Publ. RIMS Kyoto Univ. **50** (2014), 269–285
DOI 10.4171/PRIMS/133

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

by

Yuichiro Hoshi

Abstract

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, either the 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).

2010 Mathematics Subject Classification: Primary 11R04.
Keywords: number field, multiplicative group, field-theoreticity, PU-preserving homomorphism.

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 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 α?

At a more philosophical level:

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

Communicated by S. Mochizuki. Received January 23, 2013. Revised July 23, 2013.

Y. Hoshi: Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-8502, Japan;
e-mail: yuichiro@kurims.kyoto-u.ac.jp

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 $\square \in \{\circ, \bullet\}$, let ${}^{\square}k$ be an algebraically closed field and ${}^{\square}C$ a projective smooth curve over ${}^{\square}k$. Write ${}^{\square}K$ for the function field of ${}^{\square}C$, and ${}^{\square}C^{\mathrm{cl}}$ for the set of closed points of ${}^{\square}C$. For each ${}^{\square}x \in {}^{\square}C^{\mathrm{cl}}$, write $\mathcal{O}_{{}^{\square}C,{}^{\square}x} \subseteq {}^{\square}K$ for the local ring of ${}^{\square}C$ at ${}^{\square}x$, $\mathfrak{m}_{{}^{\square}C,{}^{\square}x} \subseteq \mathcal{O}_{{}^{\square}C,{}^{\square}x}$ for the maximal ideal of $\mathcal{O}_{{}^{\square}C,{}^{\square}x}$, and $\mathrm{ord}_{{}^{\square}x} \colon {}^{\square}K^{\times} \to \mathbb{Z}$ for the valuation of ${}^{\square}K$ given by mapping $f \in {}^{\square}K^{\times}$ to the order of f at ${}^{\square}x \in {}^{\square}C$. (Thus, one verifies easily that $1 + \mathfrak{m}_{{}^{\square}C,{}^{\square}x} \subseteq \mathrm{Ker}(\mathrm{ord}_{{}^{\square}x}) = \mathcal{O}^{\times}_{{}^{\square}C,{}^{\square}x} \subseteq {}^{\square}K^{\times}$.) Let
>
> $$\alpha \colon {}^{\circ}K^{\times} \xrightarrow{\sim} {}^{\bullet}K^{\times}$$
>
> be an isomorphism between the multiplicative groups of ${}^{\circ}K$, ${}^{\bullet}K$. Then 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 all ${}^{\bullet}x \in {}^{\bullet}C^{\mathrm{cl}}$ and ${}^{\circ}x := \phi({}^{\bullet}x) \in {}^{\circ}C^{\mathrm{cl}}$, we have $\mathrm{ord}_{{}^{\circ}x} = \mathrm{ord}_{{}^{\bullet}x} \circ \alpha$ and $1 + \mathfrak{m}_{{}^{\circ}C,{}^{\circ}x} = \alpha^{-1}(1 + \mathfrak{m}_{{}^{\bullet}C,{}^{\bullet}x})$.

Moreover, the issue of recovering the additive structure not only for *isomorphisms* (as in the above result) but also for suitable *homomorphisms* between the multiplicative groups of function fields has been intensively studied by M. Saïdi and A. Tamagawa in, for instance, [3, §4] and [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 paper, let $\mathfrak{Primes}$ be the set of all prime numbers, $\square \in \{\circ, \bullet\}$, ${}^{\square}k$ a *number field* (i.e., a finite extension of $\mathbb{Q}$), ${}^{\square}\mathfrak{o} \subseteq {}^{\square}k$ the ring of integers of ${}^{\square}k$, ${}^{\square}\mathcal{V}$ the set of maximal ideals of ${}^{\square}\mathfrak{o}$ (i.e., the set of nonarchimedean primes of ${}^{\square}k$), and ${}^{\square}\mathbb{Q} \subseteq {}^{\square}k$ the (uniquely determined) subfield of ${}^{\square}k$ that is isomorphic to $\mathbb{Q}$. For ${}^{\square}\mathfrak{p} \in {}^{\square}\mathcal{V}$, write ${}^{\square}\mathfrak{o}_{{}^{\square}\mathfrak{p}}$ for the localization of ${}^{\square}\mathfrak{o}$ at ${}^{\square}\mathfrak{p}$, $\mathfrak{c}({}^{\square}\mathfrak{p})$ for the residue characteristic of ${}^{\square}\mathfrak{p}$ (thus, we have a map $\mathfrak{c} \colon {}^{\square}\mathcal{V} \to \mathfrak{Primes}$), and $\mathrm{ord}_{{}^{\square}\mathfrak{p}} \colon {}^{\square}k^{\times} \twoheadrightarrow \mathbb{Z}$ for the (uniquely determined) surjective valuation of ${}^{\square}k$ associated to ${}^{\square}\mathfrak{p}$ (cf. Definition 1.1). Let

