On the Field-theoreticity of Homomorphisms Between the Multiplicative Groups of Number Fields

Yuichiro Hoshi

December 2013

Abstract. — In the present paper, we discuss the *field-theoreticity* of homomorphisms between the multiplicative groups of *number fields.* We prove that, for instance, for a given isomorphism between the multiplicative groups of number fields, it holds that either the given isomorphism or its multiplicative inverse arises from an *isomorphism of fields* if and only if the given isomorphism is *SPU-preserving* [i.e., roughly speaking, preserves the subgroups of principal units with respect to various nonarchimedean primes].

Contents

Introduction

In the present paper, we discuss the *field-theoreticity* of homomorphisms between the multiplicative groups of fields. Let us consider the following problem.

> For a homomorphism $\alpha\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ between the multiplicative groups of fields ${}^{\circ}k$ and ${}^{\bullet}k$, when does the homomorphism α arise from a *homomorphism of fields* ${}^{\circ}k \to {}^{\bullet}k$? In other words, when is the *additive structure of* ${}^{\circ}k$ compatible with the *additive structure of* ${}^{\bullet}k$ relative to the homomorphism α?

At a more philosophical level:

2010 Mathematics Subject Classification. — 11R04.
Key words and phrases. — number field, multiplicative group, field-theoreticity, PU-preserving homomorphism.
The author would like to thank *Kazumi Higashiyama* for pointing out a minor error in the proof of Lemma 2.2 of an earlier version of the present paper. The author also would like to thank the referee for comments concerning Remarks 3.3.1, 3.3.2. This research was supported by Grant-in-Aid for Scientific Research (C), No. 24540016, Japan Society for the Promotion of Science.

> How can one understand the *additive structure* of a field by the language of the *multiplicative structure* of the field?

Now let us recall the following consequence of "*Uchida's lemma*" [reviewed in [1], Proposition 1.3] that is implicit in the argument of [7], Lemmas 8-11 [cf. also [5], Lemma 4.7].

> For $\Box \in \{\circ, \bullet\}$, let ${}^{\Box}k$ be an algebraically closed field and ${}^{\Box}C$ a projective smooth curve over ${}^{\Box}k$. Write ${}^{\Box}K$ for the function field of ${}^{\Box}C$ and ${}^{\Box}C^{\mathrm{cl}}$ for the set of closed points of ${}^{\Box}C$. For each closed point ${}^{\Box}x \in {}^{\Box}C^{\mathrm{cl}}$ of ${}^{\Box}C$, write $\mathcal{O}_{{}^{\Box}C,{}^{\Box}x} \subseteq {}^{\Box}K$ for the local ring of ${}^{\Box}C$ at ${}^{\Box}x$, $\mathfrak{m}_{{}^{\Box}C,{}^{\Box}x} \subseteq \mathcal{O}_{{}^{\Box}C,{}^{\Box}x}$ for the maximal ideal of $\mathcal{O}_{{}^{\Box}C,{}^{\Box}x}$, and $\mathrm{ord}_{{}^{\Box}x} \colon {}^{\Box}K^{\times} \to \mathbb{Z}$ for the valuation of ${}^{\Box}K$ given by mapping $f \in {}^{\Box}K^{\times}$ to the order of f at ${}^{\Box}x \in {}^{\Box}C$. [Thus, one verifies easily that $1 + \mathfrak{m}_{{}^{\Box}C,{}^{\Box}x} \subseteq \mathrm{Ker}(\mathrm{ord}_{{}^{\Box}x}) = \mathcal{O}^{\times}_{{}^{\Box}C,{}^{\Box}x} \subseteq {}^{\Box}K^{\times}$.] Let
>
> $$\alpha \colon {}^{\circ}K^{\times} \xrightarrow{\sim} {}^{\bullet}K^{\times}$$
>
> be an isomorphism between the multiplicative groups of ${}^{\circ}K$, ${}^{\bullet}K$. Then it holds that the isomorphism α arises from an *isomorphism of fields* ${}^{\circ}K \xrightarrow{\sim} {}^{\bullet}K$ if and only if there exists a bijection $\phi \colon {}^{\bullet}C^{\mathrm{cl}} \xrightarrow{\sim} {}^{\circ}C^{\mathrm{cl}}$ such that, for every ${}^{\bullet}x \in {}^{\bullet}C^{\mathrm{cl}}$ and ${}^{\circ}x \overset{\mathrm{def}}{=} \phi({}^{\bullet}x) \in {}^{\circ}C^{\mathrm{cl}}$, it holds that $\mathrm{ord}_{{}^{\circ}x} = \mathrm{ord}_{{}^{\bullet}x} \circ \alpha$, and, moreover, $1 + \mathfrak{m}_{{}^{\circ}C,{}^{\circ}x} = \alpha^{-1}(1 + \mathfrak{m}_{{}^{\bullet}C,{}^{\bullet}x})$.

Moreover, the issue of recovering the additive structure for not only *isomorphisms* [as in the above result] but also suitable *homomorphisms* between the multiplicative groups of function fields has been intensively studied by *M. Saïdi* and *A. Tamagawa* in, for instance, [3], §4; [4], §5 [cf. Remark 3.3.1].

In the present paper, we discuss an *analogue for number fields* of the above result. In the remainder of this Introduction, let $\mathfrak{Primes}$ be the set of all prime numbers, $\Box \in \{\circ, \bullet\}$, ${}^{\Box}k$ a *number field* [i.e., a finite extension of the field of rational numbers], ${}^{\Box}\mathfrak{o} \subseteq {}^{\Box}k$ the ring of integers of ${}^{\Box}k$, ${}^{\Box}\mathcal{V}$ the set of maximal ideals of ${}^{\Box}\mathfrak{o}$ [i.e., the set of nonarchimedean primes of ${}^{\Box}k$], and ${}^{\Box}\mathbb{Q} \subseteq {}^{\Box}k$ the [uniquely determined] subfield of ${}^{\Box}k$ that is isomorphic to the *field of rational numbers*. For ${}^{\Box}\mathfrak{p} \in {}^{\Box}\mathcal{V}$, write ${}^{\Box}\mathfrak{o}_{{}^{\Box}\mathfrak{p}}$ for the localization of ${}^{\Box}\mathfrak{o}$ at ${}^{\Box}\mathfrak{p}$, $\mathfrak{c}({}^{\Box}\mathfrak{p})$ for the residue characteristic of ${}^{\Box}\mathfrak{p}$ [thus, we have a map $\mathfrak{c} \colon {}^{\Box}\mathcal{V} \to \mathfrak{Primes}$], and $\mathrm{ord}_{{}^{\Box}\mathfrak{p}} \colon {}^{\Box}k^{\times} \twoheadrightarrow \mathbb{Z}$ for the [uniquely determined] surjective valuation of ${}^{\Box}k$ associated to ${}^{\Box}\mathfrak{p}$ [cf. Definition 1.1]. Let

$$\alpha \colon {}^{\circ}k^{\times} \longrightarrow {}^{\bullet}k^{\times}$$

be a homomorphism between the multiplicative groups of ${}^{\circ}k$, ${}^{\bullet}k$. Then the main result of the present paper may be stated as follows [cf. Theorem 2.5].

THEOREM A. — *The following conditions are equivalent:*

(1) *The homomorphism α arises from a* **homomorphism of fields** ${}^{\circ}k \to {}^{\bullet}k$.

(2) *The homomorphism α is* **CPU-preserving** [*i.e., there exists a map $\phi \colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ such that $\mathfrak{c}({}^{\bullet}\mathfrak{p}) = \mathfrak{c}(\phi({}^{\bullet}\mathfrak{p}))$ for every ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$, and, moreover, the inclusion $1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}} \subseteq \alpha^{-1}(1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})$, where we write ${}^{\circ}\mathfrak{p} \overset{\mathrm{def}}{=} \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, holds for all but finitely many ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$*

— *cf. Definition* 1.3, (ii)], *and, moreover, there exists an* $x \in \mathbb{Q}^\times \setminus \mathbb{Z}^\times$ *such that the "x" in* ${}^\circ k$ *maps, via* α, *to the "x" in* ${}^\bullet k$.

(3) *The homomorphism* α *is* **PU-preserving** [*i.e., there exists a map* $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ *such that the inclusion* $1 + {}^\circ\mathfrak{p}^\circ\mathfrak{o}_{{}^\circ\mathfrak{p}} \subseteq \alpha^{-1}(1 + {}^\bullet\mathfrak{p}^\bullet\mathfrak{o}_{{}^\bullet\mathfrak{p}})$, *where we write* ${}^\circ\mathfrak{p} \stackrel{\text{def}}{=} \phi({}^\bullet\mathfrak{p}) \in {}^\circ\mathcal{V}$, *holds for all but finitely many* ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$ — *cf. Definition* 1.3, (i)], *and, moreover, the restriction* ${}^\circ\mathbb{Q}^\times \to {}^\bullet k^\times$ *of* α *to* ${}^\circ\mathbb{Q}^\times \subseteq {}^\circ k^\times$ *arises from a* **homomorphism of fields** ${}^\circ\mathbb{Q} \to {}^\bullet k$.

By concentrating on *surjections*, we obtain the following result [cf. Corollary 3.2].

