RIMS-1962

On the Injectivity of the Homomorphisms from the Automorphism Groups of Fields to the Outer Automorphism Groups of the Absolute Galois Groups

By

Yuichiro HOSHI and Shota TSUJIMURA

July 2022

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

ON THE INJECTIVITY OF THE HOMOMORPHISMS FROM THE AUTOMORPHISM GROUPS OF FIELDS TO THE OUTER AUTOMORPHISM GROUPS OF THE ABSOLUTE GALOIS GROUPS

YUICHIRO HOSHI AND SHOTA TSUJIMURA

JULY 2022

ABSTRACT. In the present paper, we discuss the injectivity of the natural homomorphism from the automorphism group of a given field to the outer automorphism group of the associated absolute Galois group. We prove that this natural homomorphism is injective in the case where, for instance, the given field may be embedded into the field of fractions of some Noetherian local domain of mixed characteristic.

CONTENTS

INTRODUCTION

Throughout the present paper, let k be a field and $\overline{k}$ a separable closure of k. Write $G_k \stackrel{\text{def}}{=} \text{Gal}(\overline{k}/k)$ for the absolute Galois group of k determined by the separable closure $\overline{k}$. Write, moreover, $\text{Aut}(k)$ for the group of automorphisms of the field k and $\text{Out}(G_k)$ for the group of outer automorphisms of the group G_k. Then, by considering conjugation by an automorphism of the field $\overline{k}$ that lifts each of the automorphisms of the field k, we obtain a natural homomorphism of groups

$$\text{Aut}(k) \longrightarrow \text{Out}(G_k).$$

In the present paper, we discuss the injectivity of this natural homomorphism. The main result of the present paper is as follows [cf. Corollary 1.6, Theorem 2.4, Corollary 3.3, Corollary 4.1, and Corollary 4.2]:

Theorem. *If the field k satisfies one of the following five conditions, then the natural homomorphism* $\text{Aut}(k) \to \text{Out}(G_k)$ *is injective.*

(1) *The field k admits a subfield over which k is finitely generated and transcendental.*

2020 *Mathematics Subject Classification.* 11R32, 12E30.

Key words and phrases. absolute Galois group, outer automorphism group, Kummer theory, Artin-Schreier theory, slim.

(2) *The field k is a discrete valuation field of positive characteristic.*
(3) *The field k is isomorphic to a subfield of the field of real numbers.*
(4) *The field k is isomorphic to a subfield of the field of fractions of a Noetherian local domain of mixed characteristic.*
(5) *The field k is isomorphic to the field of fractions of a Noetherian integral domain that is not a field and does not contain a field of characteristic zero.*

Note that we also have a stronger injectivity result in the case where condition (1) (respectively, (3)) of the statement of the above theorem is satisfied [cf. Theorem 1.5 (respectively, Theorem 3.2)].

Acknowledgments. The first author was supported by JSPS KAKENHI Grant Number 21K03162. This research was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University.

1. The Case of Torally Kummer-nondegenerate Fields

In the present §1, we discuss the injectivity under consideration in the case where the given field is a certain torally Kummer-nondegenerate [cf. Definition 1.8 below] field [cf. Theorem 1.10 below].

Definition 1.1. Let Σ be a nonempty set of prime numbers invertible in k.

(i) We shall write

$$k^{\Sigma} \subseteq \overline{k}$$

for the minimal subfield of $\overline{k}$ that contains the subset

$$\{ a \in \overline{k} \,|\, a^{l^n} \in k \text{ for some } l \in \Sigma \text{ and nonnegative integer } n \} \subseteq \overline{k}.$$

Thus, one verifies easily that k^{Σ} is a Galois extension field of k. We shall write

$$Q_k^{\Sigma} \stackrel{\text{def}}{=} \mathrm{Gal}(k^{\Sigma}/k).$$

Moreover, one also verifies easily that we have a natural homomorphism

$$\mathrm{Aut}(k) \longrightarrow \mathrm{Out}(Q_k^{\Sigma}).$$

(ii) We shall write

$$\widehat{\mathbb{Z}}_k \stackrel{\text{def}}{=} \varprojlim_{\mathrm{char}(k)\nmid n\geq 1} \mathbb{Z}/n\mathbb{Z}, \qquad \Lambda(\overline{k}) \stackrel{\text{def}}{=} \varprojlim_{\mathrm{char}(k)\nmid n\geq 1} \mu_n(\overline{k})$$

— where the projective limits are taken over the positive integers n not divisible by $\mathrm{char}(k)$ — and

$$\widehat{\mathbb{Z}}_{\Sigma} \twoheadleftarrow \widehat{\mathbb{Z}}_k, \qquad \Lambda_{\Sigma}(\overline{k}) \twoheadleftarrow \Lambda(\overline{k})$$

for the respective maximal pro-Σ quotients. Now observe that one verifies easily that the modules $\Lambda(\overline{k})$, $\Lambda_{\Sigma}(\overline{k})$ have natural structures of free $\widehat{\mathbb{Z}}_k$-, $\widehat{\mathbb{Z}}_{\Sigma}$-modules of rank one, respectively.

