\overline{E})^{\mathrm{Gal}(\overline{E}/E)} = 0$ under the finiteness assumption on $\mu_{l^\infty}(E)$. Thus we could also have obtained our result by $\varprojlim_{n\geq 1} H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big) = H^1\big(\mathrm{Gal}(E/F), \Lambda(\overline{E})^{\mathrm{Gal}(\overline{E}/E)}\big) = 0$.)

Next, we verify the assertion (2). Before beginning the proof, we note that the assertion (2) will never be employed in the present paper (cf. Remark 1.6.1 below); thus the reader may feel free to skip this proof. It is well-known (cf. [NSW], Proposition (1.6.7)) that we also have the following exact sequence:

$$\begin{array}{ccccc} H^1\big(\mathrm{Gal}(\overline{E}/F), \mu_n(\overline{E})\big) & \twoheadrightarrow & H^1\big(\mathrm{Gal}(\overline{E}/E), \mu_n(\overline{E})\big)^{\mathrm{Gal}(E/F)} & \twoheadrightarrow & H^2\big(\mathrm{Gal}(E/F), \mu_n(E)\big). \\ \cong\uparrow & & \cong\uparrow & & \\ F^\times/(F^\times)^n & \longrightarrow & \big(E^\times/(E^\times)^n\big)^{\mathrm{Gal}(E/F)} & & \end{array}$$

Note that, for the same reason as in the proof of $\varprojlim_{n\geq 1} H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big) = 0$ in the proof of the assertion (1) (i.e., in essence, the vanishing $\Lambda(\overline{E})^{\mathrm{Gal}(\overline{E}/E)} = 0$), we have $\varprojlim_{n\geq 1} H^2\big(\mathrm{Gal}(E/F), \mu_n(E)\big) = 0$. In light of this observation, we wish to take the projective limit of the above exact sequence to obtain the conclusion, but we should take care of certain Mittag-Leffler conditions (cf. Remark 1.6.2 below; note that some special care is required here since the index set of the projective system is not isomorphic to $\mathbb{Z}_{\geq 0}$ with the usual archimedean order).

For each $n \in \mathbb{Z}_{\geq 1}$, we have the following two short exact sequences:

$$1 \longrightarrow \big(F^\times \cap (E^\times)^n\big)/(F^\times)^n \longrightarrow F^\times/(F^\times)^n \longrightarrow A_n \longrightarrow 1;$$

$$1 \longrightarrow A_n \longrightarrow \big(E^\times/(E^\times)^n\big)^{\mathrm{Gal}(E/F)} \longrightarrow B_n \longrightarrow 1,$$

where we write A_n for the image of the natural map

$$F^\times/(F^\times)^n \longrightarrow \big(E^\times/(E^\times)^n\big)^{\mathrm{Gal}(E/F)};$$

B_n for the image of the natural map

$$\big(E^\times/(E^\times)^n\big)^{\mathrm{Gal}(E/F)} \stackrel{\cong}{\longrightarrow} H^1\big(\mathrm{Gal}(\overline{E}/E), \mu_n(\overline{E})\big)^{\mathrm{Gal}(E/F)} \longrightarrow H^2\big(\mathrm{Gal}(E/F), \mu_n(E)\big).$$

Note that $\varprojlim_{n\geq 1} H^2\big(\mathrm{Gal}(E/F), \mu_n(E)\big) = 0$ immediately implies that $\varprojlim_{n\geq 1} B_n = 0$. Then, since the operation of taking the projective limit is left exact, it follows from the second short exact sequence above, together with the equality $\varprojlim_{n\geq 1} B_n = 0$, that the natural map $\varprojlim_{n\geq 1} A_n \longrightarrow \varprojlim_{n\geq 1} \big(E^\times/(E^\times)^n\big)^{\mathrm{Gal}(E/F)} = (\widehat{E^\times})^{\mathrm{Gal}(E/F)}$ is an isomorphism. Thus it suffices to show that the natural map $\varprojlim_{n\geq 1} F^\times/(F^\times)^n \longrightarrow \varprojlim_{n\geq 1} A_n$ is surjective, which will follow immediately from the Mittag-Leffler condition (cf. Remark 1.6.2 below) of the system $\Big(\big(F^\times \cap (E^\times)^n\big)/(F^\times)^n\Big)_{n\geq 1}$ applied to the first short exact sequence above. On the other hand, the desired Mittag-Leffler condition follows immediately from the isomorphism $\big(F^\times \cap (E^\times)^n\big)/(F^\times)^n \stackrel{\cong}{\longrightarrow} H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big)$, together with the obvious fact that $H^1\big(\mathrm{Gal}(E/F), \mu_n(E)\big)$ is a finite group. This completes the proof of the assertion (2), hence also the proof of Lemma 1.6. □

Remark 1.6.1. Lemma 1.6 is closely related to [MT], Lemma 1.12. The authors decided to include the assertion (2), which will never be employed in the present paper, in Lemma 1.6 in order to make the relation between Lemma 1.6 and [MT], Lemma 1.12, clearer. It is perhaps also of interest to note that these results are highly reminiscent of the Galois theory of fields, although, at the time of writing the present paper, the authors are unable to judge how useful this observation might be.

Remark 1.6.2. In the present remark, we review the basic facts on the Mittag-Leffler condition and discuss some variant which was employed in the proof of Lemma 1.6, (2). Since Lemma 1.6, (2), is never employed in the present paper, the reader may feel free to skip this remark.

Let $(0 \longrightarrow A_\lambda \longrightarrow B_\lambda \longrightarrow C_\lambda \longrightarrow 0)_{\lambda\in\Lambda}$ be a projective system of short exact sequences of abelian groups indexed by a directed ordered set Λ. In particular, if $\lambda, \lambda' \in \Lambda$ satisfy $\lambda \leq \lambda'$, then we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_{\lambda'} & \longrightarrow & B_{\lambda'} & \longrightarrow & C_{\lambda'} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_\lambda & \longrightarrow & B_\lambda & \longrightarrow & C_\lambda & \longrightarrow & 0. \end{array}$$

We will be happy if this projective system induces a short exact sequence

$$0 \longrightarrow \varprojlim_{\lambda\in\Lambda} A_\lambda \longrightarrow \varprojlim_{\lambda\in\Lambda} B_\lambda \longrightarrow \varprojlim_{\lambda\in\Lambda} C_\lambda \longrightarrow 0,$$

but this is only left exact in general, i.e., the natural map $\varprojlim_{\lambda\in\Lambda} B_\lambda \longrightarrow \varprojlim_{\lambda\in\Lambda} C_\lambda$ is not necessarily surjective in general. On the other hand, it is well-known that, if $\Lambda = \mathbb{Z}_{\geq 0}$ with the usual archimedean order (cf. the discussion entitled "Numbers" in §0) and the system $(A_\lambda)_{\lambda\in\Lambda} = (A_n)_{n\geq 0}$ satisfies the so-called Mittag-Leffler condition (which we review below), then we also have the right-hand surjectivity. Here, we recall that the projective system $(A_n)_{n\geq 0}$ satisfies the Mittag-Leffler condition if, for every $m \geq 0$, the descending chain of subgroups

$$A_m \supset \mathrm{Im}(A_{m+1} \to A_m) \supset \mathrm{Im}(A_{m+2} \to A_m) \supset \cdots$$

stabilizes. For example, if every $A_{m+1} \longrightarrow A_m$ is surjective, or if every A_m is finite, then $(A_n)_{n\geq 0}$ obviously satisfies the Mittag-Leffler condition.

We wish to apply the fact that "Mittag-Leffler condition implies exactness" to our situation, but then it appears to be problematic that the index (directed ordered) set of our projective system is $\mathbb{Z}_{\geq 1}$ with the non-archimedean order (cf. the discussion entitled "Numbers" in §0), which is far from being isomorphic to $\mathbb{Z}_{\geq 0}$ with the usual archimedean order. Our solution to this problem is to simply make use of the fact that our index set is countable. That is to say, since our index set is directed ordered and countable, it is easily verified that we may take a cofinal subset which is isomorphic to $\mathbb{Z}_{\geq 0}$ with the usual archimedean order. Then we have only to verify the Mittag-Leffler condition for this cofinal subsystem. Finally, we note that, to verify the Mittag-Leffler condition of such a cofinal subsystem, it is sufficient (and, in fact, necessary) to see that the whole projective system under consideration itself satisfies the "Mittag-Leffler condition" in the evident sense.

Toward the end of the present section, we review the notion of Kummer containers, which played a crucial role in Hoshi's mono-anabelian reconstruction algorithm in [MnNF] and, in fact, remain indispensable in our refined, purely mono-anabelian reconstruction algorithm.

Definition 1.7. Let F be a number field and $S \subset \mathcal{V}_F$ a finite subset.

(1) We shall write

$$\mathbb{I}^{\mathrm{fin}}_{F,S} \stackrel{\mathrm{def}}{=} \bigcup_{I\subset\mathcal{V}_F\setminus S;\ \text{finite}} \Big(\prod_{\mathfrak{p}\in I} F_{\mathfrak{p}}^\times\Big) \times \Big(\prod_{\mathfrak{p}\in(\mathcal{V}_F\setminus S)\setminus I} \mathcal{O}_{F_{\mathfrak{p}}}^\times\Big) \subset \prod_{\mathfrak{p}\in\mathcal{V}_F\setminus S} F_{\mathfrak{p}}^\times$$

and $\mathbb{I}^{\mathrm{fin}}_F \stackrel{\mathrm{def}}{=} \mathbb{I}^{\mathrm{fin}}_{F,\emptyset}$; we shall refer to $\mathbb{I}^{\mathrm{fin}}_{F,S}$ (resp. $\mathbb{I}^{\mathrm{fin}}_F$) as the group of *finite S-idèles* (resp. the *finite idèles*) of F.

(2) We shall write $\mathcal{H}^\times(F,S)$ (resp. $\mathcal{H}^\times(F)$) for the subgroup of $\widehat{F^\times}$ obtained as the preimage of $\mathbb{I}^{\mathrm{fin}}_{F,S} \subset \prod_{\mathfrak{p}\in\mathcal{V}_F\setminus S} F_{\mathfrak{p}}^\times \subset \prod_{\mathfrak{p}\in\mathcal{V}_F\setminus S} \widehat{F_{\mathfrak{p}}^\times}$ via the natural homomorphism $\widehat{F^\times} \longrightarrow \prod_{\mathfrak{p}\in\mathcal{V}_F\setminus S} \widehat{F_{\mathfrak{p}}^\times}$ (resp. $\mathcal{H}^\times(F,\emptyset)$); also, we shall write $\mathcal{H}_\times(F,S) \stackrel{\mathrm{def}}{=} \mathcal{H}^\times(F,S)^{\circledast}$ (resp. $\mathcal{H}_\times(F) = \mathcal{H}_\times(F,\emptyset) = \mathcal{H}^\times(F)^{\circledast}$); we shall refer to $\mathcal{H}^\times(F,S)$ and $\mathcal{H}_\times(F,S)$ (resp. $\mathcal{H}^\times(F)$ and $\mathcal{H}_\times(F)$) as the *S-Kummer containers* (resp. the *Kummer containers*) of F.

Remark 1.7.1. It follows from [NSW], Theorem (9.1.11), (ii), that the natural homomorphism $\widehat{F^\times} \longrightarrow \prod_{\mathfrak{p}\in\mathcal{V}_F\setminus S} \widehat{F_{\mathfrak{p}}^\times}$ that appeared in Definition 1.7, (2), is

injective. Moreover, the map $\widehat{F^{\times}} \longrightarrow \prod_{\mathfrak{p} \in T} \widehat{F_{\mathfrak{p}}^{\times}}$, where T is a subset of $\mathcal{V}_F$ of Dirichlet density 1, is still injective for the same reason.

Remark 1.7.2. Finite S-idèle and S-Kummer containers are employed in the present paper only in the case where $S = \emptyset$; that is to say, the narrower notions of finite idèles and Kummer containers are sufficient for the present paper (cf. also Remark 1.8.1 below). We included these notions for a general finite subset $S \subset \mathcal{V}_F$ for the convenience of future reference.

Remark 1.7.3. We may define a natural (locally compact) "restricted product" topology on $\mathbb{I}_{F,S}^{\mathrm{fin}}$ (which is finer than the topology induced from the product topology on $\prod_{\mathfrak{p} \in \mathcal{V}_F \setminus S} F_{\mathfrak{p}}^{\times}$) in a manner similar to the standard topology on the usual full S-idèle group. However, it is unnecessary for our purpose.

Lemma 1.8. *Let F be a number field and $S \subset \mathcal{V}_F$ a finite subset. Write $\mathcal{O}_{F,S}^{\times} \subset F^{\times}$ for the group of S-units of F, i.e., the subgroup constituted by the elements $x \in F^{\times}$ such that $v_{\mathfrak{p}}(x) = 0$ for every $\mathfrak{p} \in \mathcal{V}_F \setminus S$, where $v_{\mathfrak{p}}$ denotes the normalized additive valuation of F associated to $\mathfrak{p}$ (cf. the proof of Corollary 1.5); thus $\mathcal{O}_{F,\emptyset}^{\times} = \mathcal{O}_F^{\times}$. Then $\mathcal{H}^{\times}(F,S) \subset \widehat{F^{\times}}$ coincides with the subgroup $F^{\times} \cdot \widehat{\mathcal{O}_{F,S}^{\times}} \subset \widehat{F^{\times}}$ generated by the subgroups $F^{\times} \subset \widehat{F^{\times}}$ (cf. Remark 1.1.7) and $\widehat{\mathcal{O}_{F,S}^{\times}} \subset \widehat{F^{\times}}$ (cf. Lemma 1.4, applied to the ring of S-integers of F, for the injectivity).*

Proof. Before beginning the proof, we note that the special case of Lemma 1.8 where $S = \emptyset$, which is sufficient for the purpose of the present paper (cf. Remark 1.8.1 below), is [MnNF], Lemma 3.10, (iv). Although the proof of the general case is entirely parallel to that of this special case, we include the detailed proof of Lemma 1.8 for the convenience of the reader.

We begin with preliminary observations. We have a natural exact sequence

$$1 \longrightarrow \mathcal{O}_{F,S}^{\times} \longrightarrow F^{\times} \xrightarrow{\mathrm{div}_S} \mathrm{Div}(F,S) \longrightarrow \mathrm{Cl}(F,S) \longrightarrow 0,$$

where we write $\mathrm{Div}(F,S) \stackrel{\mathrm{def}}{=} \bigoplus_{\mathfrak{p} \in \mathcal{V}_F \setminus S} \mathbb{Z}$; div_S for the homomorphism given by $y \longmapsto \left(v_{\mathfrak{p}}(y)\right)_{\mathfrak{p} \in \mathcal{V}_F \setminus S}$; $\mathrm{Cl}(F,S)$ for the cokernel of div_S — a finite abelian group, being a quotient of the ideal class group of F (cf. [Neukirch], Chapter I, Corollary (11.8)). This exact sequence is divided into the following two short exact sequences:

$$1 \longrightarrow \mathcal{O}_{F,S}^{\times} \longrightarrow F^{\times} \xrightarrow{\mathrm{div}_S} \mathrm{Im}(\mathrm{div}_S) \longrightarrow 1;$$

$$0 \longrightarrow \mathrm{Im}(\mathrm{div}_S) \longrightarrow \mathrm{Div}(F,S) \longrightarrow \mathrm{Cl}(F,S) \longrightarrow 0.$$

Our first observation is as follows. Since $\mathbb{Z}$ is a PID, the $\mathbb{Z}$-submodule $\mathrm{Im}(\mathrm{div}_S)$ of the free $\mathbb{Z}$-module $\mathrm{Div}(F,S)$ is again free; hence the first short exact sequence splits. Thus the first short exact sequence induces a (split) short exact sequence

$$1 \longrightarrow \widehat{\mathcal{O}_{F,S}^{\times}} \longrightarrow \widehat{F^{\times}} \xrightarrow{\widehat{\mathrm{div}}_S} \widehat{\mathrm{Im}(\mathrm{div}_S)} \longrightarrow 1.$$

The second observation, which is a preparation for the third one, is as follows. By applying to the second short exact sequence the long exact sequence associated to $\mathrm{Tor}^{\mathbb{Z}}_{\bullet}(-, \mathbb{Z}/n\mathbb{Z})$ (or, more directly, the snake lemma with respect to the multiplication-by-n endomorphisms), we obtain, for each $n \in \mathbb{Z}_{\geq 1}$, a left exact sequence

$$0 \longrightarrow \mathrm{Cl}(F,S)[n] \longrightarrow \mathrm{Im}(\mathrm{div}_S)/n \cdot \mathrm{Im}(\mathrm{div}_S) \longrightarrow \mathrm{Div}(F,S)/n \cdot \mathrm{Div}(F,S)$$

(cf. the discussion entitled "Rings and Modules" in §0 for the notation "$[n]$"). Then, by taking the projective limit, we obtain, in light of the finiteness of $\mathrm{Cl}(F,S)$, the injectivity of the natural homomorphism $\widehat{\mathrm{Im}(\mathrm{div}_S)} \longrightarrow \widehat{\mathrm{Div}(F,S)}$; indeed, the transition map $\mathrm{Cl}(F,S)[n'] \longrightarrow \mathrm{Cl}(F,S)[n]$, where n divides n', is given by multiplication by n'/n.

The third observation is that the commutative diagram

$$\begin{array}{ccc} \mathrm{Im}(\mathrm{div}_S) & \hookrightarrow & \mathrm{Div}(F,S) \\ \downarrow & & \downarrow \\ \widehat{\mathrm{Im}(\mathrm{div}_S)} & \hookrightarrow & \widehat{\mathrm{Div}(F,S)} \end{array}$$

is Cartesian (cf. the second observation for the injectivity of the lower horizontal arrow; Remark 1.1.4 for the injectivity of the vertical arrows). Indeed, in light of the left exact sequences discussed in the second observation, this amounts to the equality $\mathrm{Im}(\mathrm{div}_S) = \bigcap_{n \in \mathbb{Z}_{\geq 1}} \big(\mathrm{Im}(\mathrm{div}_S) + n \cdot \mathrm{Div}(F,S)\big)$, where the intersection is taken inside $\mathrm{Div}(F,S)$; this equality, in turn, follows essentially formally from the finiteness of $\mathrm{Cl}(F,S)$.

Now the main discussion is given as follows. One verifies immediately — in light of the direct product decomposition $\widehat{F_{\mathfrak{p}}^{\times}} \cong \mathcal{O}_{F_{\mathfrak{p}}}^{\times} \times \widehat{\mathbb{Z}}$ arising from Remark 1.1.6, together with the explicit description of $\widehat{\mathrm{Div}(F,S)}$ given in Remark 1.1.4 — that $\mathcal{H}^{\times}(F,S)$ coincides with the preimage of $\mathrm{Div}(F,S) \subset \widehat{\mathrm{Div}(F,S)}$ via the composite $\widehat{F^{\times}} \xrightarrow{\widehat{\mathrm{div}_S}} \widehat{\mathrm{Im}(\mathrm{div}_S)} \longrightarrow \widehat{\mathrm{Div}(F,S)}$. Then it follows from the third observation that $\mathcal{H}^{\times}(F,S)$ coincides with the preimage of $\mathrm{Im}(\mathrm{div}_S) \subset \widehat{\mathrm{Im}(\mathrm{div}_S)}$ via $\widehat{\mathrm{div}}_S$. Thus the desired equality follows formally from the following commutative diagram, whose rows are the short exact sequences discussed in the first observation:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_{F,S}^{\times} & \longrightarrow & F^{\times} & \xrightarrow{\mathrm{div}_S} & \mathrm{Im}(\mathrm{div}_S) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \widehat{\mathcal{O}_{F,S}^{\times}} & \longrightarrow & \widehat{F^{\times}} & \xrightarrow[\widehat{\mathrm{div}}_S]{} & \widehat{\mathrm{Im}(\mathrm{div}_S)} & \longrightarrow & 1, \end{array}$$

where the vertical arrows are the natural homomorphisms. This completes the proof of Lemma 1.8. □

Remark 1.8.1. Lemma 1.8 is employed in the present paper only in the case where $S = \emptyset$; that is to say, the equality $\mathcal{H}^{\times}(F) = F^{\times} \cdot \widehat{\mathcal{O}_F^{\times}}$ is sufficient for the present paper. We included the more general result for the convenience of future reference.

Lemma 1.9. *Let F be a number field. Then the natural homomorphism $\mathcal{H}^{\times}(F) \longrightarrow \prod_{\mathfrak{p} \in \mathcal{V}_F^{d=1}} \widehat{F_{\mathfrak{p}}^{\times}}$ is injective.*

Proof. This is [MnNF], Lemma 3.10, (v); note that this essentially follows, in light of the fact that $\mathcal{V}_F^{d=1} \subset \mathcal{V}_F$ is of Dirichlet density 1, from Remark 1.7.1. $\square$

2 Review of Preliminary Local Reconstruction Algorithms

In the present section, we review various "intermediate steps" of our reconstruction algorithm which were established by other researchers, concentrating on the local ones (i.e., more precisely, the ones concerning mixed characteristic local fields). In particular, we review the reconstruction algorithm for the multiplicative group of a mixed characteristic local field, the multiplicative group of the ring of integers of a mixed characteristic local field, and the field structure on the reconstructed multiplicative group in the case of $\mathbb{Q}_p$. The present and the next sections do not contain any new results.