THEOREM B. — *Suppose that the homomorphism* α *is* **surjective**. *Then it holds that either* α *or the composite* $(-)^{-1} \circ \alpha$ [*i.e., the surjection* ${}^\circ k^\times \twoheadrightarrow {}^\bullet k^\times$ *obtained by mapping* $x \in {}^\circ k^\times$ *to* $\alpha(x)^{-1} \in {}^\bullet k^\times$] *arises from an* **isomorphism of fields** ${}^\circ k \xrightarrow{\sim} {}^\bullet k$ *if and only if the surjection* α *is* **SPU-preserving** [*i.e., there exists a map* $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ *such that the equality* $1 + {}^\circ\mathfrak{p}^\circ\mathfrak{o}_{{}^\circ\mathfrak{p}} = \alpha^{-1}(1 + {}^\bullet\mathfrak{p}^\bullet\mathfrak{o}_{{}^\bullet\mathfrak{p}})$, *where we write* ${}^\circ\mathfrak{p} \stackrel{\text{def}}{=} \phi({}^\bullet\mathfrak{p}) \in {}^\circ\mathcal{V}$, *holds for all but finitely many* ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$ — *cf. Definition* 1.3, (i)].

As corollaries of Theorem A, we also prove the following results, that may be regarded as *analogues of Uchida's lemma for number fields* [cf. Theorem 3.1; Corollary 3.3].

THEOREM C. — *The homomorphism* α *arises from a* **homomorphism of fields** ${}^\circ k \to {}^\bullet k$ *if and only if there exists a map* $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ *over* $\mathfrak{Primes}$ *relative to* $\mathfrak{c}$ [*i.e.,* $\mathfrak{c}({}^\bullet\mathfrak{p}) = \mathfrak{c}(\phi({}^\bullet\mathfrak{p}))$ *for every* ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$] *such that, for* ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$, *if we write* ${}^\circ\mathfrak{p} \stackrel{\text{def}}{=} \phi({}^\bullet\mathfrak{p}) \in {}^\circ\mathcal{V}$, *then the equality*

$$\mathrm{ord}_{{}^\circ\mathfrak{p}} = \mathrm{ord}_{{}^\bullet\mathfrak{p}} \circ \alpha$$

holds for **infinitely many** ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$, *and, moreover, the inclusion*

$$1 + {}^\circ\mathfrak{p}^\circ\mathfrak{o}_{{}^\circ\mathfrak{p}} \subseteq \alpha^{-1}(1 + {}^\bullet\mathfrak{p}^\bullet\mathfrak{o}_{{}^\bullet\mathfrak{p}})$$

holds for **all but finitely many** ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$.

THEOREM D. — *Suppose that the homomorphism* α *is* **surjective**. *Then the surjection* α *arises from an* **isomorphism of fields** ${}^\circ k \xrightarrow{\sim} {}^\bullet k$ *if and only if there exists a map* $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ *such that, for* ${}^\bullet\mathfrak{p} \in S$, *if we write* ${}^\circ\mathfrak{p} \stackrel{\text{def}}{=} \phi({}^\bullet\mathfrak{p}) \in {}^\circ\mathcal{V}$, *then the equality*

$$1 + {}^\circ\mathfrak{p}^\circ\mathfrak{o}_{{}^\circ\mathfrak{p}} = \alpha^{-1}(1 + {}^\bullet\mathfrak{p}^\bullet\mathfrak{o}_{{}^\bullet\mathfrak{p}})$$

holds for all but finitely many ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$, *and, moreover, there exist a maximal ideal* ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$ *of* ${}^\bullet\mathfrak{o}$ *and a* **positive** *integer* n *such that*

$$n \cdot \mathrm{ord}_{{}^\circ\mathfrak{p}} = \mathrm{ord}_{{}^\bullet\mathfrak{p}} \circ \alpha\,.$$

1. PU-preserving Homomorphisms

In the present §1, we define and discuss the notion of a *PU-preserving* homomorphism [cf. Definition 1.3, (i), below]. In the present §1, write $\mathfrak{Primes}$ for the set of all prime numbers. For $\square \in \{\circ, \bullet\}$, let ${}^{\square}k$ be a *number field* [i.e., a finite extension of the field of rational numbers $\mathbb{Q}$]; write ${}^{\square}\mathfrak{o} \subseteq {}^{\square}k$ for the ring of integers of ${}^{\square}k$, ${}^{\square}\mathcal{V}$ for the set of maximal ideals of ${}^{\square}\mathfrak{o}$ [i.e., the set of nonarchimedean primes of ${}^{\square}k$], and ${}^{\square}\mathbb{Q} \subseteq {}^{\square}k$ for the [uniquely determined] subfield of ${}^{\square}k$ that is isomorphic to the *field of rational numbers.* Moreover, let k be a *number field*; we shall use similar notation $\mathfrak{o} \subseteq k$, $\mathcal{V}$ for objects associated to the number field k.

Definition 1.1. — Let $\mathfrak{p} \in \mathcal{V}$ be a maximal ideal of $\mathfrak{o}$.

(i) We shall write

$$\mathfrak{o}_{\mathfrak{p}}$$

for the localization of $\mathfrak{o}$ at $\mathfrak{p}$,

$$\kappa(\mathfrak{p}) \stackrel{\text{def}}{=} \mathfrak{o}/\mathfrak{p} \xrightarrow{\sim} \mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$$

for the residue field of $\mathfrak{o}$ at $\mathfrak{p}$, and

$$\mathfrak{c}(\mathfrak{p}) \stackrel{\text{def}}{=} \mathrm{char}(\kappa(\mathfrak{p}))$$

for the characteristic of $\kappa(\mathfrak{p})$. Thus, we have a map

$$\mathfrak{c} \colon \mathcal{V} \longrightarrow \mathfrak{Primes}\,.$$

(ii) We shall write

$$\mathrm{ord}_{\mathfrak{p}} \colon k^{\times} \twoheadrightarrow \mathbb{Z}$$

for the [uniquely determined] surjective valuation of k associated to $\mathfrak{p}$. Thus, one verifies easily that the kernel $\mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}}) \subseteq k^{\times}$ of $\mathrm{ord}_{\mathfrak{p}}$ *coincides* with the group $\mathfrak{o}_{\mathfrak{p}}^{\times} \subseteq k^{\times}$ of invertible elements of $\mathfrak{o}_{\mathfrak{p}}$ [cf. (i)], i.e.,

$$\mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}}) = \mathfrak{o}_{\mathfrak{p}}^{\times} \subseteq k^{\times}\,.$$

Moreover, we have a natural exact sequence of abelian groups

$$1 \longrightarrow 1 + \mathfrak{p}\mathfrak{o}_{\mathfrak{p}} \longrightarrow \mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}}) \longrightarrow \kappa(\mathfrak{p})^{\times} \longrightarrow 1\,.$$

Remark 1.1.1. — By the map $\mathfrak{c}$ [cf. Definition 1.1, (i)], let us identify $\mathfrak{Primes}$ with the "$\mathcal{V}$" that occurs in the case where we take the "k" to be a number field that is isomorphic to the *field of rational numbers* [e.g., the field ${}^{\square}\mathbb{Q}$].

Definition 1.2. — Let $\phi \colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ be a map of sets. Then we shall say that ϕ is *characteristic-compatible* if ϕ is a map over $\mathfrak{Primes}$ [relative to $\mathfrak{c}$ — cf. Definition 1.1, (i)], i.e., the diagram

$$\begin{array}{ccc} {}^{\bullet}\mathcal{V} & \xrightarrow{\ \phi\ } & {}^{\circ}\mathcal{V} \\ {\scriptstyle \mathfrak{c}}\downarrow & & \downarrow{\scriptstyle \mathfrak{c}} \\ \mathfrak{Primes} & = & \mathfrak{Primes} \end{array}$$

commutes.

REMARK 1.2.1. — One verifies easily that if a map $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ is *characteristic-compatible* [cf. Definition 1.2], then ϕ is *finite-to-one*, i.e., the inverse image of any element of ${}^{\circ}\mathcal{V}$ is *finite*.

DEFINITION 1.3. — Let $\alpha\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ be a homomorphism of groups.

(i) Let $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ be a map of sets. Then we shall say that the homomorphism α is [ϕ-]*PU-preserving* [i.e., "principal-unit-preserving"] (respectively, [ϕ-]*SPU-preserving* [i.e., "strictly principal-unit-preserving"]) if the inclusion $1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}} \subseteq \alpha^{-1}(1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})$ (respectively, the equality $1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}} = \alpha^{-1}(1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})$) [cf. Definition 1.1, (i)], where we write ${}^{\circ}\mathfrak{p} \stackrel{\mathrm{def}}{=} \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, holds for all but finitely many ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$. If, in this situation, for a maximal ideal ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$ of ${}^{\bullet}\mathfrak{o}$, the inclusion $1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}} \subseteq \alpha^{-1}(1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})$ (respectively, the equality $1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}} = \alpha^{-1}(1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})$) does not hold, then we shall say that ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$ is *PU-exceptional* (respectively, *SPU-exceptional*) for (α, ϕ).

(ii) We shall say that the homomorphism α is *CPU-preserving* [i.e., "characteristic-compatibly principal-unit-preserving"] if α is ϕ-PU-preserving [cf. (i)] for some characteristic-compatible [cf. Definition 1.2] map $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$.

REMARK 1.3.1. — In the notation of Definition 1.3, one verifies easily that if α is *ϕ-PU-preserving*, and the equality $\mathfrak{c}({}^{\bullet}\mathfrak{p}) = \mathfrak{c}(\phi({}^{\bullet}\mathfrak{p}))$ holds for all but finitely many ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$, then — by replacing ϕ by a suitable extension [to a map ${}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$] of the restriction of ϕ to the subset of ${}^{\bullet}\mathcal{V}$ consisting of ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$ such that $\mathfrak{c}({}^{\bullet}\mathfrak{p}) = \mathfrak{c}(\phi({}^{\bullet}\mathfrak{p}))$ — α is *CPU-preserving*.