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

be a homomorphism of multiplicative groups.

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 is 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* ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, *holds for all but finitely many* ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$—*cf. Definition* 1.3(ii)), *and 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* ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, *holds for all but finitely many* ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$—*cf. Definition* 1.3(i)), *and 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 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* ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, *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 and 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* ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, *then*

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

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

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

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

Theorem D. *Suppose that the homomorphism* α *is* **surjective**. *Then it arises from an* **isomorphism of fields** ${}^{\circ}k \xrightarrow{\sim} {}^{\bullet}k$ *if and only if there exists* $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ *such that, for* ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$, *if* ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, *then*

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

for all but finitely many ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$, *and 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 this section, we define and discuss the notion of a *PU-preserving* homomorphism (cf. Definition 1.3(i) below). Throughout, we use the notation specified in the Introduction before the statement of Theorem A. Moreover, let k be a *number field*; we shall use similar notation $\mathfrak{o} \subseteq k$, $\mathcal{V}$ for objects associated to 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 $\mathfrak{p}$,

$$\kappa(\mathfrak{p}) := \mathfrak{o}/\mathfrak{p} \xrightarrow{\sim} \mathfrak{o}_{\mathfrak{p}}/\mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$$

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

$$\mathfrak{c}(\mathfrak{p}) := \mathrm{char}(\kappa(\mathfrak{p}))$$

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

$$\mathfrak{c}\colon \mathcal{V} \to \mathfrak{Primes}.$$

(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 $\mathrm{Ker}(\mathrm{ord}_{\mathfrak{p}}) \subseteq k^{\times}$ *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

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

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., ${}^{\square}\mathbb{Q}$).

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 $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ is characteristic-compatible then it 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* ("principal-unit-preserving") [respectively, (ϕ-)*SPU-preserving* ("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 $1 + {}^{\circ}\mathfrak{p}\,{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}} = \alpha^{-1}(1 + {}^{\bullet}\mathfrak{p}\,{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})$], where ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, holds for all but finitely many ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$. If, in this situation, for some ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$, 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 ${}^{\bullet}\mathfrak{p}$ is *PU-exceptional* [respectively, *SPU-exceptional*] for (α, ϕ).

(ii) We shall say that the homomorphism α is *CPU-preserving* ("characteristic-compatibly principal-unit-preserving") if α is ϕ-PU-preserving for some characteristic-compatible 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 $\mathfrak{c}({}^{\bullet}\mathfrak{p}) = \mathfrak{c}(\phi({}^{\bullet}\mathfrak{p}))$ for all but finitely many ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$, then—after 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 $\mathfrak{c}({}^{\bullet}\mathfrak{p}) = \mathfrak{c}(\phi({}^{\bullet}\mathfrak{p}))$—$\alpha$ 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 induced by ι, and $\mathcal{V}_{\iota}\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ for the* (*necessarily* **surjective** *and* **characteristic-compatible**) *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 ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$,*

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

In particular, $\iota^{\times}$ is **$\mathcal{V}_{\iota}$-SPU-preserving** *and* **CPU-preserving**.