Definition 2.1. Let D be a profinite group. Then D is referred to as *of MLF-type* if there exists a mixed characteristic local field K such that D is isomorphic, as a profinite group, to the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ of K, where $\overline{K}$ is an algebraic closure of K.

Remark 2.1.1. An open subgroup of a profinite group of MLF-type is again of MLF-type. This hereditary property is frequently used in the present paper without further mention.

Lemma 2.2. *Let K be a mixed characteristic local field of residue characteristic p and of inertia degree n. Write $G_K = \mathrm{Gal}(\overline{K}/K)$ (resp. $I_K \subset G_K$; $P_K \subset G_K$) for the absolute Galois group of K determined by an algebraic closure $\overline{K}$ of K (resp. the inertia subgroup of G_K; the wild inertia subgroup of G_K). Then the following assertions hold:*

(1) P_K is a pro-p group. In particular, P_K is pro-solvable.

(2) The short exact sequence

$$1 \longrightarrow I_K/P_K \longrightarrow G_K/P_K \longrightarrow G_K/I_K \longrightarrow 1$$

is isomorphic (canonically, up to the choice of splitting, i.e., the choice of a representative of the Frobenius) to the following short exact sequence:

$$1 \longrightarrow \widehat{\mathbb{Z}}(1)^{(\neq p)} \longrightarrow \widehat{\mathbb{Z}}(1)^{(\neq p)} \rtimes \widehat{\mathbb{Z}} \longrightarrow \widehat{\mathbb{Z}} \longrightarrow 0,$$

where $\widehat{\mathbb{Z}}(1)^{(\neq p)}$ is the maximal pro-prime-to-p quotient of the Tate-twist "$\widehat{\mathbb{Z}}(1)$" associated to $\overline{K}$; the action $\widehat{\mathbb{Z}} \curvearrowright \widehat{\mathbb{Z}}(1)^{(\neq p)}$ is given by $a \cdot x \stackrel{\mathrm{def}}{=} x^{p^{na}}$. In particular, G_K/P_K is 2-step solvable, hence pro-solvable.

(3) G_K is pro-solvable.

Proof. See [NSW], Proposition (7.5.2). Note that the assertion (3) follows immediately from the assertions (1) and (2). $\square$

Lemma 2.3. *Let D be a profinite group of MLF-type. We define various numerical invariants of D, as follows.*

(1) We define a prime number $p(D)$ as the unique prime number p such that $\dim_{\mathbb{Q}_p} D^{\mathrm{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_p \geq 2$.

(2) We shall write $d(D) \stackrel{\mathrm{def}}{=} (\dim_{\mathbb{Q}_{p(D)}} D^{\mathrm{ab}} \otimes_{\widehat{\mathbb{Z}}} \mathbb{Q}_{p(D)}) - 1$.

(3) We shall write $f(D) \stackrel{\mathrm{def}}{=} \log_{p(D)}\Big(\#\big((D^{\mathrm{ab}})_{\mathrm{tor}} \otimes_{\widehat{\mathbb{Z}}} (\widehat{\mathbb{Z}}/\mathbb{Z}_{p(D)})\big) + 1\Big)$.

(4) We shall write $e(D) = d(D)/f(D)$.

Now let us consider the case where $D = \mathrm{Gal}(\overline{K}/K)$, where K is a mixed characteristic local field and $\overline{K}$ is an algebraic closure of K. Then it holds that $p(D)$ coincides with the residue characteristic of K; $d(D)$ coincides with the absolute degree (i.e., the extension degree over $\mathbb{Q}_{p(D)}$) of K; $f(D)$ coincides with the inertia degree of K (i.e., over $\mathbb{Q}_{p(D)}$); $e(D)$ coincides with the ramification index of K (i.e., over $\mathbb{Q}_{p(D)}$). In particular, roughly speaking, we have established an algorithm for reconstructing the residue characteristic, the absolute degree, the inertia degree, and the ramification index of a mixed characteristic local field K solely from the profinite group structure of $\mathrm{Gal}(\overline{K}/K)$.

Proof. Lemma 2.3 follows immediately from local class field theory, together with the well-known structure of the multiplicative group of a mixed characteristic local field. □

Lemma 2.4. *Let D be a profinite group of MLF-type. We define various objects associated to D, as follows.*

(1) We define a closed subgroup $P(D) \subset D$ as the unique maximal closed pro-$p(D)$ normal subgroup of D.

(2) We define a closed subgroup $I(D) \subset D$ as the closed subgroup that includes $P(D)$ and whose image in $D/P(D)$ is the unique maximal closed abelian normal subgroup of $D/P(D)$.

(3) We define an element $\mathrm{Frob}_D \in D/I(D)$ as the unique element whose conjugation action on $I(D)/P(D)$ (where we note that $I(D)/P(D)$ is abelian) coincides with the $p(D)^{f(D)}$-th power map.

(4) We define $k^{\times}(D) \subset D^{\mathrm{ab}}$ as the preimage of the (discrete) subgroup of $D/I(D)$ generated by Frob_D via the natural surjective homomorphism $D^{\mathrm{ab}} \twoheadrightarrow D/I(D)$, where we note that $D/I(D)$ is abelian (and, in fact, isomorphic to $\widehat{\mathbb{Z}}$).

(5) We define a surjective homomorphism $\mathrm{ord}(D)\colon k^{\times}(D) \twoheadrightarrow \mathbb{Z}$ as the composite of the natural surjective homomorphism $k^{\times}(D) \twoheadrightarrow \mathrm{Frob}_D^{\mathbb{Z}}$ defined as the restriction of the natural surjective homomorphism $D^{\mathrm{ab}} \twoheadrightarrow D/I(D)$ with the isomorphism $\mathrm{Frob}_D^{\mathbb{Z}} \stackrel{\cong}{\longrightarrow} \mathbb{Z}$ defined by $\mathrm{Frob}_D \longmapsto 1$.

(6) We define $\mathcal{O}^{\times}(D) \stackrel{\mathrm{def}}{=} \mathrm{Ker}\big(\mathrm{ord}(D)\big) \subset k^{\times}(D)$.

Now let us consider the case where $D = \mathrm{Gal}(\overline{K}/K)$, where K is a mixed characteristic local field and $\overline{K}$ is an algebraic closure of K. Then it holds that $P(D) \subset D$ coincides with the wild inertia subgroup of $D = \mathrm{Gal}(\overline{K}/K)$; $I(D) \subset D$ coincides with the inertia subgroup of $D = \mathrm{Gal}(\overline{K}/K)$; $\mathrm{Frob}_D \in D/I(D) \cong \widehat{\mathbb{Z}}$ coincides with the Frobenius element; the reciprocity map $K^\times \hookrightarrow \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} = D^{\mathrm{ab}}$ determines an isomorphism $K^\times \xrightarrow{\cong} k^\times(D) \subset D^{\mathrm{ab}}$; $\mathrm{ord}(D)\colon k^\times(D) \twoheadrightarrow \mathbb{Z}$ corresponds to the usual additive valuation $K^\times \twoheadrightarrow \mathbb{Z}$ via the isomorphism $K^\times \xrightarrow{\cong} k^\times(D)$ discussed above; $\mathcal{O}^\times(D) \subset k^\times(D)$ coincides with the subgroup corresponding to $\mathcal{O}_K^\times \subset K^\times$. In particular, roughly speaking, we have established an algorithm for reconstructing the wild inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$, the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$, the Frobenius element of the quotient of $\mathrm{Gal}(\overline{K}/K)$ by the inertia subgroup, the image of the reciprocity map of local class field theory $K^\times \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$, the surjective homomorphism from the image of the reciprocity map to $\mathbb{Z}$ corresponding to the usual additive valuation $K^\times \twoheadrightarrow \mathbb{Z}$, and the image of $\mathcal{O}_K^\times \subset K^\times$ via the reciprocity map $K^\times \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$, solely from the profinite group structure of $\mathrm{Gal}(\overline{K}/K)$.

Proof. Lemma 2.4 follows immediately from local class field theory, together with the well-known structure of the absolute Galois group of a mixed characteristic local field discussed in Lemma 2.2. □

Remark 2.4.1. We have alternative, slightly easier definitions (i.e., in essence, a slightly easier reconstruction algorithm) of $P(D) \subset I(D) \subset D$ in Lemma 2.4. The "inertia subgroup" $I(D)$ of D may also be defined as the intersection of the open subgroups $U \subset D$ such that $e(U) = e(D)$; then the wild inertia subgroup $P(D)$ of D may also be defined as the unique $p(D)$-Sylow subgroup of $I(D)$ (cf. Lemma 2.2). The advantage of the reconstruction algorithm given in Lemma 2.4 is that it may be generalized, in a straightforward fashion, to the situation where D is isomorphic to the Galois group of a (not necessarily algebraically closed) Galois extension L of a mixed characteristic local field K such that L includes both a/the maximal tamely ramified extension and a/the maximal abelian extension of K (cf. §5 below).

Now we further reconstruct the local cyclotome. It will play crucial roles both in establishing the relation between global and local objects (cf. Lemma 3.7 below) and in reconstructing the local field structure in the case where $d(D) = 1$ (cf. Lemma 2.7 below).

Lemma 2.5. *Let D be a profinite group of MLF-type. We define various objects associated to D, as follows.*

(1) Let $U \subset D$ be an open normal subgroup. Then we regard $k^\times(U)$ as a D/U-module by the natural action determined by the conjugation action of D on U (where we note that the action of $U \subset D$ on $k^\times(U)$ is trivial by construction).

(2) We define a D-module $D \curvearrowright \overline{k}^\times(D)$ by

$$\overline{k}^\times(D) \stackrel{\mathrm{def}}{=} \varinjlim_{U \subset D} k^\times(U),$$

where U ranges over the open normal subgroups of D; the transition map $k^\times(U) \longrightarrow k^\times(V)$, where $V \subset U \subset D$, is induced by the transfer map

$U^{\mathrm{ab}} \longrightarrow V^{\mathrm{ab}}$ *(cf. [IntroMLF], Lemma 1.7, (3)); the action* $D \curvearrowright \overline{k}^{\times}(D)$ *is induced by the action discussed in the construction (1) (i.e., induced by the conjugation action* $D \curvearrowright U$*).*

(3) For every $n \in \mathbb{Z}_{\geq 1}$*, we define a finite* D*-module* $\mu_n(D)$ *as the kernel of the* n*-th power map* $\overline{k}^{\times}(D) \longrightarrow \overline{k}^{\times}(D)$*. Moreover, we define a profinite* D*-module* $\Lambda^{\mathrm{loc}}(D)$ *as* $\varprojlim_{n \geq 1} \mu_n(D)$*, where the index set* $\mathbb{Z}_{\geq 1}$ *is equipped with the non-archimedean order (cf. the discussion entitled "Numbers" in §0); the transition map* $\mu_{n'}(D) \longrightarrow \mu_n(D)$*, where* n *divides* n'*, is given by the* (n'/n)*-th power map. We shall refer to* $\Lambda^{\mathrm{loc}}(D)$ *as the local cyclotome associated to* D *(cf. also Remark 2.5.2 below for another description of* $\Lambda^{\mathrm{loc}}(D)$*, which will be useful for the construction of the local-global cyclotomic synchronization isomorphism* $\Lambda^{\mathrm{gl}}(G) \xrightarrow{\cong} \Lambda^{\mathrm{loc}}(D)$ *in Lemma 3.7 below).*

(4) By construction, for each $n \in \mathbb{Z}_{\geq 1}$*, we have a natural short exact sequence* $1 \longrightarrow \mu_n(D) \longrightarrow \overline{k}^{\times}(D) \longrightarrow \overline{k}^{\times}(D) \longrightarrow 1$ *of* D*-modules, which induces a canonical isomorphism of abelian groups* $k^{\times}(D)/(k^{\times}(D))^n \xrightarrow{\cong} H^1(D, \mu_n(D))$*. Moreover, by considering (the resulting relationship between the two long exact sequences induced by) the commutative diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_{n'}(D) & \longrightarrow & \overline{k}^{\times}(D) & \xrightarrow{n'} & \overline{k}^{\times}(D) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \frac{n'}{n}} & & \downarrow{\scriptstyle \frac{n'}{n}} & & \| & & \\ 1 & \longrightarrow & \mu_n(D) & \longrightarrow & \overline{k}^{\times}(D) & \xrightarrow[n]{} & \overline{k}^{\times}(D) & \longrightarrow & 1 \end{array}$$

and taking the projective limit, we obtain a natural injective homomorphism $\mathrm{Kum}_D \colon k^{\times}(D) \hookrightarrow \widehat{k^{\times}(D)} \xrightarrow{\cong} H^1(D, \Lambda^{\mathrm{loc}}(D))$*, which we shall refer to as the Kummer map associated to* D *(cf. Remark 1.1.6 for the injectivity of* Kum_D*).*

Now let us consider the case where $D = \mathrm{Gal}(\overline{K}/K)$*, where* K *is a mixed characteristic local field and* $\overline{K}$ *is an algebraic closure of* K*. Then the following assertions hold: for every finite Galois subextension* L/K *of* $\overline{K}/K$*, the canonical isomorphism of groups* $L^{\times} \xrightarrow{\cong} k^{\times}\big(\mathrm{Gal}(\overline{K}/L)\big)$ *(cf. Lemma 2.4, (4)) is, in fact, an isomorphism of* $\mathrm{Gal}(L/K)$*-modules (or, equivalently, of* $\mathrm{Gal}(\overline{K}/K)$*-modules) relative to the natural* $\mathrm{Gal}(L/K)$*-action on* $L^{\times}$ *and the action of* $\mathrm{Gal}(L/K) = \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L)$ *on* $k^{\times}\big(\mathrm{Gal}(\overline{K}/L)\big)$ *discussed in the construction (1); we have a canonical isomorphism of* $\mathrm{Gal}(\overline{K}/K)$*-modules* $\overline{K}^{\times} \xrightarrow{\cong} \overline{k}^{\times}\big(\mathrm{Gal}(\overline{K}/K)\big)$*, as well as canonical isomorphisms of* $\mathrm{Gal}(\overline{K}/K)$*-modules* $\mu_n(\overline{K}) \xrightarrow{\cong} \mu_n\big(\mathrm{Gal}(\overline{K}/K)\big)$ *and* $\Lambda(\overline{K}) \xrightarrow{\cong} \Lambda^{\mathrm{loc}}\big(\mathrm{Gal}(\overline{K}/K)\big)$*; moreover, via these identifications, the injective homomorphism* $\mathrm{Kum}_{\mathrm{Gal}(\overline{K}/K)}$ *corresponds to the Kummer map* $K^{\times} \hookrightarrow H^1\big(\mathrm{Gal}(\overline{K}/K), \Lambda(\overline{K})\big)$*. In particular, roughly speaking, we have established an algorithm for reconstructing a group which is canonically isomorphic to the multiplicative group* $\overline{K}^{\times}$ *of* $\overline{K}$*, together with the natural action* $\mathrm{Gal}(\overline{K}/K) \curvearrowright \overline{K}^{\times}$*, the torsion* $\mathrm{Gal}(\overline{K}/K)$*-submodules* $\mu_n(\overline{K}) \subset \overline{K}^{\times}$*, the Tate-twist "*$\widehat{\mathbb{Z}}(1)$*" associated to* $\overline{K}$*, i.e.,* $\varprojlim_{n \geq 1} \mu_n(\overline{K})$*, and*

the Kummer map $K^{\times} \hookrightarrow H^1\big(\mathrm{Gal}(\overline{K}/K), \widehat{\mathbb{Z}}(1)\big)$, *solely from the profinite group structure of* $\mathrm{Gal}(\overline{K}/K)$.

Proof. The first assertion (i.e., the $\mathrm{Gal}(L/K)$-equivariance) follows immediately from a certain Isom-functoriality of local class field theory (cf. [IntroMLF], Lemma 1.7, (4)). The second assertion follows immediately from the first assertion, together with the well-known fact that the transfer map of open subgroups corresponds to the inclusion map of subfields via the reciprocity map of local class field theory (cf. [IntroMLF], Lemma 1.7, (3)). The remaining assertions follow immediately from the second assertion. This completes the proof of Lemma 2.5. □

Remark 2.5.1. In Lemma 2.5, (1), we restricted our attention to open subgroups $U \subset D$ that are normal. This normality assumption, however, was imposed merely for simplicity of exposition and is by no means essential. Of course, if an open subgroup $U \subset D$ is not normal, one cannot speak of a D-action (or D/U-action) on the objects constructed algorithmically from U, which should be defined via conjugation. Nevertheless, it is immediate that each conjugation by $\sigma \in D$ induces an isomorphism between the objects constructed algorithmically from U and from $\sigma U \sigma^{-1}$. Hence, in this manner, a natural D-action is obtained on the totality of the objects constructed algorithmically from various open subgroups of D. In particular, even if we allow U to range over all open subgroups (not necessarily normal) in the definition

$$\overline{k}^{\times}(D) \stackrel{\mathrm{def}}{=} \varinjlim_{U \subset D} k^{\times}(U),$$

the resulting D-action $D \curvearrowright \overline{k}^{\times}(D)$ is naturally defined. Since the family of open normal subgroups forms a cofinal subsystem, this coincides with the definition given in Lemma 2.5, (2). The same remark applies to any analogous situations. In the context of the present paper, it suffices to restrict our attention to open normal subgroups, as we ultimately take inductive limits and hence may work with any cofinal subsystem. Accordingly, the reader need not be concerned with the above generalization to open non-normal subgroups.

Remark 2.5.2. Here is another description of $\Lambda^{\mathrm{loc}}(D)$, which will be useful for the construction of the local-global cyclotomic synchronization isomorphism in Lemma 3.7 below. In the situation of Lemma 2.5, write $\mu^{\mathrm{loc}}_{\mathrm{base}}(D)$ for the set of torsion elements of $k^{\times}(D)$. Then we observe that $\mu^{\mathrm{loc}}(D) \stackrel{\mathrm{def}}{=} \varinjlim_{U \subset D} \mu^{\mathrm{loc}}_{\mathrm{base}}(U) \subset \overline{k}^{\times}(D) = \varinjlim_{U \subset D} k^{\times}(U)$, where U ranges over the open normal subgroups of D, coincides with the D-submodule of all torsion elements of $\overline{k}^{\times}(D)$. In particular, we have $\mu_n(D) = \mu^{\mathrm{loc}}(D)[n]$ and $\Lambda^{\mathrm{loc}}(D) = \varprojlim_{n \geq 1} \mu^{\mathrm{loc}}(D)[n]$. Also, we record here the obvious observation that, if K is a mixed characteristic local field, and $\overline{K}$ is an algebraic closure of K, then the canonical isomorphisms $K^{\times} \stackrel{\cong}{\longrightarrow} k^{\times}\big(\mathrm{Gal}(\overline{K}/K)\big)$ and $\overline{K}^{\times} \stackrel{\cong}{\longrightarrow} \overline{k}^{\times}\big(\mathrm{Gal}(\overline{K}/K)\big)$ induce canonical isomorphisms $\mu(K) \stackrel{\cong}{\longrightarrow} \mu^{\mathrm{loc}}_{\mathrm{base}}\big(\mathrm{Gal}(\overline{K}/K)\big)$ and $\mu(\overline{K}) \stackrel{\cong}{\longrightarrow} \mu^{\mathrm{loc}}\big(\mathrm{Gal}(\overline{K}/K)\big)$.

Finally, we will review the reconstruction of "field structure in the case of absolute degree one" established in [MLFTop], Definition 5.2, which is based on the following reconstruction of the norm map.

Lemma 2.6 (Reconstruction of the norm map)**.** *Let D be a profinite group of MLF-type. We construct various objects associated to D, as follows.*

(1) Recall that the maximal pro-$p(D)$ quotient $\Lambda^{\mathrm{loc}}(D)^{(p(D))}$ of $\Lambda^{\mathrm{loc}}(D)$ is (non-canonically) isomorphic, as a topological abelian group, to $\mathbb{Z}_{p(D)}$. We shall write $\mathbb{Z}_p(D)$ for the endomorphism ring $\mathrm{End}\big(\Lambda^{\mathrm{loc}}(D)^{(p(D))}\big)$, which is canonically isomorphic, as a (topological) ring, to $\mathbb{Z}_{p(D)}$. (The topological structure of $\mathbb{Z}_p(D)$ will not be of use in the present paper.) We shall write $\mathbb{Q}_p(D) \stackrel{\mathrm{def}}{=} \mathrm{Frac}\big(\mathbb{Z}_p(D)\big)$; this is canonically isomorphic to $\mathbb{Q}_{p(D)} = \mathrm{Frac}\,\mathbb{Z}_{p(D)}$.

(2) We shall write $p_{\in}(D) \in \mathbb{Z}_p(D)$ for the "$p(D)$" of the ring $\mathbb{Z}_p(D)$, i.e., $\underbrace{1 + \cdots + 1}_{p(D)} \in \mathbb{Z}_p(D)$.

(3) We shall write $\xi_{p\text{-cyc}}(D)$ for the homomorphism $D^{\mathrm{ab}} \longrightarrow \mathbb{Z}_p(D)^{\times}$ corresponding to the action $D \curvearrowright \Lambda^{\mathrm{loc}}(D)^{(p(D))}$ induced by the action $D \curvearrowright \Lambda^{\mathrm{loc}}(D)$ discussed in the definition of $\Lambda^{\mathrm{loc}}(D)$ (cf. Lemma 2.5, (3)).

