RIMS-1931

On the Outer Automorphism Groups of the Absolute Galois Groups of Mixed-characteristic Local Fields

By

Yuichiro HOSHI and Yu NISHIO

November 2020

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

ON THE OUTER AUTOMORPHISM GROUPS OF THE ABSOLUTE GALOIS GROUPS OF MIXED-CHARACTERISTIC LOCAL FIELDS

YUICHIRO HOSHI AND YU NISHIO

NOVEMBER 2020

Abstract. In the present paper, we study the outer automorphism groups of the absolute Galois groups of mixed-characteristic local fields from the point of view of anabelian geometry. Let us recall that it is well-known that the natural homomorphism from the automorphism group of a mixed-characteristic local field to the outer automorphism group of the absolute Galois group of the given mixed-characteristic local field is injective. One main result of the present paper is that if the mixed-characteristic local field satisfies certain conditions, then the set of conjugates of the image of this injective homomorphism in the outer automorphism group is infinite, which thus implies that the image of this injective homomorphism is not normal in the outer automorphism group. In particular, one may conclude that it is impossible to establish a functorial group-theoretic reconstruction, from the absolute Galois group, of the "field-theoretic" subgroup, i.e., the image of this injective homomorphism, of the outer automorphism group.

Introduction

Let p be a prime number, k a finite extension of $\mathbb{Q}_p$, and $\overline{k}$ an algebraic closure of k. Write $G_k \stackrel{\text{def}}{=} \mathrm{Gal}(\overline{k}/k)$ for the absolute Galois group of k determined by the algebraic closure $\overline{k}$ and $\mathrm{Out}(G_k)$ for the group of outer automorphisms of the group G_k [or, alternatively, the group of outer continuous automorphisms of the profinite group G_k — cf., e.g., [3], Proposition 1.2, (i), (ii)]. In the present paper, we study the outer automorphism group $\mathrm{Out}(G_k)$ from the point of view of anabelian geometry.

Write $\mathrm{Aut}(k)$ for the group of automorphisms of the field k. Thus, we have a natural homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ of groups. Let us first recall that it is well-known [cf., e.g., [4], Proposition 2.1] that this homomorphism is injective. In the present paper, let us regard $\mathrm{Aut}(k)$ as a [necessarily finite] subgroup of $\mathrm{Out}(G_k)$ by means of this injective homomorphism:

$$\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k).$$

Here, we note that it is well-known [cf., e.g., the discussion given at the final portion of [6], Chapter VII, §5] that [although a similar equality always holds for a finite extension of $\mathbb{Q}$ by the Neukirch-Uchida theorem — cf., e.g., [6], Corollary 12.2.2], in general, the equality

2010 *Mathematics Subject Classification.* 11S20.

Key words and phrases. mixed-characteristic local field, absolute Galois group, anabelian geometry, mono-anabelian geometry, group of MLF-type.

$\mathrm{Aut}(k) = \mathrm{Out}(G_k)$ does not hold. In particular, one may conclude that, roughly speaking, in general, a finite extension of $\mathbb{Q}_p$ should be considered to be "not anabelian" [cf. also [6], Chapter XII, §2, Closing remark]. Therefore, one main interest from the point of view of anabelian geometry is in the investigate of the "difference" between $\mathrm{Aut}(k)$ and $\mathrm{Out}(G_k)$. Some results concerning the "characterization" of the subgroup $\mathrm{Aut}(k)$ of $\mathrm{Out}(G_k)$ may be found in [5], §3, and [1], §3. Moreover, some results concerning this "difference" may be found in [2], §7, and [2], §8.

Write $(\mathbb{Q}_p)_+ \subseteq k_+$ for the underlying additive modules of the fields $\mathbb{Q}_p \subseteq k$, respectively. Next, let us recall that, by applying a functorial group-theoretic reconstruction algorithm established in the study of the mono-anabelian geometry of mixed-characteristic local fields [cf., e.g., [4], Definition 3.10, (vi), and [4], Proposition 3.11, (iv)], one obtains an action of the group $\mathrm{Out}(G_k)$ on the module k_+ whose restriction to the above subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ coincides with the natural action of $\mathrm{Aut}(k)$ on k_+.

One main technical result of the present paper is as follows [cf. Theorem 2.7]:

Theorem A. *Suppose that the following three conditions are satisfied:*

(1) *The prime number p is odd.*
(2) *The finite extension $k/\mathbb{Q}_p$ is of even degree.*
(3) *The finite extension $k/\mathbb{Q}_p$ is Galois, and, moreover, the Galois group $\mathrm{Gal}(k/\mathbb{Q}_p)$ is abelian.*

Then there exists an outer automorphism α of G_k such that, for each nonzero integer n, if one writes α_+^n for the action of α^n on k_+, then $\alpha_+^n((\mathbb{Q}_p)_+) \neq (\mathbb{Q}_p)_+$.