(iii) We shall write

$$k^{\times\Sigma^\infty} \stackrel{\text{def}}{=} \bigcap_{l\in\Sigma,\, n\geq 1} (k^\times)^{l^n} \subseteq k^\times$$

for the subgroup consisting of elements that are l-divisible in $k^\times$ for every prime number $l \in \Sigma$ and

$$k_{\times\Sigma^\infty} \subseteq k$$

for the minimal subfield of k that contains $k^{\times\Sigma^\infty} \subseteq k^\times$. We shall also write

$$k^{\times\infty} \subseteq k_{\times\infty}$$

for the "$k^{\times\Sigma^\infty} \subseteq k_{\times\Sigma^\infty}$" in the case where we take the "Σ" to be the set of all prime numbers invertible in k.

Lemma 1.2. *Let Σ be a nonempty set of prime numbers invertible in k, and let σ be an element of the kernel of the natural homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ (respectively, $\mathrm{Aut}(k) \to \mathrm{Out}(Q_k^\Sigma)$). Then there exists an automorphism $\widetilde{\sigma}$ of the field $\overline{k}$ (respectively, the field k^Σ) that lifts σ and, moreover, commutes with every element of G_k (respectively, of Q_k^Σ).*

Proof. This assertion is immediate. □

Lemma 1.3. *Let Σ be a nonempty set of prime numbers invertible in k, σ an element of the kernel of the natural homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(Q_k^\Sigma)$, and $\widetilde{\sigma}$ an automorphism of the field k^Σ as in Lemma 1.2. Write $c \in \widehat{\mathbb{Z}}_\Sigma^\times$ for the image of $\widetilde{\sigma} \in \mathrm{Aut}(k^\Sigma)$ by the natural homomorphism $\mathrm{Aut}(k^\Sigma) \to \mathrm{Aut}(\Lambda_\Sigma(\overline{k})) = \widehat{\mathbb{Z}}_\Sigma^\times$. Suppose that there exists a surjective homomorphism $k^\times \twoheadrightarrow \mathbb{Z}$ of modules. Then the following assertions hold:*

(i) *If $c = 1$ (respectively, $c = -1$), then the action of σ on the quotient $k^\times/k^{\times\Sigma^\infty}$ is trivial (respectively, is given by the automorphism that maps $a \in k^\times/k^{\times\Sigma^\infty}$ to $a^{-1} \in k^\times/k^{\times\Sigma^\infty}$).*
(ii) *The inclusion $c \in \{\pm 1\}$ holds.*
(iii) *If $c = 1$, then the action of σ on the complement $k \setminus k_{\times\Sigma^\infty}$ is trivial.*
(iv) *If $c = 1$, and $k_{\times\Sigma^\infty} \neq k$, then σ is trivial.*

Proof. Fix a surjective homomorphism $v\colon k^\times \twoheadrightarrow \mathbb{Z}$ of modules. Now observe that since there is no nontrivial l-divisible element of the module $\mathbb{Z}$ for every prime number l, it is immediate that this homomorphism $v\colon k^\times \twoheadrightarrow \mathbb{Z}$ factors through the natural surjective homomorphism $k^\times \twoheadrightarrow k^\times/k^{\times\Sigma^\infty}$.

First, we verify assertions (i), (ii). Let us first observe that, by applying Kummer theory, we obtain a commutative diagram of modules

$$\begin{array}{ccccc}
k^\times/k^{\times\Sigma^\infty} & \hookrightarrow & \varprojlim_n k^\times/(k^\times)^n & \hookrightarrow & H^1\big(G_k, \Lambda_\Sigma(\overline{k})\big) \\
\downarrow{\scriptstyle v} & & \downarrow{\scriptstyle v^\wedge} & & \\
\mathbb{Z} & \hookrightarrow & \widehat{\mathbb{Z}}_\Sigma = \varprojlim_n \mathbb{Z}/n\mathbb{Z} & &
\end{array}$$

— where the projective limits are taken over the positive integers n whose prime divisors are contained in Σ, the right-hand vertical arrow $v^\wedge$ is the homomorphism of modules induced by v, the horizontal arrows are injective, the upper horizontal arrows are compatible with the respective natural actions of $\widetilde{\sigma}$, and the vertical arrows are surjective. Then it follows from our choice of $\widetilde{\sigma}$

[cf. Lemma 1.2] and the definition of c that $\widetilde{\sigma}$ acts on the module $H^1(G_k, \Lambda_\Sigma(\overline{k}))$, hence also on the modules $\varprojlim_n k^\times/(k^\times)^n$ and $k^\times/k^{\times\Sigma^\infty}$, by multiplication by $c \in \widehat{\mathbb{Z}}_\Sigma^\times$, which thus proves assertion (i). This completes the proof of assertion (i). Moreover, one may also conclude from this observation that the natural action of $\widetilde{\sigma}$ on the module $\varprojlim_n k^\times/(k^\times)^n$ preserves the kernel of the homomorphism $v^\wedge$. Thus, it follows immediately from the commutativity of the above diagram that the action of c on $\widehat{\mathbb{Z}}_\Sigma$ by multiplication has to preserve the image of the natural injective homomorphism $\mathbb{Z} \hookrightarrow \widehat{\mathbb{Z}}_\Sigma$. In particular, the inclusion $c \in \{\pm 1\}$ holds, as desired. This completes the proof of assertion (ii).