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 ${}^{\bullet}\mathfrak{p} \in {}^{\bullet}\mathcal{V}$. Write ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$.*

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

$$\mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})/(1 + {}^{\circ}\mathfrak{p}\,{}^{\circ}\mathfrak{o}_{{}^{\circ}\mathfrak{p}})\ (\simeq \kappa({}^{\circ}\mathfrak{p})^{\times}) \to \mathrm{Ker}(\mathrm{ord}_{{}^{\bullet}\mathfrak{p}})/(1 + {}^{\bullet}\mathfrak{p}\,{}^{\bullet}\mathfrak{o}_{{}^{\bullet}\mathfrak{p}})\ (\simeq \kappa({}^{\bullet}\mathfrak{p})^{\times});$$
$$ {}^{\circ}k^{\times}/\mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})\ (\simeq \mathbb{Z}) \to {}^{\bullet}k^{\times}/\mathrm{Ker}(\mathrm{ord}_{{}^{\bullet}\mathfrak{p}})\ (\simeq \mathbb{Z}).$$

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

Proof. Assertion (i) follows immediately from the (easily verified) fact that, for each $\square \in \{\circ, \bullet\}$, the subgroup $\mathrm{Ker}(\mathrm{ord}_{\square\mathfrak{p}})/(1 + {}^{\square}\mathfrak{p}^{\square}\mathfrak{o}_{\square\mathfrak{p}}) \subseteq {}^{\square}k^{\times}/(1 + {}^{\square}\mathfrak{p}^{\square}\mathfrak{o}_{\square\mathfrak{p}})$ *coincides* with the *maximal torsion subgroup* of ${}^{\square}k^{\times}/(1 + {}^{\square}\mathfrak{p}^{\square}\mathfrak{o}_{\square\mathfrak{p}})$.

Next, we verify (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 α is CPU-preserving follows immediately from Remark 1.3.1, together with the fact that if $\kappa({}^{\circ}\mathfrak{p})^{\times}$ is *isomorphic* to $\kappa({}^{\bullet}\mathfrak{p})^{\times}$, then $\mathfrak{c}({}^{\circ}\mathfrak{p}) = \mathfrak{c}({}^{\bullet}\mathfrak{p})$. □

Lemma 1.6. *Let* $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ *be a map of sets and* $\alpha, \beta\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ *homomorphisms of groups. Suppose that* α *and* β *are* ϕ**-PU-preserving**. *Then the homomorphism* $\alpha \cdot \beta\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ (*mapping* $x \in {}^{\circ}k^{\times}$ *to* $\alpha(x) \cdot \beta(x) \in {}^{\bullet}k^{\times}$) *is* ϕ**-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* 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), the product of two $\mathrm{id}_{\mathbb{Q}^{\times}}$'s (which maps $x \in \mathbb{Q}^{\times}$ to $x^2 \in \mathbb{Q}^{\times}$) is *not* $\mathrm{id}_{\mathfrak{Primes}}$*-SPU-preserving*.

(ii) Moreover, in general, the product of *CPU-preserving* 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 for the product 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 of all group homomorphisms ${}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$, 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*

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

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*

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

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

§2. Field-theoreticity for certain PU-preserving homomorphisms

In this section, we prove the *field-theoreticity* of certain *PU-preserving* homomorphisms (cf. Theorem 2.5 below). We maintain the notation of §1.

Lemma 2.1. *Let $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ be a map of sets, n a positive integer, and let $x_1, \ldots, x_n \in {}^{\circ}k^{\times}$. 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 subset $S[\phi; x_1, \ldots, x_n] \subseteq {}^{\bullet}\mathcal{V}$ consisting of all maximal ideals ${}^{\bullet}\mathfrak{p}$ of ${}^{\bullet}\mathfrak{o}$ that satisfy the following condition is* **infinite**: *If ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, then $x_i \in \mathrm{Ker}(\mathrm{ord}_{{}^{\circ}\mathfrak{p}})$ for each $i \in \{1, \ldots, n\}$, and $\sharp\kappa({}^{\circ}\mathfrak{p}) = \mathfrak{c}({}^{\circ}\mathfrak{p})$.*

Proof. One verifies immediately that, to prove Lemma 2.1, it suffices to verify that the set of those $p \in \mathfrak{Primes}$ that *split completely* in the finite extension ${}^{\circ}k/{}^{\circ}\mathbb{Q}$ contains a subset of $\mathfrak{Primes}$ of *positive density*. The latter fact follows immediately, by considering the Galois closure of ${}^{\circ}k/{}^{\circ}\mathbb{Q}$, from Chebotarev's density theorem. □