Next, let us recall that the first author of the present paper proved that if p is odd, and k coincides with the [necessarily finite Galois] extension of $\mathbb{Q}_p$ obtained by adjoining a primitive p-th root of unity and a p-th root of $p \in \mathbb{Q}_p$, then the above subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ is not normal [cf. [2], Theorem G, (iii)]. In the present paper, we give a proof of an assertion in this direction by applying Theorem A. More precisely, in the present paper, we prove the following result [cf. Theorem 3.4]:

Theorem B. *Suppose that the three conditions in the statement of Theorem A are satisfied. Then the set of $\mathrm{Out}(G_k)$-conjugates of the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ is infinite.*

A formal consequence of Theorem B is as follows [cf. Corollary 3.5]:

Theorem C. *Suppose that the three conditions in the statement of Theorem A are satisfied. Then the following hold:*

(i) *The subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ is not normal.*
(ii) *There exist infinitely many distinct [necessarily finite] subgroups of $\mathrm{Out}(G_k)$ isomorphic to $\mathrm{Aut}(k)$.*

The issue of whether or not a functorial group-theoretic reconstruction, from the group G_k, of the "field-theoretic" subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ of the outer automorphism group $\mathrm{Out}(G_k)$ can be established is interesting from the point of view of the anabelian geometry of mixed-characteristic local fields. Now let us recall that if the condition (3) in the statement of Theorem A is satisfied, then, roughly speaking, one may reconstruct group-theoretically, from the group G_k, the set of $\mathrm{Out}(G_k)$-conjugates of the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ [cf. [2], Theorem F, (i), and [2], Theorem 6.12, (ii)]. On the other hand, Theorem C, (i), implies that if the three conditions in the statement of Theorem A are satisfied, then, roughly speaking, it is impossible to establish a functorial group-theoretic reconstruction of the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ itself [i.e., as opposed to the set of $\mathrm{Out}(G_k)$-conjugates of the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$].

0. Notational conventions

Sets. If G is a group, and T is a set equipped with an action of G, then we shall write $T^G \subseteq T$ for the subset of G-invariants of T.

Topological groups. If G is a topological group, then 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] and $G^{\mathrm{ab/tor}}$ for the quotient of G^{ab} by the closure of the subgroup of G^{ab} of torsion elements.

Rings. If R is a ring, then we shall write R_+ for the underlying additive module of R and $R^\times$ for the multiplicative module of units of R.

Fields. We shall refer to a field isomorphic to a finite extension of $\mathbb{Q}_p$, for some prime number p, as an *MLF*. Here, "MLF" is to be understood as an abbreviation for "mixed-characteristic local field".

1. Existence of an automorphism with a certain unipotency condition of a group of MLF-type

In the present §1, we prove that a certain group of MLF-type admits an automorphism that satisfies a certain unipotency condition [cf. Theorem 1.5 below]. In the present §1, let G be a [profinite — cf. [3], Proposition 1.2, (i), (ii)] group of MLF-type [cf. [3], Definition 1.1]. Thus, by applying the various functorial group-theoretic reconstruction algorithms of [4], §3 [cf. [4], Definition 3.5, (i), (ii), (iii); [4], Definition 3.10, (ii), (iv), (vi)], to the group G of MLF-type, we obtain

- a prime number $p(G)$,
- positive integers $d(G)$ and $f(G)$,
- a normal closed subgroup $P(G) \subseteq G$ of G, and
- topological modules $\mathcal{O}^{\prec}(G) \subseteq k^\times(G)$ and $k_+(G)$

[cf. also [4], Summary 3.15]. In the present §1, suppose, moreover, that $p(G)$ is odd, and that $d(G) > 1$.

Proposition 1.1 (Jannsen-Wingberg)**.** *The profinite group G is topologically generated by $d(G)+3$ elements σ, τ, $x_0, \ldots, x_{d(G)}$ subject to the following conditions and relations.*

(1) *The normal closed subgroup $P(G)$ of G is topologically normally generated by $x_0, \ldots, x_{d(G)}$.*
(2) *The elements σ, τ satisfy the relation $\sigma\tau\sigma^{-1} = \tau^{p(G)^{f(G)}}$.*

(3) *The topological generators under consideration satisfy the relation*

$$\sigma x_0 \sigma^{-1} = (x_0^{h^{p(G)-1}} \tau x_0^{h^{p(G)-2}} \tau \cdots x_0^{h} \tau)^{\frac{\pi g}{p(G)-1}} x_1^{p(G)^s} \delta,$$

where s, g, h are some positive integers such that

$$g(h^{p(G)-1} + h^{p(G)-2} + \cdots + h) \neq p(G) - 1,$$

π is the unique element of $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ whose image in $\mathbb{Z}_p$ is given by 1 if $p = p(G)$ (resp. by 0 if $p \neq p(G)$), and δ is an element of the commutator subgroup of G.

Proof. This assertion follows from [6], Theorem 7.5.14, together with [4], Proposition 3.6. [Note that it follows from the discussion preceding [6], Theorem 7.5.14, that one may take the "g" and "h" of [6], Theorem 7.5.14, to be positive integers greater than $p(G)$.] $\square$

In the remainder of the present §1, let us fix topological generators σ, τ, $x_0, \ldots, x_{d(G)}$ of G as in Proposition 1.1. Write $S \stackrel{\text{def}}{=} \{0, 1, \ldots, d(G)\}$. Moreover, for each $i \in S$, write

- $y_i \in k_+(G)$ for the image of x_i in $k_+(G)$ and
- $z_i \in \mathcal{O}^{\prec}(G)^{\text{ab/tor}}$ for the image of x_i in $\mathcal{O}^{\prec}(G)^{\text{ab/tor}}$

[cf. the condition (1) of Proposition 1.1; [4], Lemma 1.5, (ii); [4], Proposition 3.6; [4], Definition 3.10, (i), (ii), (vi)].

