Isomorphisms of Galois groups of number fields with restricted ramification

Ryoji Shimizu
RIMS, Kyoto University, Kyoto, Japan

Correspondence
Ryoji Shimizu, RIMS, Kyoto University, Kyoto, 606-8502, Japan.
Email: shimizur@kurims.kyoto-u.ac.jp

Funding information
Japan Society for the Promotion of Science, Grant/Award Number: Grant Number 21J11879

Abstract
Let $K$ be a number field and $S$ a set of primes of $K$. We write $K_S/K$ for the maximal extension of $K$ unramified outside $S$ and $G_{K,S}$ for its Galois group. In this paper, we answer the following question under some assumptions: “For $i = 1, 2$, let $K_i$ be a number field, $S_i$ a (sufficiently large) set of primes of $K_i$ and $\sigma : G_{K_1,S_1} \rightarrow G_{K_2,S_2}$ an isomorphism. Is $\sigma$ induced by a unique isomorphism between $K_{1,S_1}/K_1$ and $K_{2,S_2}/K_2$?” Here, the main assumption is about the Dirichlet density of $S_i$.

KEYWORDS
Anabelian geometry, Dirichlet density, Neukirch–Uchida theorem, restricted ramification

MSC (2020)
11R32, 11S15, 11R45

1 INTRODUCTION

Let $K$ be a number field and $S$ a set of primes of $K$. We write $K_S/K$ for the maximal extension of $K$ unramified outside $S$ and $G_{K,S}$ for its Galois group.

The Neukirch–Uchida theorem, which is one of the most important results in anabelian geometry, states that if the absolute Galois groups of number fields are isomorphic, then the number fields are isomorphic (cf. [5] and [9]). Moreover, Uchida also proved that the isomorphisms of the absolute Galois groups of number fields arise functorially from unique isomorphisms of number fields (cf. [9, Theorem]). On the other hand, Ivanov in [2, 3] and [4], and successively the author in [8], studied a generalization of the Neukirch–Uchida theorem where one replaces the absolute Galois groups by the Galois groups of the maximal extensions with restricted ramification. These results prompt the following natural question (cf. [6, (12.3.4) Question]):

For $i = 1, 2$, let $K_i$ be a number field, $S_i$ a (sufficiently large) set of primes of $K_i$, and $\sigma : G_{K_1,S_1} \rightarrow G_{K_2,S_2}$ an isomorphism. Is $\sigma$ induced by a unique isomorphism between $K_{1,S_1}/K_1$ and $K_{2,S_2}/K_2$?

In this paper, to approach this question, we mainly refine arguments in [8].

In Section 2, we prove the faithfulness of the Galois action on the Galois group of the maximal multiple $\mathbb{Z}_l$-extension. By this result, we obtain the “uniqueness” in question under a mild assumption.

In Section 3, we develop a way, based on [8, section 3], to show that isomorphisms of Galois groups are induced by (unique) field isomorphisms under some assumptions, for example, about the Dirichlet density. Then, by using this, we prove the main result (more precisely, see Theorem 3.4): For $i = 1, 2$, let $K_i$ be a number field, $S_i$ a set of primes of $K_i$, and $\sigma : G_{K_1,S_1} \rightarrow G_{K_2,S_2}$ an isomorphism. Assume that for $i = 1, 2$ and for any finite Galois subextension $L_i$ of $K_{1,S_i}/K_i$, the Dirichlet density of $P_{S_i,\text{f}} \cap \text{cs}(L_i/Q)$ is not zero, where $P_{S_i,\text{f}} \cap \text{cs}(L_i/Q)$ is the set of prime numbers that split completely in $L_i$ and such that the places of $K_i$ lying over them are contained in $S_i$ (cf. Notations). Then, there exists a unique isomorphism $\tau : K_{2,S_2} \rightarrow K_{1,S_1}$ such that $K_1 = \tau(K_2)$ and $\sigma$ coincides with the isomorphism induced by $\tau$. 
In Section 4, we see some applications of the main theorem, for example, about the set of outer isomorphisms of $G_{K,S}$ (Corollary 4.5).

In the Appendix, we study intersections of decomposition groups in $G_{K,S}$. The results not only are interesting in themselves, but also give an alternative proof of the “uniqueness” in question.