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 $x, y \in \mathbb{Q}^{\times}$ with $y \notin \{1, -1\}$. Then the subset $S_{x,\langle y\rangle} \subseteq \mathfrak{Primes}$ consisting of all $p \in \mathfrak{Primes}$ that satisfy the following condition is* **infinite**: *$x, y \in \mathrm{Ker}(\mathrm{ord}_p)$, and 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 proof of [2, Theorem 1]. For the reader's convenience (and to make it clear that the argument given in [2] works under our assumption $y \notin \{1, -1\}$), we review the argument as follows:

Since $y \notin \{1, -1\}$, it is immediate that, by replacing y by y^{-1} if necessary, we may assume that $|y| > 1$. 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 $a_n := x_1 \cdot y_2^n - x_2 \cdot y_1^n$. Now if $a_n = 0$ for some n, then Lemma 2.2 is immediate. Thus, assume that $a_n \neq 0$ for every n. Next, observe that $S_{x,\langle y\rangle}$ *coincides* with the set of $p \in \mathfrak{Primes}$ 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 towards a contradiction that $S_{x,\langle y\rangle}$ is *finite*. Write $n_0 := \sharp(\mathbb{Z}/(\prod_{p \in S_{x,\langle y\rangle}} p^{\mathrm{ord}_p(a_0)+1})\mathbb{Z})^\times$. (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 $p \in S_{x,\langle y\rangle}$,

$$\mathrm{ord}_p(a_{n_0 \cdot n}) \leq \mathrm{ord}_p(a_0).$$

Indeed, first observe that since $y \in \mathrm{Ker}(\mathrm{ord}_p)$, it follows that $y_1, y_2 \in \mathrm{Ker}(\mathrm{ord}_p)$, which implies that $y_1^{n_0}, y_2^{n_0} \equiv 1 \pmod{p^{\mathrm{ord}_p(a_0)+1}}$ (cf. the final part 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, $\mathrm{ord}_p(a_{n_0 \cdot n}) \leq \mathrm{ord}_p(a_0)$, as desired.

Next, one deduces 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. □

Remark 2.2.1. If, in Lemma 2.2, one omits the assumption that $y \notin \{1, -1\}$, then the conclusion no longer holds. More precisely, for $x \in \mathbb{Q}^\times$ and $y \in \{1, -1\}$, the set $S_{x,\langle y\rangle}$ is infinite if and only if $(x, y) \in \{(1, 1), (1, -1), (-1, -1)\}$. Indeed, the *sufficiency* is immediate. To verify the *necessity*, observe that since $1^2 = (-1)^2 = 1$, it follows 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 $S_{x,\langle y\rangle} = \{2\}$ when $(x, y) = (-1, 1)$, the necessity follows.

Lemma 2.3. *Let $x \in k^\times$. Then $x \in \mathbb{Q}^\times$ 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. First, one verifies easily that the condition $x^{\mathfrak{c}(\mathfrak{p})-1} \in 1 + \mathfrak{p}\mathfrak{o}_\mathfrak{p}$ implies that $x \in \mathrm{Ker}(\mathrm{ord}_\mathfrak{p})$. Hence these conditions are *equivalent*, and moreover the image of $x \in \mathrm{Ker}(\mathrm{ord}_\mathfrak{p})$ in $\mathrm{Ker}(\mathrm{ord}_\mathfrak{p})/(1 + \mathfrak{p}\mathfrak{o}_\mathfrak{p}) \xrightarrow{\sim} \kappa(\mathfrak{p})^\times$ is *annihilated by* $\mathfrak{c}(\mathfrak{p}) - 1$, i.e., *contained in the prime subfield* ($\simeq \mathbb{Z}/\mathfrak{c}(\mathfrak{p})\mathbb{Z}$) of $\kappa(\mathfrak{p})$. Thus, Lemma 2.3 follows immediately from Chebotarev's density theorem. □

Proposition 2.4. *Let $\phi\colon {}^\bullet\mathcal{V} \to {}^\circ\mathcal{V}$ be a map of sets.*

(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*

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

of Lemma 1.8 is **injective**.