Lemma 1.2. *The topological module $k_+(G)$ has a natural structure of $\mathbb{Q}_{p(G)}$-vector space of dimension $d(G)$.*

Proof. It follows immediately from the definition of $k_+(G)$ [cf. [4], Definition 3.10, (vi)] that $k_+(G)$ has a natural structure of $\mathbb{Q}_{p(G)}$-vector space. Moreover, it follows from [4], Proposition 3.6, and [4], Proposition 3.11, (iv), that this $\mathbb{Q}_{p(G)}$-vector space $k_+(G)$ is of dimension $d(G)$. $\square$

Lemma 1.3. *The $d(G)$ elements $y_1, \ldots, y_{d(G)}$ form a basis of the $\mathbb{Q}_{p(G)}$-vector space $k_+(G)$ [cf. Lemma 1.2].*

Proof. Since $\{x_i\}_{i \in S}$ topologically normally generates $P(G)$ [cf. the condition (1) of Proposition 1.1], $\{z_i\}_{i \in S}$ topologically generates $\mathcal{O}^{\prec}(G)^{\text{ab/tor}}$ ($\subseteq G^{\text{ab/tor}}$) [cf. [4], Definition 3.10, (i), (ii)]. Moreover, since $\mathcal{O}^{\prec}(G)^{\text{ab/tor}} \otimes_{\mathbb{Z}_{p(G)}} (\mathbb{Z}_{p(G)}/p(G)^n \mathbb{Z}_{p(G)})$ is a finite $p(G)$-group for every positive integer n [cf. [4], Proposition 3.11, (i)], $\{z_i\}_{i \in S}$ is also a generator of $\mathcal{O}^{\prec}(G)^{\text{ab/tor}}$ even if we regard $\mathcal{O}^{\prec}(G)^{\text{ab/tor}}$ as a $\mathbb{Z}_{p(G)}$-module. Next, let us observe that it follows from the relation (2) of Proposition 1.1 that the image of τ in $G^{\text{ab/tor}}$ is trivial. Thus, it follows from the relation (3) of Proposition 1.1 that the relation $1 = {z_0}^H {z_1}^{p(G)^s}$ in $\mathcal{O}^{\prec}(G)^{\text{ab/tor}}$ holds for some nonzero [cf. the second display of Proposition 1.1, (3)] integer H. Therefore, if we write $T \stackrel{\text{def}}{=} S \setminus \{0\}$, then $\{z_i \otimes 1\}_{i \in T}$ is a generator of $\mathbb{Q}_{p(G)}$-vector space $\mathcal{O}^{\prec}(G)^{\text{ab/tor}} \otimes_{\mathbb{Z}_{p(G)}} \mathbb{Q}_{p(G)}$. Here, let us observe that we have a natural topological isomorphism $k_+(G) \xrightarrow{\sim} \mathcal{O}^{\prec}(G)^{\text{ab/tor}} \otimes_{\mathbb{Z}_{p(G)}} \mathbb{Q}_{p(G)}$, by definition, that maps $y_i \in k_+(G)$ to $z_i \otimes 1 \in \mathcal{O}^{\prec}(G)^{\text{ab/tor}} \otimes_{\mathbb{Z}_{p(G)}}$

$\mathbb{Q}_{p(G)}$ for each $i \in S$. This isomorphism is also an isomorphism of $\mathbb{Q}_{p(G)}$-vector spaces by construction. Moreover, since $k_+(G) \simeq \mathcal{O}^{\prec}(G)^{\mathrm{ab/tor}} \otimes_{\mathbb{Z}_{p(G)}} \mathbb{Q}_{p(G)}$ is a $\mathbb{Q}_{p(G)}$-vector space of dimension $d(G)$ [cf. Lemma 1.2], $\{z_i \otimes 1\}_{i \in T}$ is a basis of the $\mathbb{Q}_{p(G)}$-vector space $\mathcal{O}^{\prec}(G)^{\mathrm{ab/tor}} \otimes_{\mathbb{Z}_{p(G)}} \mathbb{Q}_{p(G)}$. Therefore, it follows from the condition imposed on the isomorphism $k_+(G) \xrightarrow{\sim} \mathcal{O}^{\prec}(G)^{\mathrm{ab/tor}} \otimes_{\mathbb{Z}_{p(G)}} \mathbb{Q}_{p(G)}$ that $\{y_i\}_{i \in T}$ is a basis of the $\mathbb{Q}_{p(G)}$-vector space $k_+(G)$. ☐

Lemma 1.4. *The element $y_{d(G)-1}$ is a nonzero element of $k_+(G)$.*

Proof. This assertion follows from Lemma 1.3 [cf. also our assumption that $d(G) > 1$]. ☐

Theorem 1.5. *Let G be a group of MLF-type. Suppose that $p(G)$ is odd, and that $d(G) > 1$. Then there exists an automorphism α of G such that, for each nonzero integer n, if one writes α_+^n for the automorphism of the $\mathbb{Q}_{p(G)}$-vector space $k_+(G)$ induced by α^n, then $\alpha_+^n \neq \mathrm{id}$, and, moreover, the equality $(\alpha_+^n - \mathrm{id})^2 = 0$ in the ring of endomorphisms of $k_+(G)$ holds.*