**Notations**

1. Given a set $A$, we write $\#A$ for its cardinality.
2. For a profinite group $G$, let $[G, G]$ be the closed subgroup of $G$, which is (topologically) generated by the commutators in $G$. We write $G^{ab} \overset{\text{def}}{=} G/[G, G]$ for the maximal abelian quotient of $G$.
3. For a profinite group $G$, we say that $G$ is topologically infinitely generated if $G$ is not topologically finitely generated.
4. Given a profinite group $G$ and a prime number $l$, we write $G^{(l)}$ for the maximal pro-$l$ quotient of $G$.
5. Given a Galois extension $L/K$, we write $G(L/K)$ for its Galois group $\text{Gal}(L/K)$. Given a field $K$, we write $\overline{K}$ for a separable closure of $K$, and $G_K$ for the absolute Galois group $G(\overline{K}/K)$ of $K$.

6. A number field is a finite extension of the field of rational numbers $\mathbb{Q}$. For a (possibly infinite) algebraic extension $F$ of $\mathbb{Q}$, we write $P = P_F$ for the set of primes of $F$, $P_\infty = P_{F, \infty}$ for the set of archimedean primes of $F$, and, for a prime number $l$, $P_l = P_{F,l}$ for the set of nonarchimedean primes of $F$ above $l$. Further, for a set of primes $S \subset P_F$, we set $S' = S \setminus (P_\infty \cap S)$, $P_S = \{ p \in P_{\mathbb{Q}} \mid P_{F,p} \subset S \}$. For $Q \subset C \subset F' \subset \overline{\mathbb{Q}}$, we write $S(F')$ for the set of primes of $F'$ above the primes in $S$, that is, $S(F') = \{ p \in P_{F'} \mid P_{F,p} \subset S \}$. For convenience, we say that $F'/F$ is ramified at a prime $p$ of $F$ if it is above a real prime of $F$. We write $F_S/F$ for the maximal extension of $F$ unramified outside $S$ and $G_{F,S}$ for its Galois group. When $P_\infty \subset S$, we set $\mathcal{O}_{F,S} = \{ a \in F \mid |a|_p \leq 1 \text{ for all } p \notin S \}$, where $| \cdot |_p$ is an absolute valuation associated to $p$.

7. For $i = 1, 2$, let $A_i$ be a (commutative) ring. Write $\text{Iso}(A_2, A_1)$ for the set of ring isomorphisms from $A_2$ to $A_1$. For $i = 1, 2$, let $B_i$ be a ring containing $A_i$. Write $\text{Iso}(B_2/A_2, B_1/A_1) = \{ \tau \in \text{Iso}(B_2, B_1) \mid \tau(A_2) = A_1 \}$. For $i = 1, 2$, let $K_i$ be a number field, $L_i/K_i$ an algebraic extension, and $S_i$ a set of primes of $K_i$. Write

$$\text{Iso}(K_2, S_2, (K_1, S_1)) = \{ \tau \in \text{Iso}(K_2, K_1) \mid \tau \text{ induces a bijection between } S_2 \text{ and } S_1 \},$$

$$\text{Iso}(L_2/K_2, S_2, (L_1/K_1, S_1)) = \{ \tau \in \text{Iso}(L_2/K_2, L_1/K_1) \mid \tau \text{ induces a bijection between } S_2 \text{ and } S_1 \}.$$ 

For a number field $K$ and a set of primes $S$ of $K$, write $\text{Aut}(K, S) = \text{Iso}(K, S), (K, S))$.

8. For a profinite group $G$, write $\text{Inn}(G)$ for the set of inner automorphisms of $G$. For $i = 1, 2$, let $G_i$ be a profinite group. Write $\text{Iso}(G_1, G_2)$ for the set of isomorphisms of profinite groups from $G_1$ to $G_2$. Note that the group $\text{Inn}(G_2)$ acts on $\text{Iso}(G_1, G_2)$ by the rule $\sigma(\phi) = \sigma \phi \sigma^{-1}$ for $\sigma \in \text{Inn}(G)$ and $\phi \in \text{Iso}(G_1, G_2)$. We call $\text{OutIso}(G_1, G_2) = \text{Iso}(G_1, G_2)/\text{Inn}(G_2)$ the set of outer isomorphisms from $G_1$ to $G_2$. Write $\text{Out}(G) = \text{OutIso}(G, G)$.