(4) We shall write $\mathrm{Nm}_{\mathrm{abs}}(D)$ for the homomorphism $k^{\times}(D) \longrightarrow \mathbb{Q}_p(D)^{\times}$ defined by

$$a \longmapsto \xi_{p\text{-cyc}}(D)(a^{-1}) \cdot p_{\in}(D)^{f(D)\cdot \mathrm{ord}(D)(a)}.$$

Then, for a mixed characteristic local field K and an algebraic closure $\overline{K}$ of K, it holds that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} & \xrightarrow{\xi_{p\text{-cyc}}(\mathrm{Gal}(\overline{K}/K))} & \mathbb{Z}_p\big(\mathrm{Gal}(\overline{K}/K)\big)^{\times} \\ \| & & \downarrow \cong \\ \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} & \xrightarrow[\xi_{p\text{-cyc}}]{} & \mathbb{Z}_p^{\times}, \end{array}$$

where the lower horizontal arrow is the usual p-adic cyclotomic character, and the right-hand vertical arrow is induced by the canonical identification discussed in the construction (1); the following diagram also commutes:

$$\begin{array}{ccc} k^{\times}\big(\mathrm{Gal}(\overline{K}/K)\big) & \xrightarrow{\mathrm{Nm}_{\mathrm{abs}}(\mathrm{Gal}(\overline{K}/K))} & \mathbb{Q}_p\big(\mathrm{Gal}(\overline{K}/K)\big)^{\times} \\ \cong \downarrow & & \downarrow \cong \\ K^{\times} & \xrightarrow[\mathrm{Nm}_{K/\mathbb{Q}_{p(\mathrm{Gal}(\overline{K}/K))}}]{} & \mathbb{Q}_{p(\mathrm{Gal}(\overline{K}/K))}^{\times}, \end{array}$$

where the left-hand vertical arrow is the canonical identification discussed in Lemma 2.4 (i.e., in essence, the reciprocity map of local class field theory), the right-hand vertical arrow is induced by the canonical identification discussed in the construction (1), and the lower horizontal arrow is the usual norm map. In particular, roughly speaking, we have established an algorithm for reconstructing homomorphisms corresponding to the p-adic cyclotomic character $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \longrightarrow \mathbb{Z}_p^{\times}$ and the norm map $\mathrm{Nm}_{K/\mathbb{Q}_p} : K^{\times} \longrightarrow \mathbb{Q}_p^{\times}$ solely from the profinite group structure of $\mathrm{Gal}(\overline{K}/K)$.

Proof. The only non-trivial thing is the commutativity of the second diagram, which follows from [MLFTop], Lemma 4.1, (iii). □

Lemma 2.7 (Reconstruction of the field structure in the case of absolute degree one)**.** *Let D be a profinite group of MLF-type such that $d(D) = 1$ (cf. Lemma 2.3, (2)). Then $\mathrm{Nm}_{\mathrm{abs}}(D)\colon k^{\times}(D) \longrightarrow \mathbb{Q}_p(D)^{\times}$ (cf. Lemma 2.6, (4)) is an isomorphism of groups, hence it uniquely extends to an isomorphism of monoids $\mathrm{Nm}_{\mathrm{abs}}(D)^{\circledast}\colon k^{\times}(D)^{\circledast} \longrightarrow (\mathbb{Q}_p(D)^{\times})^{\circledast} = \mathbb{Q}_p(D)_{\times}$, where we write $\mathbb{Q}_p(D)_{\times}$ for the underlying multiplicative monoid of $\mathbb{Q}_p(D)$. In particular, there exists a unique addition structure on $k^{\times}(D)^{\circledast}$ that makes $k^{\times}(D)^{\circledast}$ into a field and $\mathrm{Nm}_{\mathrm{abs}}(D)^{\circledast}$ into a field isomorphism; we shall write $k_{\mathrm{fld}}(D)$ for the resulting field whose underlying multiplicative monoid is $k^{\times}(D)^{\circledast}$.*

Then, for a mixed characteristic local field $K \cong \mathbb{Q}_p$ and an algebraic closure $\overline{K}$ of K, the canonical group isomorphism $K^{\times} \xrightarrow{\cong} k^{\times}\big(\mathrm{Gal}(\overline{K}/K)\big)$ extends (uniquely) to a field isomorphism $K \xrightarrow{\cong} k_{\mathrm{fld}}\big(\mathrm{Gal}(\overline{K}/K)\big)$. In particular, roughly speaking, we have established an algorithm for reconstructing the natural field structure on the image of the reciprocity map of local class field theory $\mathbb{Q}_p^{\times} \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)^{\mathrm{ab}}$ solely from the profinite group structure of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.

Proof. Lemma 2.7 follows immediately from Lemma 2.6. □

3 Preliminary Global Reconstruction Algorithms: Reconstruction of the Kummer Container

In the present section, we continue the review of the "intermediate steps" of our reconstruction algorithm which were established by other researchers, switching our attention to the global ones. More specifically, we will review the reconstruction of the Kummer containers from the Galois groups of solvably closed Galois extensions. As in the previous section, the present section contains no new results.

The "global" profinite groups of interest in the present paper are defined as follows.

Definition 3.1. Let G be a profinite group. Then G is referred to as a profinite group of *GSC-type* if there exists an isomorphism $G \xrightarrow{\cong} \mathrm{Gal}(E/F)$ of profinite groups for some number field F and a solvably closed Galois extension E of F.

Remark 3.1.1. An open subgroup of a profinite group of GSC-type is again of GSC-type. This hereditary property is frequently used in the present paper without further mention.

Next, we review the notion of "localization" of an infinite extension of a number field.

Definition 3.2. Let E be a field which is isomorphic to a(n) (not necessarily finite) algebraic extension of $\mathbb{Q}$.

(1) We shall refer to as a *non-archimedean prime* of E a system $(\mathfrak{p}_M)_{M \subset E}$ consisting of non-archimedean primes $\mathfrak{p}_M$ of M, where M ranges over the

subfields of E that are number fields, such that, for every inclusion of subfields $M \subset M'$ of E that are number fields, $\mathfrak{p}_M$ underlies $\mathfrak{p}_{M'}$. We shall write $\mathcal{V}_E$ for the set of non-archimedean primes of E.

(2) Let $\widetilde{\mathfrak{p}}$ be a non-archimedean prime of E. Then we shall write $E_{\widetilde{\mathfrak{p}}}$ for the inductive limit $\bigcup_M M_{\widetilde{\mathfrak{p}}(M)}$, where M ranges over the subfields of E that are number fields; $\widetilde{\mathfrak{p}}(M)$ denotes the prime of M that underlies $\widetilde{\mathfrak{p}}$; (we recall that) $M_{\widetilde{\mathfrak{p}}(M)}$ denotes the completion of M at $\widetilde{\mathfrak{p}}(M)$. We will regard $E_{\widetilde{\mathfrak{p}}}$ as an E-algebra in the evident way; we will refer to it as the *localization* of E at $\widetilde{\mathfrak{p}}$.

Remark 3.2.1. It is immediate that, if E is a number field, then the notion of a non-archimedean prime of E introduced in Definition 3.2 coincides (up to canonical identifications) with the standard one defined for a number field.

Remark 3.2.2. Let E be a (not necessarily finite) Galois extension of a number field F and $\widetilde{\mathfrak{p}} \in \mathcal{V}_E$. Write $\mathfrak{p}$ for the prime of F that underlies $\widetilde{\mathfrak{p}}$. Then (it is easily verified that) the natural group homomorphism $\mathrm{Gal}(E_{\widetilde{\mathfrak{p}}}/F_{\mathfrak{p}}) \longrightarrow \mathrm{Gal}(E/F)$ is continuous and injective, where we note that the Galoisness of the field extension E/F implies the Galoisness of $E_{\widetilde{\mathfrak{p}}}/F_{\mathfrak{p}}$, and its image coincides with the (non-archimedean) decomposition subgroup $D_{\widetilde{\mathfrak{p}}}$ of $\mathrm{Gal}(E/F)$ associated to $\widetilde{\mathfrak{p}}$, i.e., the stabilizer subgroup of $\widetilde{\mathfrak{p}}$ with respect to the natural action $\mathrm{Gal}(E/F) \curvearrowright \mathcal{V}_E$.

Remark 3.2.3. Suppose that we are in the situation of Remark 3.2.2 and, moreover, that E is solvably closed. Then $E_{\widetilde{\mathfrak{p}}}$ is algebraically closed. Indeed, in light of the fact that the absolute Galois group of a mixed characteristic local field is pro-solvable (cf. Lemma 2.2, (3)), this follows essentially formally from the Grunwald–Wang theorem (cf. [NSW], Theorem (9.2.8)).

Lemma 3.3. *Let F be a number field and E a solvably closed Galois extension of F. Write $\mathbb{V}(E/F) \subset 2^{\mathrm{Gal}(E/F)}$ for the set of non-archimedean decomposition subgroups of* $\mathrm{Gal}(E/F)$. *Then the natural map $\mathcal{V}_E \longrightarrow \mathbb{V}(E/F)$ (cf. Remark 3.2.2) is an isomorphism of* $\mathrm{Gal}(E/F)$*-sets, where* $\mathrm{Gal}(E/F) \curvearrowright \mathbb{V}(E/F)$ *is defined as the conjugation action. In particular, the natural map $\mathcal{V}_F \longrightarrow \mathrm{Gal}(E/F)\backslash\mathbb{V}(E/F)$ is a bijection.*

Proof. Lemma 3.3 follows from [GSAn], Proposition 1.4, (iv). □

Remark 3.3.1. Suppose that we are in the situation of Lemma 3.3. Then it follows immediately from Lemma 3.3 that every non-archimedean decomposition subgroup of $\mathrm{Gal}(E/F)$ is normally terminal in $\mathrm{Gal}(E/F)$. Here, we recall that a subgroup D of a group G is said to be *normally terminal* in G if, for every $g \in G$, the equality $gDg^{-1} = D$ implies $g \in D$.

Theorem 3.4 below, which is a famous classical result of Neukirch, is of central importance in our discussion, since we wish to make use of local reconstruction results to obtain global ones. Here, we note that this result also played a crucial role in Uchida's original proof of the Neukirch–Uchida theorem.

Theorem 3.4 (Neukirch's reconstruction of non-archimedean decomposition subgroups)**.** *Let G be a profinite group of GSC-type. We shall write $\mathbb{V}(G) \subset 2^G$ for the set of closed subgroups D of G satisfying the following condition:*

D is maximal among closed subgroups of G of MLF-type. In other words, D is of MLF-type, and every closed subgroup $D' \subset G$ of MLF-type satisfying $D \subset D'$ is, in fact, equal to D.

Then, for a number field F and a solvably closed Galois extension E of F, the set $\mathbb{V}\big(\mathrm{Gal}(E/F)\big) \subset 2^{\mathrm{Gal}(E/F)}$ coincides with the set of non-archimedean decomposition subgroups of $\mathrm{Gal}(E/F)$. In particular, roughly speaking, we have established an algorithm for reconstructing the set of non-archimedean decomposition subgroups of $\mathrm{Gal}(E/F)$ solely from the profinite group structure of $\mathrm{Gal}(E/F)$.

Proof. See [NSW], Corollary (12.1.11) (where we note that, while [NSW], Corollary (12.1.11) is stated only for the case where E is an algebraic closure of F, the same proof applies to our more general situation). □

Remark 3.4.1. Let G be a profinite group of GSC-type. Then it follows immediately from Remark 3.2.3 that $D \in \mathbb{V}(G)$ is "of MLF-type in a manner compatible with the assumption that G is of GSC-type" (cf. Remark 3.4.2 below for more precise discussion) and, in particular, of MLF-type. This implies that we may apply various local reconstruction algorithms to each $D \in \mathbb{V}(G)$ to obtain various pieces of information concerning G.

Remark 3.4.2. In the context of Remark 3.4.1, merely pointing out that D is (abstractly!) of MLF-type is insufficient. For instance, let us imagine a situation where $D = \mathrm{Gal}(E_{\widetilde{\mathfrak{p}}}/F_{\mathfrak{p}}) \subset G = \mathrm{Gal}(E/F)$, and $E_{\widetilde{\mathfrak{p}}}$ is not an algebraic closure of $F_{\mathfrak{p}}$, but by some "accident", the profinite group D itself happens to be of MLF-type (although this does not actually occur in our situation thanks to Remark 3.2.3). In this case, while we may certainly apply various local reconstruction algorithms to D, the interpretation of D as $\mathrm{Gal}(E_{\widetilde{\mathfrak{p}}}/F_{\mathfrak{p}})$ — i.e., the identity isomorphism $D \xrightarrow{\mathrm{id}} \mathrm{Gal}(E_{\widetilde{\mathfrak{p}}}/F_{\mathfrak{p}})$ — is incompatible with these algorithms; indeed, this isomorphism does not provide a proof of the fact that D is of MLF-type.

Ultimately, in the context of Remark 3.4.1, what matters is not merely that D is of MLF-type, but rather that D is "of MLF-type in a manner compatible with the assumption that G is of GSC-type". To formulate this rigorously: we say that an inclusion of profinite groups $D \subset G$ is a *GSC-decomposition-pair* if there exist a number field F, a solvably closed Galois extension E of F, $\mathfrak{p} \in \mathcal{V}_F$, and $\widetilde{\mathfrak{p}} \in \mathcal{V}_E$ lying over $\mathfrak{p}$ such that there exists an isomorphism of profinite groups $\phi\colon G \xrightarrow{\cong} \mathrm{Gal}(E/F)$ satisfying $\phi(D) = \mathrm{Gal}(E_{\widetilde{\mathfrak{p}}}/F_{\mathfrak{p}})$. While this rigorous formulation is not explicitly employed in the present paper, it is useful to keep it in mind to avoid confusion.

Definition 3.5. Let G be a profinite group of GSC-type. Then we shall write $\mathbb{V}^{\mathrm{base}}(G)$ for the quotient set $G\backslash\mathbb{V}(G)$ with respect to the conjugation action $G \curvearrowright \mathbb{V}(G)$.

Remark 3.5.1. Let F be a number field and E a solvably closed Galois extension of F. Then it follows from Lemma 3.3 and Theorem 3.4 that we have a canonical bijection $\mathcal{V}_F \xrightarrow{\cong} \mathbb{V}^{\mathrm{base}}\big(\mathrm{Gal}(E/F)\big)$.

Now we would like to establish a reconstruction algorithm for what we call the global cyclotome $\Lambda^{\mathrm{gl}}(G)$, where G is a profinite group of GSC-type, together with a canonical isomorphism $\Lambda^{\mathrm{gl}}(G) \xrightarrow{\cong} \Lambda^{\mathrm{loc}}(D)$ for each decomposition subgroup $D \in \mathbb{V}(G)$, which we call the local-global cyclotomic synchronization isomorphism (or, alternatively, the local-global cyclotomic rigidity isomorphism).

The first step is to reconstruct the group of finite idèles $\mathbb{I}_F^{\mathrm{fin}}$ (cf. Definition 1.7, (1)) for each open subgroup $H \subset G$, which is again of GSC-type. Note that, while we have already reconstructed the local components of $\mathbb{I}_F^{\mathrm{fin}}$ (cf. Lemma 2.4), we need some more preparation, because $\mathbb{I}_F^{\mathrm{fin}}$ should be reconstructed as a subgroup of a certain direct product indexed by (not the set $\mathbb{V}\big(\mathrm{Gal}(E/F)\big)$ of non-archimedean decomposition subgroups of $\mathrm{Gal}(E/F)$, which corresponds to the non-archimedean primes of E, but rather) the set $\mathbb{V}^{\mathrm{base}}\big(\mathrm{Gal}(E/F)\big)$ of the conjugacy classes of non-archimedean decomposition subgroups of $\mathrm{Gal}(E/F)$, which corresponds to the non-archimedean primes of F (cf. Lemma 3.3). That is to say, we need to "synchronize" beforehand (the objects associated to) mutually conjugate decomposition subgroups of $\mathrm{Gal}(E/F)$. This synchronization may be regarded as a formal consequence of the fact that a non-archimedean decomposition subgroup is normally terminal in $\mathrm{Gal}(E/F)$ (cf. Remark 3.3.1).

Lemma 3.6 (Reconstruction of the group of finite idèles and the global cyclotome)**.** *Let G be a profinite group of GSC-type. Then the following assertions hold:*

(1) Let $D, D' \in \mathbb{V}(G)$ be mutually conjugate in G. Then the isomorphism $D^{\mathrm{ab}} \xrightarrow{\cong} (D')^{\mathrm{ab}}$ induced by the conjugation action of an element $\sigma \in G$ satisfying $D' = \sigma D \sigma^{-1} \subset G$ is, in fact, independent of the choice of such $\sigma \in G$ and induces the following commutative diagram:

$$\begin{array}{ccccc} \mathcal{O}^{\times}(D) & \hookrightarrow & k^{\times}(D) & \hookrightarrow & D^{\mathrm{ab}} \\ \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\ \mathcal{O}^{\times}(D') & \hookrightarrow & k^{\times}(D') & \hookrightarrow & (D')^{\mathrm{ab}}. \end{array}$$

In particular, we have canonical isomorphisms $\mathcal{O}^{\times}(D) \xrightarrow{\cong} \mathcal{O}^{\times}(D')$ and $k^{\times}(D) \xrightarrow{\cong} k^{\times}(D')$.

(2) Let $D, D', D'' \in \mathbb{V}(G)$ be mutually conjugate in G. Then the composite of the isomorphisms $k^{\times}(D) \xrightarrow{\cong} k^{\times}(D')$ and $k^{\times}(D') \xrightarrow{\cong} k^{\times}(D'')$ discussed in the assertion (1) coincides with the isomorphism $k^{\times}(D) \xrightarrow{\cong} k^{\times}(D'')$ discussed in the assertion (1); a similar compatibility holds also for "$\mathcal{O}^{\times}(-)$". In particular, for each $v \in \mathbb{V}^{\mathrm{base}}(G) = G\backslash\mathbb{V}(G)$ (cf. Definition 3.5), we may define the "diagonals" $k^{\times}(G, v) \subset \prod_{D \in \mathbb{V}(G),\, [D]=v} k^{\times}(D)$ and $\mathcal{O}^{\times}(G, v) \subset \prod_{D \in \mathbb{V}(G),\, [D]=v} \mathcal{O}^{\times}(D)$.

(3) For each finite subset $\Sigma \subset \mathbb{V}^{\mathrm{base}}(G)$, we set $\mathbb{I}_{\Sigma}^{\mathrm{fin}}(G) \stackrel{\mathrm{def}}{=} \big(\prod_{v \in \Sigma} k^{\times}(G, v)\big) \times \big(\prod_{v \in (\mathbb{V}^{\mathrm{base}}(G) \setminus \Sigma)} \mathcal{O}^{\times}(G, v)\big) \subset \prod_{v \in \mathbb{V}^{\mathrm{base}}(G)} k^{\times}(G, v) \subset \prod_{D \in \mathbb{V}(G)} D^{\mathrm{ab}}$. Moreover, we set $\mathbb{I}^{\mathrm{fin}}(G) \stackrel{\mathrm{def}}{=} \varinjlim_{\Sigma \subset \mathbb{V}^{\mathrm{base}}(G)} \mathbb{I}_{\Sigma}^{\mathrm{fin}}(G) \subset \prod_{v \in \mathbb{V}^{\mathrm{base}}(G)} k^{\times}(G, v) \subset \prod_{D \in \mathbb{V}(G)} D^{\mathrm{ab}}$. Now suppose that E is a solvably closed Galois extension of a number field F; write ϕ for the canonical bijection $\phi\colon \mathcal{V}_F \xrightarrow{\cong} \mathbb{V}^{\mathrm{base}}\big(\mathrm{Gal}(E/F)\big)$ discussed in Remark 3.5.1. Then, for each $\mathfrak{p} \in \mathcal{V}_F$, we have canonical isomorphisms of groups $F_{\mathfrak{p}}^{\times} \xrightarrow{\cong} k^{\times}\big(\mathrm{Gal}(E/F), \phi(\mathfrak{p})\big)$ and $\mathcal{O}_{F_{\mathfrak{p}}}^{\times} \xrightarrow{\cong} \mathcal{O}^{\times}\big(\mathrm{Gal}(E/F), \phi(\mathfrak{p})\big)$; hence also a canonical isomorphism of groups $\mathbb{I}_F^{\mathrm{fin}} \xrightarrow{\cong} \mathbb{I}^{\mathrm{fin}}\big(\mathrm{Gal}(E/F)\big)$.

In particular, roughly speaking, we have established an algorithm for reconstructing a group which is canonically isomorphic to $\mathbb{I}_F^{\mathrm{fin}}$ *solely from the profinite group structure of* $\mathrm{Gal}(E/F)$.