Proof. Let α be an automorphism of G as in the discussion preceding [6], Theorem 7.5.15, i.e., defined by the equalities $\alpha(\sigma) = \sigma$, $\alpha(\tau) = \tau$, $\alpha(x_{d(G)}) = x_{d(G)}x_{d(G)-1}$, and $\alpha(x_i) = x_i$ for $i \in S \backslash \{d(G)\}$. First, we prove that $\alpha_+^n \neq \mathrm{id}$ for each nonzero integer n. If $\alpha_+^n = \mathrm{id}$, then $y_{d(G)} = \alpha_+^n(y_{d(G)}) = y_{d(G)} + ny_{d(G)-1}$, which thus implies that $y_{d(G)-1} = 0$ in $k_+(G)$. However, this contradicts Lemma 1.4. Thus, we conclude that $\alpha_+^n \neq \mathrm{id}$. Next, let us observe that, for each nonzero integer n, it follows from the easily verified equality $(\alpha_+^n - \mathrm{id})^2(y_i) = 0$ for every $i \in S$ and Lemma 1.3 that the equality $(\alpha_+^n - \mathrm{id})^2 = 0$ in $\mathrm{End}(k_+(G))$ holds, as desired. This completes the proof of Theorem 1.5. ☐

Corollary 1.6. *Let G be a group of MLF-type. Suppose that $p(G)$ is odd, and that $d(G) > 1$. Then the following hold:*

(i) *The image of the natural homomorphism from the outer automorphism group of G to the automorphism group of $k_+(G)$ is infinite.*
(ii) *The image of the natural homomorphism from the outer automorphism group of G to the automorphism group of G^{ab} is infinite.*
(iii) *The image of the natural homomorphism from the outer automorphism group of G to the automorphism group of $k^\times(G)$ is infinite.*
(iv) *The outer automorphism group of G is infinite.*

Proof. Assertion (i) follows from Theorem 1.5. Assertion (ii) follows from assertion (i), together with the definition of $k_+(G)$ [cf. [4], Definition 3.10, (vi)]. Assertion (iii) follows from assertion (ii) and the [easily verified] density of $k^\times(G)$ in G^{ab} [cf. [4], Definition 3.10, (iv)]. Assertion (iv) follows from assertion (i). ☐

Remark 1.7. Let us recall that it follows immediately from [2], Corollary 5.5, that each of the three images discussed in Corollary 1.6, (i), (ii), (iii), in the case where $d(G)$ is equal to 1 is trivial.

2. Existence of a special automorphism of the absolute Galois group of an absolutely abelian MLF of even degree

In the present §2, we prove that the absolute Galois group of a certain MLF admits an automorphism that has an interesting property [cf. Theorem 2.7 below]. In the present §2, let k be an MLF and $\overline{k}$ an algebraic closure of k. We shall write

- $G_k \stackrel{\text{def}}{=} \mathrm{Gal}(\overline{k}/k)$ for the absolute Galois group of k determined by the algebraic closure $\overline{k}$,
- $\mathcal{O}_k$ for the ring of integers of k,
- p_k for the residue characteristic of k,
- $k^{(d=1)} \subseteq k$ for the [uniquely determined] minimal MLF contained in k,
- $d_k \stackrel{\text{def}}{=} [k : k^{(d=1)}]$ for the degree of the finite extension $k/k^{(d=1)}$,
- $\mathrm{Nm}_{k/k^{(d=1)}} \colon k^{\times} \to k^{(d=1)\times}$ for the norm map with respect to the finite extension $k/k^{(d=1)}$,
- $\mathrm{Tr}_{k/k^{(d=1)}} \colon k_+ \to k_+^{(d=1)}$ for the trace map with respect to the finite extension $k/k^{(d=1)}$,
- $\log_k \colon \mathcal{O}_k^{\times} \to k_+$ for the p_k-adic logarithm, and
- $\mathcal{I}_k$ for the log-shell of k.

Write, moreover, $\mathrm{Aut}(G_k)$, $\mathrm{Aut}(k_+)$, and $\mathrm{Aut}(k^{\times})$ for the groups of automorphisms of the group G_k, the module k_+, and the module $k^{\times}$, respectively. Thus, it follows from [4], Proposition 3.11, (i), (iv), that we have homomorphisms

$$\mathrm{Aut}(G_k) \longrightarrow \mathrm{Aut}(k_+),\ \mathrm{Aut}(G_k) \longrightarrow \mathrm{Aut}(k^{\times}).$$

Definition 2.1.

(i) We shall say that $\alpha \in \mathrm{Aut}(k_+)$ is $(\mathbb{Q}_{p_k})_+$-*characteristic* if $\alpha(k_+^{(d=1)}) = k_+^{(d=1)}$.

(ii) We shall say that $\alpha \in \mathrm{Aut}(k_+)$ is $(\mathbb{Q}_{p_k})_+$-*preserving* if α is $(\mathbb{Q}_{p_k})_+$-characteristic, and $\alpha|_{k_+^{(d=1)}}$ is the identity automorphism of $k_+^{(d=1)}$.