9. Given an algebraic extension $K$ of $\mathbb{Q}$ and $p \in P_{K,f}$, we write $\kappa(p)$ for the residue field at $p$. When $K$ is a number field, we write $K_p$ for the completion of $K$ at $p$, and, in general, we write $K_p$ for the union of $K_p^\infty$ for finite subextensions $K'/\mathbb{Q}$ of $K/\mathbb{Q}$.

10. Let $L/K$ be a finite extension of number fields and $q \in P_{L,f}$, and set $p = q|_K$. We write $f_{q|_K} = [\kappa(q) : \kappa(p)]$. We write $\kappa(L/K)$ for the set of nonarchimedean primes of $K$, which split completely in $L/K$.

11. Let $K$ be a number field and $p \in P_{K,f}$, and set $p = p|_\mathbb{Q}$. Define the residual degree (resp. the local degree) of $p$ as $f_{p|_\mathbb{Q}}$ (resp. $[K_p : \mathbb{Q}_p]$). We set $\mathfrak{d}(p) = \#(\kappa(p) = p^{f_{p|_\mathbb{Q}}})$.

12. For a number field $K$ and a set of primes $S \subset P_K$, we set

$$\delta_{\sup}(S) = \limsup_{s \to 1+0} \frac{\sum_{p \in S} \mathfrak{d}(p)^{-s}}{\log \frac{1}{s-1}}, \quad \delta_{\inf}(S) = \liminf_{s \to 1+0} \frac{\sum_{p \in S} \mathfrak{d}(p)^{-s}}{\log \frac{1}{s-1}},$$

where “$s \to 1 + 0$” means that 1 is approached from above on $\mathbb{R}$. If $\delta_{\sup}(S) = \delta_{\inf}(S)$, then write $\delta(S)$ (the Dirichlet density of $S$) for them. The term “$\delta(S) \neq 0$” will always mean that $S$ has a positive Dirichlet density or $S$ does not have a Dirichlet density. Note that $\delta(S) \neq 0$ if and only if $\delta_{\sup}(S) > 0$. 

(13) For \( Q \subset F \subset F' \subset \overline{Q} \) with \( F'/F \) Galois, \( q \in P_{F',f} \), and \( p = q|_F \), write \( D_q(F'/F) \subset G(F'/F) \) for the decomposition group (i.e., the stabilizer) of \( q \) in \( G(F'/F) \). We sometimes write \( D_q = D_q(F'/F) \), when no confusion arises. There exists a canonical isomorphism \( D_q = D_q(F'/F) \simeq G(F'/F) \), and we will identify \( D_q(F'/F) \) with \( G(F'/F) \) via this isomorphism.

(14) Let \( p \) be a prime number. A \( p \)-adic field is a finite extension of the field of \( p \)-adic numbers \( \mathbb{Q}_p \). Let \( \kappa \) be a \( p \)-adic field.

We write \( V_\kappa \) for the ramification subgroup of \( G_\kappa \), and set \( G_\kappa^{\text{tor}} \overset{\text{def}}{=} G_\kappa/V_\kappa \). Let \( \lambda/\kappa \) be a Galois extension. We say that \( G(\lambda/\kappa) \) is full if \( \kappa \) is algebraically closed.

(15) Given an abelian group \( A \), we write \( A_{\text{tor}} \) for the torsion subgroup of \( A \).

(16) Given an abelian profinite group \( A \), we write \( \overline{A}_{\text{tor}} \) for the closure in \( A \) of \( A_{\text{tor}} \), and set \( A/\text{tor} \overset{\text{def}}{=} A/\overline{A}_{\text{tor}} \).

(17) Given a field \( K \), we write \( \mu(K) \) for the group consisting of the roots of unity in \( K \). For \( n \in \mathbb{Z}_{>0} \) not divisible by the characteristic of \( K \), we write \( \mu_n(K) \subset \mu(K) \) for the subgroup of order \( n \). For a prime number \( l \) distinct from the characteristic of \( K \), we set \( \mu_l^{\infty}(K) = \bigcup_{n \in \mathbb{Z}_{>0}} \mu^{n}(K) \subset \mu(K) \).

2 | THE FAITHFULNESS OF THE GALOIS ACTION ON THE GALOIS GROUP OF THE MAXIMAL MULTIPLE \( \mathbb{Z}_l \)-EXTENSION

In the rest of this paper, let \( K \) be a number field and \( S \subset P_K \) a set of primes of \( K \).