(4) *We have a canonical group homomorphism* $\mathbb{I}^{\mathrm{fin}}(G) \longrightarrow G^{\mathrm{ab}}$ *(cf. the proof for the details); we shall write* $\mu_{\mathrm{base}}^{\mathrm{gl}}(G)$ *for the torsion part of the kernel of this homomorphism, i.e.,* $\mu_{\mathrm{base}}^{\mathrm{gl}}(G) \stackrel{\mathrm{def}}{=} \mathrm{Ker}(\mathbb{I}^{\mathrm{fin}}(G) \to G^{\mathrm{ab}})_{\mathrm{tor}}$. *Now suppose that* E *is a solvably closed Galois extension of a number field* F*; in particular, we have a natural (i.e., the "diagonal") injective homomorphism* $F^{\times} \hookrightarrow \mathbb{I}_F^{\mathrm{fin}}$. *Then the isomorphism* $\mathbb{I}^{\mathrm{fin}}\big(\mathrm{Gal}(E/F)\big) \stackrel{\cong}{\longrightarrow} \mathbb{I}_F^{\mathrm{fin}}$ *induces an injective homomorphism between their subgroups* $\mu_{\mathrm{base}}^{\mathrm{gl}}\big(\mathrm{Gal}(E/F)\big) \hookrightarrow \mu(F)$ *(where we regard* $\mu(F) = (F^{\times})_{\mathrm{tor}} \subset F^{\times}$ *as a subgroup of* $\mathbb{I}_F^{\mathrm{fin}}$ *through the natural injective homomorphism* $F^{\times} \hookrightarrow \mathbb{I}_F^{\mathrm{fin}}$ *discussed above). Moreover, this homomorphism is, in fact, an isomorphism if* F *is totally imaginary.*

(5) *Let* H *be an open normal subgroup of* G*, which is again of GSC-type. Then the conjugation action of* G *on* H *induces actions of* G *on* $\mathbb{I}^{\mathrm{fin}}(H)$ *and on* $\mu_{\mathrm{base}}^{\mathrm{gl}}(H)$. *Now suppose that* E *is a solvably closed Galois extension of a number field* F *and that* F'/F *is a finite Galois subextension of* E/F. *Then the natural homomorphism* $\mu_{\mathrm{base}}^{\mathrm{gl}}\big(\mathrm{Gal}(E/F')\big) \hookrightarrow \mu(F')$ *discussed in the assertion (4) is compatible with the respective actions of* $\mathrm{Gal}(E/F)$.

(6) *Let* H' *and* H'' *be open normal subgroups of* G*, which are again of GSC-type, such that* $H'' \subset H'$. *Then we have a canonical* G*-homomorphism* $\mu_{\mathrm{base}}^{\mathrm{gl}}(H') \longrightarrow \mu_{\mathrm{base}}^{\mathrm{gl}}(H'')$ *(cf. the proof for the details). Now suppose that* E *is a solvably closed Galois extension of a number field* F*; let* F'/F *and* F''/F *be finite Galois subextensions of* E/F *such that* $F' \subset F''$. *Then the* $\mathrm{Gal}(E/F)$*-homomorphism* $\mu_{\mathrm{base}}^{\mathrm{gl}}\big(\mathrm{Gal}(E/F')\big) \longrightarrow \mu_{\mathrm{base}}^{\mathrm{gl}}\big(\mathrm{Gal}(E/F'')\big)$ *fits into the following commutative diagram as the left-hand vertical arrow:*

$$\begin{array}{ccc} \mu_{\mathrm{base}}^{\mathrm{gl}}\big(\mathrm{Gal}(E/F'')\big) & \longrightarrow & \mu(F'') \\ \uparrow & & \uparrow \\ \mu_{\mathrm{base}}^{\mathrm{gl}}\big(\mathrm{Gal}(E/F')\big) & \longrightarrow & \mu(F') \end{array}$$

where the right-hand vertical arrow is induced by the inclusion map $F' \hookrightarrow F''$*; the horizontal arrows are the natural ones discussed in the assertion (4).*

(7) *We define a* G*-module* $\mu^{\mathrm{gl}}(G) \stackrel{\mathrm{def}}{=} \varinjlim_H \mu_{\mathrm{base}}^{\mathrm{gl}}(H)$, *where* H *ranges over the open normal subgroups of* G*; the transition maps are the ones discussed in the assertion (6). Also, we define a profinite* G*-module* $\Lambda^{\mathrm{gl}}(G) \stackrel{\mathrm{def}}{=} \varprojlim_{n \geq 1} \mu^{\mathrm{gl}}(G)[n]$, *where the index set* $\mathbb{Z}_{\geq 1}$ *is equipped with the non-archimedean order (cf. the discussion entitled "Numbers" in §0); the transition map* $\mu^{\mathrm{gl}}(G)[n'] \longrightarrow \mu^{\mathrm{gl}}(G)[n]$*, where* n *divides* n'*, is given by the* (n'/n)*-th power map. Then, for every solvably closed Galois extension* E *of a number field* F*, the homomorphism discussed in the assertion (6) determines a canonical* $\mathrm{Gal}(E/F)$*-isomorphism* $\mu^{\mathrm{gl}}\big(\mathrm{Gal}(E/F)\big) \stackrel{\cong}{\longrightarrow} \mu(E)$*;*

hence a canonical $\mathrm{Gal}(E/F)$*-isomorphism* $\Lambda^{\mathrm{gl}}\big(\mathrm{Gal}(E/F)\big) \xrightarrow{\cong} \Lambda(E)$ *(cf. Definition 1.2).*

Proof. The assertion (1) follows immediately from the fact that D and D' are normally terminal in G. The assertion (2) follows formally from the definition of the isomorphisms under consideration. The assertion (3) is immediate.

The assertion (4) is [MnNF2], Lemma 3.6, (iii). Here, however, we briefly record the construction of the homomorphism $\mathbb{I}^{\mathrm{fin}}(G) \longrightarrow G^{\mathrm{ab}}$ in the assertion (4) for the convenience of the reader. Let G/U be a finite abelian quotient of G. Recall that only finitely many primes ramify in a finite extension of number fields; this implies that there exists a finite subset $\Sigma \subset \mathbb{V}^{\mathrm{base}}(G)$ such that the composite homomorphism $\mathcal{O}^{\times}(D) \hookrightarrow D^{\mathrm{ab}} \longrightarrow G/U$, where $D \in \mathbb{V}(G)$, is trivial except for the case where the image of D in $\mathbb{V}^{\mathrm{base}}(G)$ is in Σ. Thus we have a natural homomorphism $\mathbb{I}^{\mathrm{fin}}(G) \longrightarrow G/U$, hence $\mathbb{I}^{\mathrm{fin}}(G) \longrightarrow G^{\mathrm{ab}}$.

The assertion (5) is immediate. Next, we give the construction of the homomorphism in the assertion (6). For this, it suffices to give a reconstruction algorithm for the natural map $\mathbb{I}^{\mathrm{fin}}(H') \longrightarrow \mathbb{I}^{\mathrm{fin}}(H'')$ corresponding to "$\mathbb{I}^{\mathrm{fin}}_{F'} \longrightarrow \mathbb{I}^{\mathrm{fin}}_{F''}$". Then it even suffices to give a reconstruction algorithm, for each $D' \in \mathbb{V}(H')$, of the natural map $k^{\times}(D') \longrightarrow k^{\times}(D' \cap H'')$ corresponding to the inclusion of local fields. On the other hand, this is induced from the transfer map $(D')^{\mathrm{ab}} \longrightarrow (D' \cap H'')^{\mathrm{ab}}$ (cf. [IntroMLF], Lemma 1.7, (3)). Then the commutativity of the diagram in the assertion (6) follows immediately from the construction. Finally, the assertion (7) is immediate. This completes the proof of Lemma 3.6. $\square$

Now we obtain the local-global cyclotomic synchronization isomorphism, as follows.

Lemma 3.7. *Let G be a profinite group of GSC-type. Then the following assertions hold:*

(1) For every $D \in \mathbb{V}(G)$, the natural map $\mu^{\mathrm{gl}}_{\mathrm{base}}(G) \subset \prod_{D' \in \mathbb{V}(G)} (D')^{\mathrm{ab}} \overset{\mathrm{proj.}}{\longrightarrow} D^{\mathrm{ab}}$ factors through $\mu^{\mathrm{loc}}_{\mathrm{base}}(D) \subset D^{\mathrm{ab}}$ (cf. Remark 2.5.2 for the notation "$\mu^{\mathrm{loc}}_{\mathrm{base}}(-)$"), where "proj." means the projection to the component indexed by $D \in \mathbb{V}(G)$; thus we have a natural homomorphism $\mu^{\mathrm{gl}}_{\mathrm{base}}(G) \longrightarrow \mu^{\mathrm{loc}}_{\mathrm{base}}(D)$. For every solvably closed Galois extension E of a number field F and $\widetilde{\mathfrak{p}} \in \mathcal{V}_E$ lying over $\mathfrak{p} \in \mathcal{V}_F$, this homomorphism fits into the following commutative diagram as the upper horizontal arrow (cf. Remark 3.2.2 for the notation "$D_{\widetilde{\mathfrak{p}}}$"):

$$\begin{array}{ccc} \mu^{\mathrm{gl}}_{\mathrm{base}}\big(\mathrm{Gal}(E/F)\big) & \longrightarrow & \mu^{\mathrm{loc}}_{\mathrm{base}}(D_{\widetilde{\mathfrak{p}}}) \\ \downarrow & & \downarrow \cong \\ \mu(F) & \longrightarrow & \mu(F_{\mathfrak{p}}), \end{array}$$

where the left-hand vertical arrow (resp. the right-hand vertical arrow; the lower horizontal arrow) is the one discussed in Lemma 3.6, (4) (resp. the one discussed in Remark 2.5.2; the one induced by the natural homomorphism $F \hookrightarrow F_{\mathfrak{p}}$).

(2) *Fix $D \in \mathbb{V}(G)$. Then, for every open normal subgroup $H \subset G$, the conjugation action of D on $\mu_{\mathrm{base}}^{\mathrm{loc}}(D \cap H)$ is compatible with the action $G \curvearrowright \mu_{\mathrm{base}}^{\mathrm{gl}}(H)$ through the inclusion homomorphism $D \hookrightarrow G$ and the homomorphism $\mu_{\mathrm{base}}^{\mathrm{gl}}(H) \longrightarrow \mu_{\mathrm{base}}^{\mathrm{loc}}(D \cap H)$ discussed in the assertion (1). In particular, by taking the inductive limit, where H ranges over the open normal subgroups of G, we obtain a D-isomorphism $\mu^{\mathrm{gl}}(G) \xrightarrow{\cong} \mu^{\mathrm{loc}}(D)$, which we shall refer to as the local-global cyclotomic synchronization isomorphism. Now let E be a solvably closed Galois extension of a number field F and $\widetilde{\mathfrak{p}} \in \mathcal{V}_E$ a non-archimedean prime lying over $\mathfrak{p} \in \mathcal{V}_F$. Then the local-global synchronization isomorphism $\mu^{\mathrm{gl}}\big(\mathrm{Gal}(E/F)\big) \xrightarrow{\cong} \mu^{\mathrm{loc}}\big(\mathrm{Gal}(E_{\widetilde{\mathfrak{p}}}/F_{\mathfrak{p}})\big)$ fits into the following commutative diagram as the upper horizontal arrow:*

$$\begin{array}{ccc} \mu^{\mathrm{gl}}\big(\mathrm{Gal}(E/F)\big) & \xrightarrow{\cong} & \mu^{\mathrm{loc}}\big(\mathrm{Gal}(E_{\widetilde{\mathfrak{p}}}/F_{\mathfrak{p}})\big) \\ \cong\downarrow & & \downarrow\cong \\ \mu(E) & \xrightarrow{\cong} & \mu(E_{\widetilde{\mathfrak{p}}}), \end{array}$$

where the left-hand vertical arrow (resp. the right-hand vertical arrow; the lower horizontal arrow) is the one discussed in Lemma 3.6, (7) (resp. the one discussed in Remark 2.5.2; the one induced by the natural homomorphism $E \hookrightarrow E_{\widetilde{\mathfrak{p}}}$).

(3) *In the situation of the assertion (2), by taking the limit of the isomorphism $\mu^{\mathrm{gl}}(G)[n] \xrightarrow{\cong} \mu^{\mathrm{loc}}(D)[n]$, we also obtain a D-isomorphism $\Lambda^{\mathrm{gl}}(G) \xrightarrow{\cong} \Lambda^{\mathrm{loc}}(D)$, which we shall also refer to as the local-global cyclotomic synchronization isomorphism.*

Proof. Lemma 3.7 follows immediately from the various definitions involved. Note that (any sufficiently large subfield of) the solvably closed extension E of F is necessarily totally imaginary, since $\sqrt{-1} \in E$. □

The reconstruction algorithm for the global cyclotome, together with the local-global cyclotomic synchronization isomorphism, allows us to reconstruct the Kummer container for certain open subgroups of a profinite group of GSC-type.

Lemma 3.8 (Reconstruction of the Kummer container)**.** *Let G be a profinite group of GSC-type. We construct an abelian subgroup $\mathcal{H}^{\times}(G) \subset H^1\big(G, \Lambda^{\mathrm{gl}}(G)\big)$ as the unique abelian subgroup that fits into the following commutative diagram and, moreover, makes it Cartesian:*

$$\begin{array}{ccc} \mathcal{H}^{\times}(G) & \longrightarrow & \mathbb{I}^{\mathrm{fin}}(G) \\ {\scriptstyle incl.}\downarrow & & \downarrow \\ H^1\big(G, \Lambda^{\mathrm{gl}}(G)\big) & \longrightarrow & \prod_{D \in \mathbb{V}(G)} H^1\big(D, \Lambda^{\mathrm{loc}}(D)\big), \end{array}$$

where the lower horizontal arrow is induced by the inclusion homomorphisms $D \hookrightarrow G$ and the local-global synchronization isomorphisms $\Lambda^{\mathrm{gl}}(G) \xrightarrow{\cong} \Lambda^{\mathrm{loc}}(D)$

discussed in Lemma 3.7 (i.e., where D varies over $D \in \mathbb{V}(G)$); the right-hand vertical arrow is the "inclusion" (cf. the construction of $\mathbb{I}^{\mathrm{fin}}(G)$). Also, we define $\mathcal{H}_{\times}(G) \stackrel{\mathrm{def}}{=} \mathcal{H}^{\times}(G)^{\circledast}$. Then, for every number field F, every solvably closed Galois extension E of F, and every finite Galois subextension F'/F of E/F, we have canonical isomorphisms $\mathcal{H}^{\times}(F') \stackrel{\cong}{\longrightarrow} \mathcal{H}^{\times}\big(\mathrm{Gal}(E/F')\big)$; $\mathcal{H}_{\times}(F') \stackrel{\cong}{\longrightarrow} \mathcal{H}_{\times}\big(\mathrm{Gal}(E/F')\big)$. In particular, roughly speaking, we have established an algorithm for reconstructing an object which is canonically isomorphic to the Kummer container $\mathcal{H}_{\times}(F)$ of F solely from the profinite group structure of $\mathrm{Gal}(E/F)$, where E is a solvably closed Galois extension of a number field F.

Proof. Lemma 3.8 follows immediately from various intermediate reconstruction results involved, together with the definition of the Kummer container. □

Remark 3.8.1. Here, we would like to emphasize the importance of the local-global cyclotomic synchronization isomorphisms in the context of reconstructing the Kummer container as in Lemma 3.8.

The advantage of the local cyclotome $\Lambda^{\mathrm{loc}}(D)$ lies in the very fact that it enables the construction of the natural homomorphism Kum_D from $k^{\times}(D) \subset D^{\mathrm{ab}}$ to $H^1\big(D, \Lambda^{\mathrm{loc}}(D)\big)$: the construction of Kum_D depends heavily on the construction of $\Lambda^{\mathrm{loc}}(D)$, and there is no natural homomorphism from $k^{\times}(D)$ to $H^1\big(D, \Lambda^{\mathrm{gl}}(G)\big)$. Therefore, the use of $\Lambda^{\mathrm{loc}}(D)$ is indispensable for obtaining the right-hand vertical arrow of the diagram in Lemma 3.8.

On the other hand, the global cyclotome $\Lambda^{\mathrm{gl}}(G)$ has the evident advantage of being a global object in nature: even if one attempted to replace $\Lambda^{\mathrm{gl}}(G)$ with $\Lambda^{\mathrm{loc}}(D)$ (for some D), one would ultimately need to synchronize the various $\Lambda^{\mathrm{loc}}(D)$'s as D varies over $\mathbb{V}(G)$. This essentially amounts to nothing other than obtaining a global object corresponding to $\Lambda^{\mathrm{gl}}(G)$ (although alternative constructions might exist) together with the local-global synchronization isomorphisms. That is to say, the use of (an object corresponding to) $\Lambda^{\mathrm{gl}}(G)$ and the local-global synchronization isomorphisms is indispensable for obtaining the lower horizontal arrow of the diagram in Lemma 3.8.

In summary, we have no alternative but to employ both the local and global cyclotomes and to bridge them via the local-global synchronization isomorphisms. This may also be regarded as an instance of a general feature of the mono-anabelian setting: identifications that are routinely performed in ordinary arithmetic by means of the ring-theoretic structure — here, the identification of the various cyclotomes with one another — must be undone in the group-theoretic context, and group-theoretically recovering such an isomorphism may have non-trivial consequences, as the present remark illustrates.

4 Purely Mono-anabelian Reconstruction of Number Fields

In the present section, we establish a "purely" mono-anabelian reconstruction algorithm for number fields from the Galois groups of solvably closed Galois extensions. In particular, we obtain an alternative, mono-anabelian proof of the classical Neukirch–Uchida theorem for number fields. This may also be regarded as a refinement of the previous works of Hoshi [MnNF] and [MnNF2],

which gave mono-anabelian reconstruction algorithms for number fields based on the classical Neukirch–Uchida theorem.

Let E be a solvably closed Galois extension of a number field F. Recall that we have already reconstructed from $\mathrm{Gal}(E/F)$ the ring $\prod_{v \in \mathcal{V}_F^{d=1}} F_v$ (cf. Lemma 2.7) and the image of the natural injective homomorphism $\mathcal{H}_\times(F) = \text{“}F^\times \cdot \widehat{\mathcal{O}_F^\times}\text{”} \cup \{0\} \hookrightarrow \prod_{v \in \mathcal{V}_F^{d=1}} F_v$ (cf. Lemma 1.9; Lemma 2.7; Lemma 3.8). In particular, if we moreover succeed in reconstructing the subset “F” $\subset \mathcal{H}_\times(F)$, then we obtain a mono-anabelian reconstruction algorithm for the ring F; varying the open subgroups of $\mathrm{Gal}(E/F)$, we obtain a mono-anabelian reconstruction algorithm for $\mathrm{Gal}(E/F) \curvearrowright E$. (More precisely, we will use the inverse image of $\mathcal{V}_F^{d=1} \subset \mathcal{V}_F$ via the surjection $\mathcal{V}_E \twoheadrightarrow \mathcal{V}_F$ as the index set of the ring $\prod_v F_v$, but this difference is inessential — cf. Lemma 4.4 below.) Now we present such an algorithm. The technical core of our approach is Lemma 4.2 below, which is a formal consequence of a classical result dating back roughly half a century.

Lemma 4.1. *Let G be a group. Write η for the natural homomorphism $G \longrightarrow \hat{G}$, where we recall that we write $\hat{G}$ for the profinite completion of G (cf. the discussion entitled “Topological Groups” in §0). Then the correspondence $U \longmapsto \eta^{-1}(U)$ determines an inclusion-preserving bijection from the set of open subgroups of $\hat{G}$ to the set of subgroups of G of finite index.*

Proof. It is immediate that the map under consideration is inclusion-preserving. The injectivity follows from the fact that $\mathrm{Im}(\eta) \subset \hat{G}$ is dense. (Thus the inverse will be given by simply taking the closure inside $\hat{G}$.) The surjectivity follows from the fact that, for every subgroup $H \subset G$ of finite index, there exists a normal subgroup $H' \subset G$ of finite index such that $H' \subset H$. The details are left to the reader. □

Remark 4.1.1. We shall say that a group G is *profinite complete* if the natural homomorphism $G \longrightarrow \hat{G}$ is an isomorphism. Then (the underlying group of) the profinite completion of a group is not necessarily profinite complete, i.e., the natural homomorphism $\hat{G} \longrightarrow \hat{\hat{G}}$ is not necessarily an isomorphism, even if we restrict our attention to abelian groups; this is in contrast with the situation of Kummer completion discussed in Remark 1.1.5.

Here is an example; since the present remark will never be employed in the present paper, the reader may feel free to skip the following example. Let G be the direct sum $\bigoplus_{n \geq 1} \mathbb{Z}/2\mathbb{Z}$ of countably many copies of $\mathbb{Z}/2\mathbb{Z}$; write $\eta\colon G \longrightarrow \hat{G}$ for the natural homomorphism, which has dense image. Observe that the natural injective homomorphism $G \hookrightarrow \prod_{n \geq 1} \mathbb{Z}/2\mathbb{Z}$ extends, by the universal property of the profinite completion, to a continuous homomorphism $\hat{G} \longrightarrow \prod_{n \geq 1} \mathbb{Z}/2\mathbb{Z}$, which is surjective since its image is compact and dense. In particular, $\hat{G}$ is uncountable; thus, since G is countable, $\mathrm{Im}(\eta) \subset \hat{G}$ is a proper subgroup. Next, since $\hat{G}$ is annihilated by 2, hence may be regarded as a $\mathbb{Z}/2\mathbb{Z}$-vector space, there exists a subgroup $H \subset \hat{G}$ of index 2 such that $\mathrm{Im}(\eta) \subset H$. Then the subgroup $H \subset \hat{G}$ is dense and proper, hence is (not closed, and thus) not open. Thus, in light of Lemma 4.1, the natural homomorphism $\hat{G} \longrightarrow \hat{\hat{G}}$ is not an isomorphism of groups. (Indeed, suppose that the natural homomorphism $\hat{G} \longrightarrow \hat{\hat{G}}$ is an isomorphism of groups; then it follows from Lemma 4.1 that the inverse map $\hat{\hat{G}} \longrightarrow \hat{G}$ is continuous, hence, in fact, a homeomorphism

— cf. the fact that $\hat{G}$ and $\hat{\hat{G}}$ are compact and Hausdorff. Thus it follows, again, from Lemma 4.1 that every subgroup of $\hat{G}$ of finite index is open — in contradiction to the existence of the above H.)