(iii) We shall say that $\alpha \in \mathrm{Aut}(k_+)$ is *group-theoretic* if α is contained in the image of the first homomorphism $\mathrm{Aut}(G_k) \to \mathrm{Aut}(k_+)$ of the above display.

(iv) We shall say that $\alpha \in \mathrm{Aut}(k^{\times})$ is *group-theoretic* if α is contained in the image of the second homomorphism $\mathrm{Aut}(G_k) \to \mathrm{Aut}(k^{\times})$ of the above display.

(v) We shall say that $\alpha \in \mathrm{Aut}(G_k)$ is $(\mathbb{Q}_{p_k})_+$-*characteristic* if the group-theoretic automorphism of k_+ induced by α is $(\mathbb{Q}_{p_k})_+$-characteristic.

(vi) We shall say that $\alpha \in \mathrm{Aut}(G_k)$ is $(\mathbb{Q}_{p_k})_+$-*preserving* if the group-theoretic automorphism of k_+ induced by α is $(\mathbb{Q}_{p_k})_+$-preserving.

Lemma 2.2. *The diagram of modules*

$$\begin{tikzcd}
\mathcal{O}_k^{\times} \arrow[r, "\log_k"] \arrow[d, "\mathrm{Nm}_{k/k^{(d=1)}}"'] & k_+ \arrow[d, "\mathrm{Tr}_{k/k^{(d=1)}}"] \\
\mathcal{O}_{k^{(d=1)}}^{\times} \arrow[r, "\log_{k^{(d=1)}}"'] & k_+^{(d=1)}
\end{tikzcd}$$

commutes.

Proof. Since $k_+^{(d=1)}$ is torsion-free, by replacing k by the Galois closure of k over $k^{(d=1)}$, we may assume without loss of generality that k is absolutely Galois, i.e., that k is Galois over $k^{(d=1)}$ [cf. [2], Definition 4.2, (i)]. Then Lemma 2.2 follows immediately from the well-known fact that the p_k-adic logarithm is compatible with the respective natural actions of $\mathrm{Gal}(k/k^{(d=1)})$ on $\mathcal{O}_k^\times$ and on k_+. $\square$

Lemma 2.3. *Let α be an automorphism of G_k. Write $\alpha_+ \in \mathrm{Aut}(k_+)$ and $\alpha^\times \in \mathrm{Aut}(k^\times)$ for the respective group-theoretic automorphisms induced by α. Then the following hold:*

(i) *The automorphism $\alpha^\times$ fits into a commutative diagram of modules*

$$\begin{tikzcd} k^\times \arrow[r, "\mathrm{Nm}_{k/k^{(d=1)}}"] \arrow[d, "\alpha^\times"'] & k^{(d=1)\times} \arrow[d, equal] \\ k^\times \arrow[r, "\mathrm{Nm}_{k/k^{(d=1)}}"'] & k^{(d=1)\times}. \end{tikzcd}$$

(ii) *The automorphism α_+ fits into a commutative diagram of modules*

$$\begin{tikzcd} k_+ \arrow[r, "\mathrm{Tr}_{k/k^{(d=1)}}"] \arrow[d, "\alpha_+"'] & k_+^{(d=1)} \arrow[d, equal] \\ k_+ \arrow[r, "\mathrm{Tr}_{k/k^{(d=1)}}"'] & k_+^{(d=1)}. \end{tikzcd}$$

In particular, the automorphism α_+ restricts to an automorphism of $\mathrm{Ker}(\mathrm{Tr}_{k/k^{(d=1)}})$, i.e., the equality $\alpha_+(\mathrm{Ker}(\mathrm{Tr}_{k/k^{(d=1)}})) = \mathrm{Ker}(\mathrm{Tr}_{k/k^{(d=1)}})$ holds.

Proof. Assertion (i) follows immediately from [2], Proposition 4.9, (i). Next, we verify assertion (ii). Let us first recall that it follows from the construction of α_+ [cf. [4], Definition 3.10, (vi)] and the definition of log-shell that the diagram

$$\begin{tikzcd} \mathcal{O}_k^\times \arrow[r, "\log_k"] \arrow[d, "\alpha^\times"'] & \mathcal{I}_k \arrow[d, "\alpha_+"] \\ \mathcal{O}_k^\times \arrow[r, "\log_k"'] & \mathcal{I}_k \end{tikzcd}$$

commutes. Therefore, by Lemma 2.2 and assertion (i), we get the equality

$$\mathrm{Tr}_{k/k^{(d=1)}}(\alpha_+(\log_k(x))) = \mathrm{Tr}_{k/k^{(d=1)}}(\log_k(x)) \quad (x \in \mathcal{O}_k^\times).$$

Now let us observe that this equality implies that α_+ is compatible with the trace map with respect to the finite extension $k/k^{(d=1)}$ on $p_k\mathcal{I}_k$. Since, for an arbitrary $x \in k_+$, there exists an integer n such that $p_k^n x \in p_k\mathcal{I}_k$ [cf. [4], Lemma 1.2, (vi)], we conclude that α_+ is compatible with the trace map on k_+. $\square$

Lemma 2.4. *Suppose that p_k is odd, and that $d_k = 2$. Then there exists an automorphism $\alpha \in \mathrm{Aut}(G_k)$ such that, for every nonzero integer n, α^n is not $(\mathbb{Q}_{p_k})_+$-characteristic.*