Let \( l \) be a prime number. We set \( \Gamma_K = \Gamma_{K,l} \overset{\text{def}}{=} G_{ab,(l)}^{(l)/\text{tor}} \). Then, \( \Gamma_K \) is a free \( \mathbb{Z}_l \)-module. Set \( r_{l}(K) \overset{\text{def}}{=} \text{rank}_{\mathbb{Z}_l} \Gamma_K \), and write \( K^{(\infty)} = K^{(\infty,l)} \) for the extension of \( K \) corresponding to \( \Gamma_K \). \( K^{(\infty,l)}/K \) is unramified outside \( P_l \) by class field theory, and hence, if \( P_l \subset S \), \( \Gamma_{K,l} = G_{ab,(l)}^{(l)/\text{tor}} \).

By [6, (10.3.20) Proposition], we have \( r_C(K) + 1 \leq r_{l}(K) \leq [K : \mathbb{Q}] \), where \( r_C(K) \) is the number of complex primes of \( K \). For a finite extension \( L/K \), define \( \pi_{l,K}^{C} = \pi_{l,K,J}^{C} \) to be the canonical homomorphism \( \Gamma_{l,K} \to \Gamma_{K,J} \). We write \( \text{Hom}_{cts}(\Gamma_{K,l}, \mathbb{Z}_l) \) for the set of continuous homomorphisms from \( \Gamma_{K,l} \) to \( \mathbb{Z}_l \), where \( \mathbb{Z}_l \) is equipped with the profinite topology. Then, \( \text{Hom}_{cts}(\Gamma_{K,l}, \mathbb{Z}_l) = \text{Hom}_{\mathbb{Z}}(\Gamma_{K,l}, \mathbb{Z}_l) \simeq \mathbb{Z}_l^{[K]}(l) \).

**Lemma 2.1.** Let \( K \) be a number field, \( L \) a finite Galois extension of \( K \), and \( l \) a prime number. Assume that \( L \) has a complex prime. Then, the canonical action of \( G(\lambda/K) \) on \( \Gamma_{L,l} \) induced by conjugation is faithful.

**Proof.** Write \( K' \) for the subextension of \( L/K \) corresponding to the kernel of the homomorphism \( G(L/K) \to \text{Aut}(\Gamma_{L,l}) \) induced by the canonical action. Then, we have \( r_{l}(L) = \text{rank}_{\mathbb{Z}_l} \text{Hom}_{cts}(\Gamma_{L,l}, \mathbb{Z}_l) = \text{rank}_{\mathbb{Z}_l} \text{Hom}_{cts}(\Gamma_{L,l}, \mathbb{Z}_l)G(G(L'/K)/G(K'/L')) \).

By [8, Lemma 3.1], this means that \( r_{l}(L) = r_{l}(K') \). It follows from [8, Lemma 3.2] that \( L = K' \).

**Proposition 2.2.** Assume \( #P_{S,l} \geq 1 \) and that \( K_S \) has a complex prime. Let \( \tau \in \text{Aut}(K_S) \). Assume \( \tau(K) = K \) and that the automorphism of \( G_{K,S} \) induced by the conjugation action of \( \tau \) is trivial. Then, \( \tau \) is trivial.

**Proof.** Write \( K_0 \) for the Aut\((K_S)\)-invariant subgroup of \( K_S \). Then, \( K_S/K_0 \) is Galois. Take \( l \in P_{S,l} \). Let \( L \) be any finite Galois subextension of \( K_S/K_0 \) containing \( K \), and having a complex prime. Then, by assumption, the action of \( \tau|_L \) on \( \Gamma_{L,l} \) is trivial. Therefore, by Lemma 2.1, \( \tau|_L \) is trivial. Thus, \( \tau \) is trivial.

**Corollary 2.3.** Assume \( #P_{S,l} \geq 1 \) and that \( K_S \) has a complex prime. Let \( U \) be an open normal subgroup of \( G_{K,S} \). Then, the conjugation action of \( G_{K,S} \) on \( U \) is faithful. In particular, \( G_{K,S} \) has a trivial center.

**Proof.** Write \( L \) for the finite Galois subextension of \( K_S/K \) corresponding to \( U \). Let \( \tau \in G_{K,S}(\subset \text{Aut}(K_S)) \) such that the automorphism of \( U(= G_{L,S}(L)) \) induced by the conjugation action of \( \tau \) is trivial. Then, by Proposition 2.2, \( \tau \) is trivial.