Next, we verify assertion (iii). Suppose that $c = 1$. Let a be an element of the complement $k \setminus k_{\times\Sigma^\infty}$ [so $1-a \in k^\times$]. Then it follows from assertion (i) that there exist $x, y \in k^{\times\Sigma^\infty}$ such that

$$\sigma(a) = xa, \qquad \sigma(1-a) = y(1-a).$$

Observe that since $1 = \sigma(1) = \sigma(1-a) + \sigma(a)$, we obtain that $1 = y + (x-y)a$. Thus, if $x \neq y$, then $a = (1-y)/(x-y) \in k_{\times\Sigma^\infty}$, which contradicts our choice of a. In particular, we conclude that $x = y$, which thus implies that the equalities $x = y = 1$, hence also the equality $\sigma(a) = a$, hold, as desired. This completes the proof of assertion (iii).

Finally, we verify assertion (iv). Suppose that $c = 1$, and that $k_{\times\Sigma^\infty} \neq k$. Then it follows from assertion (iii) that, to verify assertion (iv), it suffices to verify the equality $\sigma(a) = a$ for each $a \in k_{\times\Sigma^\infty}$. Let a be an element of $k_{\times\Sigma^\infty}$. Then since [we have assumed that] $k_{\times\Sigma^\infty} \neq k$, there exists an element b of the complement $k \setminus k_{\times\Sigma^\infty}$. Then since [it is immediate that] b, $a-b \in k \setminus k_{\times\Sigma^\infty}$, it follows from assertion (iii) that $\sigma(a) = \sigma(a-b) + \sigma(b) = (a-b) + b = a$, as desired. This completes the proof of assertion (iv), hence also of Lemma 1.3. □

Lemma 1.4. *Let Σ be a nonempty set of prime numbers invertible in k. Suppose that the following two conditions are satisfied:*

(1) *There exists a surjective homomorphism $k^\times \twoheadrightarrow \mathbb{Z}$ of modules.*
(2) *There exists an element $a_0 \in k^\times$ such that the field $k_{\times\Sigma^\infty}(a_0)$ [i.e., obtained by adjoining a_0 to $k_{\times\Sigma^\infty}$] is [either infinite or] of degree ≥ 3 over $k_{\times\Sigma^\infty}$.*

Then the natural homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(Q_k^\Sigma)$ *is injective.*

Proof. Let σ be an element of the kernel of the homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(Q_k^\Sigma)$. Now observe that it follows from condition (2) that $k_{\times\Sigma^\infty} \neq k$. Thus, it follows from Lemma 1.3, (i), (ii), (iv), together with condition (1), that, to verify Lemma 1.4, it suffices to verify that the automorphism of the quotient $k^\times/k^{\times\Sigma^\infty}$ induced by σ does not coincide with the automorphism that maps $a \in k^\times/k^{\times\Sigma^\infty}$ to $a^{-1} \in k^\times/k^{\times\Sigma^\infty}$.

Assume that the automorphism of the quotient $k^\times/k^{\times\Sigma^\infty}$ induced by σ coincides with the automorphism that maps $a \in k^\times/k^{\times\Sigma^\infty}$ to $a^{-1} \in k^\times/k^{\times\Sigma^\infty}$. Fix an element $a_0 \in k^\times$ as in condition (2). Then, by our assumption, there exist $x, y \in k^{\times\Sigma^\infty}$ such that

$$\sigma(a_0) = \frac{x}{a_0}, \qquad \sigma(1-a_0) = \frac{y}{1-a_0}.$$

In particular, since $1 = \sigma(1) = \sigma(1-a_0) + \sigma(a_0)$, which thus implies that $a_0^2 + (y-x-1)a_0 + x = 0$, we conclude that the field $k_{\times\Sigma^\infty}(a_0)$ ($\subseteq k$) is of degree ≤ 2 over $k_{\times\Sigma^\infty}$, which contradicts our choice of a_0. This completes the proof of Lemma 1.4. □

Theorem 1.5. *Suppose that the field k admits a subfield over which k is finitely generated and transcendental. Let l be a prime number invertible in k. Then the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(Q_k^{\{l\}})$ *is injective.*

Proof. Let $k_0 \subseteq k$ be a subfield over which k is finitely generated and transcendental. Let us first observe that we may assume without loss of generality, by replacing k_0 by a suitable subfield of k, that the extension k/k_0 is of transcendental degree one. Moreover, we may assume without loss of generality, by replacing k_0 by the algebraic closure of k_0 in k, that k coincides with the function field of some smooth proper curve over k_0. Then, by considering the various discrete valuations on k associated to the closed points of the smooth proper curve, one verifies immediately that the field k satisfies conditions (1), (2) of Lemma 1.4 [i.e., in the case where we take the "Σ" of Lemma 1.4 to be $\{l\}$]. In particular, it follows from Lemma 1.4 that the homomorphism under consideration is injective, as desired. This completes the proof of Theorem 1.5. □

Corollary 1.6. *Suppose that the field k admits a subfield over which k is finitely generated and transcendental. Then the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ *is injective.*

Proof. This assertion is a formal consequence of Theorem 1.5. □

Definition 1.7. We shall write

$$k_{\mathrm{div}} \subseteq \overline{k}$$

for the minimal subfield of $\overline{k}$ that contains the subset

$$\bigcup_K K^{\times\infty} \subseteq \overline{k}$$

[cf. Definition 1.1, (iii)] — where the union is taken over the subfields K of $\overline{k}$ finite over k.