Remark 4.1.2. Here are two supplemental remarks on Remark 4.1.1.

First, by a highly non-trivial theorem of Nikolov and Segal (cf. [NS], Theorem 1.1), every subgroup of finite index of a topologically finitely generated profinite group is open; in particular, the phenomenon discussed above does not occur for the profinite completion of a finitely generated group.

Secondly, one could define the notion of, say, "topological profinite completion" $\hat{G}^{\mathrm{tp}}$ of a topological group G, as the projective limit $\varprojlim_H G/H$, where H ranges over the open normal subgroups of G of finite index; then the natural homomorphism $G \longrightarrow \hat{G}^{\mathrm{tp}}$ is an isomorphism for every profinite group G.

Lemma 4.2. *Let F be a number field and $H \subset F^{\times}$ a finitely generated subgroup. Write $\mathcal{N}'$ for the (necessarily finite — cf. the assumption that H is finitely generated) subset of $\mathcal{V}_F$ constituted by such $v \in \mathcal{V}_F$ that the image of $H \subset F^{\times}$ via the natural homomorphism $F^{\times} \longrightarrow F_v^{\times}$ is not included in $\mathcal{O}_{F_v}^{\times} \subset F_v^{\times}$. (Thus, roughly speaking, $\mathcal{N}'$ is the finite set of "zeros" and "poles" of the elements of H.)*

Recall that, for $v \in \mathcal{V}_F \setminus \mathcal{N}'$, we have a canonical homomorphism $\widehat{H} \longrightarrow \widehat{\mathcal{O}_{F_v}^{\times}} = \mathcal{O}_{F_v}^{\times}$ (cf. Remark 1.1.1; Remark 1.1.6). Let $\mathcal{V}_F = \mathcal{N} \cup \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_n$ be a finite partition of $\mathcal{V}_F$, where $\mathcal{N}$ is of natural density 0 and $\mathcal{N}' \subset \mathcal{N}$ (cf. also Remark 4.2.2 below). Then there exists $i \in \{1, \ldots, n\}$ such that the natural homomorphism $\widehat{H} \longrightarrow \prod_{v \in \mathcal{V}_i} \mathcal{O}_{F_v}^{\times}$ is injective.

Proof. Lemma 4.2 may be regarded as a formal consequence of [congtop], Theorem A. (For the convenience of the interested reader, we refer to [TsjmGS], §1 and Remark 3.13.1, for a simpler proof of this result in a slightly more general form, and to [TsjmGS], Corollary C, for a generalization to semi-abelian varieties.) However, in view of the importance of Lemma 4.2 in the present paper, we provide the details of the deduction. We use the notation as in the statement. Also, we write η for the natural homomorphism $H \longrightarrow \widehat{H}$, for which we may apply Lemma 4.1 in light of Remark 1.1.3. Then, it follows immediately from [congtop], Theorem A, that there exists $i \in \{1, \ldots, n\}$ such that $\mathcal{V}_i$ is ample in the sense of [congtop], §1. We will show that this i satisfies the desired condition. Write f for the natural homomorphism $\widehat{H} \longrightarrow \prod_{v \in \mathcal{V}_i} \mathcal{O}_{F_v}^{\times}$, the injectivity of which we wish to show. It suffices to show that every open subgroup $U \subset \widehat{H}$ satisfies $\mathrm{Ker}\, f \subset U$. Let $U \subset \widehat{H}$ be an open subgroup. Then, by Lemma 4.1, $\eta^{-1}(U) \subset H$ is a subgroup of finite index. Since $\mathcal{V}_i$ is ample, there exist finitely many $v_1, \ldots, v_m \in \mathcal{V}_i$ such that $\bigcap_{1 \leq j \leq m} \eta^{-1}\big(K(v_j)\big) \subset \eta^{-1}(U)$, where we write $K(v_j)$ for the inverse image of $1 + \mathfrak{m}_{v_j} \subset \mathcal{O}_{F_{v_j}}^{\times}$ via the natural homomorphism $\widehat{H} \longrightarrow \mathcal{O}_{F_{v_j}}^{\times}$; $\mathfrak{m}_{v_j}$ for the maximal ideal of $\mathcal{O}_{F_{v_j}}$. In light of the inclusion-preserving bijectivity of Lemma 4.1, the inclusion $\eta^{-1}\Big(\bigcap_{1 \leq j \leq m} K(v_j)\Big) = \bigcap_{1 \leq j \leq m} \eta^{-1}\big(K(v_j)\big) \subset \eta^{-1}(U)$ implies that $\bigcap_{1 \leq j \leq m} K(v_j) \subset U$, where we note that $K(v_j)$ is open in $\widehat{H}$. On the other hand, it follows immediately from the definition that $\mathrm{Ker}\, f \subset \bigcap_{1 \leq j \leq m} K(v_j)$. Thus we have $\mathrm{Ker}\, f \subset U$, as desired. This completes the proof of Lemma 4.2. $\square$

Remark 4.2.1. Lemma 4.2 remains true even if we replace the condition "such that the natural homomorphism $\widehat{H} \longrightarrow \prod_{v \in \mathcal{V}_i} \mathcal{O}_{F_v}^{\times}$ is injective" in the final portion with the stronger condition "such that the natural homomorphism $\widehat{H} \longrightarrow \prod_{v \in \mathcal{V}_i} (\mathcal{O}_{F_v}/\mathfrak{m}_v)^{\times}$ is injective", where we write $\mathfrak{m}_v$ for the maximal ideal of $\mathcal{O}_{F_v}$; indeed, the same proof applies *verbatim* to this stronger form, which is, in essence, the form in which the result is stated in [congtop], Theorem A (cf. also [TsjmGS], Theorem 0.1). We do not need this stronger result in the present paper.

Remark 4.2.2. In Lemma 4.2, we assumed that $\mathcal{N}$ is of natural density 0 in order to keep the statement a formal consequence of the original result [congtop], Theorem A, in which "density" means natural density. In fact, the weaker assumption that $\mathcal{N}$ is of Dirichlet density 0 suffices; indeed, the resulting stronger version of Lemma 4.2 follows immediately from [TsjmGS], Theorem 0.1, applied to "X" = $\mathrm{Spec}(\mathcal{O}_F)$, "$Z$" = $\mathcal{N}$, and "Γ" = H. We do not need this stronger version in the present paper.

Lemma 4.3. *Let F be a number field that is Galois over $\mathbb{Q}$ and F' a number field. Suppose that, for every prime number p that splits completely in F, p also splits completely in F'. Then there exists a field homomorphism $F' \hookrightarrow F$.*

Proof. We wish to apply [NSW], Theorem (12.2.5), which requires us to reduce to the case where F' is also Galois over $\mathbb{Q}$. Fix an algebraic closure $F' \hookrightarrow \overline{\mathbb{Q}}$ and let $\widetilde{F'}$ be the Galois closure of F' over $\mathbb{Q}$ inside $\overline{\mathbb{Q}}$. It is (necessary and) sufficient to show that there exists a field homomorphism $\widetilde{F'} \longrightarrow F$. Let p be a prime number that splits completely in F. Then, by assumption, p also splits completely in F'. Thus, to apply [NSW], Theorem (12.2.5), to obtain the desired embedding, it suffices to show that, for every prime number p, p splits completely in F' (if and) only if p also splits completely in $\widetilde{F'}$. On the other hand, this is easily verified by a standard Galois-theoretic consideration, as follows. Let p be a prime number that splits completely in F'. This amounts to saying that, for every prime $\mathfrak{p}$ of $\overline{\mathbb{Q}}$ lying over p, the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/F')$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ includes the decomposition subgroup of $\mathfrak{p}$. In light of the fact that the set of such decomposition subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ constitutes a single conjugacy class, this inclusion implies that every conjugate $\sigma\,\mathrm{Gal}(\overline{\mathbb{Q}}/F')\sigma^{-1}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/F')$ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ also includes the decomposition subgroup of $\mathfrak{p}$ for every $\mathfrak{p}$ lying over p. Hence we conclude that $\mathrm{Gal}(\overline{\mathbb{Q}}/\widetilde{F'}) = \bigcap_{\sigma} \sigma\,\mathrm{Gal}(\overline{\mathbb{Q}}/F')\sigma^{-1}$ also satisfies the same condition, as desired. This allows us to apply [NSW], Theorem (12.2.5), which completes the proof of Lemma 4.3. □

Lemma 4.4. *Let F be a number field and $\mathcal{S}$ a set equipped with a surjection $\phi\colon \mathcal{S} \twoheadrightarrow \mathcal{V}_F^{d=1}$; for $v \in \mathcal{S}$, we write F_v for $F_{\phi(v)}$ for brevity. Then the elements in the image of the natural injection $F \hookrightarrow \prod_{v \in \mathcal{V}_F^{d=1}} F_v \hookrightarrow \prod_{v \in \mathcal{S}} F_v$ are characterized as $a \in \prod_{v \in \mathcal{S}} F_v$ satisfying the following conditions:*

- *(i) a is in the image of the natural injective homomorphism $\mathcal{H}_{\times}(F) \hookrightarrow \prod_{v \in \mathcal{S}} F_v$ (cf. Lemma 1.9 for the injectivity).*
- *(ii) a is algebraic over $\mathbb{Q}$ with respect to the natural $\mathbb{Q}$-algebra structure of $\prod_{v \in \mathcal{S}} F_v$.*

(iii) *The minimal polynomial of a over $\mathbb{Q}$ (cf. the condition (ii)) is irreducible in the polynomial ring $\mathbb{Q}[X]$, i.e., the subring $\mathbb{Q}[a] \subset \prod_{v \in \mathcal{S}} F_v$ is, in fact, a field.*

(iv) *For every prime number p such that every $\mathfrak{p} \in \mathcal{V}_F$ lying over p belongs to $\mathcal{V}_F^{d=1}$ — or, equivalently, such that p splits completely in the extension $F/\mathbb{Q}$ — p splits completely in the finite extension $\mathbb{Q}[a]/\mathbb{Q}$ (cf. the condition (iii)). Put another way, for every prime number p such that the cardinality of the set of ring homomorphisms $F \longrightarrow \mathbb{Q}_p$ is equal to $[F : \mathbb{Q}]$, the cardinality of the set of ring homomorphisms $\mathbb{Q}[a] \longrightarrow \mathbb{Q}_p$ is equal to $\left[\mathbb{Q}[a] : \mathbb{Q}\right]$ (cf. the condition (iii)).*

Proof. It is immediate that, if a is in the image of the natural injection $F \hookrightarrow \prod_{v \in \mathcal{S}} F_v$, then a satisfies the conditions (i), (ii), (iii); as for the condition (iv), we note that, if a prime number p splits completely in F, then it splits completely in the subfield $\mathbb{Q}[a] \subset F$ as well.

To show the converse, first we note that it follows immediately from the condition (i) that we may assume that $\mathcal{S} = \mathcal{V}_F^{d=1}$ and that ϕ is the identity map. Secondly, we will reduce to the case of an arbitrary finite Galois extension of F, as follows. (We will only apply this reduction to the case where the finite Galois extension of F is taken to be the Galois closure of F over $\mathbb{Q}$.) Let F'/F be a finite Galois extension. Then F' is also a number field, and thus we have the following commutative diagram, where the injectivity of the middle vertical arrow follows from Lemma 1.6, (1), together with the definition of the Kummer containers:

$$\begin{array}{ccccc} F' & \hookrightarrow & \mathcal{H}_\times(F') & \hookrightarrow & \prod_{w \in \mathcal{V}_{F'}^{d=1}} F'_w \\ \uparrow & & \uparrow & & \uparrow \\ F & \hookrightarrow & \mathcal{H}_\times(F) & \hookrightarrow & \prod_{v \in \mathcal{V}_F^{d=1}} F_v. \end{array}$$

Note that $\mathrm{Gal}(F'/F)$ acts naturally on the upper horizontal sequence of this diagram. To simplify the notation, we think of F, F', and $\mathcal{H}_\times(F)$ as subsets of $\mathcal{H}_\times(F')$. We wish to show that the assertion holds for F under the additional assumption that the assertion holds for F'. We observe that, if $a \in \prod_{v \in \mathcal{V}_F^{d=1}} F_v$ satisfies the four conditions in the statement (which, in particular, implies that $a \in \mathcal{H}_\times(F)$), then $a \in \mathcal{H}_\times(F')$ satisfies the corresponding four conditions for F', where, for the condition (iv), we note that, if a prime number splits completely in F', then it also splits completely in F. Then, in light of our additional assumption, it follows that $a \in F'$. Thus we have only to show that the left-hand commutative square of the above diagram is a pull-back diagram, i.e., $F = F' \cap \mathcal{H}_\times(F)$. On the other hand, this equality follows immediately from the facts that $F = (F')^{\mathrm{Gal}(F'/F)}$ and that $\mathcal{H}_\times(F) \subset \mathcal{H}_\times(F')^{\mathrm{Gal}(F'/F)}$. This completes the proof of the reduction to an arbitrary finite Galois extension F' of F.

Applying the above reduction to the case where F' is taken to be the Galois closure of F over $\mathbb{Q}$, we may assume that F is Galois over $\mathbb{Q}$. Let F be a number field that is Galois over $\mathbb{Q}$ and $a \in \prod_{v \in \mathcal{V}_F^{d=1}} F_v$ satisfy the four conditions in the statement. We may also assume that $a \neq 0$. In particular, $a \in \mathcal{H}^\times(F)$ (cf. the condition (i) and the additional assumption that $a \neq 0$), and a is algebraic over $\mathbb{Q}$ (cf. the condition (ii)). Let n denote the extension degree $\left[\mathbb{Q}[a] : \mathbb{Q}\right]$ and

$f(X) \in \mathbb{Q}[X]$ the minimal polynomial of a over $\mathbb{Q}$, which is irreducible (cf. the condition (iii)) and of degree n. It follows from the condition (iv), in light of Lemma 4.3, that there exists an embedding $\mathbb{Q}[a] \longrightarrow F$ — which is, at least a priori, *not necessarily compatible* with the natural injection into $\prod_{v \in \mathcal{V}_F^{d=1}} F_v$! — that is to say, $f(X)$ has a root in F. Then, by our assumption that F is Galois over $\mathbb{Q}$, $f(X)$ has n distinct roots in F, for which we write $b_1, \ldots, b_n \in F^\times$. Our goal is to show that $a = b_i$ in $\mathcal{H}^\times(F)$ for some $i \in \{1, \ldots, n\}$.

Write $t_v \colon \widehat{F^\times} \longrightarrow \widehat{F_v^\times}$ for the natural homomorphism, where $v \in \mathcal{V}_F$. Choose $a' \in F^\times$ and $a'' \in \widehat{\mathcal{O}_F^\times}$ such that $a = a'a''$ (cf. Lemma 1.8), and write $S \subset \mathcal{V}_F$ for the (necessarily finite) set of primes constituted by the "zeros" and "poles" of $a', b_1, \ldots, b_n$, i.e., the set of primes constituted by such a prime $v \in \mathcal{V}_F$ that the image of at least one of $a', b_1, \ldots, b_n \in F^\times$ via the natural homomorphism $F^\times \longrightarrow F_v^\times$ is not contained in $\mathcal{O}_{F_v}^\times$; $\mathcal{N}'' \stackrel{\text{def}}{=} S \cap \mathcal{V}_F^{d=1}$; $H \stackrel{\text{def}}{=} \mathcal{O}_{F,S}^\times \subset F^\times$ for the group of "S-units" of F (cf. the proof of Corollary 1.5), which is finitely generated by the well-known "S-unit version of Dirichlet's unit theorem" (cf. [Neukirch], Chapter I, Corollary (11.7)). Then $a', b_1, \ldots, b_n \in H$; moreover, since $\mathcal{O}_F^\times \subset H$, the image of a'' via the natural homomorphism $\widehat{\mathcal{O}_F^\times} \longrightarrow \widehat{F^\times}$ belongs to the image of the natural homomorphism $\widehat{H} \longrightarrow \widehat{F^\times}$. Thus $a, b_1, \ldots, b_n$ belong to the image of the natural homomorphism $\widehat{H} \longrightarrow \widehat{F^\times}$, which is injective by (the "S-unit" case — cf. Remark 1.5.1 — of) Corollary 1.5. We regard $\widehat{H} \subset \widehat{F^\times}$ via this natural injection; hence $a, b_1, \ldots, b_n \in \widehat{H}$.

For every $v \in \mathcal{V}_F^{d=1}$, there exists a unique $i \in \{1, \ldots, n\}$ such that $t_v(a) = t_v(b_i) \in F_v^\times \subset \widehat{F_v^\times}$, since $t_v(a)$ is a root of $f(X)$ in the field F_v. This means that there exists a finite partition $\mathcal{V}_F^{d=1} = \mathcal{N}'' \cup \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_n$ of $\mathcal{V}_F^{d=1}$ such that, for each $i \in \{1, \ldots, n\}$, the images of a and b_i via the natural homomorphism $\widehat{F^\times} \longrightarrow \prod_{v \in \mathcal{V}_i} \widehat{F_v^\times}$ coincide, i.e., the equality $\left(t_v(a)\right)_{v \in \mathcal{V}_i} = \left(t_v(b_i)\right)_{v \in \mathcal{V}_i}$ holds. On the other hand, applying Lemma 4.2 to the finite partition $\mathcal{V}_F = \mathcal{N} \cup \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_n$, where $\mathcal{N} \stackrel{\text{def}}{=} (\mathcal{V}_F \setminus \mathcal{V}_F^{d=1}) \cup \mathcal{N}''$ — a set of natural density 0 which includes the "zeros" and "poles" of the elements of H (cf. the inclusion $S \subset \mathcal{N}$) — we conclude that, for some $i \in \{1, \ldots, n\}$, the natural homomorphism $\widehat{H} \longrightarrow \prod_{v \in \mathcal{V}_i} \mathcal{O}_{F_v}^\times$ is injective. Since, by construction, the natural homomorphism $\widehat{H} \longrightarrow \prod_{v \in \mathcal{V}_i} \mathcal{O}_{F_v}^\times$ is compatible with the t_v's, we deduce from this injectivity and the equality $\left(t_v(a)\right)_{v \in \mathcal{V}_i} = \left(t_v(b_i)\right)_{v \in \mathcal{V}_i}$ that $a = b_i$ for some $i \in \{1, \ldots, n\}$, as desired. This completes the proof of Lemma 4.4. $\square$

Remark 4.4.1. Our use of the ring "$\prod_{v \in \mathcal{V}_F^{d=1}} F_v$" — where F denotes the base number field under consideration — as the ambient ring (cf. Theorem 4.5, (1), below), which is based on the reconstruction of the field structures of "$\mathbb{Q}_p$" (cf. Lemma 2.7), follows the basic strategy of [MnNF2] (cf. also the comment (C2) in the Introduction). Indeed, in [MnNF2], this kind of direct product is exploited — in the case where $F \cong \mathbb{Q}$ — both as the container and as a means of singling out certain subfields of the container that correspond to solvable extensions of $\mathbb{Q}$ (cf. [MnNF2], Definition 2.4 and Definition 2.6). This use is parallel to ours, except that our application of the ambient ring structure to the reconstruction of subfields is restricted neither to the case where $F \cong \mathbb{Q}$ nor to subfields that correspond to solvable extensions of $\mathbb{Q}$. This heavier use of the ambient ring structure in Lemma 4.4 is precisely what allows one to avoid the

application of the classical Neukirch–Uchida theorem in [MnNF2] (cf. [MnNF2], Proposition 3.4 and Remark 3.9.2), hence to obtain our purely mono-anabelian reconstruction algorithm. Thus, very roughly speaking, the situation may be summarized by the following schematic "equation", in which the second term of the right-hand side is precisely what allows one to dispense with the application of the classical Neukirch–Uchida theorem:

$$\begin{pmatrix} \text{our purely} \\ \text{mono-anab.} \\ \text{algorithm} \\ \text{(cf. Theorem 4.6} \\ \text{below)} \end{pmatrix} = \begin{pmatrix} \text{purely mono-anab.} \\ \text{portions of} \\ \text{Hoshi's algorithm} \\ \text{(cf. [MnNF2],} \\ \text{Theorem 3.9)} \end{pmatrix} + \begin{pmatrix} \text{further application} \\ \text{of reconstructed} \\ \text{field str. of "}\mathbb{Q}_p\text{"} \\ \text{(cf. Lemma 2.7;} \\ \text{Lemma 4.4)} \end{pmatrix}.$$

Remark 4.4.2. In the context of Lemma 4.4, the following interesting problems remain open, to the authors' knowledge, at the time of writing the present paper:

(Q-1) Can one remove the conditions (iii), (iv) from Lemma 4.4? That is to say, do the conditions (i), (ii) already characterize the image of F?

(Q-2) Can one replace the condition (i) in Lemma 4.4 with the following weaker condition?