(ii) *Suppose, moreover, that the image of ${}^\bullet\mathcal{V} \xrightarrow{\phi} {}^\circ\mathcal{V} \xrightarrow{\mathfrak{c}} \mathfrak{Primes}$ is* **cofinite**. *Let ${}^\circ J$ be an* **infinite** *subgroup of ${}^\circ\mathbb{Q}^\times$. Then the homomorphism of groups*

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

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

(iii) *The homomorphism of groups*

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

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 $\alpha({}^\circ k^\times) = \{1\}$, 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 ${}^\circ\mathfrak{p} := \phi({}^\bullet\mathfrak{p}) \in {}^\circ\mathcal{V}$ 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 (i).

Next, we verify assertion (ii). It follows from (i) that, to verify (ii), we may assume 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 $\alpha({}^\circ k^\times) = \{1\}$, take $x \in {}^\circ k^\times = {}^\circ\mathbb{Q}^\times$ and $y \in {}^\circ J \setminus ({}^\circ J \cap \{1, -1\})$. 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 all maximal ideals ${}^\bullet\mathfrak{p}$ of ${}^\bullet\mathfrak{o}$ that satisfy the following condition is *infinite*: If ${}^\circ\mathfrak{p} := \phi({}^\bullet\mathfrak{p})$, 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 ${}^{\bullet}\mathfrak{p} \in T$. By the definition of T, 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 (ii).

Finally, we verify (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*, take a $\mathfrak{c}$-*PU-preserving* homomorphism $\alpha\colon {}^{\circ}\mathbb{Q}^{\times} \to {}^{\bullet}k^{\times}$. By Lemma 2.3, 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 (iii). □

Remark 2.4.1. If, in 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 two *distinct* endomorphisms of $\mathbb{Q}^{\times}$ obtained by mapping $x \in \mathbb{Q}^{\times}$ to $x \in \mathbb{Q}^{\times}$ and $x^3 \in \mathbb{Q}^{\times}$, respectively, are contained in $\mathrm{Hom}^{\mathrm{id}_{\mathfrak{Primes}}\text{-}\mathrm{PU}}(\mathbb{Q}^{\times}, \mathbb{Q}^{\times})$ and coincide on the nontrivial subgroup $\{1, -1\} \subseteq \mathbb{Q}^{\times}$.

Theorem 2.5. *For* $\square \in \{\circ, \bullet\}$*, let* ${}^{\square}k$ *be a* **number field***; write* ${}^{\square}\mathcal{V}$ *for the set of maximal ideals of the ring of integers of* ${}^{\square}k$*, and* ${}^{\square}\mathbb{Q} \subseteq {}^{\square}k$ *for the subfield of* ${}^{\square}k$ *that is isomorphic to* $\mathbb{Q}$*. Let* $\alpha\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ *be a homomorphism of groups. Then the following conditions are equivalent:*

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

(2) α *is* **CPU-preserving** *and 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) α *is* **PU-preserving** *and 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. First, it follows from Lemma 1.8 that we may assume that ${}^{\circ}k = {}^{\circ}\mathbb{Q}$. Next, it follows from Proposition 2.4(iii) that we may assume that ${}^{\bullet}k = {}^{\bullet}\mathbb{Q}$. 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 $\mathrm{Hom}^{\mathrm{id}_{\mathfrak{Primes}}\text{-}\mathrm{PU}}({}^{\circ}\mathbb{Q}^{\times}, {}^{\bullet}\mathbb{Q}^{\times})$, the implication follows immediately from Proposition 2.4(ii).

Finally, we verify (3)⇒(1). Suppose that (3) is satisfied. Let $\phi\colon {}^{\bullet}\mathcal{V} \to {}^{\circ}\mathcal{V}$ be such that α is ϕ-*PU-preserving*. One verifies easily that it suffices to verify

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, $\alpha(x + y) = \alpha(x) + \alpha(y)$).