Definition 1.8. We shall say that the field k is *TKND* [i.e., torally Kummer-nondegenerate] [cf. [1], Definition 6.6, (ii)] if the following two conditions are satisfied:

(1) The field k is of characteristic zero.
(2) The field extension $\overline{k}/k_{\mathrm{div}}$ is infinite.

Lemma 1.9. *Let K be a finite extension field of k. Then the following assertions hold:*

(i) *The equality* $k_{\mathrm{div}} = K_{\mathrm{div}}$ *holds.*
(ii) *If there exists a surjective homomorphism* $k^\times \twoheadrightarrow \mathbb{Z}$ *of modules, then there exists a surjective homomorphism* $K^\times \twoheadrightarrow \mathbb{Z}$ *of modules.*

Proof. Assertion (i) is immediate. Assertion (ii) may be verified, for instance, by considering the norm map associated to the finite field extension K/k. □

Theorem 1.10. *Suppose that the field k is TKND, and that there exists a surjective homomorphism* $k^\times \twoheadrightarrow \mathbb{Z}$ *of modules. Then the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ *is injective.*

Proof. Let us first observe that it is immediate that every element of k transcendental over $k_{\times\infty}$ satisfies condition (2) of Lemma 1.4 [i.e., imposed on "a_0"]. In particular, if the field extension $k/k_{\times\infty}$ is not algebraic, then it follows from Lemma 1.4 that the map under consideration is injective. Thus, to verify Theorem 1.10, we may assume without loss of generality that the field extension $k/k_{\times\infty}$ is algebraic.

Next, let us observe that it is immediate that we have inclusions $k_{\times\infty} \subseteq k_{\mathrm{div}} \subseteq \overline{k}$ of fields. In particular, the [necessarily infinite — cf. condition (2) of Definition 1.8] field extension $\overline{k}/k_{\mathrm{div}}$ is algebraic. Thus, since [it is immediate that] the extension field $\overline{k}$ of k coincides with the union of the finite extension field of k contained in $\overline{k}$, one may conclude that there exists a finite extension field K of k contained in $\overline{k}$ such that the inequality $[K : K \cap k_{\mathrm{div}}] \geq 3$ holds. Fix such a finite extension field K of k. Then it follows immediately from Lemma 1.9, (i), that we have inclusions $K_{\times\infty} \subseteq K \cap K_{\mathrm{div}} = K \cap k_{\mathrm{div}} \subseteq K$ of fields. Thus, since K is of characteristic zero [cf. condition (1) of Definition 1.8], and the inequalities $[K : K_{\times\infty}] \geq [K : K \cap k_{\mathrm{div}}] \geq 3$ hold, we conclude that there exists an element $a_0 \in K^{\times}$ such that the field $K_{\times\infty}(a_0)$ is of degree ≥ 3 over $K_{\times\infty}$.

Let σ be an element of the kernel of the homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$, and let $\widetilde{\sigma}$ be an automorphism of the field $\overline{k}$ as in Lemma 1.2. Then since [it is immediate from our choice of $\widetilde{\sigma}$] the action of $\widetilde{\sigma}$ on G_k by conjugation preserves every open subgroup of G_k, one verifies easily from elementary field theory that $\widetilde{\sigma}$ restricts to an automorphism of the fixed finite extension field K of k. Moreover, it is also immediate from our choice of $\widetilde{\sigma}$ that the resulting automorphism $\widetilde{\sigma}|_K$ of the field K is contained in the kernel of the natural homomorphism $\mathrm{Aut}(K) \to \mathrm{Out}(\mathrm{Gal}(\overline{k}/K))$. In particular, it follows from Lemma 1.4 [i.e., in the case where we take the "Σ" of Lemma 1.4 to be the set of all prime numbers], together with the argument in the preceding paragraph and Lemma 1.9, (ii), that the restriction of $\widetilde{\sigma}$ to K, hence also the automorphism σ of k, is trivial, as desired. This completes the proof of Theorem 1.10. □

2. The Case of Discrete Valuation Fields of Positive Characteristic

In the present §2, we discuss the injectivity under consideration in the case where the given field is a discrete valuation field of positive characteristic [cf. Theorem 2.4 below].