LEMMA 1.4. — *Let $\iota\colon {}^{\circ}k \to {}^{\bullet}k$ be a* **homomorphism of fields**. *Write $\iota^{\times}\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ for the homomorphism between the multiplicative groups induced by ι and $\mathcal{V}_{\iota}\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ for the [necessarily* **surjective** *and* **characteristic-compatible** *— cf. Definition* 1.2] *map obtained by mapping ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$ to $\iota^{-1}({}^{\bullet}\mathfrak{p}) \cap {}^{\circ}\mathfrak{o} \in {}^{\circ}\mathcal{V}$. Then, for every ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$, the* **equality**

$$1 + \mathcal{V}_{\iota}({}^{\bullet}\mathfrak{p}){}^{\circ}\mathfrak{o}_{\mathcal{V}_{\iota}({}^{\bullet}\mathfrak{p})} = (\iota^{\times})^{-1}(1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})$$

holds. In particular, the homomorphism $\iota^{\times}$ is **$\mathcal{V}_{\iota}$-SPU-preserving** *and* **CPU-preserving** [*cf. Definition* 1.3].

PROOF. — This follows immediately from the various definitions involved. □

LEMMA 1.5. — *Let $\alpha\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ be a homomorphism of groups, $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ a map of sets, and ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$ a maximal ideal of ${}^{\bullet}\mathfrak{o}$. Write ${}^{\circ}\mathfrak{p} \stackrel{\mathrm{def}}{=} \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$. Then the following hold:*

(i) *Suppose that α is* **ϕ-PU-preserving**, *and that ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$ is* **not PU-exceptional** *for (α, ϕ) [cf. Definition* 1.3, (i)]. *Then it holds that* $\mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}}) \subseteq \alpha^{-1}(\mathrm{Ker}(\mathrm{ord}_{{}^{\bullet}\mathfrak{p}}))$. *In* *particular, α determines homomorphisms of groups*

$$\mathrm{Ker}(\mathrm{ord}_{{}^\circ\mathfrak{p}})/(1+{}^\circ\mathfrak{p}{}^\circ\mathfrak{o}_{{}^\circ\mathfrak{p}}) \quad (\simeq \kappa({}^\circ\mathfrak{p})^\times) \longrightarrow \mathrm{Ker}(\mathrm{ord}_{{}^\bullet\mathfrak{p}})/(1+{}^\bullet\mathfrak{p}{}^\bullet\mathfrak{o}_{{}^\bullet\mathfrak{p}}) \quad (\simeq \kappa({}^\bullet\mathfrak{p})^\times)\,;$$

$${}^\circ k^\times/\mathrm{Ker}(\mathrm{ord}_{{}^\circ\mathfrak{p}}) \quad (\simeq \mathbb{Z}) \longrightarrow {}^\bullet k^\times/\mathrm{Ker}(\mathrm{ord}_{{}^\bullet\mathfrak{p}}) \quad (\simeq \mathbb{Z})\,.$$

(ii) *Suppose that α is* **ϕ-SPU-preserving**, *and that ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$ is* **not SPU-exceptional** *for (α, ϕ) [cf. Definition* 1.3, (i)]. *Suppose, moreover, that α is* **surjective**. *Then the two displayed homomorphisms of* (i) *are* **isomorphisms**. *Moreover, the surjection α is* **CPU-preserving** [*cf. Definition* 1.3, (ii)].

PROOF. — Assertion (i) follows immediately from the [easily verified] fact that, for each $\Box \in \{\circ, \bullet\}$, the subgroup $\mathrm{Ker}(\mathrm{ord}_{{}^\Box\mathfrak{p}})/(1+{}^\Box\mathfrak{p}{}^\Box\mathfrak{o}_{{}^\Box\mathfrak{p}}) \subseteq {}^\Box k^\times/(1+{}^\Box\mathfrak{p}{}^\Box\mathfrak{o}_{{}^\Box\mathfrak{p}})$ *coincides* with the *maximal torsion subgroup* of ${}^\Box k^\times/(1+{}^\Box\mathfrak{p}{}^\Box\mathfrak{o}_{{}^\Box\mathfrak{p}})$. Next, we verify assertion (ii). The assertion that the two displayed homomorphisms of (i) are *isomorphisms* follows immediately from the various definitions involved, together with the [easily verified] fact that every *surjective* endomorphism of $\mathbb{Z}$ is an *isomorphism*. The assertion that the surjection α is *CPU-preserving* follows immediately from Remark 1.3.1, together with the [easily verified] fact that if $\kappa({}^\circ\mathfrak{p})^\times$ is *isomorphic* to $\kappa({}^\bullet\mathfrak{p})^\times$, then it holds that $\mathfrak{c}({}^\circ\mathfrak{p}) = \mathfrak{c}({}^\bullet\mathfrak{p})$. This completes the proof of Lemma 1.5. □

LEMMA 1.6. — *Let $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ be a map of sets and α, $\beta\colon {}^\circ k^\times \to {}^\bullet k^\times$ homomorphisms of groups. Suppose that α and β are* **ϕ-PU-preserving** [*cf. Definition* 1.3, (i)]. *Then the homomorphism $\alpha \cdot \beta\colon {}^\circ k^\times \to {}^\bullet k^\times$ obtained by forming the product of α and β [i.e., the homomorphism ${}^\circ k^\times \to {}^\bullet k^\times$ given by mapping $x \in {}^\circ k^\times$ to $\alpha(x)\cdot\beta(x) \in {}^\bullet k^\times$] is* **$\phi$-PU-preserving**.

PROOF. — This follows immediately from the various definitions involved. □

REMARK 1.6.1. — In the situation of Lemma 1.6:

(i) In general, the product of two *ϕ-SPU-preserving* [cf. Definition 1.3, (i)] homomorphisms is *not ϕ-SPU-preserving*. Indeed, although the identity automorphism $\mathrm{id}_{\mathbb{Q}^\times}$ of $\mathbb{Q}^\times$ is $\mathrm{id}_{\mathfrak{Primes}}$-*SPU-preserving* [cf. Remark 1.1.1], [one verifies easily that] the product of two $\mathrm{id}_{\mathbb{Q}^\times}$ [i.e., the endomorphism of $\mathbb{Q}^\times$ given by mapping $x \in \mathbb{Q}^\times$ to $x^2 \in \mathbb{Q}^\times$] is *not* $\mathrm{id}_{\mathfrak{Primes}}$-*SPU-preserving*.

(ii) Moreover, in general, the product of *CPU-preserving* [cf. Definition 1.3, (ii)] homomorphisms is *not CPU-preserving*. Indeed, suppose that k is *Galois* over $\mathbb{Q}$. Then it follows from Lemma 1.4 that the automorphism $g^\times$ of $k^\times$ determined by an element $g \in \mathrm{Gal}(k/\mathbb{Q})$ of $\mathrm{Gal}(k/\mathbb{Q})$ is *CPU-preserving*. Write Nm of all such automorphisms $g^\times$. [Thus, Nm is the composite of the *norm map* $k^\times \to \mathbb{Q}^\times$ and the natural inclusion $\mathbb{Q}^\times \hookrightarrow k^\times$]. Assume that the difference $\delta\colon k^\times \to k^\times$ of Nm and the endomorphism of $k^\times$ given by mapping $x \in k^\times$ to $x^{[k:\mathbb{Q}]} \in k^\times$ is *CPU-preserving*. Then one verifies immediately that the restriction of δ to the subgroup $\mathbb{Q}^\times \subseteq k^\times$ is *trivial*. Thus, it follows immediately from Proposition 2.4, (i), below that we obtain a *contradiction*.

DEFINITION 1.7. — Let $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ be a map of sets. Then we shall write

$$\mathrm{Hom}({}^\circ k^\times, {}^\bullet k^\times)$$

for the [abelian] group consisting of homomorphisms of groups ${}^\circ k^\times \to {}^\bullet k^\times$ and

$$\mathrm{Hom}^{\phi\text{-PU}}({}^\circ k^\times, {}^\bullet k^\times) \subseteq \mathrm{Hom}({}^\circ k^\times, {}^\bullet k^\times)$$

for the subgroup [cf. Lemma 1.6] of *ϕ-PU-preserving* homomorphisms ${}^\circ k^\times \to {}^\bullet k^\times$.

LEMMA 1.8. — *Let $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ be a map of sets. Then the homomorphism of groups*

$$\mathrm{Hom}^{\phi\text{-PU}}({}^\circ k^\times, {}^\bullet k^\times) \longrightarrow \mathrm{Hom}({}^\circ\mathbb{Q}^\times, {}^\bullet k^\times)$$

[*cf. Definition* 1.7] *induced by the natural inclusion* ${}^\circ\mathbb{Q}^\times \hookrightarrow {}^\circ k^\times$ **factors** *through the subgroup* $\mathrm{Hom}^{(\mathfrak{c}\circ\phi)\text{-PU}}({}^\circ\mathbb{Q}^\times, {}^\bullet k^\times) \subseteq \mathrm{Hom}({}^\circ\mathbb{Q}^\times, {}^\bullet k^\times)$ [*cf. Remark* 1.1.1]*. In particular, we obtain a homomorphism of groups*

$$\mathrm{Hom}^{\phi\text{-PU}}({}^\circ k^\times, {}^\bullet k^\times) \longrightarrow \mathrm{Hom}^{(\mathfrak{c}\circ\phi)\text{-PU}}({}^\circ\mathbb{Q}^\times, {}^\bullet k^\times)\,.$$

PROOF. — This follows immediately from the various definitions involved. $\square$

2. FIELD-THEORETICITY FOR CERTAIN PU-PRESERVING HOMOMORPHISMS

In the present §2, we prove the *field-theoreticity* for certain *PU-preserving* homomorphisms [cf. Theorem 2.5 below]. We maintain the notation of the preceding §1.