Proof. It follows from Theorem 1.5 and [4], Proposition 3.6, that there exists a group-theoretic automorphism $\alpha_+ \in \mathrm{Aut}(k_+)$ such that, for every nonzero integer n, α_+^n is not the identity automorphism but satisfies the equality $(\alpha_+^n - \mathrm{id})^2 = 0$ in $\mathrm{End}(k_+)$. Here, let us observe that we can write $k = k^{(d=1)}(\sqrt{a})$ for some $a \in k^{(d=1)}$. Assume that α_+^n is $(\mathbb{Q}_{p_k})_+$-characteristic for some nonzero integer n. Thus, $\alpha_+^n(1) = b$ for some $b \in k^{(d=1)}$. Moreover, it follows from the final portion of Lemma 2.3, (ii), that $\alpha_+^n(\sqrt{a}) = c\sqrt{a}$ for some $c \in k^{(d=1)}$. Thus, since α_+ is an automorphism of $\mathbb{Q}_{p_k}$-vector space, it follows that, for arbitrary x, $y \in k^{(d=1)}$, the equalities

$$0 = (\alpha_+^n - \mathrm{id})^2(x + y\sqrt{a}) = x(b-1)^2 + y(c-1)^2\sqrt{a}$$

hold. Thus, we have $(b, c) = (1, 1)$. In particular, α_+^n is the identity automorphism. However, this is a contradiction. $\square$

Remark 2.5. One may conclude from Lemma 2.4 that it is impossible to establish a functorial group-theoretic reconstruction algorithm for constructing, from an arbitrary group G of MLF-type, a submodule of the module $k_+(G)$ which "corresponds" to the submodule $k_+^{(d=1)} \subseteq k_+$ of k_+. Put another way, one may conclude from Lemma 2.4 that the submodule $k_+^{(d=1)} \subseteq k_+$ of k_+ should be considered to be "not group-theoretic".

Lemma 2.6. *Suppose that d_k is even, and that k is absolutely abelian, i.e., that k is Galois over $k^{(d=1)}$, and, moreover, the Galois group $\mathrm{Gal}(k/k^{(d=1)})$ is abelian [cf. [2], Definition 4.2, (ii)]. Then the following hold:*

(i) *There exists a quadratic extension k' of $k^{(d=1)}$ contained in k such that G_k is a characteristic subgroup of $G_{k'} \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{k}/k')$. In particular, we have a natural homomorphism $\phi\colon \mathrm{Aut}(G_{k'}) \to \mathrm{Aut}(G_k)$.*

(ii) *Let k' be a quadratic exension of $k^{(d=1)}$ as in assertion (i) and α' an automorphism of $G_{k'}$ which is not $(\mathbb{Q}_{p_k})_+$-characteristic. Then $\phi(\alpha') \in \mathrm{Aut}(G_k)$ [cf. (i)] is not $(\mathbb{Q}_{p_k})_+$-characteristic.*

Proof. First, we verify assertion (i). Since the MLF k is absolutely abelian, and d_k is even, $\mathrm{Gal}(k/k^{(d=1)})$ is a finite abelian group of even order. Thus, it follows immediately from elementary group theory and Galois theory that there exists a quadratic extension k' of $k^{(d=1)}$ contained in k. Next, we verify that G_k is a characteristic subgroup of $G_{k'}$. Let β be an automorphism of $G_{k'}$. Since k is absolutely abelian, k is Galois-specifiable [cf. [2], Definition 6.1, and [2], Theorem F, (i)]. Thus, it follows from Galois theory that there exists $\tau \in \mathrm{Gal}(\overline{k}/k^{(d=1)})$ such that $\beta(G_k) = \tau G_k \tau^{-1}$. Moreover, since k is absolutely abelian, G_k is a normal subgroup of $\mathrm{Gal}(\overline{k}/k^{(d=1)})$. In particular, we get $\beta(G_k) = \tau G_k \tau^{-1} = G_k$. This completes the proof of assertion (i).

Next, we verify assertion (ii). Let us first observe that it follows immediately from the various definitions involved that the diagram

$$\begin{tikzcd} k_+^{(d=1)} \arrow[r, hook] \arrow[d, "\phi(\alpha')_+|_{k_+^{(d=1)}}"'] & k'_+ \arrow[r, hook] \arrow[d, "\alpha'_+"'] & k_+ \arrow[d, "\phi(\alpha')_+"] \\ \alpha'_+(k_+^{(d=1)}) \arrow[r, hook] & k'_+ \arrow[r, hook] & k_+ \end{tikzcd}$$

commutes, where the horizontal arrows are the natural inclusions, and we write α'_+ (resp. $\phi(\alpha')_+$) for the group-theoretic automorphism induced by $\alpha' \in \mathrm{Aut}(G_{k'})$ (resp. $\phi(\alpha') \in \mathrm{Aut}(G_k)$). Since α'_+ is not $(\mathbb{Q}_{p_k})_+$-characteristic, $\alpha'_+(k_+^{(d=1)}) \neq k_+^{(d=1)}$. Thus, we conclude from the above diagram that $\phi(\alpha')_+$, hence also $\phi(\alpha')$, is not $(\mathbb{Q}_{p_k})_+$-characteristic. This completes the proof of assertion (ii). □