> *"If $a \neq 0$, then $a \in \prod_{v \in \mathcal{S}} F_v^\times$, and the image of a via the natural injective homomorphism $\prod_{v \in \mathcal{S}} F_v^\times \hookrightarrow \prod_{v \in \mathcal{S}} \widehat{F_v^\times}$ (cf. Remark 1.1.6) lies in the image of the natural injective homomorphism $\widehat{F^\times} \hookrightarrow \prod_{v \in \mathcal{S}} \widehat{F_v^\times}$ (cf. Remark 1.7.1)."*

One may also consider these two modifications simultaneously.

Remark 4.4.3. In the context of Lemma 4.4, it is of interest to compare the case of number fields with the case of function fields of curves over finite fields, where the classical proof of the Neukirch–Uchida theorem is already essentially purely mono-anabelian (cf. [Sawada]). We note first that this algorithmic proof proceeds by means of class field theory, rather than Kummer theory. Nevertheless, the following structural contrast seems illuminating: in the function field case, the unit group corresponding to $\mathcal{O}_F^\times$ is the multiplicative group of the field of constants, hence *finite*, while, in the number field case, Dirichlet's unit theorem — reflecting the presence of the archimedean primes — implies that $\mathcal{O}_F^\times$ is, in general, infinite. It is the latter circumstance that gives rise to the gap between $F^\times$ and the Kummer container $\mathcal{H}^\times(F) = F^\times \cdot \widehat{\mathcal{O}_F^\times}$ (cf. Lemma 1.8); the treatment of this gap — via the finite partition of $\mathcal{V}_F^{d=1}$ and Lemma 4.2 — constitutes the technical heart of the present paper. In this context, it is perhaps not a coincidence that the fields treated in [MS], Theorem 2 — i.e., $\mathbb{Q}$ and imaginary quadratic fields — are precisely the number fields whose unit groups are finite, in which case the gap in question vanishes (cf. the corresponding observation in [MS], §7). A similar observation also applies to [Mao], Theorem 1.2, although the mechanism is different: by the Kronecker–Weber theorem (cf. [Neukirch], Chapter V, Theorem (1.10)), the abelian number fields treated there are precisely the number fields embeddable into some cyclotomic extension of $\mathbb{Q}$; such an extension is generated over $\mathbb{Q}$ by roots of unity, i.e., by *torsion* elements of its unit group, and the Kummer completion has no effect on these torsion

elements, in the sense that the natural homomorphism $(\mathcal{O}_F^\times)_{\mathrm{tor}} \longrightarrow \left(\widehat{\mathcal{O}_F^\times}\right)_{\mathrm{tor}}$ is an isomorphism for every number field F (cf. Remark 1.1.3; [Neukirch], Chapter I, Theorem (7.4)).

On the other hand, in the present paper, the number field case is rescued by two tools that admit no obvious counterparts in positive characteristic: the reconstruction of the ring structure of "$\mathbb{Q}_p$" (cf. Lemma 2.7) and the availability of the core "$\mathbb{Q}$" (cf. the conditions (ii), (iii), (iv) of Lemma 4.4). In fact, these two tools may be regarded as a local instance and a global instance of a single phenomenon: the field $\mathbb{Q}_p$ is itself a "core" in the local setting, i.e., every mixed characteristic local field of residue characteristic p includes $\mathbb{Q}_p$ canonically, and thus the ambient ring "$\prod_{v \in \mathcal{V}_F^{d=1}} F_v$" (cf. Remark 4.4.1) is nothing other than a product of copies of the local core. It is tempting to relate this "coricity" to the reconstructibility of the ring structure of "$\mathbb{Q}_p$" (although the former, by itself, neither obviously implies nor obviously follows from the latter). In positive characteristic, by contrast, no such core exists — a subfield of the form $\mathbb{F}_p((t))$ of a positive characteristic local field depends on the choice of the uniformizer "t" — so that even the notion of "absolute degree" is unavailable.

In light of this state of affairs, the authors expect that, ultimately, it will be possible to establish even stronger results for number fields than for function fields (cf., e.g., [MST], Theorem D; also the subsequent work [TT2]) — an expectation rooted in the point of view, expressed at the end of the discussion of Step (3) in the Introduction, that considerations based on "cores" constitute a fruitful direction of further development.

Lemma 4.4 readily implies, in light of the various already established algorithms, that we may algorithmically reconstruct a number field (which is canonically isomorphic to) F from the profinite group structure of $\mathrm{Gal}(E/F)$, where E is a solvably closed Galois extension of F (cf. Theorem 4.5, (2), below). Moreover, by applying this algorithm to each open normal subgroup $\mathrm{Gal}(E/F')$ of $\mathrm{Gal}(E/F)$ to obtain the reconstruction algorithm for "$\mathrm{Gal}(E/F) \curvearrowright F'$", and by taking the inductive limit, we obtain the desired reconstruction algorithm for "$\mathrm{Gal}(E/F) \curvearrowright E$" (cf. Theorem 4.5, (5), below). We record this reconstruction algorithm as follows.

Theorem 4.5 (Purely mono-anabelian reconstruction of number fields)**.** *Let G be a profinite group of GSC-type. Then the following assertions hold:*

(1) We shall write $\mathcal{R}(G)$ for the commutative ring $\prod_{D \in \mathbb{V}(G);\, d(D)=1} k_{\mathrm{fld}}(D)$ (cf. Lemma 2.7). For every solvably closed Galois extension E of a number field F, we have a canonical isomorphism $\mathcal{R}\big(\mathrm{Gal}(E/F)\big) \xrightarrow{\cong} \prod_{\widetilde{\mathfrak{p}} \in \mathcal{V}_E;\, [F_{\mathfrak{p}}:\mathbb{Q}_p]=1} F_{\mathfrak{p}}$ of rings, where we write $\mathfrak{p}$ (resp. p) for the non-archimedean prime of F (resp. the prime number) underlying $\widetilde{\mathfrak{p}}$.

(2) The composite of the natural map $\mathcal{H}^\times(G) \longrightarrow \mathbb{I}^{\mathrm{fin}}(G)$ which appeared in the construction of $\mathcal{H}^\times(G)$ (cf. Lemma 3.8) with the natural "projection" map from $\mathbb{I}^{\mathrm{fin}}(G) \subset \prod_{v \in \mathbb{V}^{\mathrm{base}}(G)} k^\times(G, v) \subset \prod_{D \in \mathbb{V}(G)} k^\times(D)$ to $\prod_{D \in \mathbb{V}(G);\, d(D)=1} k^\times(D)$ is injective. Thus it extends to an injective homomorphism $\mathcal{H}_\times(G) \hookrightarrow \prod_{D \in \mathbb{V}(G);\, d(D)=1} k_{\mathrm{fld}}(D)$ of monoids. We shall write $\mathbf{F}(G)$ for the subset of $\prod_{D \in \mathbb{V}(G);\, d(D)=1} k_{\mathrm{fld}}(D)$ constituted by the elements a satisfying the following conditions:

(i) *a is in the image of the natural injective homomorphism $\mathcal{H}_{\times}(G) \hookrightarrow \prod_{D \in \mathbb{V}(G);\, d(D)=1} k_{\mathrm{fld}}(D)$.*

(ii) *a is algebraic over $\mathbb{Q}$ with respect to the natural $\mathbb{Q}$-algebra structure of $\prod_{D \in \mathbb{V}(G);\, d(D)=1} k_{\mathrm{fld}}(D)$.*

(iii) *The minimal polynomial of a over $\mathbb{Q}$ (cf. the condition (ii)) is irreducible in the polynomial ring $\mathbb{Q}[X]$, i.e., the subring $\mathbb{Q}[a] \subset \prod_{D \in \mathbb{V}(G);\, d(D)=1} k_{\mathrm{fld}}(D)$ is, in fact, a field.*

(iv) *For every prime number p such that $d(D) = 1$ for every $D \in \mathbb{V}(G)$ with $p(D) = p$, p splits completely in the finite extension $\mathbb{Q}[a]/\mathbb{Q}$ (cf. the condition (iii)).*

Then $\mathbf{F}(G)$ is a subring of $\mathcal{R}(G)$; in fact, $\mathbf{F}(G)$ is a number field. Moreover, for every solvably closed Galois extension E of a number field F, we have the following commutative diagram:

$$\begin{array}{ccc} \mathbf{F}\big(\mathrm{Gal}(E/F)\big) & \hookrightarrow & \mathcal{R}\big(\mathrm{Gal}(E/F)\big) \\ \cong \downarrow & & \downarrow \cong \\ F & \hookrightarrow & \prod_{\widetilde{\mathfrak{p}} \in \mathcal{V}_E;\, [F_{\mathfrak{p}}:\mathbb{Q}_p]=1} F_{\mathfrak{p}}, \end{array}$$

where we write $\mathfrak{p}$ (resp. p) for the non-archimedean prime of F (resp. the prime number) underlying $\widetilde{\mathfrak{p}}$; the upper horizontal arrow is the inclusion map; the lower horizontal arrow is the natural one; the right-hand vertical arrow is the isomorphism of rings discussed in the assertion (1). In particular, roughly speaking, we have established an algorithm for reconstructing a field which is canonically isomorphic to F solely from the profinite group structure of $\mathrm{Gal}(E/F)$, where E is a solvably closed Galois extension of a number field F.

(3) *Let H be an open normal subgroup of G, which is again of GSC-type. Then the conjugation action of G on H induces an action of G on $\mathbf{F}(H)$. Now suppose that E is a solvably closed Galois extension of a number field F and that F'/F is a finite Galois subextension of E/F. Then the ring isomorphism $\mathbf{F}\big(\mathrm{Gal}(E/F')\big) \xrightarrow{\cong} F'$ discussed in the assertion (2) is compatible with the respective actions of $\mathrm{Gal}(E/F)$.*

(4) *Let H' and H'' be open normal subgroups of G, which are again of GSC-type, such that $H'' \subset H'$. Then we have a canonical ring homomorphism $\mathbf{F}(H') \hookrightarrow \mathbf{F}(H'')$ compatible with the respective actions of G (cf. the proof for the details). Now suppose that E is a solvably closed Galois extension of a number field F; let F'/F and F''/F be finite Galois subextensions of E/F such that $F' \subset F''$. Then the $\mathrm{Gal}(E/F)$-homomorphism $\mathbf{F}\big(\mathrm{Gal}(E/F')\big) \hookrightarrow \mathbf{F}\big(\mathrm{Gal}(E/F'')\big)$ fits into the following commutative diagram as the left-hand vertical arrow:*

$$\begin{array}{ccc} \mathbf{F}\big(\mathrm{Gal}(E/F'')\big) & \xrightarrow{\cong} & F'' \\ \uparrow & & \uparrow \\ \mathbf{F}\big(\mathrm{Gal}(E/F')\big) & \xrightarrow{\cong} & F' \end{array}$$

where the right-hand vertical arrow is the inclusion homomorphism $F' \hookrightarrow F''$*; the horizontal arrows are the natural ones discussed in the assertion (3).*

(5) *We define a field* $\widetilde{\mathbf{F}}(G) \stackrel{\text{def}}{=} \varinjlim_H \mathbf{F}(H)$ *equipped with an action of* G*, where* H *ranges over the open normal subgroups of* G*; the transition maps are the ones discussed in the assertion (4). Then, for every solvably closed Galois extension* E *of a number field* F*, the homomorphisms discussed in the assertion (4) determine a canonical* $\mathrm{Gal}(E/F)$*-isomorphism* $\widetilde{\mathbf{F}}\big(\mathrm{Gal}(E/F)\big) \xrightarrow{\cong} E$*. In particular, roughly speaking, we have established an algorithm for reconstructing a (solvably closed) field which is canonically isomorphic to* E*, together with an action of* $\mathrm{Gal}(E/F)$ *corresponding to the natural action* $\mathrm{Gal}(E/F) \curvearrowright E$*, solely from the profinite group structure of* $\mathrm{Gal}(E/F)$*, where* E *is a solvably closed Galois extension of a number field* F*.*

Proof. The assertion (1) follows immediately from the constructions (cf. Lemma 2.7). The assertion (2) follows immediately from Lemma 1.9 and Lemma 4.4, where we note that, for a solvably closed Galois extension E of a number field F with $G = \mathrm{Gal}(E/F)$, the condition "$d(D) = 1$ for every $D \in \mathbb{V}(G)$ with $p(D) = p$" on p amounts to the condition that p splits completely in the extension $F/\mathbb{Q}$. The assertion (3) follows immediately from the constructions.

To define the ring homomorphism $\mathbf{F}(H') \hookrightarrow \mathbf{F}(H'')$ in the assertion (4), note that $\mathbf{F}(H')$ is a subring of $\mathcal{R}(H') = \prod_{D \in \mathbb{V}(H');\, d(D)=1} k_{\mathrm{fld}}(D)$ and that $\mathbf{F}(H'')$ is a subring of $\mathcal{R}(H'') = \prod_{D \in \mathbb{V}(H'');\, d(D)=1} k_{\mathrm{fld}}(D)$. Then, since the index set of the latter is a subset of the index set of the former (since we are restricting our attention to the "decomposition subgroups of absolute degree one"), we have a natural projection $\mathcal{R}(H') \twoheadrightarrow \mathcal{R}(H'')$. This induces the desired ring homomorphism $\mathbf{F}(H') \hookrightarrow \mathbf{F}(H'')$. Then the remainder of the assertion (4) follows immediately from the constructions.

Finally, the assertion (5) follows immediately from the previous assertions. This completes the proof of Theorem 4.5. □

Theorem 4.6 (Summary of Theorem 4.5, (5))**.** *We have established a purely mono-anabelian reconstruction algorithm for the action* $\mathrm{Gal}(E/F) \curvearrowright E$*, whose input data is the abstract profinite group* $\mathrm{Gal}(E/F)$ *and whose output data is a field* $\widetilde{\mathbf{F}}\big(\mathrm{Gal}(E/F)\big)$ *which is canonically isomorphic to the field* E *together with the action of* $\mathrm{Gal}(E/F)$ *on it, where* E *is a solvably closed Galois extension of a number field* F*.*

Proof. Theorem 4.6 is merely a rough summary of a certain portion of Theorem 4.5, (5). The use of the modifier "purely" indicates that neither the construction nor the verification of the algorithm relies on the corresponding (or any) bi-anabelian result (cf. also Remark 4.6.1 below). □

Remark 4.6.1. In the proof of Theorem 4.6, we reviewed the meaning of the modifier "purely", which was introduced in the Introduction. However, we have not made precise whether this modifier is to be understood as asserting independence from *the corresponding* bi-anabelian result or independence from *any* bi-anabelian result. In fact, this is a delicate issue to which the authors themselves do not have a definitive answer — that is to say, the definition of

the term "purely mono-anabelian result" has not been fixed completely — and this delicacy may indeed be observed in Theorem 4.6 itself, as follows.

First, since we speak of a "*purely*" mono-anabelian result, independence from the corresponding bi-anabelian result is a minimal requirement; this is precisely what distinguishes such a result from the impurely mono-anabelian results (cf. (L3) in the Introduction). Theorem 4.6 does, of course, satisfy this minimal requirement, i.e., the independence from the Neukirch–Uchida theorem (cf. Corollary 4.7 below).

On the other hand, in light of the meaning of the word "pure", one may also feel that only those results obtained without the use of *any* bi-anabelian result deserve to be called purely mono-anabelian. (Suppose, for instance, that an algorithm similar to that of Theorem 4.5 had been constructed by relying on a variant of Corollary 4.7 below in which one considers only the case where $F_\circ$ and $F_\bullet$ are Galois over $\mathbb{Q}$ — would one then wish to call the resulting algorithm purely mono-anabelian?) Theorem 4.6 "almost" satisfies even this stricter requirement: at least, it makes no use of any bi-anabelian result in the sense explained in (L1) in the Introduction. Unfortunately, however, one may also say that this stricter requirement is not satisfied completely; as we explain in Remark 4.6.2 below, there are various kinds of bi-anabelian results that were not covered by the discussion of (L1), and Lemma 4.3, on which the present proof of Theorem 4.6 does depend, may also be regarded as a sort of bi-anabelian result — more specifically, as a sort of "weak Hom-version" result.

Thus, the authors' use of the term "purely mono-anabelian" for Theorem 4.5 may be regarded as a proposal: although the precise definition of the term still involves some ambiguity, a result that comes this close to being completely "pure" should be counted as purely mono-anabelian. Of course, it may well happen that, as the mathematical understanding of the situation deepens, one will eventually be able to establish Theorem 4.6 in a completely "pure" fashion.

Remark 4.6.2. In the context of Remark 4.6.1, let us discuss certain kinds of "bi-anabelian results" that were not covered by the discussion of (L1) in the Introduction. As explained in (L1), a typical assertion in bi-anabelian geometry is the full faithfulness of a certain functor $\Phi\colon \mathcal{C} \longrightarrow \mathcal{D}$ — typically, the formation of "fundamental groups" — whose domain $\mathcal{C}$ is taken to be a groupoid; a result of this kind is often referred to as an "Isom-version" result. (If $\mathcal{C}$ is not taken to be a groupoid, then the full faithfulness is often referred to as a "Hom-version" result.) Then we observe that "Isom-version" may be divided into the following two versions:

- "Aut-version": the bijectivity of the map $\mathrm{Aut}_{\mathcal{C}}(X) \longrightarrow \mathrm{Aut}_{\mathcal{D}}\big(\Phi(X)\big)$ for every object X of $\mathcal{C}$;
- "weak Isom-version": the implication "$\Phi(X) \cong \Phi(Y)$ in $\mathcal{D} \implies X \cong Y$ in $\mathcal{C}$" for all objects X, Y of $\mathcal{C}$.

A result of any of these kinds may usually be regarded as a bi-anabelian result.

Corollary 4.7 (Bi-anabelian Neukirch–Uchida theorem)**.** *For $\square \in \{\circ, \bullet\}$, let $E_\square$ be a solvably closed Galois extension of a number field $F_\square$. Write $\mathrm{Isom}(E_\circ/F_\circ, E_\bullet/F_\bullet)$ for the set of field isomorphisms $\sigma\colon E_\circ \xrightarrow{\cong} E_\bullet$ that satisfy $\sigma(F_\circ) = F_\bullet$, and $\mathrm{Isom}\big(\mathrm{Gal}(E_\circ/F_\circ), \mathrm{Gal}(E_\bullet/F_\bullet)\big)$ for the set of isomorphisms*

$\mathrm{Gal}(E_\circ/F_\circ) \xrightarrow{\cong} \mathrm{Gal}(E_\bullet/F_\bullet)$ *of profinite groups. Then the map*

$$\mathrm{Isom}(E_\circ/F_\circ, E_\bullet/F_\bullet) \longrightarrow \mathrm{Isom}\big(\mathrm{Gal}(E_\circ/F_\circ), \mathrm{Gal}(E_\bullet/F_\bullet)\big);\ \sigma \longmapsto (\tau \mapsto \sigma\tau\sigma^{-1})$$

is bijective.

Proof. Corollary 4.7 follows essentially formally from Theorem 4.5, (5) (or Theorem 4.6), where we recall that we have established a "purely" mono-anabelian reconstruction algorithm (cf. the proof of Theorem 4.6). However, we present a sketch of the deduction of the bi-anabelian result from our mono-anabelian result for the convenience of the reader.

First, we note that the map under consideration coincides with the composition of the natural map

$$\mathrm{Isom}(E_\circ/F_\circ, E_\bullet/F_\bullet) \xrightarrow{\cong} \mathrm{Isom}\big(\mathrm{Gal}(E_\circ/F_\circ) \curvearrowright E_\circ, \mathrm{Gal}(E_\bullet/F_\bullet) \curvearrowright E_\bullet\big)$$

with the "forgetful" map

$$\mathrm{Isom}\big(\mathrm{Gal}(E_\circ/F_\circ) \curvearrowright E_\circ, \mathrm{Gal}(E_\bullet/F_\bullet) \curvearrowright E_\bullet\big) \longrightarrow \mathrm{Isom}\big(\mathrm{Gal}(E_\circ/F_\circ), \mathrm{Gal}(E_\bullet/F_\bullet)\big);$$

moreover, one verifies immediately that the former is bijective. Thus it suffices to show that the latter is also bijective; put another way, our task is to show that a certain forgetful functor Φ between certain groupoids is fully faithful. More precisely, the domain $\mathcal{C}$ of our forgetful functor is the groupoid each of whose objects is a triple consisting of a profinite group G, a field M, and an action $G \curvearrowright M$ such that there exists a solvably closed Galois extension E of a number field F such that $(G \curvearrowright M) \cong \big(\mathrm{Gal}(E/F) \curvearrowright E\big)$ in the evident sense; the codomain $\mathcal{D}$ is the groupoid each of whose objects is a profinite group that is isomorphic to the Galois group of some solvably closed Galois extension of a number field. Then it is implicit in Theorem 4.5 (or Theorem 4.6) that the algorithm $G \longmapsto \big(G \curvearrowright \widetilde{\mathbf{F}}(G)\big)$ determines a functor $\Psi\colon \mathcal{D} \longrightarrow \mathcal{C}$; one verifies immediately that $\Phi \circ \Psi = \mathrm{id}_{\mathcal{D}}$; the identity isomorphism of G, together with the canonical G-isomorphism $\widetilde{\mathbf{F}}(G) \xrightarrow{\cong} \widetilde{\mathbf{F}}\big(\mathrm{Gal}(M/M^G)\big) \xrightarrow{\cong} M$ which was discussed in Theorem 4.5, (5), gives a natural isomorphism $\Psi \circ \Phi \cong \mathrm{id}_{\mathcal{C}}$. This completes the proof of Corollary 4.7. $\square$

Remark 4.7.1. The present paper has established what is, to the authors' knowledge, the first purely mono-anabelian version of the Neukirch–Uchida theorem for general number fields (cf. Theorem 4.6; Corollary 4.7; also [MS], Theorem 2, and [Mao], Theorem 1.2, for previously known purely mono-anabelian results for special number fields). On the other hand, various variants of the (bi-anabelian) Neukirch–Uchida theorem for number fields have been established in the literature. The main direction of such variants is to replace the absolute Galois group by a suitable smaller quotient (cf., e.g., [ST], Theorem 2; [Shimizu1], Theorem 2.4; [Shimizu2], §7; [Ozaki], Theorem 1; [KS], Theorem 1.2 and Theorem 1.3); also, recently, the second author, jointly with Minamide and Sawada, generalized the base fields from number fields to suitable (possibly infinite) algebraic extensions of $\mathbb{Q}$ (cf. [MST], Theorem D).