LEMMA 2.1. — *Let $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ be a map of sets, n a positive integer, and $x_1, \ldots, x_n \in {}^\circ k^\times$ elements of ${}^\circ k^\times$. Suppose that the image of the composite ${}^\bullet\mathcal{V} \stackrel{\phi}{\to} {}^\circ\mathcal{V} \stackrel{\mathfrak{c}}{\to} \mathfrak{Primes}$ is of* **density one***. Then the subset $S[\phi; x_1, \ldots, x_n] \subseteq {}^\bullet\mathcal{V}$ consisting of maximal ideals ${}^\bullet\mathfrak{p} \in {}^\bullet\mathcal{V}$ of ${}^\bullet\mathfrak{o}$ that satisfy the following condition is* **infinite***: If we write ${}^\circ\mathfrak{p} \stackrel{\mathrm{def}}{=} \phi({}^\bullet\mathfrak{p}) \in {}^\circ\mathcal{V}$, then $x_i \in \mathrm{Ker}(\mathrm{ord}_{{}^\circ\mathfrak{p}})$ for each $i \in \{1, \ldots, n\}$, and, moreover, $\sharp\kappa({}^\circ\mathfrak{p}) = \mathfrak{c}({}^\circ\mathfrak{p})$.*

PROOF. — Let us observe that one verifies immediately that, in order to verify Lemma 2.1, it suffices to verify that the set of prime numbers $p \in \mathfrak{Primes}$ that *split completely* in the finite extension ${}^\circ k/{}^\circ\mathbb{Q}$ contains a subset of $\mathfrak{Primes}$ of *positive density*. On the other hand, this follows immediately, by considering the *Galois closure* of ${}^\circ k/{}^\circ\mathbb{Q}$, from *Čhebotarev's density theorem*. This completes the proof of Lemma 2.1. $\square$

LEMMA 2.2. — *For $p \in \mathfrak{Primes}$, write $\mathrm{ord}_p\colon \mathbb{Q}^\times \twoheadrightarrow \mathbb{Z}$ for the surjective p-adic valuation. Let x, $y \in \mathbb{Q}^\times$ be such that $y \notin \{1, -1\}$. Then the subset $S_{x,\langle y\rangle} \subseteq \mathfrak{Primes}$ consisting of prime numbers $p \in \mathfrak{Primes}$ that satisfy the following condition is* **infinite***: x, $y \in \mathrm{Ker}(\mathrm{ord}_p)$, and, moreover, the image of x in $\mathbb{F}_p^\times$ is* **contained** *in the subgroup of $\mathbb{F}_p^\times$ generated by the image of y in $\mathbb{F}_p^\times$.*

PROOF. — This follows from [the argument given in the proof of] [2], Theorem 1. For the reader's convenience [and, moreover, in order to make it clear that the argument given in the proof of [2], Theorem 1, works under our assumption that "$y \notin \{1, -1\}$"], however, we review the argument as follows:

Let us first observe that since $y \notin \{1, -1\}$, it is immediate that, to verify Lemma 2.2, by replacing y by y^{-1} if necessary, we may assume without loss of generality that the absolute value $|y|$ of y is *greater than one*. Write (x_1, x_2), (y_1, y_2) for the [uniquely determined] pairs of nonzero rational integers such that $x_1\mathbb{Z} + x_2\mathbb{Z} = \mathbb{Z}$; $y_1\mathbb{Z} + y_2\mathbb{Z} = \mathbb{Z}$; x_2, $y_2 > 0$; $x = x_1/x_2$; $y = y_1/y_2$. For each nonnegative integer n, write $a_n \stackrel{\text{def}}{=} x_1 \cdot y_2^n - x_2 \cdot y_1^n$. Now if $a_n = 0$ for some n, then Lemma 2.2 is immediate. Thus, we may assume without loss of generality that $a_n \neq 0$ for every n. Next, let us observe that one verifies easily that $S_{x,\langle y\rangle}$ *coincides* with the set of prime numbers $p \in \mathfrak{Primes}$ such that x, $y \in \mathrm{Ker}(\mathrm{ord}_p)$ but $a_n \notin \mathrm{Ker}(\mathrm{ord}_p)$ for some n. To verify Lemma 2.2, assume that $S_{x,\langle y\rangle}$ is *finite*. Write $n_0 \stackrel{\text{def}}{=} \sharp\big(\mathbb{Z}/(\prod_{p\in S_{x,\langle y\rangle}} p^{\mathrm{ord}_p(a_0)+1})\mathbb{Z}\big)^{\times}$. [Thus, one verifies easily that, for every $p \in S_{x,\langle y\rangle}$ and $z \in \mathbb{Q}^{\times}$, if $z \in \mathrm{Ker}(\mathrm{ord}_p)$, then $z^{n_0} \equiv 1 \pmod{p^{\mathrm{ord}_p(a_0)+1}}$.]

Now I claim that the following assertion holds:

> Claim 2.2.A: For each nonnegative integer n and $p \in S_{x,\langle y\rangle}$, it holds that $\mathrm{ord}_p(a_{n_0\cdot n}) \leq \mathrm{ord}_p(a_0)$.

Indeed, let us first observe that since $y \in \mathrm{Ker}(\mathrm{ord}_p)$, it holds that y_1, $y_2 \in \mathrm{Ker}(\mathrm{ord}_p)$, which thus implies that $y_1^{n_0}$, $y_2^{n_0} \equiv 1 \pmod{p^{\mathrm{ord}_p(a_0)+1}}$ [cf. the discussion at the final portion of the preceding paragraph]. Thus, we conclude that $a_{n_0\cdot n} - a_0 = x_1 \cdot (y_2^{n_0\cdot n} - 1) - x_2 \cdot (y_1^{n_0\cdot n} - 1) \equiv 0 \pmod{p^{\mathrm{ord}_p(a_0)+1}}$, i.e., $\mathrm{ord}_p(a_0) < \mathrm{ord}_p(a_{n_0\cdot n} - a_0)$. In particular, it holds that $\mathrm{ord}_p(a_{n_0\cdot n}) \leq \mathrm{ord}_p(a_0)$, as desired. This completes the proof of Claim 2.2.A.

Next, let us observe that one verifies immediately from Claim 2.2.A that $|a_{n_0\cdot n}| \leq |a_0 \cdot x_1 \cdot x_2|$ for sufficiently large n. Thus, since $|y|^n - |x| \leq |x - y^n| = |a_n|/|x_2 \cdot y_2^n| \leq |a_n|$, and $1 < |y|$, we obtain a *contradiction*. This completes the proof of Lemma 2.2. $\square$

REMARK 2.2.1. — If, in the situation of Lemma 2.2, one omits our assumption that "$y \notin \{1, -1\}$", then the conclusion no longer holds. More precisely, for $x \in \mathbb{Q}^{\times}$ and $y \in \{1, -1\}$, it holds that the set "$S_{x,\langle y\rangle}$" discussed in Lemma 2.2 is *infinite* if and only if $(x, y) \in \{(1, 1), (1, -1), (-1, -1)\}$. Indeed, the *sufficiency* is immediate. To verify the *necessity*, let us observe that since $1^2 = (-1)^2 = 1$, it holds that $x^2 \equiv 1 \pmod{p}$ for every $p \in S_{x,\langle y\rangle}$. Thus, since $S_{x,\langle y\rangle}$ is *infinite*, we conclude that $x^2 = 1$. In particular, since [one verifies easily that] the set "$S_{x,\langle y\rangle}$" that occurs in the case where we take the "(x, y)" to be $(-1, 1)$ *coincides* with $\{2\}$ [hence *finite*], the *necessity* under consideration follows.

LEMMA 2.3. — *Let $x \in k^{\times}$ be an element of $k^{\times}$. Then it holds that $x \in \mathbb{Q}^{\times}$ if and only if $x^{\mathfrak{c}(\mathfrak{p})-1} \in 1 + \mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$ for all but finitely many $\mathfrak{p} \in \mathcal{V}$.*

PROOF. — Let us first observe that one verifies easily that the condition that $x^{\mathfrak{c}(\mathfrak{p})-1} \in 1 + \mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$ implies that $x \in \mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}})$. Thus, one verifies immediately that the condition that $x^{\mathfrak{c}(\mathfrak{p})-1} \in 1 + \mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$ is *equivalent* to the condition that $x \in \mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}})$, and, moreover, the image of $x \in \mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}})$ in $\mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}})/(1+\mathfrak{p}\mathfrak{o}_{\mathfrak{p}})$ is *annihilated by* $\mathfrak{c}(\mathfrak{p}) - 1$, i.e., that the image of $x \in \mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}})$ in $\mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}})/(1+\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}) \xrightarrow{\sim} \kappa(\mathfrak{p})^{\times}$ is *contained in the prime subfield* [i.e., $\simeq \mathbb{Z}/\mathfrak{c}(\mathfrak{p})\mathbb{Z}$] of $\kappa(\mathfrak{p})$. Thus, Lemma 2.3 follows immediately from *Čhebotarev's density theorem*. This completes the proof of Lemma 2.3. $\square$

PROPOSITION 2.4. — *Let $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ be a map of sets. Then the following hold:*

(i) *Suppose that the image of the composite ${}^{\bullet}\mathcal{V} \xrightarrow{\phi} {}^{\circ}\mathcal{V} \xrightarrow{\mathfrak{c}} \mathfrak{Primes}$ is of* **density one**. *Then the homomorphism of groups*

$$\mathrm{Hom}^{\phi\text{-PU}}({}^{\circ}k^{\times}, {}^{\bullet}k^{\times}) \longrightarrow \mathrm{Hom}^{(\mathfrak{c}\circ\phi)\text{-PU}}({}^{\circ}\mathbb{Q}^{\times}, {}^{\bullet}k^{\times})$$

of Lemma 1.8 *is* **injective**.