Theorem 2.7. *Let k be an absolutely abelian MLF such that p_k is odd, and d_k is even. Then there exists an automorphism $\alpha \in \mathrm{Aut}(G_k)$ such that, for each nonzero integer n, α^n is not $(\mathbb{Q}_{p_k})_+$-characteristic.*

Proof. This assertion follows from Lemma 2.4 and Lemma 2.6, (i), (ii). □

3. The outer automorphism group of the absolute Galois group of an absolutely abelian MLF of even degree

In the present §3, we discuss the outer automorphism group of the absolute Galois group of a certain MLF. In the present §3, we maintain the notational conventions introduced at the beginning of the preceding §2. Write, moreover, $\mathrm{Aut}(k)$ for the group of automorphisms of the field k and $\mathrm{Out}(G_k)$ for the group of outer automorphisms of the group G_k. Thus, we have a natural injective [cf. [4], Proposition 2.1] homomorphism $\mathrm{Aut}(k) \hookrightarrow \mathrm{Out}(G_k)$ of groups. In the present §3, let us regard $\mathrm{Aut}(k)$ as a subgroup of $\mathrm{Out}(G_k)$:

$$\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k).$$

Lemma 3.1. *Let K be a field and L a finite Galois extension of K of extension degree invertible in L. Let α be an automorphism of the module L_+ which is compatible, relative to some automorphism of $\mathrm{Gal}(L/K)$ [which is not necessarily the identity automorphism], with the natural action of $\mathrm{Gal}(L/K)$ on L_+ and fits into the commutative diagram of modules*

$$\begin{tikzcd} L_+ \arrow[r, "\mathrm{Tr}_{L/K}"] \arrow[d, "\alpha"'] & K_+ \arrow[d, equal] \\ L_+ \arrow[r, "\mathrm{Tr}_{L/K}"'] & K_+, \end{tikzcd}$$

where we write $\mathrm{Tr}_{L/K}$ for the trace map with respect to the finite extension L/K. Then α restricts to the identity automorphism of the submodule $K_+ \subseteq L_+$.

Proof. Write $\beta \overset{\text{def}}{=} \alpha - \mathrm{id} \in \mathrm{End}(L_+)$. Then it is immediate that the sequence

$$0 \longrightarrow \mathrm{Ker}(\beta) \longrightarrow L_+ \longrightarrow \mathrm{Im}(\beta) \longrightarrow 0,$$

hence also [cf. our assumption that α is compatible, relative to some automorphism of $\mathrm{Gal}(L/K)$, with the natural action of $\mathrm{Gal}(L/K)$] the sequence

$$0 \longrightarrow \mathrm{Ker}(\beta)^{\mathrm{Gal}(L/K)} \longrightarrow K_+ \longrightarrow \mathrm{Im}(\beta)^{\mathrm{Gal}(L/K)},$$

is exact. Now observe that it follows from the commutative diagram in the statement of Lemma 3.1 and the definition of β that the image of $\mathrm{Im}(\beta)$ by $\mathrm{Tr}_{L/K}$ is zero. Thus, since $\mathrm{Im}(\beta)^{\mathrm{Gal}(L/K)}$ is contained in K_+, and the degree of the finite extension L/K is invertible in L, we conclude that $\mathrm{Im}(\beta)^{\mathrm{Gal}(L/K)} = \{0\}$. In particular, it follows from the above exact sequence that $\mathrm{Ker}(\beta)^{\mathrm{Gal}(L/K)} = K_+$, which implies that $\alpha(x) = x$ for each $x \in K_+$. This completes the proof of Lemma 3.1. $\square$

Theorem 3.2. *Let k be an MLF and α an automorphism of G_k. Suppose that $d_k = 2$. Write $\alpha_+ \in \mathrm{Aut}(k_+)$ for the group-theoretic automorphism induced by α. Then the following are equivalent:*

(1) *The automorphism α is $(\mathbb{Q}_{p_k})_+$-preserving.*
(2) *The automorphism α is $(\mathbb{Q}_{p_k})_+$-characteristic.*
(3) *The automorphism α_+ is compatible with the natural action of $\mathrm{Gal}(k/k^{(d=1)})$ on k_+.*

Proof. First, (1)$\Longrightarrow$(2) is immediate. Next, we verify (2)$\Longrightarrow$(3). Suppose that (2) is satisfied. Let us first observe that one may write $k = k^{(d=1)}(\sqrt{a})$ for some $a \in k^{(d=1)}$. Since (2) is satisfied, $\alpha_+(1) = b$ for some $b \in k^{(d=1)}$. Moreover, it follows from the final portion of Lemma 2.3, (ii), that $\alpha_+(\sqrt{a}) = c\sqrt{a}$ for some $c \in k^{(d=1)}$. Thus, since α_+ is an automorphism of $\mathbb{Q}_{p_k}$-vector space, it follows that, for arbitrary x, $y \in k^{(d=1)}$, the equalities

$$\sigma(\alpha_+(x + y\sqrt{a})) = \sigma(bx + cy\sqrt{a}) = \alpha_+(\sigma(x + y\sqrt{a})) \quad (\sigma \in \mathrm{Gal}(k/k^{(d=1)}))$$

hold. This completes the proof of (2)$\Longrightarrow$(3). Finally, (3)$\Longrightarrow$(1) follows immediately from Lemma 2.3, (ii), and Lemma 3.1. $\square$