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 that $x + y \neq 0$. Now, to complete the verification of Claim 2.5.A, we will prove

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). Then

$$\alpha(x + y) \pmod{1 + {}^{\bullet}\mathfrak{p}^{\bullet}\mathfrak{o}_{\bullet\mathfrak{p}}} = \alpha(x) + \alpha(y) \pmod{1 + {}^{\bullet}\mathfrak{p}^{\bullet}\mathfrak{o}_{\bullet\mathfrak{p}}}.$$

Indeed, write ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$. 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 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 from the definition of $\alpha_{\mathfrak{p}}$; the second and sixth follow from the choices of $x_{\mathbb{Q}}$, $y_{\mathbb{Q}}$; the fourth follows from our assumption that $\alpha|_{\circ\mathbb{Q}^{\times}}$ arises from a *homomorphism of fields* ${}^{\circ}\mathbb{Q} \to {}^{\bullet}k$; the eighth follows from the various definitions involved. This completes the proof of Claim 2.5.B.

Now, 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 (3)⇒(1). □

Remark 2.5.1. If, in 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, 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 this section, we prove analogues of Uchida's lemma reviewed in the Introduction in the case of *number fields* (cf. Theorem 3.1 and Corollary 3.3 below).

Theorem 3.1. *For $\square \in \{\circ, \bullet\}$, let ${}^{\square}k$ be a* **number field***; 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 ${}^{\square}\mathfrak{o}$. Write $\mathfrak{Primes}$ for the set of all prime numbers. Let $\alpha\colon {}^{\circ}k^{\times} \to {}^{\bullet}k^{\times}$ be a homomorphism of groups. Then the following conditions are equivalent:*

(1) *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 ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, then:*

   (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*

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

   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*

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

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

Proof. The implication (1)⇒(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 (2)⇒(1). Suppose that condition (2) is satisfied. Now since α is *CPU-preserving* (cf. condition (b)), it follows from the equivalence (1)⇔(2) of Theorem 2.5 that it suffices to verify

> 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 ${}^{\bullet}k$.

Now since α is *CPU-preserving* (cf. (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, we may assume that ${}^{\circ}k = {}^{\circ}\mathbb{Q}$. Next, again since α is *CPU-preserving*, it follows immediately from Proposition 2.4(iii) that we may assume 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 $S_{(\mathrm{b})}$ be a *cofinite* subset of $\mathfrak{Primes}$ such that the displayed inclusion of (b) holds for ${}^{\bullet}\mathfrak{p} \in S_{(\mathrm{b})}$, and $S_{(\mathrm{a}),(\mathrm{b})}$ an *infinite* subset of $S_{(\mathrm{b})}$ such that the displayed equality of (a) holds for ${}^{\bullet}\mathfrak{p} \in S_{(\mathrm{a}),(\mathrm{b})}$. 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

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

(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 $\mathfrak{c}({}^{\square}\mathfrak{p})$ (i.e., $J_{{}^{\square}\mathfrak{p}} =$ "$\mathfrak{c}({}^{\square}\mathfrak{p})^{\mathbb{Z}}$"). Then 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 $-1 \in {}^{\circ}k^{\times}$ to $-1 \in {}^{\bullet}k^{\times}$.
- If ${}^{\bullet}\mathfrak{p} \notin S_{(\mathrm{b})}$, then β maps $\mathfrak{c}(\phi({}^{\bullet}\mathfrak{p})) \in {}^{\circ}k^{\times}$ to $\mathfrak{c}({}^{\bullet}\mathfrak{p}) \in {}^{\bullet}k^{\times}$.
- If ${}^{\bullet}\mathfrak{p} \in S_{(\mathrm{b})}$, then β maps $\mathfrak{c}(\phi({}^{\bullet}\mathfrak{p})) \in {}^{\circ}k^{\times}$ to $\mathfrak{c}({}^{\bullet}\mathfrak{p})^{n_{{}^{\bullet}\mathfrak{p}}} \in {}^{\bullet}k^{\times}$ (concerning $n_{{}^{\bullet}\mathfrak{p}}$, we refer to the final part of the preceding paragraph).

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

(i) the composite

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

is *trivial*, i.e., 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) $\mathrm{Ker}(\gamma) \subseteq {}^{\circ}k^{\times}$ *coincides* with the subgroup of ${}^{\circ}k^{\times}$ consisting of all $x \in {}^{\circ}k^{\times}$ such that $\alpha(x) = \beta(x)$.