(ii) *Suppose, moreover, that the image of the composite ${}^{\bullet}\mathcal{V} \xrightarrow{\phi} {}^{\circ}\mathcal{V} \xrightarrow{\mathfrak{c}} \mathfrak{Primes}$ is* **cofinite** [*i.e., its complement in $\mathfrak{Primes}$ is* **finite**]. *Let ${}^{\circ}J \subseteq {}^{\circ}\mathbb{Q}^{\times}$ be an* **infinite** *subgroup of ${}^{\circ}\mathbb{Q}^{\times}$. Write $\mathrm{Hom}({}^{\circ}J, {}^{\bullet}k^{\times})$ for the* [*abelian*] *group consisting of homomorphisms of groups ${}^{\circ}J^{\times} \to {}^{\bullet}k^{\times}$. Then the homomorphism of groups*

$$\mathrm{Hom}^{\phi\text{-PU}}({}^{\circ}k^{\times}, {}^{\bullet}k^{\times}) \longrightarrow \mathrm{Hom}({}^{\circ}J, {}^{\bullet}k^{\times})$$

induced by the natural inclusion ${}^{\circ}J \hookrightarrow {}^{\circ}k^{\times}$ is **injective**.

(iii) *The homomorphism of groups*

$$\mathrm{Hom}^{\mathrm{id}_{\mathfrak{Primes}}\text{-PU}}({}^{\circ}\mathbb{Q}^{\times}, {}^{\bullet}\mathbb{Q}^{\times}) \longrightarrow \mathrm{Hom}^{\mathfrak{c}\text{-PU}}({}^{\circ}\mathbb{Q}^{\times}, {}^{\bullet}k^{\times})$$

induced by the natural inclusion ${}^{\bullet}\mathbb{Q}^{\times} \hookrightarrow {}^{\bullet}k^{\times}$ is **bijective**.

PROOF. — First, we verify assertion (i). Let $\alpha\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ be a *ϕ-PU-preserving* homomorphism such that $\alpha({}^{\circ}\mathbb{Q}^{\times}) = \{1\}$. To verify that $\alpha({}^{\circ}k^{\times}) = \{1\}$, let us take $x \in {}^{\circ}k^{\times}$ and ${}^{\bullet}\mathfrak{p} \in S[\phi; x]$ [cf. the notation of Lemma 2.1] that is *not PU-exceptional* for (α, ϕ) [cf. Definition 1.3, (i)]. Write ${}^{\circ}\mathfrak{p} \stackrel{\text{def}}{=} \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$ and $\alpha_{\mathfrak{p}}\colon \kappa({}^{\circ}\mathfrak{p})^{\times} \to \kappa({}^{\bullet}\mathfrak{p})^{\times}$ for the homomorphism induced by α [cf. Lemma 1.5, (i)]. Then since $\sharp\kappa({}^{\circ}\mathfrak{p}) = \mathfrak{c}({}^{\circ}\mathfrak{p})$ [cf. the definition of $S[\phi; x]$ in Lemma 2.1], and $\alpha({}^{\circ}\mathbb{Q}^{\times}) = \{1\}$, one verifies easily that $\alpha_{\mathfrak{p}}(\kappa({}^{\circ}\mathfrak{p})^{\times}) = \{1\}$, which thus implies that

$$\alpha(x) \pmod{{}^{\bullet}\mathfrak{p}} = \alpha_{\mathfrak{p}}(x \pmod{{}^{\circ}\mathfrak{p}}) = 1\,.$$

Thus, by allowing ${}^{\bullet}\mathfrak{p}$ to *vary*, it follows immediately from Lemma 2.1 that $\alpha(x) = 1$. This completes the proof of assertion (i).

Next, we verify assertion (ii). Let us first observe that it follows from assertion (i) that, to verify assertion (ii), by replacing ${}^{\circ}k$ by ${}^{\circ}\mathbb{Q}$, we may assume without loss of generality that ${}^{\circ}k = {}^{\circ}\mathbb{Q}$. Let $\alpha\colon {}^{\circ}k^{\times} = {}^{\circ}\mathbb{Q}^{\times} \to {}^{\bullet}k^{\times}$ be a *ϕ-PU-preserving* homomorphism such that $\alpha({}^{\circ}J) = \{1\}$. To verify that $\alpha({}^{\circ}k^{\times}) = \{1\}$, let us take $x \in {}^{\circ}k^{\times} = {}^{\circ}\mathbb{Q}^{\times}$ and $y \in {}^{\circ}J \setminus ({}^{\circ}J \cap \{1, -1\})$. Then let us observe that it follows immediately from Lemma 2.2, together with our assumption that the image of $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V} = \mathfrak{Primes}$ is *cofinite*, that the subset $T \subseteq {}^{\bullet}\mathcal{V}$ consisting of maximal ideals ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$ of ${}^{\bullet}\mathfrak{o}$ that satisfy the following condition is *infinite*: If we write ${}^{\circ}\mathfrak{p} \stackrel{\text{def}}{=} \phi({}^{\bullet}\mathfrak{p})$, then

- ${}^{\bullet}\mathfrak{p}$ is *not PU-exceptional* for (α, ϕ),
- x, $y \in \mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})$, and
- the image of x in $\mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})/(1+{}^{\circ}\mathfrak{p}\mathfrak{o}_{{}^{\circ}\mathfrak{p}})$ is *contained* in the subgroup of $\mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})/(1+{}^{\circ}\mathfrak{p}\mathfrak{o}_{{}^{\circ}\mathfrak{p}})$ generated by the image of y in $\mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})/(1 + {}^{\circ}\mathfrak{p}\mathfrak{o}_{{}^{\circ}\mathfrak{p}})$.

Let ${}^{\bullet}\mathfrak{p} \in T$ be an element of T. Then it follows immediately from the definition of T that there exists an integer n such that $x \cdot y^{n} \in 1 + {}^{\circ}\mathfrak{p}\mathfrak{o}_{{}^{\circ}\mathfrak{p}}$. Thus, since [we have assumed that] $\alpha({}^{\circ}J) = \{1\}$, it follows that $\alpha(x) = \alpha(x \cdot y^{n}) \in 1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}$. In particular, since T is *infinite*, we conclude that $\alpha(x) \in \bigcap_{{}^\bullet\mathfrak{p}\in T}(1 + {}^\bullet\mathfrak{p}{}^\bullet\mathfrak{o}_{{}^\bullet\mathfrak{p}}) = \{1\}$, i.e., $\alpha(x) = 1$. This completes the proof of assertion (ii).

Finally, we verify assertion (iii). The *injectivity* of the homomorphism under consideration follows immediately from the *injectivity* of the natural inclusion ${}^\bullet\mathbb{Q}^\times \hookrightarrow {}^\bullet k^\times$. Next, to verify the *surjectivity* of the homomorphism under consideration, let us take a $\mathfrak{c}$-*PU-preserving* homomorphism $\alpha\colon {}^\circ\mathbb{Q}^\times \to {}^\bullet k^\times$. Then it follows immediately from Lemma 2.3 that α *factors* through the subgroup ${}^\bullet\mathbb{Q}^\times \subseteq {}^\bullet k^\times$ of ${}^\bullet k^\times$; thus, we obtain a homomorphism ${}^\circ\mathbb{Q}^\times \to {}^\bullet\mathbb{Q}^\times$. On the other hand, since α is $\mathfrak{c}$-*PU-preserving*, one verifies immediately from Lemma 1.4 that this homomorphism ${}^\circ\mathbb{Q}^\times \to {}^\bullet\mathbb{Q}^\times$ is $\mathrm{id}_{\mathfrak{Primes}}$-*PU-preserving*. This completes the proof of assertion (iii). □

REMARK 2.4.1. — If, in the situation of Proposition 2.4, (ii), one replaces our assumption that "${}^\circ J$ is *infinite*" by the assumption that "${}^\circ J$ is *nontrivial*", then the conclusion no longer holds. Indeed, one verifies easily that the *distinct* two endomorphisms of $\mathbb{Q}^\times$ obtained by mapping $x \in \mathbb{Q}^\times$ to $x \in \mathbb{Q}^\times$, $x^3 \in \mathbb{Q}^\times$, respectively, are *contained* in $\mathrm{Hom}^{\mathrm{id}_{\mathfrak{Primes}}\text{-PU}}(\mathbb{Q}^\times, \mathbb{Q}^\times)$ and *coincide* on the *nontrivial* subgroup $\{1, -1\} \subseteq \mathbb{Q}^\times$.

THEOREM 2.5. — *For* $\Box \in \{\circ, \bullet\}$, *let* ${}^\Box k$ *be a* **number field** [*i.e., a finite extension of the field of rational numbers*]*; write* ${}^\Box\mathcal{V}$ *for the set of maximal ideals of the ring of integers of* ${}^\Box k$ [*i.e., the set of nonarchimedean primes of* ${}^\Box k$] *and* ${}^\Box\mathbb{Q} \subseteq {}^\Box k$ *for the* [*uniquely determined*] *subfield of* ${}^\Box k$ *that is isomorphic to the field of rational numbers. Let*

$$\alpha\colon {}^\circ k^\times \longrightarrow {}^\bullet k^\times$$

be a homomorphism between the multiplicative groups of ${}^\circ k$, ${}^\bullet k$. *Then the following conditions are equivalent:*

(1) *The homomorphism* α *arises from a* **homomorphism of fields** ${}^\circ k \to {}^\bullet k$.

(2) *The homomorphism* α *is* **CPU-preserving** [*cf. Definition* 1.3, (ii)], *and, moreover, there exists an* $x \in \mathbb{Q}^\times \setminus \mathbb{Z}^\times$ *such that the "x" in* ${}^\circ k$ *maps, via* α, *to the "x" in* ${}^\bullet k$.