In the present §2, let p be a prime number. Suppose that the field k is of characteristic p. For each power $q > 1$ of p, write

$$\wp_q : k \longrightarrow k$$

for the Artin-Schreier map of degree q, i.e., the endomorphism of the underlying additive module of the field k that maps $a \in k$ to $a^q - a \in k$. Write, moreover,

$$\wp_{p^\infty}(k) \stackrel{\mathrm{def}}{=} \bigcap_{n \geq 1} \mathrm{Im}(\wp_{p^n}) \subseteq k.$$

Lemma 2.1. *Let σ be an element of the kernel of the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$, *and let $\widetilde{\sigma}$ be an automorphism of the field $\overline{k}$ as in Lemma 1.2. Suppose that there exists a surjective homomorphism $k^{\times} \twoheadrightarrow \mathbb{Z}$ of modules. Then the following assertions hold:*

(i) *The natural action of $\widetilde{\sigma}$ on the set of elements of $\overline{k}$ algebraic over the prime field of k is trivial.*

(ii) *The natural action of σ on the quotient module $k/\wp_{p^\infty}(k)$ is trivial.*

Proof. First, we verify assertion (i). Write $c \in \widehat{\mathbb{Z}}_k^{\times}$ for the image of $\widetilde{\sigma} \in \mathrm{Aut}(\overline{k})$ by the natural homomorphism $\mathrm{Aut}(\overline{k}) \to \mathrm{Aut}(\Lambda(\overline{k})) = \widehat{\mathbb{Z}}_k^{\times}$. Then since [we have assumed that] the field k is of positive characteristic, it is immediate that, to verify assertion (i), it suffices to verify the equality $c = 1$. To this end, observe that it follows immediately from elementary theory of finite fields that $c \in \widehat{\mathbb{Z}}_k^{\times}$ is contained in the closed subgroup of $\widehat{\mathbb{Z}}_k^{\times}$ generated by $p \in \widehat{\mathbb{Z}}_k^{\times}$. Thus, since the closed subgroup of $\widehat{\mathbb{Z}}_k^{\times}$ generated by $p \in \widehat{\mathbb{Z}}_k^{\times}$ is torsion-free [cf., e.g., [2], Lemma 7.5.4], it follows from

Lemma 1.3, (ii) [i.e., in the case where we take the "Σ" of Lemma 1.3 to be the set of all prime numbers invertible in k], that $c = 1$, as desired. This completes the proof of assertion (i).

Next, we verify assertion (ii). Let us first observe that it is immediate that, to verify assertion (ii), it suffices to verify that, for each power $q > 1$ of p, the natural action of σ on the quotient module $k/\mathrm{Im}(\wp_q)$ is trivial. To this end, observe that, by applying Artin-Schreier theory, we obtain an isomorphism of modules

$$k/\mathrm{Im}(\wp_q) \xrightarrow{\sim} H^1\big(G_k, \mathrm{Ker}(\overline{\wp}_q)\big)$$

— where we write $\overline{\wp}_q$ for the "$\wp_q$" in the case where we take the "k" to be $\overline{k}$ — compatible with the respective natural actions of $\widetilde{\sigma}$. Now since [it is immediate that] every element of $\mathrm{Ker}(\overline{\wp}_q)$ is algebraic over the prime field of k, it follows from our choice of $\widetilde{\sigma}$ and assertion (i) that the natural action of $\widetilde{\sigma}$ on the codomain of this isomorphism, hence also on the domain of this isomorphism, is trivial, as desired. This completes the proof of assertion (ii), hence also of Lemma 2.1. $\square$

Lemma 2.2. *Suppose that the field k admits a nontrivial discrete valuation $v\colon k^\times \to \mathbb{Z}$. Write $V \subseteq k$ for the valuation ring associated to v. Let $q > 1$ be a power of p, and let a be an element of k. Then the following assertions hold:*

(i) *If $a \notin V$, then the inequalities $v(\wp_q(a)) \leq -q < 0$ hold.*
(ii) *The inclusion $a \in V$ is equivalent to the inclusion $\wp_q(a) \in V$.*
(iii) *The inclusion $\wp_{p^\infty}(k) \subseteq V$ holds.*

Proof. Assertion (i) is immediate. Assertion (ii) follows from assertion (i). Assertion (iii) follows immediately from assertions (i), (ii). This completes the proof of Lemma 2.2. $\square$

Lemma 2.3. *Suppose that the field k admits a nontrivial discrete valuation $v\colon k^\times \to \mathbb{Z}$. Let σ be an element of the kernel of the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$. *Then the automorphism σ of k preserves the complement $k \setminus V \subseteq k$ and induces the identity automorphism of $k \setminus V$.*

Proof. Let a be an element of the complement $k \setminus V$. Then it follows from Lemma 2.1, (ii), that there exists an element $x \in \wp_{p^\infty}(k)$ such that $\sigma(a) = a + x$. Assume that $x \neq 0$, which thus implies that $0 \leq v(x) < \infty$ [cf. Lemma 2.2, (iii)]. Let n be a positive integer that is prime to p and $> -v(x)/v(a) + 1$. Then since $a \notin V$, it is immediate that

$$v\big(\sigma(a^n) - a^n\big) = v\big((a+x)^n - a^n\big) = v(a)(n-1) + v(x) < 0.$$

On the other hand, again by applying Lemma 2.1, (ii), one may conclude that $\sigma(a^n) - a^n \in \wp_{p^\infty}(k)$, which thus implies [cf. Lemma 2.2, (iii)] that $\sigma(a^n) - a^n \in V$. Thus, we obtain a contradiction. This completes the proof of Lemma 2.3. $\square$

Theorem 2.4. *Suppose that the field k is a discrete valuation field of positive characteristic. Then the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ *is injective.*

Proof. Let σ be an element of the kernel of the homomorphism under consideration, a an element of $k^\times$, and $v\colon k^\times \to \mathbb{Z}$ a nontrivial discrete valuation on k. Then it is immediate that there exists an element $a_0 \in k^\times$ such that $v(a_0) < 0$ and $v(a \cdot a_0) < 0$. Then it follows from Lemma 2.3 that $a \cdot a_0 = \sigma(a \cdot a_0) = \sigma(a) \cdot \sigma(a_0) = \sigma(a) \cdot a_0$, which thus implies that $\sigma(a) = a$, as desired. This completes the proof of Theorem 2.4. $\square$

Remark 2.4.1.