Lemma 3.3. *Let α be an automorphism of G_k. Suppose that k is absolutely Galois. If the image of α in $\mathrm{Out}(G_k)$ is contained in $\mathrm{N}_{\mathrm{Out}(G_k)}(\mathrm{Aut}(k))$, then α is $(\mathbb{Q}_{p_k})_+$-preserving.*

Proof. Suppose that the image of α in $\mathrm{Out}(G_k)$ is contained in $\mathrm{N}_{\mathrm{Out}(G_k)}(\mathrm{Aut}(k))$. Thus, α_+ is compatible, relative to some automorphism of $\mathrm{Gal}(k/k^{(d=1)})$ [which is not necessarily the identity automorphism], with the natural action of $\mathrm{Gal}(k/k^{(d=1)}) = \mathrm{Aut}(k)$ on k_+. In particular, it follows from Lemma 2.3, (ii), and Lemma 3.1 that α is $(\mathbb{Q}_{p_k})_+$-preserving. $\square$

Theorem 3.4. *Let k be an absolutely abelian MLF such that p_k is odd, and d_k is even. Then the set of $\mathrm{Out}(G_k)$-conjugates of the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ is infinite.*

Proof. This assertion follows from Theorem 2.7 and Lemma 3.3. $\square$

Corollary 3.5. *Let k be an absolutely abelian MLF such that p_k is odd, and d_k is even. Then the following hold:*

(i) *The subgroup* $\mathrm{Aut}(k)$ *of* $\mathrm{Out}(G_k)$ *is not normal.*

(ii) *There exist infinitely many distinct [necesarily finite] subgroups of* $\mathrm{Out}(G_k)$ *isomorphic to* $\mathrm{Aut}(k)$*.*

Proof. These assertions follow immediately from Theorem 3.4. □

Remark 3.6. Let us recall from [2], Theorem G, (iii), that if p_k is odd, and k is obtained by adjoining, to $k^{(d=1)}$, a primitive p_k-th root of unity and a p_k-th root of p_k, then the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ is not normal.

Remark 3.7. The issue of whether or not a functorial group-theoretic reconstruction, from the group G_k, of the "field-theoretic" subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ of the outer automorphism group $\mathrm{Out}(G_k)$ can be established is interesting from the point of view of the anabelian geometry of mixed-characteristic local fields. Now let us recall that if the MLF k is absolutely abelian, then, roughly speaking, one may reconstruct group-theoretically, from the group G_k, the set of $\mathrm{Out}(G_k)$-conjugates of the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ [cf. [2], Theorem F, (i), and [2], Theorem 6.12, (ii)]. On the other hand, Corollary 3.5, (i), implies that if p_k is odd, d_k is even, and k is absolutely abelian, then, roughly speaking, it is impossible to establish a functorial group-theoretic reconstruction of the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$ itself [i.e., as opposed to the set of $\mathrm{Out}(G_k)$-conjugates of the subgroup $\mathrm{Aut}(k) \subseteq \mathrm{Out}(G_k)$].

Corollary 3.8. *Let k be an MLF such that p_k is odd, and $d_k = 2$. Then the group-theoretic automorphism of k_+ induced by an automorphism of G_k which lifts an element of the center of* $\mathrm{Out}(G_k)$ *is the identity automorphism of k_+.*

Proof. Let γ be an element of the center of $\mathrm{Out}(G_k)$. Write $\gamma_+ \in \mathrm{Aut}(k_+)$ for the group-theoretic automorphism of k_+ induced by an automorphism of G_k which lifts γ. [Note that one verifies easily that γ_+ does not depend on the choice of such a lifting.] Then it follows from Lemma 3.3 that γ_+ is $(\mathbb{Q}_{p_k})_+$-preserving.

Next, let $\alpha_+ \in \mathrm{Aut}(k_+)$ be a group-theoretic automorphism of k_+ which is not $(\mathbb{Q}_{p_k})_+$-characteristic [cf. Theorem 2.7]. Then since γ is an element of the center of $\mathrm{Out}(G_k)$, one verifies immediately that γ_+ commutes with α_+. In particular, since γ_+ is $(\mathbb{Q}_{p_k})_+$-preserving, γ_+ restricts to the identity automorphism of $\alpha_+(k_+^{(d=1)}) \subseteq k_+$. Thus, since $d_k = 2$, and $k_+^{(d=1)} \neq \alpha_+(k_+^{(d=1)})$, we conclude that γ_+ is the identity automorphism of k_+, as desired. This completes the proof of Corollary 3.8. □

Acknowledgments

The first author would like to thank Shinichi Mochizuki for a discussion related to the content of §1. The first author was supported by JSPS KAKENHI Grant Number 18K03239. The second author would like to express a deepest gratitude to Hiroki Nishio and Keiko Nishio, for giving him constant support, warm encouragements. This research was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

References

[1] Y. Hoshi, A note on the geometricity of open homomorphisms between the absolute Galois groups of p-adic local fields, Kodai Math. J. 36 (2013), no. 2, 284–298.

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

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

[4] Y. Hoshi, Introduction to mono-anabelian geometry, to appear in Proceedings of the conference "Fundamental Groups in Arithmetic Geometry", Paris, France 2016.

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

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