3 | ISOMORPHISMS OF FIELDS

In this section, we develop a way, based on [8, section 3], to show that isomorphisms of Galois groups are induced by (unique) field isomorphisms. By using this, we prove the main result.

In the rest of this paper, fix an algebraic closure \( \overline{Q} \) of \( Q \), and suppose that all number fields and all algebraic extensions of them are subfields of \( \overline{Q} \). Write \( \overline{K} \) for the Galois closure of \( K/\overline{Q} \). For \( i = 1,2 \), let \( K_i \) be a number field and \( S_i \) a set of primes of \( K_i \) with \( P_{K_i,\infty} \subset S_i \).
Before we see the following, let us recall the concept of local correspondence. For an isomorphism $\sigma : G_{K_1, S_1} \sim G_{K_2, S_2}$, the local correspondence is a one-to-one correspondence between the sets of the decomposition groups in $G_{K_i, S_i}$ at nonarchimedean primes for $i = 1, 2$ induced by $\sigma$ (more precisely, see [8, Definition 2.5]). It is established under some assumptions (cf. [8, Theorem 2.6]), and plays an essential role to obtain field isomorphisms (cf. [8, section 3]).

**Proposition 3.1.** Let $\sigma : G_{K_1, S_1} \sim G_{K_2, S_2}$ be an isomorphism, and for $i = 1, 2$, $U_i$ an open normal subgroup of $G_{K_i, S_i}$ with $\sigma(U_1) = U_2$. For $i = 1, 2$, write $L_i$ for the finite Galois subextension of $K_{i, S_i}/K_i$ corresponding to $U_i$. Let $T_i \subset S_{i,f}(L_i)$ for $i = 1, 2$. Assume that the following conditions hold:

(a) The good local correspondence between $T_1$ and $T_2$ holds for $\sigma|_{U_1}$ (cf. [8, Definition 2.5]).
(b) There exists a finite extension $L/L_1L_2$ such that $L/Q$ is Galois and $\delta(T_1(L)) \neq 0$ for (at least) one $i$.
(c) $P_{S_{i,f}} \cap P_{S_{2,f}} \neq \emptyset$.
(d) $L_i$ has a complex prime for (at least) one $i$.

Then, there exists $\tau \in G(L/Q)$ such that for any open normal subgroups $U'_1, U'_2$ of $G_{K_1, S_1}, G_{K_2, S_2}$ containing $U_1, U_2$, respectively, with $\sigma(U'_1) = U'_2$, it follows that $K_1 = \tau(K_2)$, $L'_1 = \tau(L'_2)$, and the isomorphism $G(L'_1/K_1) \sim G(L'_2/K_2)$ induced by $\sigma$ coincides with the isomorphism induced by $\tau|_{L'_i}$, where $L'_1, L'_2$ are finite Galois subextensions of $L_1/K_1, L_2/K_2$, corresponding to $U'_1, U'_2$, respectively.

**Proof.** By (d) and symmetry, we may assume that $L_2$ has a complex prime. Write $\overline{\sigma}_{L_1} : G(L_1/K_1) \sim G(L_2/K_2)$ for the isomorphism induced by $\sigma$. Take $l \in P_{S_{1,f}} \cap P_{S_{2,f}}$, where the existence follows from (c). Write $\overline{\sigma}_{L_1,l} : \Gamma_{L_1,l} \sim \Gamma_{L_2,l}$ for the isomorphism induced by $\sigma|_{U_1}$.