(i) Let us first observe that if the given field k [i.e., of characteristic p] is perfect, then the following two conditions are equivalent:

(1) The field k is of cardinality p.

(2) The natural homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ is injective.

Indeed, the implication (1) $\Rightarrow$ (2) is immediate from the [easily verified] fact that the group $\mathrm{Aut}(k)$ is trivial whenever condition (1) is satisfied. Next, to verify the implication (2) $\Rightarrow$ (1), observe that the p-th power Frobenius endomorphism of a perfect field of characteristic p is an automorphism. Moreover, let us also observe that it is immediate that the p-th power Frobenius endomorphism of a field of characteristic p commutes with an arbitrary automorphism of the field. Thus, one may conclude that if k is perfect, then the p-th power Frobenius endomorphism of k is contained in the kernel of the natural homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$. In particular, condition (2) implies the condition that the p-th power Frobenius endomorphism of k is the identity automorphism, which thus implies condition (1).

(ii) Here, we note that if the field k is perfect, then since [it is immediate that] there is no nontrivial p-divisible element of the module $\mathbb{Z}$, there is no nontrivial homomorphism $k^\times \to \mathbb{Z}$ of modules, hence also no nontrivial discrete valuation on k.

(iii) Note that, in the situation of Theorem 2.4, if one omits the hypothesis that k is a discrete valuation field, then it no longer holds that the homomorphism under consideration is injective in general. For instance, let us consider the case where the field k is given by an algebraic closure of a finite field [which thus implies that k is of positive characteristic]. Then it follows from the discussion of (i) that the natural homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ is not injective.

Remark 2.4.2. Note that, in the situation of Theorem 2.4, if one omits the hypothesis that k is of positive characteristic, then it no longer holds that the homomorphism under consideration is injective in general. For instance, let us consider the case where the field k is given by the field $\mathbb{C}((t))$ of formal Laurent series over the field $\mathbb{C}$ of complex numbers [which thus implies that k is a discrete valuation field]. Then it is well-known that the homomorphism of Kummer theory

$$k^\times \longrightarrow \mathrm{Hom}\big(G_k, \Lambda(\overline{k})\big)$$

maps $t \in k^\times$ to an isomorphism $G_k \xrightarrow{\sim} \Lambda(\overline{k})$ and, moreover, factors through the natural surjective homomorphism $k^\times \twoheadrightarrow k^\times/\mathbb{C}^\times$. Thus, since [it is immediate that] the automorphism of the field k that maps $f(t) \in k$ to $f(2t) \in k$ induces the respective identity automorphisms of the modules $k^\times/\mathbb{C}^\times$ and $\Lambda(\overline{k})$, we conclude that the image of this [nontrivial] automorphism of the field k by the natural homomorphism $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ is trivial.

3. The Case of Subfields of the Field of Real Numbers

In the present §3, we discuss the injectivity under consideration in the case where the given field may be embedded into the field $\mathbb{R}$ of real numbers [cf. Theorem 3.2 and Corollary 3.3 below].

Lemma 3.1. *Let $f,\ g\colon k \hookrightarrow \mathbb{R}$ be embeddings of fields. Then the following four conditions are equivalent:*

(1) *The equality $f = g$ holds.*

(2) *The outer homomorphism* $G_{\mathbb{R}} \to G_k$ *induced by* f *coincides with the outer homomorphism* $G_{\mathbb{R}} \to G_k$ *induced by* g.
(3) *The homomorphism* $G_{\mathbb{R}} = G_{\mathbb{R}}^{\mathrm{ab}}/2G_{\mathbb{R}}^{\mathrm{ab}} \to G_k^{\mathrm{ab}}/2G_k^{\mathrm{ab}}$ *induced by* f *coincides with the homomorphism* $G_{\mathbb{R}} = G_{\mathbb{R}}^{\mathrm{ab}}/2G_{\mathbb{R}}^{\mathrm{ab}} \to G_k^{\mathrm{ab}}/2G_k^{\mathrm{ab}}$ *induced by* g.
(4) *If one writes* $\mathbb{R}_{>0} \stackrel{\mathrm{def}}{=} \{a \in \mathbb{R} \,|\, a > 0\}$, *then the equality* $f^{-1}(\mathbb{R}_{>0}) = g^{-1}(\mathbb{R}_{>0})$ *holds.*