(3) *The homomorphism* α *is* **PU-preserving** [*cf. Definition* 1.3, (i)], *and, moreover, the restriction* ${}^\circ\mathbb{Q}^\times \to {}^\bullet k^\times$ *of* α *to* ${}^\circ\mathbb{Q}^\times \subseteq {}^\circ k^\times$ *arises from a* **homomorphism of fields** ${}^\circ\mathbb{Q} \to {}^\bullet k$.

PROOF. — The implication (1) ⇒ (2) follows immediately from Lemma 1.4, together with the various definitions involved. Next, we verify the implication (2) ⇒ (3). Suppose that condition (2) is satisfied. Let us first observe that it follows from Lemma 1.8 that, to verify the implication under consideration, by replacing ${}^\circ k$ by ${}^\circ\mathbb{Q}$, we may assume without loss of generality that ${}^\circ k = {}^\circ\mathbb{Q}$. Next, let us observe that it follows from Proposition 2.4, (iii), that, to verify the implication under consideration, by replacing ${}^\bullet k$ by ${}^\bullet\mathbb{Q}$, we may assume without loss of generality that ${}^\bullet k = {}^\bullet\mathbb{Q}$. Then since the isomorphism ${}^\circ\mathbb{Q}^\times \xrightarrow{\sim} {}^\bullet\mathbb{Q}^\times$ determined by the *identity automorphism* of $\mathbb{Q}^\times$ is *contained* in $\mathrm{Hom}^{\mathrm{id}_{\mathfrak{Primes}}\text{-PU}}({}^\circ\mathbb{Q}^\times, {}^\bullet\mathbb{Q}^\times)$, the implication under consideration follows immediately from Proposition 2.4, (ii). This completes the proof of the implication (2) ⇒ (3).

Finally, we verify the implication (3) ⇒ (1). Suppose that condition (3) is satisfied. Let $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ be such that α is ϕ-*PU-preserving*. Now let us observe that one verifies easily that, to verify the implication (3) $\Rightarrow$ (1), it suffices to verify that the following assertion holds:

> Claim 2.5.A: For x, $y \in {}^{\circ}k^{\times}$, if $x + y = 0$ (respectively, $x + y \neq 0$), then $\alpha(x) + \alpha(y) = 0$ (respectively, $\alpha(x + y) = \alpha(x) + \alpha(y)$).

The remainder of the proof of the implication (3) $\Rightarrow$ (1) is devoted to verifying Claim 2.5.A.

Now let us observe that since the restriction $\alpha|_{{}^{\circ}\mathbb{Q}^{\times}} : {}^{\circ}\mathbb{Q}^{\times} \to {}^{\bullet}k^{\times}$ arises from a *homomorphism of fields* ${}^{\circ}\mathbb{Q} \to {}^{\bullet}k$, one verifies easily that the "-1" in ${}^{\circ}k^{\times}$ maps, via α, to the "-1" in ${}^{\bullet}k^{\times}$; in particular, if $x + y = 0$ [i.e., $y = -x$], then $\alpha(x) + \alpha(y) = 0$ [i.e., $\alpha(y) = -\alpha(x)$]. Thus, we may assume without loss of generality that $x + y \neq 0$. Then, to complete the verification of Claim 2.5.A, I claim that the following assertion holds:

> Claim 2.5.B: Let ${}^{\bullet}\mathfrak{p} \in S[\phi; x, y, x + y]$ [cf. the notation of Lemma 2.1] be such that ${}^{\bullet}\mathfrak{p}$ is *not PU-exceptional* for (α, ϕ) [cf. Definition 1.3, (i)]. Then it holds that
>
> $$\alpha(x + y) \pmod{1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}} = \alpha(x) + \alpha(y) \pmod{1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}}.$$

Indeed, write ${}^{\circ}\mathfrak{p} \stackrel{\text{def}}{=} \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$. Then let us observe that since $\sharp\kappa({}^{\circ}\mathfrak{p}) = \mathfrak{c}({}^{\circ}\mathfrak{p})$, there exist $x_{\mathbb{Q}}$, $y_{\mathbb{Q}} \in {}^{\circ}\mathbb{Q}^{\times}$ such that $x_{\mathbb{Q}}$, $y_{\mathbb{Q}}$, $x_{\mathbb{Q}} + y_{\mathbb{Q}} \in \mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})$, and, moreover, the images of $x_{\mathbb{Q}}$, $y_{\mathbb{Q}}$ in $\mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})/(1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}})$ *coincide* with the images of x, y in $\mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})/(1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}})$, respectively. Thus, the following equalities hold:

$$\begin{aligned}
\alpha(x + y) \pmod{1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}} &= \alpha_{\mathfrak{p}}(x + y \pmod{1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}}}) \\
&= \alpha_{\mathfrak{p}}(x_{\mathbb{Q}} + y_{\mathbb{Q}} \pmod{1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}}}) \\
&= \alpha(x_{\mathbb{Q}} + y_{\mathbb{Q}}) \pmod{1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}} \\
&= \alpha(x_{\mathbb{Q}}) + \alpha(y_{\mathbb{Q}}) \pmod{1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}} \\
&= \alpha_{\mathfrak{p}}(x_{\mathbb{Q}} \pmod{1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}}}) + \alpha_{\mathfrak{p}}(y_{\mathbb{Q}} \pmod{1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}}}) \\
&= \alpha_{\mathfrak{p}}(x \pmod{1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}}}) + \alpha_{\mathfrak{p}}(y \pmod{1 + {}^{\circ}\mathfrak{p}{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}}}) \\
&= \alpha(x) \pmod{1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}} + \alpha(y) \pmod{1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}} \\
&= \alpha(x) + \alpha(y) \pmod{1 + {}^{\bullet}\mathfrak{p}{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}}}
\end{aligned}$$

— where we write $\alpha_{\mathfrak{p}} : \kappa({}^{\circ}\mathfrak{p})^{\times} \to \kappa({}^{\bullet}\mathfrak{p})^{\times}$ for the homomorphism induced by α [cf. Lemma 1.5, (i)]; the first, third, fifth, and seventh equalities follow immediately from the definition of $\alpha_{\mathfrak{p}}$; the second and sixth equalities follow immediately from the choices of $x_{\mathbb{Q}}$, $y_{\mathbb{Q}}$; the fourth equality follows immediately from our assumption that $\alpha|_{{}^{\circ}\mathbb{Q}^{\times}}$ arises from a *homomorphism of fields* ${}^{\circ}\mathbb{Q} \to {}^{\bullet}k$; the eighth equality follows immediately from the various definitions involved. This completes the proof of Claim 2.5.B.

Thus, by allowing ${}^{\bullet}\mathfrak{p}$ to *vary*, it follows immediately from Claim 2.5.B, together with Lemma 2.1, that Claim 2.5.A holds. This completes the proof of Claim 2.5.A, hence also of the implication (3) $\Rightarrow$ (1). $\square$

REMARK 2.5.1. — If, in the situation of Theorem 2.5, one replaces "$\mathbb{Q}^{\times} \setminus \mathbb{Z}^{\times}$" in condition (2) by either "$\mathbb{Q}^{\times}$" or "$\mathbb{Q}^{\times} \setminus \{1\}$", then the conclusion no longer holds. Indeed, one verifies easily that the automorphism of $\mathbb{Q}^\times$ obtained by mapping $x \in \mathbb{Q}^\times$ to $x^{-1} \in \mathbb{Q}^\times$ is *CPU-preserving*, maps $-1 \in \mathbb{Q}^\times$ to $-1 \in \mathbb{Q}^\times$, but does *not arise from a homomorphism of fields* $\mathbb{Q} \to \mathbb{Q}$.

3. Uchida's Lemma for Number Fields

In the present §3, we prove analogues of *Uchida's lemma* reviewed in the Introduction in the case of *number fields* [cf. Theorem 3.1; Corollary 3.3 below].

THEOREM 3.1. — *For $\square \in \{\circ, \bullet\}$, let ${}^\square k$ be a* **number field** *[i.e., a finite extension of the field of rational numbers]; write ${}^\square \mathfrak{o} \subseteq {}^\square k$ for the ring of integers of ${}^\square k$ and ${}^\square \mathcal{V}$ for the set of maximal ideals of ${}^\square \mathfrak{o}$ [i.e., the set of nonarchimedean primes of ${}^\square k$]. Write $\mathfrak{Primes}$ for the set of all prime numbers. Let*

$$\alpha \colon {}^\circ k^\times \longrightarrow {}^\bullet k^\times$$

be a homomorphism between the multiplicative groups of ${}^\circ k$, ${}^\bullet k$. Then the following conditions are equivalent:

(1) *The homomorphism α arises from a* **homomorphism of fields** *${}^\circ k \to {}^\bullet k$.*

(2) *There exists a map $\phi \colon {}^\bullet \mathcal{V} \to {}^\circ \mathcal{V}$ over $\mathfrak{Primes}$ [relative to, for each $\square \in \{\circ, \bullet\}$, the map ${}^\square \mathcal{V} \to \mathfrak{Primes}$ obtained by mapping ${}^\square \mathfrak{p} \in {}^\square \mathcal{V}$ to the residue characteristic of ${}^\square \mathfrak{p}$] such that, for ${}^\bullet \mathfrak{p} \in {}^\bullet \mathcal{V}$, if we write ${}^\circ \mathfrak{p} \stackrel{\mathrm{def}}{=} \phi({}^\bullet \mathfrak{p}) \in {}^\circ \mathcal{V}$, then the following hold:*