Here, we claim that there exists $\tau \in G(L_2/Q)$ such that $L_1 = \tau(L_2)$ and $\overline{\sigma}_{L_1,l} = (\overline{\tau}|_{L_2,l})^*$, where $(\overline{\tau}|_{L_2,l})^*$ : $\Gamma_{L_2,l} \sim \Gamma_{L_2,l}$ is the isomorphism induced by $\tau|_{L_2}$. To prove this claim, we use a string of techniques invented in [8, section 3]. By (a), (b), and [8, Proposition 3.3], there exists $\tau \in G(L_2/Q)$ such that $\overline{\sigma}_{L_1,l} \circ \pi_{L_1/l_1} = (\overline{\tau}|_{L_2,l})^* \circ \pi_{L_2/\tau(L_2)}$. Then, we have $\overline{\tau}|_{L_2,l}^* \circ \overline{\sigma}_{L_1,l} \circ \pi_{L_1/l_1} = \pi_{L_1/\tau(L_2)}$. By [8, Lemma 3.4], we obtain $L_1^{(\infty,j)} = \tau(L_2) = L_1\tau(L_2)^{(\infty,j)}$, and hence $L_1^{(\infty,j)}L = L_1\tau(L_2)^{(\infty,j)}L = L_1\tau(L_2)^{(\infty,j)}L = L\tau(L_2)^{(\infty,j)}$. By [8, Proposition 3.5], we obtain $L_1 = \tau(L_2)$. Further, since $\text{Im}(\pi_{L_1/l_1})$ is open in $\Gamma_{L_1,l}, \overline{\sigma}_{L_1,l}$ coincides with $(\overline{\tau}|_{L_2,l})^*$.

Write $(\overline{\tau}|_{L_2,l})^* : \text{Aut}(L_1) \sim \text{Aut}(L_2)$ for the isomorphism induced by $\tau|_{L_2}$. By the equality $\overline{\sigma}_{L_1,l} = (\overline{\tau}|_{L_2,l})^*$, for any $\tau_1 \in G(L_1/K_1)$, the actions of $\overline{\tau}_1(\tau_1)$ and $(\overline{\tau}|_{L_2,l})^*(\tau_1)$ on $\Gamma_{L_2,l}$ coincide. Therefore, by Lemma 2.1, we obtain $\overline{\tau}_1(\tau_1) = (\overline{\tau}|_{L_2,l})^*(\tau_1)$, so that $\overline{\sigma}_{L_1,l} = (\overline{\tau}|_{L_2,l})^*$. Hence, $\tau|_{L_2}$ is compatible with the actions of $G(L_2/K_2)$ and $G(L_1/K_1)$ on $L_2$ and $L_1$. Thus, for any $U'_1, U'_2$ as in the assertion, $\tau|_{L_2}$ induces an isomorphism between $L_2^{G(L_2/K_2)} = L'_2$ and $L_1^{G(L_1/K_1)} = L'_1$. Further, the isomorphism $G(L'_1/K_1) \sim G(L'_2/K_2)$ induced by $\sigma$ coincides with the isomorphism induced by $\tau|_{L'_2}$.

Before we see the following, let us review condition $(\ast_1)$ (cf. [8, Definition 1.16]). Due to its complexity, we do not treat its precise definition here. However, note that condition $(\ast_1)$ is weaker than the condition (independent of $l$) that $\delta(S) \neq 0$ (cf. [8, Proposition 1.20]).

**Theorem 3.2.** Let $\sigma : G_{K_1, S_1} \sim G_{K_2, S_2}$ be an isomorphism, and for $i = 1, 2$, $V_i$ a closed normal subgroup of $G_{K_i, S_i}$ with $\sigma(V_1) = V_2$. For $i = 1, 2$, write $M_i$ for the Galois subextension of $K_{i, S_i}/K_i$ corresponding to $V_i$. Assume that the following conditions hold:

(a) $P_{S_{i,f}} \geq 2$ for $i = 1, 2$.
(b) For (at least) one $i$ and for any finite Galois subextension $L_i$ of $M_i/K_i$, $\delta(P_{S_{i,f}} \cap cs(L_i/Q)) \neq 0$.
(c) For the $i$ in condition (b), there exists a prime number $l \in P_{S_{i,f}} \cap P_{S_{2,f}}$ such that $S_{3-i}$ satisfies condition $(\ast_1)$ (cf. [8, Definition 1.16]).
(d) $M_i$ has a complex prime for (at least) one $i$.
Then, there exists an isomorphism \( \tau : M_2 \sim M_1 \) such that \( K_1 = \tau(K_2) \) and the isomorphism \( G(M_1/K_1) \sim G(M_2/K_2) \) induced by \( \sigma \) coincides with the isomorphism induced by \( \tau \).