Proof. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are immediate. Next, we verify the implication (3) $\Rightarrow$ (4). Suppose that condition (4) is not satisfied. Then there exists an element $a \in k$ such that $f(a)g(a) < 0$. Now observe that it is immediate that the finite extension field of $\mathbb{R}$ corresponding to the open subgroup of $G_{\mathbb{R}} = G_{\mathbb{R}}^{\mathrm{ab}}/2G_{\mathbb{R}}^{\mathrm{ab}}$ obtained by pulling back, by the homomorphism $G_{\mathbb{R}} = G_{\mathbb{R}}^{\mathrm{ab}}/2G_{\mathbb{R}}^{\mathrm{ab}} \to G_k^{\mathrm{ab}}/2G_k^{\mathrm{ab}}$ induced by f (respectively, by g), the open subgroup of $G_k^{\mathrm{ab}}/2G_k^{\mathrm{ab}}$ corresponding to the finite extension field $k(\sqrt{a})$ of k is given by $\mathbb{R}(\sqrt{f(a)})$ (respectively, by $\mathbb{R}(\sqrt{g(a)})$). Thus, since $f(a)g(a) < 0$, condition (3) is not satisfied, as desired. This completes the proof of the implication (3) $\Rightarrow$ (4).

Finally, we verify the implication (4) $\Rightarrow$ (1). Suppose that condition (1) is not satisfied. Then there exists an element $a \in k$ such that $f(a) \neq g(a)$. We may assume without loss of generality, by replacing a by $-a$ if necessary, that $f(a) < g(a)$. Thus, one verifies easily that there exists a rational number $c \in \mathbb{Q}$ such that $f(a) < c < g(a)$. In particular, since [it is immediate that] $c = f(c) = g(c)$, we may assume without loss of generality, by replacing a by $a - c$, that $f(a) < 0 < g(a)$. Thus, we conclude that condition (4) is not satisfied, as desired. This completes the proof of the implication (4) $\Rightarrow$ (1), hence also of Lemma 3.1. ☐

Theorem 3.2. *Suppose that the field* k *is isomorphic to a subfield of the field of real numbers. Then the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Aut}(G_k^{\mathrm{ab}}/2G_k^{\mathrm{ab}})$ *is injective.*

Proof. Let σ be an element of the kernel of the homomorphism $\mathrm{Aut}(k) \to \mathrm{Aut}(G_k^{\mathrm{ab}}/2G_k^{\mathrm{ab}})$, and let $\iota\colon k \hookrightarrow \mathbb{R}$ be an embedding of fields. Then it is immediate that the homomorphism $G_{\mathbb{R}} = G_{\mathbb{R}}^{\mathrm{ab}}/2G_{\mathbb{R}}^{\mathrm{ab}} \to G_k^{\mathrm{ab}}/2G_k^{\mathrm{ab}}$ induced by ι coincides with the homomorphism $G_{\mathbb{R}} = G_{\mathbb{R}}^{\mathrm{ab}}/2G_{\mathbb{R}}^{\mathrm{ab}} \to G_k^{\mathrm{ab}}/2G_k^{\mathrm{ab}}$ induced by $\iota \circ \sigma$. Thus, we conclude from the implication (3) $\Rightarrow$ (1) of Lemma 3.1 that $\iota = \iota \circ \sigma$, which thus implies that σ is trivial, as desired. This completes the proof of Theorem 3.2. ☐

Corollary 3.3. *Suppose that the field* k *is isomorphic to a subfield of the field of real numbers. Then the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ *is injective.*

Proof. This assertion is a formal consequence of Theorem 3.2. ☐

4. Consequences

In the present §4, we give some consequences of the results obtained in the previous sections [cf. Corollary 4.1, Corollary 4.2, and Corollary 4.5 below].

Corollary 4.1. *Suppose that the field* k *is isomorphic to a subfield of the field of fractions of a Noetherian local domain of mixed characteristic. Then the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ *is injective.*

Proof. It follows from Theorem 1.10 that, to verify Corollary 4.1, it suffices to verify the following two assertions:
(1) The field k is TKND.
(2) There exists a surjective homomorphism $k^{\times} \twoheadrightarrow \mathbb{Z}$ of modules.

Assertion (1) is an immediate consequence of [3], Proposition 2.3. Next, we verify assertion (2). Let us first recall that an arbitrary Noetherian local domain that is not a field is dominated by a discrete valuation ring. In particular, one may conclude that the field k is isomorphic to a subfield of a field K that admits a nontrivial discrete varluation $v\colon K^{\times} \to \mathbb{Z}$ whose valuation ring is of positive residue characteristic $p > 0$. Then since $v(p) > 0$, it is immediate that the composite of the injective homomorphism $k^{\times} \hookrightarrow K^{\times}$ that arises from an isomorphism of k with a subfield of K and the homomorphism $v\colon K^{\times} \to \mathbb{Z}$ of modules is nontrivial. In particular, there exists a surjective homomorphism $k^{\times} \twoheadrightarrow \mathbb{Z}$ of modules, as desired. This completes the proof of assertion (2), hence also of Corollary 4.1. □

Corollary 4.2. *Let R be a Noetherian integral domain. Suppose that R is not a field and does not contain a field of characteristic zero. Suppose, moreover, that the field k is isomorphic to the field of fractions of R. Then the natural homomorphism* $\mathrm{Aut}(k) \to \mathrm{Out}(G_k)$ *is injective.*