Here, we note that, just as in the case of the original proofs of the Neukirch–Uchida theorem for number fields (cf. the discussion preceding Q.1 in the Introduction), the proofs of the variants cited above do not yield (purely) mono-anabelian reconstruction algorithms for the base fields. Thus, these variants constitute non-trivial instances of the question Q.4 in the Introduction; as a possible direction of future research, it would be of interest to establish (purely) mono-anabelian versions of them (cf., in the case of [ST], the partial results of [MS] and [Mao] discussed in the second through fourth paragraphs of §5 below).

In the case where one attempts to apply the techniques of the present paper in a direct fashion, the reconstruction of the ring structure of "$\mathbb{Q}_p$" constitutes an essential ingredient (cf. Lemma 2.7). From this point of view, it appears difficult — at least immediately — to apply the techniques of the present paper to the settings of, e.g., [Shimizu1], [Shimizu2], [Ozaki], [KS], and [MST] (cf. also the comment (C1) in the Introduction). On the other hand, the techniques of the present paper may be applied, in a direct fashion, to the "finite-step solvable" setting of [ST] and indeed yield non-trivial results; this is precisely the content of §5 below, as well as of the subsequent work [TT2].

5 Toward the Finite-step Solvable Variants

In the subsequent work [TT2], we will develop "finite-step solvable" variants of the purely mono-anabelian reconstruction algorithm discussed so far. The purpose of the present section is to establish, as a first step toward this development, the following result: we have a purely mono-anabelian reconstruction algorithm for "$\mathrm{Gal}(F_m/F) \curvearrowright F_m$" from "$\mathrm{Gal}(F_{m+4}/F)$", where $m \in \mathbb{Z}_{\geq 1}$ and F is a number field, i.e., a "4-step loss" finite-step solvable purely mono-anabelian reconstruction algorithm for number fields (cf. Theorem 5.6 below; also Remark 5.2.1 below for the reason why our algorithm requires the assumption $m \geq 1$). For the "finite-step solvable" notations such as "F_m/F", see the discussion entitled "Fields and Field Extensions" in §0. Moreover, by replacing the use of the "2-step loss" (purely mono-anabelian) reconstruction algorithm for non-archimedean decomposition subgroups in [ST] with the "1-step loss" refinement which the authors learned of through an announcement by Akio Tamagawa at a conference (cf. Remark 5.5.1 below), we may easily modify our algorithm to "3-step loss". Since the definitive treatment of the finite-step solvable variants will be given in [TT2], we content ourselves, in the present section, with an outline of the proof; the point is that the techniques of the present paper, combined with the (purely mono-anabelian) reconstruction algorithm for non-archimedean decomposition subgroups in [ST] (resp. a refinement of this algorithm, announced by Akio Tamagawa), already yield the "4-step loss" (resp. "3-step loss") algorithm as they stand. The authors plan to obtain, in [TT2], "i-step loss" finite-step solvable purely mono-anabelian reconstruction algorithms for number fields with $i \leq 2$, and also to include the case $m = 0$, by building on, and substantially extending, the techniques of the present paper.

Here, before turning to our argument, we briefly compare our "4-step loss" result (cf. Theorem 5.6 below) with the previous works [ST], [Mao], and [MS]. First, our result may be regarded as a partial refinement of the bi-anabelian result of [ST], which asserts, roughly speaking, that the isomorphism class of

the field extension F_m/F is determined, in a functorial bi-anabelian fashion, by the abstract topological group $\mathrm{Gal}(F_{m+3}/F)$ (resp. $\mathrm{Gal}(F_{m+4}/F)$), where $m \in \mathbb{Z}_{\geq 2}$ (resp. $m \in \{0, 1\}$) and F is a number field (cf. [ST], Theorem 2). While, unfortunately, our result is less sharp than that of [ST] in that it does not cover the case $m = 0$ and requires a larger "step loss" (i.e., "4" as opposed to "3") when $m \geq 2$, it has the evident advantage of being (purely) mono-anabelian. On the other hand, we should emphasize that our result relies on the reconstruction of the non-archimedean decomposition subgroups — an intermediate result of [ST] which is itself purely mono-anabelian.

Next, in the recent work [MS], Mao and Saïdi established a mono-anabelian reconstruction algorithm for "$\mathrm{Gal}(F_m/F) \curvearrowright F_m$" from "$\mathrm{Gal}(F_{m+9}/F)$", where $m \geq 3$, i.e., a "9-step loss" algorithm (cf. [MS], Theorem 1). However, as is emphasized in [MS], Introduction, their algorithm depends on the statement of the bi-anabelian result of [ST] in an essential way; in particular, their algorithm is not "purely" mono-anabelian in the sense of the present paper (cf. the proof of Theorem 4.6), and it does not yield an alternative proof of the bi-anabelian result of [ST]. Thus, our algorithm improves on the algorithm of [MS] both in the "step loss" (i.e., "4" as opposed to "9") and in the "purity", i.e., its independence from the bi-anabelian result; in particular, our algorithm yields, as a formal consequence, a bi-anabelian result of the same step loss (cf. the proof of Corollary 4.7).

Finally, in [Mao], Mao established a purely mono-anabelian reconstruction algorithm for an abelian number field F from "$\mathrm{Gal}(F_6/F)$" (cf. [Mao], Theorem 1.2; also [MS], Theorem 2, which treats, in a similar fashion, the case where F is an imaginary quadratic field or $\mathbb{Q}$). Our algorithm may be regarded as a refinement of these results in the sense that it applies to arbitrary number fields and only requires the input "$\mathrm{Gal}(F_5/F)$" (i.e., the case where $m = 1$, in which F itself is reconstructed at an intermediate stage of the reconstruction of F_1; we note that the case $m = 0$ is not available here — cf. the limitation $m \geq 1$ in our result).

Now we begin our argument. Let us first explain the typical mechanism by which a "loss" arises in the finite-step solvable setting. As may be observed in the proof of Theorem 4.5, (5), as well as in several lemmas preceding it (cf. Lemma 2.5, (2); Lemma 3.6, (7); Lemma 3.7, (2)), a typical argument of the present paper proceeds in two steps: first, we establish an algorithm $\mathbf{A}$ whose input data is a profinite group G of GSC-type and whose output data $\mathbf{A}\big(\mathrm{Gal}(E/F)\big)$ is an object associated to the base field F; then, by applying $\mathbf{A}$ to the various open subgroups $H \subset G$ and taking a suitable limit of the outputs "$\mathbf{A}(H)$", we obtain an algorithm $\widetilde{\mathbf{A}}$ whose output data $\widetilde{\mathbf{A}}\big(\mathrm{Gal}(E/F)\big)$ is an object associated to E itself. Here, the second step depends on the fact that every open subgroup of a profinite group of GSC-type is again of GSC-type; it is precisely this hereditary property that makes the expression "$\mathbf{A}(H)$" meaningful. In the finite-step solvable setting, the analogous hereditary property fails in general. To discuss this failure precisely, we introduce the following terminology.

Definition 5.1. Let G be a profinite group and $m \in \mathbb{Z}_{\geq 0}$. Then G is referred to as *of MLF^m-type* (resp. *of NF^m-type*) if there exists a mixed characteristic local field (resp. a number field) F such that G is isomorphic to $\mathrm{Gal}(F_m/F)$ as a profinite group.

Let F be a number field, $m \in \mathbb{Z}_{\geq 0}$, and E/F a finite subextension of F_m/F (so that the meaning of the symbol "E" differs substantially from that in the preceding sections). Then the open subgroup $\mathrm{Gal}(F_m/E)$ of $G = \mathrm{Gal}(F_m/F)$ is not necessarily of NF^m-type — or, more precisely, is not necessarily "of NF^m-type in a manner compatible with the assumption on G" (cf. Remark 3.4.2). The same remark applies to profinite groups of MLF^m-type. Thus, in the finite-step solvable setting, one cannot simply apply an algorithm of the type "**A**" to an arbitrary open subgroup $H \subset G$; instead, one must restrict one's attention to a suitable class of open subgroups for which (a suitable variant of) **A** still makes sense. It is precisely this restriction that gives rise to the "loss".

Let us illustrate this phenomenon by means of a basic example, i.e., the abelianization. Suppose that $m \in \mathbb{Z}_{\geq 1}$ and $E \subset F_{m-1}$. Then, since a/the maximal abelian extension E_1 of E is included in $F_m = (F_{m-1})_1$, the natural continuous surjective homomorphism $G_E^{\mathrm{ab}} \twoheadrightarrow \mathrm{Gal}(F_m/E)^{\mathrm{ab}}$ is an isomorphism, where we write G_E for the absolute Galois group of E. That is to say, if G is of NF^m-type (or of MLF^m-type), and an open subgroup $H \subset G$ includes $G[m-1]$, then H^{ab} is the "genuine abelianization" that we seek; on the other hand, for an open subgroup $H \subset G$ that does not include $G[m-1]$, no such interpretation of H^{ab} is available. Consequently, a naive imitation of the algorithm in the solvably closed case only allows one to reconstruct, from "$\mathrm{Gal}(F_m/F)$", at most "$\mathrm{Gal}(F_m/F) \curvearrowright F_{m-1}$", i.e., the open subgroups that one may employ are those corresponding to the subfields of F_{m-1}. This is one typical source of a "1-step loss".

In the remainder of the present section, we review (a slightly modified version — cf. (SC-6) below — of) the algorithm of Theorem 4.6 and examine what kind of "loss" arises in its finite-step solvable variant. As a result, we will obtain a "4-step loss" finite-step solvable version of Theorem 4.6 (cf. Theorem 5.6 below).

Let $\widetilde{F}$ be a solvably closed Galois extension of a number field F (for which we wrote "E" in the preceding sections). The goal is to reconstruct the action on the solvably closed field $\mathrm{Gal}(\widetilde{F}/F) \curvearrowright \widetilde{F}$ from the abstract profinite group structure of $\mathrm{Gal}(\widetilde{F}/F)$. Here, we also keep in mind that the ultimate goal of the finite-step solvable variant would be to reconstruct the action $\mathrm{Gal}(F_m/F) \curvearrowright F_m$ from the abstract profinite group structure of $\mathrm{Gal}(F_m/F)$ alone (where $m \in \mathbb{Z}_{\geq 2}$).

(SC-1) Reconstruct, from $G = \mathrm{Gal}(\widetilde{F}/F)$, the set of non-archimedean decomposition subgroups $\mathbb{V} \stackrel{\mathrm{def}}{=} \mathbb{V}(G) \subset 2^G$ (cf. Theorem 3.4). In light of this reconstruction, we will treat G as a "profinite group equipped with the additional structure constituted by a certain set $\mathbb{V}$ of closed subgroups" in the following discussion. Here, we note that this additional structure is naturally inherited by the open subgroups of G (cf. Remark 3.2.2; Lemma 3.3).

(SC-2) For each $D \in \mathbb{V}$, reconstruct $\mathcal{O}^\times(D) \subset k^\times(D) \subset D^{\mathrm{ab}}$ (cf. Lemma 2.4). (In particular, in the course of this procedure, we also obtain the subset $\mathbb{V}^{d=1} \subset \mathbb{V}$ constituted by the D's such that $d(D) = 1$ — cf. Lemma 2.3.) Moreover, we apply similar algorithms to the open subgroups of D. In particular, we also reconstruct $D \curvearrowright \overline{k}^\times(D)$ (cf. Lemma 2.5, (2)), the local divisible cyclotome $D \curvearrowright \mu^{\mathrm{loc}}(D)$ as a D-submodule of $\overline{k}^\times(D)$

(cf. Remark 2.5.2), and, by taking the projective limit, the local profinite cyclotome $D \curvearrowright \Lambda^{\mathrm{loc}}(D)$ (cf. Lemma 2.5, (3)).

(SC-3) For each $D \in \mathbb{V}^{d=1}$ (cf. (SC-2)), reconstruct the field $k_{\mathrm{fld}}(D) \cong \mathbb{Q}_{p(D)}$ (cf. Lemma 2.6; Lemma 2.7).

(SC-4) Apply Kummer theory to the short exact sequence $1 \to \mu_n(D) \to \overline{k}^{\times}(D) \stackrel{(-)^n}{\to} \overline{k}^{\times}(D) \to 1$ and take the projective limit, where n varies over $\mathbb{Z}_{\geq 1}$, to obtain $\mathrm{Kum}_D \colon k^{\times}(D) \hookrightarrow H^1\big(D, \Lambda^{\mathrm{loc}}(D)\big)$ (cf. Lemma 2.5, (4)). Moreover, we perform the same procedure for each open subgroup U of D.

(SC-5) For each open (normal) subgroup H of G, reconstruct $\mu^{\mathrm{gl}}_{\mathrm{base}}(H) \subset \mathbb{I}^{\mathrm{fin}}(H)$ (cf. Lemma 3.6), by making use of the inclusions $\mathcal{O}^{\times}(D \cap H) \subset k^{\times}(D \cap H) \subset (D \cap H)^{\mathrm{ab}}$ obtained in (SC-2). Here, we note that, in the construction of $\mathbb{I}^{\mathrm{fin}}(H)$, one makes use of the fact that, for each $D \in \mathbb{V}$, $D \cap H$ is normally terminal in H (cf. Remark 3.3.1; Lemma 3.6, (1)). In particular, we construct the global divisible cyclotome $G \curvearrowright \mu^{\mathrm{gl}}(G)$, the global profinite cyclotome $G \curvearrowright \Lambda^{\mathrm{gl}}(G)$, and, for each $D \in \mathbb{V}$, the local-global cyclotomic synchronization isomorphism $\Lambda^{\mathrm{gl}}(G) \stackrel{\cong}{\longrightarrow} \Lambda^{\mathrm{loc}}(D)$ (cf. Lemma 3.7).

(SC-6) Fix an open (normal) subgroup H of G. By using the action $H \curvearrowright \Lambda^{\mathrm{gl}}(G)$, the actions $(D \cap H) \curvearrowright \Lambda^{\mathrm{loc}}(D)$ for $D \in \mathbb{V}$, and the local-global cyclotomic synchronization isomorphisms $\Lambda^{\mathrm{gl}}(G) \stackrel{\cong}{\longrightarrow} \Lambda^{\mathrm{loc}}(D)$ for $D \in \mathbb{V}$, construct a natural homomorphism

$$H^1\big(H, \Lambda^{\mathrm{gl}}(G)\big) \longrightarrow \prod_{D \in \mathbb{V}} H^1\big(D \cap H, \Lambda^{\mathrm{loc}}(D)\big)$$

(cf. Lemma 3.8; note, however, that, with the finite-step solvable variants in mind, here we always take $\Lambda^{\mathrm{gl}}(G)$ — i.e., as opposed to "$\Lambda^{\mathrm{gl}}(H)$" for each open subgroup $H \subset G$ — as the global cyclotome and $\Lambda^{\mathrm{loc}}(D)$ as the local cyclotome).

(SC-7) We continue to fix H as in (SC-6). By using $\mathrm{Kum}_{D \cap H}$ (i.e., an analogue of Kum_D for "U" $= D \cap H$) obtained in (SC-4) for $D \in \mathbb{V}$, construct a natural injective homomorphism $\mathbb{I}^{\mathrm{fin}}(H) \hookrightarrow \prod_{D \in \mathbb{V}} H^1\big(D \cap H, \Lambda^{\mathrm{loc}}(D)\big)$. Pulling back this homomorphism via the displayed homomorphism in (SC-6), we obtain the Kummer container $\mathcal{H}^{\times}(H) \subset H^1\big(H, \Lambda^{\mathrm{gl}}(G)\big)$ (cf. Lemma 3.8).

(SC-8) Apply Lemma 4.4 to the natural map

$$\mathcal{H}_{\times}(H) \hookrightarrow \mathcal{R}(H) \stackrel{\mathrm{def}}{=} \prod_{\substack{D \in \mathbb{V} \\ d(D)=1 \\ D \subset H}} k_{\mathrm{fld}}(D)$$

determined by (SC-3) and (SC-7) to reconstruct the number field $\mathbf{F}(H) \subset \mathcal{R}(H)$ (cf. Theorem 4.5, (2)). By letting G act on the various "H"s by conjugation and taking the inductive limit, where H ranges over the open normal subgroups of G, we reconstruct $G \curvearrowright \widetilde{\mathbf{F}}(G)$ (cf. Theorem 4.5, (3),

(5)). This is the desired solvably closed field equipped with the action of G.

What happens if one attempts to carry out the same argument in the finite-step solvable setting? The obstructions (i.e., the sources of the "loss") are of two kinds: the one arising in (SC-1), and those arising in (SC-2) and thereafter — the latter including the issue of "genuine abelianization" discussed above. We now turn to the finite-step solvable variant in detail; for each $i \in \{1, \ldots, 8\}$, the discussion entitled (FSS-i) below is intended to be the finite-step solvable counterpart of (SC-i). Here, we note in advance that the assumption $m \in \mathbb{Z}_{\geq 1}$ (i.e., as opposed to $m \in \mathbb{Z}_{\geq 0}$) will play a crucial role in (FSS-4), i.e., in local Kummer theory; this is closely related to the following elementary observation, which will be of fundamental importance throughout the discussion in the finite-step solvable setting.

Lemma 5.2. *For every field F, a/the maximal abelian extension F_1 of F contains every root of unity. In particular, if F is a perfect field, then, for every $m \in \mathbb{Z}_{\geq 1}$ and $n \in \mathbb{Z}_{\geq 1}$, it holds that $F_m^{\times} \subset (F_{m+1}^{\times})^n$, where F_{m+1} (resp. F_m) denotes a maximal $(m+1)$-step solvable extension of F (resp. the maximal m-step solvable extension of F inside F_{m+1}).*

Proof. The proof is elementary and left to the reader. □

Remark 5.2.1. A similar assertion to the latter half of Lemma 5.2 is false for $m = 0$; for instance, for $F = \mathbb{Q}$, we have $2^{1/3} \notin \mathbb{Q}_1$ (i.e., $F^{\times} \not\subset (F_1^{\times})^3$). This failure is precisely the reason why the assumption $m \geq 1$ is required in (FSS-4) below.

(FSS-1)

First, the result corresponding to (SC-1) is Theorem 5.5 below.

Lemma 5.3. *Let F be a number field, $m \in \mathbb{Z}_{\geq 0}$, F_m a maximal m-step solvable extension of F, and $\widetilde{\mathfrak{p}} \in \mathcal{V}_{F_m}$ a non-archimedean prime lying over $\mathfrak{p} \in \mathcal{V}_F$. Then the localization $(F_m)_{\widetilde{\mathfrak{p}}}$ is a maximal m-step solvable extension of $F_{\mathfrak{p}}$. In particular, every non-archimedean decomposition subgroup of $\mathrm{Gal}(F_m/F)$ is of MLF^m-type (cf. also Remark 3.4.2).*

Proof. This follows essentially formally from the Grunwald–Wang theorem (cf. [NSW], Theorem (9.2.8)). □

Remark 5.3.1. Suppose that we are in the situation of Lemma 5.3. Then it follows from Lemma 5.3 that, for every $n \in \mathbb{Z}_{\geq 0}$ such that $n \leq m$, we have $D_{\widetilde{\mathfrak{p}}}[n] = D_{\widetilde{\mathfrak{p}}} \cap \mathrm{Gal}(F_m/F)[n]$ (cf. Remark 3.2.2 for the notation "$D_{\widetilde{\mathfrak{p}}}$").