(a) *For $\square \in \{\circ, \bullet\}$, if we write $\mathrm{ord}_{{}^\square \mathfrak{p}} \colon {}^\square k^\times \twoheadrightarrow \mathbb{Z}$ for the [uniquely determined] surjective valuation of ${}^\square k$ associated to ${}^\square \mathfrak{p}$, then it holds that*

$$\mathrm{ord}_{{}^\circ \mathfrak{p}} = \mathrm{ord}_{{}^\bullet \mathfrak{p}} \circ \alpha$$

for **infinitely many** *${}^\bullet \mathfrak{p} \in {}^\bullet \mathcal{V}$.*

(b) *For $\square \in \{\circ, \bullet\}$, if we write ${}^\square \mathfrak{o}_{{}^\square \mathfrak{p}} \subseteq {}^\square k$ for the localization of ${}^\square \mathfrak{o}$ at the maximal ideal ${}^\square \mathfrak{p} \subseteq {}^\square \mathfrak{o}$, then it holds that*

$$1 + {}^\circ \mathfrak{p} {}^\circ \mathfrak{o}_{{}^\circ \mathfrak{p}} \subseteq \alpha^{-1}(1 + {}^\bullet \mathfrak{p} {}^\bullet \mathfrak{o}_{{}^\bullet \mathfrak{p}})$$

for **all but finitely many** *${}^\bullet \mathfrak{p} \in {}^\bullet \mathcal{V}$.*

PROOF. — The implication (1) $\Rightarrow$ (2) follows immediately from Lemma 1.4, together with the well-known fact that the finite extension ${}^\bullet k / {}^\circ k$ [determined by the homomorphism of fields ${}^\circ k \to {}^\bullet k$] is *unramified at all but finitely many nonarchimedean primes*. Next, we verify the implication (2) $\Rightarrow$ (1). Suppose that condition (2) is satisfied. Now since α is *CPU-preserving* [cf. conditions (b)], it follows from the equivalence (1) $\Leftrightarrow$ (2) of Theorem 2.5 that, to verify the implication (2) $\Rightarrow$ (1), it suffices to verify that the following assertion holds:

> Claim 3.1.A: There exists an $x \in \mathbb{Q}^\times \setminus \mathbb{Z}^\times$ such that the "x" in ${}^\circ k$ maps, via α, to the "x" in ${}^\bullet k$.

The remainder of the proof of the implication (2) $\Rightarrow$ (1) is devoted to verifying Claim 3.1.A.

Now let us observe that since α is *CPU-preserving* [cf. condition (b)], it follows immediately from Lemma 1.8, together with the well-known fact that the finite extension $^\circ k/^\circ\mathbb{Q}$ is *unramified at all but finitely many nonarchimedean primes*, that, to verify Claim 3.1.A, by replacing $^\circ k$ by $^\circ\mathbb{Q}$, we may assume without loss of generality that $^\circ k = {}^\circ\mathbb{Q}$. Next, let us observe that again by the fact that α is *CPU-preserving* [cf. condition (b)], it follows immediately from Proposition 2.4, (iii), that, by replacing $^\bullet k$ by $^\bullet\mathbb{Q}$, we may assume without loss of generality that $^\bullet k = {}^\bullet\mathbb{Q}$. In particular, one verifies immediately from Remark 1.1.1 that ϕ is the *identity automorphism* of $\mathfrak{Primes}$.

Let $S_{(\mathrm{b})} \subseteq \mathfrak{Primes}$ be a *cofinite* [i.e., its complement in $\mathfrak{Primes}$ is *finite*] subset of $\mathfrak{Primes}$ such that the displayed inclusion of condition (b) for $^\bullet\mathfrak{p} \in S_{(\mathrm{b})} \subseteq \mathfrak{Primes} = {}^\bullet\mathcal{V}$ holds and $S_{(\mathrm{a}),(\mathrm{b})} \subseteq S_{(\mathrm{b})}$ an *infinite* subset of $S_{(\mathrm{b})}$ such that the displayed equality of condition (a) for $^\bullet\mathfrak{p} \in S_{(\mathrm{a}),(\mathrm{b})} \subseteq \mathfrak{Primes} = {}^\bullet\mathcal{V}$ holds. Then it follows immediately from Lemma 1.5, (i), that, for each $^\bullet\mathfrak{p} \in S_{(\mathrm{b})}$, there exists a [uniquely determined] [not necessarily positive] integer $n_{^\bullet\mathfrak{p}}$ such that the equality

$$n_{^\bullet\mathfrak{p}} \cdot \mathrm{ord}_{^\circ\mathfrak{p}} = \mathrm{ord}_{^\bullet\mathfrak{p}} \circ \alpha$$

holds. [Thus, if $^\bullet\mathfrak{p} \in S_{(\mathrm{a}),(\mathrm{b})}$, then $n_{^\bullet\mathfrak{p}} = 1$.]

For $\square \in \{\circ, \bullet\}$ and $^\square\mathfrak{p} \in {}^\square\mathcal{V}$, write $J_{^\square\mathfrak{p}}\ (\simeq \mathbb{Z}) \subseteq {}^\square k^\times$ for the subgroup of $^\square k^\times$ generated by the [element of $^\square k^\times = {}^\square\mathbb{Q}^\times$ corresponding to the] residue characteristic $\mathfrak{c}(^\square\mathfrak{p})$ of $^\square\mathfrak{p}$ [i.e., $J_{^\square\mathfrak{p}} =$ "$\mathfrak{c}(^\square\mathfrak{p})^{\mathbb{Z}}$"]. Then one verifies easily that the various inclusions $J_{^\square\mathfrak{p}} \hookrightarrow {}^\square k^\times$ and the inclusion $^\square k^\times_{\mathrm{tor}} \hookrightarrow {}^\square k^\times$ [where we write $^\square k^\times_{\mathrm{tor}} \subseteq {}^\square k^\times$ for the *maximal torsion subgroup* of $^\square k^\times$, i.e., $^\square k^\times =$"$\{1, -1\}$"] determine an *isomorphism* of abelian groups

$$^\square k^\times_{\mathrm{tor}} \oplus \Big(\bigoplus_{^\square\mathfrak{p} \in {}^\square\mathcal{V}} J_{^\square\mathfrak{p}} \Big) \xrightarrow{\sim} {}^\square k^\times .$$

Write $\beta \colon {}^\circ k^\times \to {}^\bullet k^\times$ for the homomorphism defined as follows [cf. the above displayed isomorphism]:

- β maps the "-1" in $^\circ k^\times$ to the "-1" in $^\bullet k^\times$.
- If $^\bullet\mathfrak{p} \notin S_{(\mathrm{b})}$, then β maps the "$\mathfrak{c}(\phi(^\bullet\mathfrak{p}))$" in $^\circ k^\times$ to the "$\mathfrak{c}(^\bullet\mathfrak{p})$" in $^\bullet k^\times$.
- If $^\bullet\mathfrak{p} \in S_{(\mathrm{b})}$, then β maps the "$\mathfrak{c}(\phi(^\bullet\mathfrak{p}))$" in $^\circ k^\times$ to the "$\mathfrak{c}(^\bullet\mathfrak{p})^{n_{^\bullet\mathfrak{p}}}$" in $^\bullet k^\times$ [where we refer to the discussion at the final portion of the preceding paragraph concerning "$n_{^\bullet\mathfrak{p}}$"].

Write, moreover, $\gamma \stackrel{\mathrm{def}}{=} \alpha \cdot \beta^{-1} \colon {}^\circ k^\times \to {}^\bullet k^\times$ for the product of α and β^{-1}. Then one verifies immediately from the definition of β, together with the various definitions involved, that

(i) the composite

$$^\circ k^\times \xrightarrow{\gamma} {}^\bullet k^\times \xrightarrow{\bigoplus_{^\bullet\mathfrak{p} \in S_{(\mathrm{b})}} \mathrm{ord}_{^\bullet\mathfrak{p}}} \bigoplus_{^\bullet\mathfrak{p} \in S_{(\mathrm{b})}} \mathbb{Z}$$

is *trivial*, i.e., the homomorphism γ *factors* through the kernel $^\bullet k^\times_{\mathrm{tor}} \oplus \big(\bigoplus_{^\bullet\mathfrak{p} \notin S_{(\mathrm{b})}} J_{^\bullet\mathfrak{p}} \big) \subseteq {}^\bullet k^\times$ of $\bigoplus_{^\bullet\mathfrak{p} \in S_{(\mathrm{b})}} \mathrm{ord}_{^\bullet\mathfrak{p}}$, and, moreover,

(ii) the kernel $\mathrm{Ker}(\gamma) \subseteq {}^\circ k^\times$ of γ *coincides* with the subgroup of $^\circ k^\times$ consisting of elements $x \in {}^\circ k^\times$ such that $\alpha(x) = \beta(x)$.

Now let us observe that the kernel ${}^{\bullet}k^{\times}_{\mathrm{tor}} \oplus \left(\bigoplus_{{}^{\bullet}\mathfrak{p} \notin S_{(\mathrm{b})}} J_{{}^{\bullet}\mathfrak{p}}\right) \subseteq {}^{\bullet}k^{\times}$ discussed in (i) is of *finite rank*, and $S_{(\mathrm{a}),(\mathrm{b})}$ is *infinite*. Thus, by considering the composite of the natural inclusion $\bigoplus_{{}^{\bullet}\mathfrak{p} \in S_{(\mathrm{a}),(\mathrm{b})}} J_{\phi({}^{\bullet}\mathfrak{p})} \hookrightarrow {}^{\circ}k^{\times}$ and the homomorphism γ, we conclude from (i), (ii), together with the various definitions involved, that there exists a *nontorsion* element $x \in (\bigoplus_{{}^{\bullet}\mathfrak{p} \in S_{(\mathrm{a}),(\mathrm{b})}} J_{\phi({}^{\bullet}\mathfrak{p})} \subseteq)\ {}^{\circ}k^{\times}$ such that $\alpha(x) = x$. This completes the proof of Claim 3.1.A, hence also of Theorem 3.1. □

COROLLARY 3.2. — *For* $\square \in \{\circ, \bullet\}$, *let* ${}^{\square}k$ *be a* **number field** [*i.e., a finite extension of the field of rational numbers*]. *Let*

$$\alpha\colon {}^{\circ}k^{\times} \twoheadrightarrow {}^{\bullet}k^{\times}$$

be a **surjection** *between the multiplicative groups of* ${}^{\circ}k$, ${}^{\bullet}k$. *Then it holds that either* α *or the composite* $(-)^{-1} \circ \alpha$ [*i.e., the surjection* ${}^{\circ}k^{\times} \twoheadrightarrow {}^{\bullet}k^{\times}$ *obtained by mapping* $x \in {}^{\circ}k^{\times}$ *to* $\alpha(x)^{-1} \in {}^{\bullet}k^{\times}$] *arises from an* **isomorphism of fields** ${}^{\circ}k \xrightarrow{\sim} {}^{\bullet}k$ *if and only if the surjection* α *is* **SPU-preserving** [*cf. Definition* 1.3, (i)].