Proof. Since R is not a field and does not contain a field of characteristic zero, there exists a nonzero prime ideal of R of positive residue characteristic. Thus, we may assume without loss of generality, by replacing R by the localization at this prime ideal, that R is a Noetherian local domain of positive residue characteristic that is not a field. In particular, if k is of characteristic zero, then the injectivity under consideration follows from Corollary 4.1. Thus, we may assume without loss of generality that k is of positive characteristic. Now let us recall that an arbitrary Noetherian local domain that is not a field is dominated by a discrete valuation ring. In particular, we may assume without loss of generality that R is a discrete valuation ring. Then the injectivity under consideration follows from Theorem 2.4. This completes the proof of Corollary 4.2. □

Remark 4.2.1. Note that, in the situation of Corollary 4.2, if one omits the hypothesis that R is not a field, then it no longer holds that the homomorphism under consideration is injective in general. For instance, let us consider the case where the domain R is given by an algebraic closure of a finite field [which thus implies that R does not contain a field of characteristic zero]. Then, as discussed in Remark 2.4.1, (iii), the homomorphism under consideration is not injective.

Remark 4.2.2. Note that, in the situation of Corollary 4.2, if one omits the hypothesis that R does not contain a field of characteristic zero, then it no longer holds that the homomorphism under consideration is injective in general. For instance, let us consider the case where the domain R is given by the ring $\mathbb{C}[[t]]$ of formal power series over the field $\mathbb{C}$ of complex numbers [which thus implies that R is not a field]. Then, as discussed in Remark 2.4.2, the homomorphism under consideration is not injective.

Definition 4.3. We shall say that a profinite group is *slim* if every open subgroup of the profinite group is center-free. Note that one verifies easily that a profinite group is slim if and only if the centralizer of every normal open subgroup in the profinite group is trivial.

Lemma 4.4. *Suppose that, for every finite Galois extension field K of k contained in $\overline{k}$, if one writes $G_K \stackrel{\mathrm{def}}{=} \mathrm{Gal}(\overline{k}/K) \subseteq G_k$ for the absolute Galois group of K determined by the separable closure $\overline{k}$, then the natural homomorphism* $\mathrm{Aut}(K) \to \mathrm{Out}(G_K)$ *is injective. Then the profinite group G_k is slim.*

Proof. Let K be a finite Galois extension field of k contained in $\overline{k}$, and let $\widetilde{\sigma} \in G_k$ be an element of the centralizer of G_K in G_k. Then it is tautology that the image of the restriction $\widetilde{\sigma}|_K \in \mathrm{Gal}(K/k) \subseteq \mathrm{Aut}(K)$ by the natural homomorphism $\mathrm{Aut}(K) \to \mathrm{Out}(G_K)$ is trivial. Thus, it follows from the injectivity assumption of the statement of Lemma 4.4 that $\widetilde{\sigma} \in G_K$. In particular, by allowing "K" to vary, we conclude that $\widetilde{\sigma}$ is trivial, as desired. This completes the proof of Lemma 4.4. □

Corollary 4.5. *Suppose that one of the following five conditions is satisfied:*

(1) *The field k admits a subfield over which k is finitely generated and transcendental.*
(2) *The field k is TKND and admits a surjective homomorphism $k^\times \twoheadrightarrow \mathbb{Z}$ of modules.*
(3) *The field k is a discrete valuation field of positive characteristic.*
(4) *The field k is isomorphic to a subfield of the field of fractions of a Noetherian local domain of mixed characteristic.*
(5) *The field k is isomorphic to the field of fractions of a Noetherian integral domain that is not a field and does not contain a field of characteristic zero.*

Then the profinite group G_k is slim.

Proof. Suppose that the field k satisfies condition (1) (respectively, (3); (4); (5)). Then one verifies immediately that every finite extension field of k contained in $\overline{k}$ satisfies condition (1) (respectively, (3); (4); (5)). In particular, the slimness of G_k follows from Lemma 4.4, together with Corollary 1.6 (respectively, Theorem 2.4; Corollary 4.1; Corollary 4.2).

Finally, suppose that the field k satisfies condition (2). Then it follows from Lemma 1.9, (i), (ii), that every finite extension field of k contained in $\overline{k}$ satisfies condition (2). In particular, the slimness of G_k follows from Lemma 4.4, together with Theorem 1.10. This completes the proof of Corollary 4.5. □

REFERENCES

[1] Y. Hoshi, S. Mochizuki, and S. Tsujimura, *Combinatorial construction of the absolute Galois group of the field of rational numbers*, RIMS Preprint **1935** (December 2020).

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

[3] S. Tsujimura, Construction of non-$\times\mu$-indivisible TKND-AVKF-fields, *Kodai Math. J.* **45** (2022), no. **1**, 38–48.

(Yuichiro Hoshi) RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KYOTO UNIVERSITY, KYOTO 606-8502, JAPAN

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

(Shota Tsujimura) RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KYOTO UNIVERSITY, KYOTO 606-8502, JAPAN

Email address: stsuji@kurims.kyoto-u.ac.jp