Lemma 5.4. *Let F be a number field, $n \in \mathbb{Z}_{\geq 2}$, F_n a maximal n-step solvable extension of F, F_{n-1} the maximal $(n-1)$-step solvable extension of F inside F_n, and E/F a finite subextension of F_{n-1}/F. Write $\mathbb{V}(F_n/E) \subset 2^{\mathrm{Gal}(F_n/E)}$ for the set of non-archimedean decomposition subgroups of $\mathrm{Gal}(F_n/E)$. Then the natural map $\mathcal{V}_{F_n} \longrightarrow \mathbb{V}(F_n/E)$ (cf. Remark 3.2.2) is an isomorphism of $\mathrm{Gal}(F_n/E)$-sets, where $\mathrm{Gal}(F_n/E) \curvearrowright \mathbb{V}(F_n/E)$ is defined as the conjugation action. In particular, the natural map $\mathcal{V}_E \longrightarrow \mathrm{Gal}(F_n/E)\backslash\mathbb{V}(F_n/E)$ is a bijection, and every non-archimedean decomposition subgroup of $\mathrm{Gal}(F_n/E)$ is normally terminal in $\mathrm{Gal}(F_n/E)$ (cf. Remark 3.3.1).*

Proof. Lemma 5.4 follows immediately from Lemma 5.2 and [ST], Proposition 1.5 (cf. also [ST], Corollary 1.6). □

Theorem 5.5 (Saïdi–Tamagawa's "2-step loss" reconstruction of non-archimedean decomposition subgroups)**.** *Let $n \in \mathbb{Z}_{\geq 2}$ and G a profinite group of NF^{n+2}-type (cf. Definition 5.1). Then one may construct, solely from the profinite group structure of G, a set $\mathbb{V}(G \twoheadrightarrow G/G[n]) \subset 2^{G/G[n]}$ of closed subgroups of the maximal n-step solvable quotient $G/G[n]$ of G (cf. the discussion entitled "Topological Groups" in §0) which satisfies the following property: for every number field F, every maximal $(n+2)$-step solvable extension F_{n+2} of F, and every isomorphism $G \xrightarrow{\cong} \mathrm{Gal}(F_{n+2}/F)$ of profinite groups, the induced isomorphism $G/G[n] \xrightarrow{\cong} \mathrm{Gal}(F_n/F)$ — where F_n denotes the maximal n-step solvable extension of F inside F_{n+2} — maps $\mathbb{V}(G \twoheadrightarrow G/G[n])$ bijectively onto the set of non-archimedean decomposition subgroups of* $\mathrm{Gal}(F_n/F)$.

Proof. See [ST], Theorem 1.25 (cf. also [ST], Introduction, Theorem 3). □

Remark 5.5.1. The authors learned, through an announcement by Akio Tamagawa at a conference, that a "1-step loss" refinement of Theorem 5.5 (i.e., a similar reconstruction for profinite groups of NF^{n+1}-type) has been obtained in his more recent joint work with Mohamed Saïdi (which, to the best of the authors' knowledge, has not yet been made public at the time of writing the present paper).

Summarizing the discussion so far: by [ST], Theorem 1.25 (resp. a refinement of this result, announced by Akio Tamagawa — cf. Remark 5.5.1), starting from "$\mathrm{Gal}(F_{m+4}/F)$" (resp. "$\mathrm{Gal}(F_{m+3}/F)$") as the input data, we may reconstruct "$\mathrm{Gal}(F_{m+2}/F)$ equipped with the set $\mathbb{V}$ of non-archimedean decomposition subgroups".

(FSS-2)

In the following discussion, we will observe that a straightforward application of the arguments in (SC-2) and later yields an algorithm which reconstructs $G/G[m] = \mathrm{Gal}(F_m/F) \curvearrowright F_m$, taking "the profinite group $G = \mathrm{Gal}(F_{m+2}/F)$ equipped with the set $\mathbb{V} \subset 2^G$ of non-archimedean decomposition subgroups" as its input data.

First, in light of Lemma 5.3, together with the fact that $m + 2 \geq 2$, the application of the algorithms to each $D \in \mathbb{V}$ in (SC-2), as well as the reconstruction of $\mathbb{V}^{d=1} \subset \mathbb{V}$, carries over without change (cf. Remark 2.4.1). Here, we note that, since a/the maximal tamely ramified extension of a mixed characteristic local field is 2-step solvable (cf. Lemma 2.2), $m + 2 \geq 2$ implies that $D/P(D)$ is the "genuine tame quotient"; it is precisely for this reason that the reconstruction algorithm for $k^{\times}(D)$ makes sense.

In the application of the algorithms to the open subgroups U of D, however, some care is required. Indeed, by the issue of "genuine abelianization" discussed above, one can expect the application of similar algorithms only for the U's such that $D[m+1] \subset U$; that is to say, without this assumption, the possibility that U^{ab} is an inappropriate object is not excluded. It is here that the local "1-step

loss" arises; in other words, it is already suggested at this point that, when we let the global open subgroups $H \subset G$ vary later, we may only consider the H's such that $G[m+1] \subset H$ (cf. Remark 5.3.1, applied to "F_m" $= F_{m+2}$).

On the other hand, no further loss arises here. The point is that, since the formation of the inertia subgroups and the wild inertia subgroups is compatible with passing to open subgroups, $U/P(U)$ is automatically the "genuine tame quotient", and thus the reconstruction algorithms for $k^\times(U) \subset U^{\mathrm{ab}}$, etc., make sense. As a consequence, for $D \in \mathbb{V}$ (or, more generally, D of MLF^{m+2}-type), we may reconstruct $D \curvearrowright k^\times_{m+1}(D) \overset{\mathrm{def}}{=} \varinjlim_{D[m+1] \subset U \subset D} k^\times(U)$, where U ranges over the open normal subgroups of D that include $D[m+1]$ (cf. Lemma 2.5, (2)). (As the notation suggests, if $D = \mathrm{Gal}(K_{m+2}/K)$, where K is a mixed characteristic local field, then $k^\times_{m+1}(D)$ is canonically isomorphic, as a D-module, to $K^\times_{m+1}$, where K_{m+1} denotes the maximal $(m+1)$-step solvable extension of K inside K_{m+2}.) Moreover, since cyclotomic extensions are abelian (cf. Lemma 5.2), we may also reconstruct the D-modules $\mu^{\mathrm{loc}}(D)$ and $\Lambda^{\mathrm{loc}}(D)$ from $k^\times_{m+1}(D)$.

(FSS-3)

As for (SC-3), Lemma 2.6 and Lemma 2.7 may be applied, in an entirely similar fashion, in the finite-step solvable setting.

(FSS-4)

Some care is required for (SC-4) — we will apply the assumption $m \in \mathbb{Z}_{\geq 1}$ (as opposed to $m \in \mathbb{Z}_{\geq 0}$) here. We have obtained $k^\times(U) \subset U^{\mathrm{ab}}$ and $H^1\big(U, \Lambda^{\mathrm{loc}}(D)\big)$ with "1-step loss". However, the reconstruction of the appropriate relationship $k^\times(U) \hookrightarrow H^1\big(U, \Lambda^{\mathrm{loc}}(D)\big)$ between them produces a further loss, which results in "2-step loss" in total. Let us explain the details.

The problem arises from the fact that, for $n \geq 2$, the n-th power map $k^\times_{m+1}(D) \longrightarrow k^\times_{m+1}(D)$ is not surjective. That is to say, the counterpart, in the present situation, of the short exact sequence $1 \to \mu_n(D) \to \overline{k}^\times(D) \overset{(-)^n}{\to} \overline{k}^\times(D) \to 1$ in (SC-4) is $1 \to \mu_n(D) \to k^\times_{m+1}(D) \overset{(-)^n}{\to} \big(k^\times_{m+1}(D)\big)^n \to 1$ (i.e., rather than $1 \to \mu_n(D) \to k^\times_{m+1}(D) \overset{(-)^n}{\to} k^\times_{m+1}(D) \to 1$). The relationship obtained by taking the cohomology exact sequence of this short exact sequence with respect to the action of $U/D[m+1]$ is an isomorphism between $\varprojlim_{n \geq 1}\Big(k^\times(U) \cap \big(k^\times_{m+1}(D)\big)^n\Big)/\big(k^\times(U)\big)^n$ and $H^1\big(U/D[m+1], \Lambda^{\mathrm{loc}}(D)\big)$ (cf. Lemma 1.3, (2)); here, we note that, if we take the cohomology exact sequence with respect to the action of U, then $H^1\big(U, k^\times_{m+1}(D)\big)$ may not vanish (since we cannot apply "Hilbert 90"), which implies that the connecting homomorphism is not necessarily surjective. The situation may be summarized in the following diagram:

$$
\begin{array}{ccc}
k^{\times,\mathrm{div}}(U) & \xrightarrow{\text{reconstructed}} & H^1\big(U/D[m+1], \Lambda^{\mathrm{loc}}(D)\big) \\
\big\downarrow & & \big\downarrow \\
k^\times(U) & \underset{???}{\overset{\text{(desired)}}{\dashrightarrow}} & H^1\big(U, \Lambda^{\mathrm{loc}}(D)\big),
\end{array}
$$

where we write $k^{\times,\mathrm{div}}(U)$ for the subgroup of $k^{\times}(U)$ constituted by the elements that are divisible in $k^{\times}_{m+1}(D)$. That is to say, what we obtain is not the homomorphism that we really want, but only a portion of it. If we restrict ourselves to the case where $D[m] \subset U$ (i.e., the case where $k^{\times}(U) \subset$ "$k^{\times}_{m}(D)$"), however, the assumption $m \geq 1$ implies that every n-th root (where $n \in \mathbb{Z}_{\geq 1}$) of every element of $k^{\times}(U)$ is contained in $k^{\times}_{m+1}(D)$, i.e., $k^{\times,\mathrm{div}}(U) = k^{\times}(U)$ (cf. Lemma 5.2; also Remark 5.2.1); hence a natural homomorphism $\mathrm{Kum}_{U \subset D} \colon k^{\times}(U) \hookrightarrow H^1\big(U, \Lambda^{\mathrm{loc}}(D)\big)$ may be constructed.

(FSS-5)

In view of the "loss" that arose in (FSS-2), we need to restrict ourselves to the open subgroups $H \subset G$ such that $G[m+1] \subset H$ in order to carry out arguments similar to (SC-5) (cf. Remark 5.3.1). Here, we note that, since $m + 1 \geq 1$, this restriction causes no problem from the viewpoint of the reconstruction of the global cyclotome (cf. Lemma 5.2). Indeed, for such an H, the analogue of Lemma 3.6, (1) — which is, in essence, the assertion that the various "$D \cap H$"s are normally terminal in H — follows from Lemma 5.4, applied to the subextension of "F_{m+2}/F" corresponding to H (where we note that the assumption $G[m+1] \subset H$ guarantees that this subextension is included in "F_{m+1}/F"). The rest of the argument is similar; in particular, we construct $\mathbb{I}^{\mathrm{fin}}(H \subset G, \mathbb{V})$, as well as the global cyclotome $\Lambda^{\mathrm{gl}}(G, \mathbb{V})$ and the local-global cyclotomic synchronization isomorphisms $\Lambda^{\mathrm{gl}}(G, \mathbb{V}) \xrightarrow{\cong} \Lambda^{\mathrm{loc}}(D)$.

(FSS-6)

In an entirely similar fashion to (SC-6), for each open subgroup $H \subset G$, one constructs a natural homomorphism

$$H^1\big(H, \Lambda^{\mathrm{gl}}(G, \mathbb{V})\big) \longrightarrow \prod_{D \in \mathbb{V}} H^1\big(D \cap H, \Lambda^{\mathrm{loc}}(D)\big).$$

(FSS-7)

If an open subgroup $H \subset G$ satisfies $G[m] \subset H$, then, by (FSS-4), we obtain $\mathbb{I}^{\mathrm{fin}}(H \subset G, \mathbb{V}) \hookrightarrow \prod_{D \in \mathbb{V}} H^1\big(D \cap H, \Lambda^{\mathrm{loc}}(D)\big)$ (cf. also Remark 5.3.1). Thus, together with (FSS-6), $\mathcal{H}^{\times}(H \subset G, \mathbb{V}) \subset H^1\big(H, \Lambda^{\mathrm{gl}}(G, \mathbb{V})\big)$ is constructed in an entirely similar fashion to (SC-7) (i.e., under the assumption that $G[m] \subset H$).

(FSS-8)

If an open normal subgroup $H \subset G$ satisfies $G[m] \subset H$, then the $\mathcal{H}^{\times}(H \subset G, \mathbb{V})$ obtained in (FSS-7) determines a natural map $\mathcal{H}_{\times}(H \subset G, \mathbb{V}) \hookrightarrow \mathcal{R}(H \subset G, \mathbb{V}) \stackrel{\mathrm{def}}{=} \prod_{\substack{D \in \mathbb{V} \\ d(D)=1 \\ D \subset H}} k_{\mathrm{fld}}(D)$ (cf. (FSS-3)), and $\mathbf{F}(H \subset G, \mathbb{V}) \subset \mathcal{R}(H \subset G, \mathbb{V})$ may be reconstructed in an entirely similar fashion to (SC-8). By letting H vary — i.e., by forming $\mathbf{F}_m(G, \mathbb{V}) \stackrel{\mathrm{def}}{=} \varinjlim_H \mathbf{F}(H \subset G, \mathbb{V})$, where H ranges over the open normal subgroups of G that include $G[m]$ — we obtain the "2-step loss" reconstruction algorithm for $G/G[m] \curvearrowright \mathbf{F}_m(G, \mathbb{V})$ from $(G, \mathbb{V})$, as desired.

Summary of the "4-step loss" finite-step solvable algorithm

Let us summarize the above discussion. First, in (FSS-1), starting from "$\mathrm{Gal}(F_{m+4}/F)$", we reconstruct, by the result of [ST], "$\mathrm{Gal}(F_{m+2}/F)$ equipped with the set of non-archimedean decomposition subgroups". (If one uses the result mentioned in Remark 5.5.1, one may instead start from "$\mathrm{Gal}(F_{m+3}/F)$".) Next, in (FSS-2) through (FSS-8), we apply the arguments in the solvably closed case of the present paper — straightforwardly, but carefully — to reconstruct "$\mathrm{Gal}(F_m/F) \curvearrowright F_m$" under the assumption that $m \in \mathbb{Z}_{\geq 1}$. Putting these together, we obtain the desired "4-step loss" (or, by the result mentioned in Remark 5.5.1, "3-step loss") reconstruction algorithm. We record this as a theorem.

Theorem 5.6 (Summary of the "4-step loss" finite-step solvable purely mono-anabelian reconstruction algorithm)**.** *Let $m \in \mathbb{Z}_{\geq 1}$. Then we have established a purely mono-anabelian reconstruction algorithm for the action $\mathrm{Gal}(F_m/F) \curvearrowright F_m$, whose input data is the abstract profinite group $G \stackrel{\mathrm{def}}{=} \mathrm{Gal}(F_{m+4}/F)$ and whose output data is a field $\mathbf{F}_m(G', \mathbb{V})$ — where we write $G' \stackrel{\mathrm{def}}{=} G/G[m+2]$ for the maximal $(m+2)$-step solvable quotient of G, and $\mathbb{V} \stackrel{\mathrm{def}}{=} \mathbb{V}(G \twoheadrightarrow G') \subset 2^{G'}$ for the set of closed subgroups of G' reconstructed from G in Theorem 5.5 (cf. (FSS-1)) — equipped with an action of the maximal m-step solvable quotient $G'/G'[m]$ of G', which is canonically isomorphic to the field F_m together with the action of $\mathrm{Gal}(F_m/F)$ $\left(\cong G'/G'[m]\right)$ on it, where F is a number field, F_{m+4} is a maximal $(m+4)$-step solvable extension of F, and F_m is the maximal m-step solvable extension of F inside F_{m+4}.*

Remark 5.6.1. A similar remark to Remark 4.6.1 applies to Theorem 5.6 as well.

Remark 5.6.2. By replacing the use of Theorem 5.5 in (FSS-1) with its "1-step loss" refinement mentioned in Remark 5.5.1, we obtain, in an entirely similar fashion, a "3-step loss" refinement of Theorem 5.6, i.e., a purely mono-anabelian reconstruction algorithm for the action $\mathrm{Gal}(F_m/F) \curvearrowright F_m$ whose input data is the abstract profinite group $\mathrm{Gal}(F_{m+3}/F)$, where $m \geq 1$ and F is a number field.

Declaration on the Use of AI Tools

In the preparation of the present paper, the first author made use of AI assistants (Claude Code, Anthropic) to improve the English exposition and to detect typographical and other minor errors and notational inconsistencies in earlier drafts. Every suggestion produced by the AI assistants was adopted only after verification by the authors. All mathematical ideas and arguments in the present paper are due to the authors, who bear sole responsibility for its correctness.

Acknowledgements

The authors would like to express their sincere gratitude to Professor Yuichiro Hoshi for numerous helpful discussions and warm encouragement.

This research was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University, as well as by the Center for Research in Next Generation Geometry. This work is part of the "Arithmetic and Homotopic Galois Theory" project, supported by the CNRS France-Japan AHGT International Research Network between the RIMS Kyoto University, the LPP of Lille University, and the DMA of ENS PSL.

The second author would like to thank the Research Institute for Mathematical Sciences, Kyoto University, for giving him an opportunity to lecture on some introductory aspects of anabelian geometry (including an introduction to the Neukirch–Uchida theorem) to the general public in the summer of 2024. Although the mono-anabelian aspect of anabelian geometry was not discussed in that introductory lecture, the preparation for it stimulated him to start thinking about the mono-anabelian reconstruction problem of number fields.

The fundamental ideas in the present series of papers were obtained in early 2025, and the authors informed several researchers working in and around anabelian geometry about the project. The authors regret the considerable delay in making the present paper publicly available — during which the results were strengthened, and the exposition substantially revised — and any effect it may have had on related work.

References

[Letter] A. Grothendieck, *Letter to G. Faltings* (June 1983), in L. Schneps and P. Lochak (eds.), *Geometric Galois Actions 1. Around Grothendieck's Esquisse d'un Programme*, *London Math. Soc. Lect. Note Ser.* **242**, Cambridge Univ. Press (1997).

[congtop] F. Grunewald and D. Segal, On congruence topologies in number fields, *J. Reine Angew. Math.* **311/312** (1979), 389–396.

[MnNF] Y. Hoshi, Mono-anabelian reconstruction of number fields, *RIMS Kôkyûroku Bessatsu* **B76** (2019), 1–77.

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

[IntroMLF] Y. Hoshi, Introduction to the mono-anabelian geometry of mixed characteristic local fields, *Publ. Math. Besançon Algèbre Théorie Nr.* **2021** (2022), 5–44.

[MnNF2] Y. Hoshi, Mono-anabelian reconstruction of solvably closed Galois extensions of number fields, *J. Math. Sci. Univ. Tokyo* **29** (2022), no. 3, 257–283.

[KS] I. Karshon and M. Shusterman, Pro-ℓ-by-cyclotomic and tamely ramified variants of the Neukirch-Uchida theorem, preprint, arXiv:2601.01251 (2026).

[Mao] Y. Mao, The 6-step solvable mono-anabelian reconstruction of abelian number fields, preprint, arXiv:2508.17775 (2025).

[MS] Y. Mao and M. Saïdi, The m-step solvable mono-anabelian geometry of number fields, preprint, arXiv:2511.05192 (2025).

[MST] A. Minamide, K. Sawada, and S. Tsujimura, Families preserving isomorphisms via techniques in anabelian geometry: with an application to a generalized Neukirch-Uchida theorem, RIMS Preprint **1998** (July 2026).

[MT] A. Minamide and S. Tsujimura, Anabelian geometry for Henselian discrete valuation fields with quasi-finite residues, RIMS Preprint **1973** (June 2023), to appear in *Amer. J. Math.*

[GeoAnbd] S. Mochizuki, The geometry of anabelioids, *Publ. Res. Inst. Math. Sci.* **40** (2004), 819–881.

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

[AbsTopI] S. Mochizuki, Topics in absolute anabelian geometry I: Generalities, *J. Math. Sci. Univ. Tokyo* **19** (2012), no. 2, 139–242.

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

[Neukirch] J. Neukirch, *Algebraic Number Theory*, *Grundlehren der Mathematischen Wissenschaften*, **322**, Springer-Verlag, Berlin, 1999.

[NSW] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields*, second edition, *Grundlehren der Mathematischen Wissenschaften*, **323**, Springer-Verlag, Berlin, 2008.

[NS] N. Nikolov and D. Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds, *Ann. of Math. (2)* **165** (2007), no. 1, 171–238.

[Ozaki] M. Ozaki, A number field analogue of the Grothendieck conjecture for curves over finite fields, preprint, arXiv:2507.20159 (2025).

[ST] M. Saïdi and A. Tamagawa, The m-step solvable anabelian geometry of number fields, *J. Reine Angew. Math.* **789** (2022), 153–186.

[Sawada] K. Sawada, Algorithmic approach to Uchida's theorem for one-dimensional function fields over finite fields, Inter-universal Teichmüller theory summit 2016, *RIMS Kôkyûroku Bessatsu* **B84** (2021), 1–21.

[Shimizu1] R. Shimizu, Isomorphisms of Galois groups of number fields with restricted ramification, *Math. Nachr.* **296** (2023), no. 7, 3026–3033.

[Shimizu2] R. Shimizu, The pro-$\mathcal{C}$ anabelian geometry of number fields, preprint, arXiv:2303.02931 (2023).

[Stacks] The Stacks Project Authors, *The Stacks Project*, `https://stacks.math.columbia.edu`.

[TT2] R. Tachihara and S. Tsujimura, Purely Mono-anabelian Reconstruction of Number Fields II: Finite-step Solvable Case, in preparation.

[TsjmGS] S. Tsujimura, A Grunewald–Segal principle for semi-abelian varieties, RIMS Preprint **2003** (September 2026).

[Uchida1] K. Uchida, Isomorphisms of Galois groups, *J. Math. Soc. Japan* **28** (1976), 617–620.

[Uchida2] K. Uchida, Isomorphisms of Galois groups of algebraic function fields, *Ann. of Math. (2)* **106** (1977), 589–598.

[Uchida3] K. Uchida, Isomorphisms of Galois groups of solvably closed Galois extensions, *Tôhoku Math. J. (2)* **31** (1979), no. 3, 359–362.

Reiya Tachihara
Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan
`rtach@kurims.kyoto-u.ac.jp`

Shota Tsujimura
Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan
`stsuji@kurims.kyoto-u.ac.jp`