PROOF. — The *necessity* follows from Lemma 1.4. Next, we verify the *sufficiency*. Suppose that α is *SPU-preserving*. Then one verifies immediately from Lemma 1.5, (ii), that either α or the composite $(-)^{-1} \circ \alpha$ satisfies condition (2) of the statement of Theorem 3.1. In particular, the *sufficiency* under consideration follows from Theorem 3.1. This completes the proof of Corollary 3.2. □

COROLLARY 3.3. — *For* $\square \in \{\circ, \bullet\}$, *let* ${}^{\square}k$ *be a* **number field** [*i.e., a finite extension of the field of rational numbers*]; *write* ${}^{\square}\mathfrak{o} \subseteq {}^{\square}k$ *for the ring of integers of* ${}^{\square}k$ *and* ${}^{\square}\mathcal{V}$ *for the set of maximal ideals of* ${}^{\square}\mathfrak{o}$ [*i.e., the set of nonarchimedean primes of* ${}^{\square}k$]. *Let*

$$\alpha\colon {}^{\circ}k^{\times} \twoheadrightarrow {}^{\bullet}k^{\times}$$

be a **surjection** *between the multiplicative groups of* ${}^{\circ}k$, ${}^{\bullet}k$. *Then the following conditions are equivalent:*

(1) *The surjection* α *arises from an* **isomorphism of fields** ${}^{\circ}k \xrightarrow{\sim} {}^{\bullet}k$.

(2) *There exists a map* $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ *such that, for* ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$, *if we write* ${}^{\circ}\mathfrak{p} \stackrel{\mathrm{def}}{=} \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, *then the following hold:*

(a) *For* $\square \in \{\circ, \bullet\}$, *if we write* $\mathrm{ord}_{{}^{\square}\mathfrak{p}}\colon {}^{\square}k^{\times} \twoheadrightarrow \mathbb{Z}$ *for the* [*uniquely determined*] *surjective valuation of* ${}^{\square}k$ *associated to* ${}^{\square}\mathfrak{p}$, *then there exist a maximal ideal* ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$ *of* ${}^{\bullet}\mathfrak{o}$ *and a* **positive** *integer* n *such that*

$$n \cdot \mathrm{ord}_{{}^{\circ}\mathfrak{p}} = \mathrm{ord}_{{}^{\bullet}\mathfrak{p}} \circ \alpha\,.$$

(b) *For* $\square \in \{\circ, \bullet\}$, *if we write* ${}^{\square}\mathfrak{o}_{{}^{\square}\mathfrak{p}}$ *for the localization of* ${}^{\square}\mathfrak{o}$ *at the maximal ideal* ${}^{\square}\mathfrak{p} \subseteq {}^{\square}\mathfrak{o}$, *then it holds that*

$$1 + {}^{\circ}\mathfrak{p}\,{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}} = \alpha^{-1}(1 + {}^{\bullet}\mathfrak{p}\,{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})$$

for all but finitely many ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$.

PROOF. — This follows immediately from Corollary 3.2, together with the various definitions involved. □

REMARK 3.3.1.

(i) The issue of recovering the additive structure in the case of *function fields* has been intensively studied by *M. Saïdi* and *A. Tamagawa* [cf., e.g., [3], §4; [4], §5]. Moreover, they considered not only *isomorphisms* [as in *Uchida's lemma* — cf. Introduction] but also suitable *homomorphisms* between multiplicative groups. In particular, the main results of the present paper may also be regarded as *analogues* in the case of *number fields* of the results of *Saïdi-Tamagawa*.

(ii) One may think that the proofs of the main results of the present paper are *similar* to the proof of *Uchida's lemma*, as well as the proofs of the results of Saïdi-Tamagawa discussed in (i) [cf., e.g., [4], Proposition 5.3], from the following point of view. That is to say, both the proofs consist of the following two steps:

(1) We first prove that the homomorphism under consideration between the multiplicative groups of the given global fields is *compatible* with the additive structures of the *residue fields at various primes involving*.

(2) By considering residue classes at various primes involving and applying the *compatibility* of (1), we conclude that the homomorphism under consideration between the multiplicative groups of the global fields is *compatible* with their additive structures.

(iii) In the case of *function fields*, the behaviors of *minimal functions* or *functions with unique poles* are discussed in order to perform the step (1) of (ii) [cf. the discussions of [3], §4; [4], §5; [7], §3]. On the other hand, in the case of *number fields*, to perform the step (1) of (ii), the behaviors of *elements of* $\mathbb{Q}^\times \setminus \mathbb{Z}^\times$ [in stead of such functions] are discussed [cf. the proof of Theorem 2.5].

REMARK 3.3.2.

(i) Let us recall that *Uchida's lemma* [cf. Introduction], as well as the results of Saïdi-Tamagawa discussed in Remark 3.3.1, (i) [cf., e.g., [4], Proposition 5.3], was studied in the context of the *anabelian geometry*. More precisely, in [7], *Uchida's lemma* was studied in order to prove that

> ($*$) every continuous isomorphism between the absolute Galois groups of the function fields of curves over finite fields arises from an isomorphism [of fields] between the original function fields.

Here, we note that an analogous result of the result ($*$) for *number fields* was already proved [cf. [6]].

(ii) On the other hand, one may find some *essential differences* between the proof [given in [7]] of the result ($*$) of (i) and the proof [given in [6]] of its analogous result for *number fields*. For instance, although the proof in the case of *function fields* is in a "*mono-anabelian fashion*" or "*algorithmic*", the proof in the case of *number fields* is in a "*bi-anabelian fashion*" or *not* "*algorithmic*" [cf., e.g., [1], Introduction, as well as [1], Remarks 1.9.5, 1.9.8].

(iii) Now let us recall the outline of the proof of the result ($*$) of (i) given in [7]. The proof given in [7] may be summarized as follows:

(1) First, we prove that a continuous isomorphism between the absolute Galois groups of the function fields of curves over finite fields determines a *bijection* between the sets of decomposition subgroups associated to primes.

(2) Next, by means of the *bijection* of (1), together with *class field theory*, we prove that the continuous isomorphism under consideration determines an isomorphism between the multiplicative groups of the original function fields which satisfies the condition [involving "$\mathrm{ord}_{\Box_x}$" and "$1 + \mathfrak{m}_{\Box_C, \Box_x}$"] in the statement of *Uchida's lemma* reviewed in the Introduction.

(3) Finally, by applying *Uchida's lemma*, we conclude that the isomorphism between the multiplicative groups of (2) determines an isomorphism [of fields] between the function fields.

Here, we note that an analogous result of (1) in this outline for *number fields* has been proved by *J. Neukirch*. Moreover, the main results of the present paper may be regarded as an analogue in the case of *number fields* of (3) in this outline.

(iv) However, by the difficulty arising from the *archimedean portions in the idele groups of number fields*, at the time of writing, the author is not able to prove an analogue of (2) in the outline of (iii) for [arbitrary] *number fields*. In particular, at the time of writing, the author is not able to obtain a *similar proof* to the proof given in [7] of an analogous result of the result ($*$) of (i) for [arbitrary] *number fields*.

(v) On the other hand, if the number field under consideration is a *subfield of an imaginary quadratic field*, then one can prove immediately an analogue of (2) of (iii) from the *finiteness* [i.e., *compactness*] of the group of units in the ring of integers. Thus, by means of the result of *J. Neukirch*, together with the main results of the present paper [cf. the final portion of (iii)], one can obtain a *similar proof* to the proof given in [7] of an analogous result of the result ($*$) of (i) for such a number fields. We leave the routine details to the interested reader.

REFERENCES

[1] S. Mochizuki, *Topics in Absolute Anabelian Geometry III: Global Reconstruction Algorithms*, RIMS Preprint **1626** (March 2008).

[2] P. Moree and P. Stevenhagen, A two-variable Artin conjecture, *J. Number Theory* **85** (2000), 291-304.

[3] M. Saïdi and A. Tamagawa, A prime-to-p version of Grothendieck's anabelian conjecture for hyperbolic curves over finite fields of characteristic $p > 0$, *Publ. Res. Inst. Math. Sci.* **45** (2009), no. **1**, 135-186.

[4] M. Saïdi and A. Tamagawa, On the Hom-form of Grothendieck's birational anabelian conjecture in positive characteristic, *Algebra Number Theory* **5** (2011), no. **2**, 131-184.

[5] A. Tamagawa, The Grothendieck conjecture for affine curves, *Compositio Math.* **109** (1997), 135-194.

[6] K. Uchida, Isomorphisms of Galois groups, *J. Math. Soc. Japan* **28** (1976), no. **4**, 617-620.

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

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

E-mail address: yuichiro@kurims.kyoto-u.ac.jp