Now let us observe that the kernel 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 γ, we conclude from (i), (ii), together with the var-

ious definitions involved, that there exists a *nontorsion* $x \in (\bigoplus_{\bullet\mathfrak{p} \in S_{(a),(b)}} J_{\phi(\bullet\mathfrak{p})} \subseteq) \ {}^{\circ}k^{\times}$ 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**. *Let* $\alpha\colon {}^{\circ}k^{\times} \twoheadrightarrow {}^{\bullet}k^{\times}$ *be a* **surjective** *group homomorphism. Then 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* α *is* **SPU-preserving**.

Proof. The *necessity* follows from Lemma 1.4. Next, we verify the *sufficiency*. Suppose that α is *SPU-preserving*. Then from Lemma 1.5(ii), either α or $(-)^{-1} \circ \alpha$ satisfies condition (2) of Theorem 3.1. In particular, the *sufficiency* follows from Theorem 3.1. □

Corollary 3.3. *For* $\square \in \{\circ, \bullet\}$, *let* ${}^{\square}k$ *be a* **number field**; *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* ${}^{\square}\mathfrak{o}$ *Let* $\alpha\colon {}^{\circ}k^{\times} \twoheadrightarrow {}^{\bullet}k^{\times}$ *be a* **surjective** *group homomorphism. Then the following conditions are equivalent:*

(1) 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* ${}^{\circ}\mathfrak{p} := \phi({}^{\bullet}\mathfrak{p}) \in {}^{\circ}\mathcal{V}$, *then:*

   (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*

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

   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] and [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 to the proofs of the results of Saïdi–Tamagawa discussed in (i) (cf., e.g., [4, Proposition 5.3]). 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 involved*.

(2) By considering residue classes at various primes 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 step (1) of (ii) (cf. [3, §4]; [4, §5]; [7, §3]). On the other hand, in the case of *number fields*, to perform step (1) of (ii), the behaviors of *elements of* $\mathbb{Q}^{\times} \setminus \mathbb{Z}^{\times}$ 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]), were studied in the context of *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 between the original function fields.

Here, we note that an analogue of (∗) 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 (∗) and the proof (in [6]) of its analogue 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 and Remarks 1.9.5, 1.9.8]).

(iii) Now let us recall the outline of the proof of (∗) given in [7].

(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 $\mathrm{ord}_{\square_x}$ and $1+\mathfrak{m}_{\square_{C,\square_x}}$) 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 between the function fields.

Here, we note that an analogue of (1) 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).

(iv) However, by the difficulty arising from the *archimedean portions in the idele groups of number fields*, at the time of this writing, the author is not able to prove an analogue of (2) for (arbitrary) *number fields*. In particular, the author is not able to obtain a proof similar to the proof in [7] of an analogue of $(*)$ 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) 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 part of (iii)), one can obtain a proof similar to the proof given in [7] of an analogue of $(*)$ for such number fields. We leave the routine details to the interested reader.

Acknowledgements

The author would like to thank Kazumi Higashiyama for pointing out a minor error in the proof of Lemma 2.2 in an earlier version of the present paper. The author 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.

References

[1] S. Mochizuki, Topics in absolute anabelian geometry III: Global reconstruction algorithms, RIMS Preprint 1626 (2008).

[2] P. Moree and P. Stevenhagen, A two-variable Artin conjecture, J. Number Theory **85** (2000), 291–304. Zbl 0966.11042 MR 1802718

[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. RIMS Kyoto Univ. **45** (2009), 135–186. Zbl 1188.14016 MR 2512780

[4] M. Saïdi and A. Tamagawa, On the Hom-form of Grothendieck's birational anabelian conjecture in positive characteristic, Algebra Number Theory **5** (2011), 131–184. Zbl 1235.14026 MR 2833788

[5] A. Tamagawa, The Grothendieck conjecture for affine curves, Compos. Math. **109** (1997), 135–194. Zbl 0899.14007 MR 1478817

[6] K. Uchida, Isomorphisms of Galois groups, J. Math. Soc. Japan **28** (1976), 617–620. Zbl 0329.12013 MR 0432593

[7] K. Uchida, Isomorphisms of Galois groups of algebraic function fields, Ann. of Math. **106** (1977), 589–598. Zbl 0372.12017 MR 0460279