Proof. Let \( U_1 \) be any open normal subgroup of \( G_{K_1, S_1} \) containing \( V_1 \). Set \( U_2 \overset{\text{def}}{=} \sigma(U_1) \). For \( i = 1, 2 \), write \( L_i \) for the finite Galois subextension of \( K_{i, S_i}/K_i \) corresponding to \( U_i \). Let \( U'_1, U'_2 \) be any open normal subgroups of \( G_{K_1, S_1}, G_{K_2, S_2} \) containing \( U_1, U_2 \), respectively, with \( \sigma(U'_1) = U'_2 \). For \( i = 1, 2 \), write \( L'_i \) for the finite Galois subextension of \( L_i/K_i \) corresponding to \( U'_i \). We set

\[
\mathfrak{U}_{U_1} = \left\{ \tau \in G_{\mathbb{Q}} \mid \text{for any } U'_1, U'_2 \text{ as above, } K_1 = \tau(K_2), L'_1 = \tau(L'_2) \text{ and the isomorphism } G(L'_1/K_1) \sim G(L'_2/K_2) \text{ induced by } \sigma \text{ coincides with the isomorphism induced by } \tau|_{L'_2} \right\}.
\]

Note that \( \mathfrak{U}_{U_1} \) is a closed subset of \( G_{\mathbb{Q}} \). In order to prove the existence of \( \tau \) in the assertion, it suffices to show that \( \mathfrak{U}_{U_1} \neq \emptyset \) for every \( U_1 \) as above. Indeed, having shown this, we obtain \( \cap U_1 \mathfrak{U}_{U_1} \neq \emptyset \). Moreover, by (d), we may assume that \( L_1 \) has a complex prime for (at least) one \( i \). By symmetry, we may assume that the \( i \) in (b) is 1.

Now, we set \( L \overset{\text{def}}{=} L_1L_2 \). We claim that \( P_{S_1, f} \cap \text{cs}(L/\mathbb{Q}) = P_{S_1, f} \cap \text{cs}(L_1/\mathbb{Q}) \). To prove this claim, we use some techniques of the local correspondence invented in [8]. By (b) and [8, Lemma 4.1], we have \( \delta_{\text{sup}}(S_1) \geq \delta_{\text{sup}}((P_{S_1, f} \cap \text{cs}(K_1/\mathbb{Q}))(K_1)) = [K_1 : \mathbb{Q}]\delta_{\text{sup}}(P_{S_1, f} \cap \text{cs}(K_1/\mathbb{Q})) > 0 \). Hence, by [8, Proposition 1.20], \( S_1 \) satisfies condition \((\star l)\) for the prime number \( l \) in (c). Therefore, by (a), (c), and [8, Theorem 2.6], the local correspondence between \( S_1 \) and \( S_2 \) holds for \( \sigma \). By (a) and [8, Proposition 2.8], \( P_{S_1, f} = P_{S_2, f} \) and the good local correspondence between \( P_{S_1, f}(K_1) \) and \( P_{S_2, f}(K_2) \) holds for \( \sigma \). Further, by [8, Remark 2.7], the good local correspondence between \( P_{S_1, f}(L_1) \) and \( P_{S_2, f}(L_2) \) holds for \( \sigma \). Again by [8, Proposition 2.8], we have \( P_{S_1, f} \cap \text{cs}(L_1/\mathbb{Q}) = P_{S_2, f} \cap \text{cs}(L_2/\mathbb{Q}) \). Then, we have

\[
P_{S_1, f} \cap \text{cs}(L_1/\mathbb{Q}) = P_{S_1, f} \cap \text{cs}(L_1L_2/\mathbb{Q})
= P_{S_1, f} \cap \text{cs}(L_1/\mathbb{Q}) \cap \text{cs}(L_2/\mathbb{Q})
= P_{S_1, f} \cap \text{cs}(L_1/\mathbb{Q}).
\]

Therefore,

\[
\delta_{\text{sup}}(P_{S_1, f}(L_1)) = \delta_{\text{sup}}((P_{S_1, f} \cap \text{cs}(L_1/\mathbb{Q}))(L_1)) = [L_1 : \mathbb{Q}]\delta_{\text{sup}}(P_{S_1, f} \cap \text{cs}(L_1/\mathbb{Q})) = [L_1 : \mathbb{Q}]\delta_{\text{sup}}(P_{S_1, f} \cap \text{cs}(L_1'/\mathbb{Q})) > 0,
\]

where the second equality follows from [8, Lemma 4.1]. Thus, by Proposition 3.1, we obtain \( \mathfrak{U}_{U_1} \neq \emptyset \). \( \square \)

Remark 3.3. Let us see equivalent and sufficient conditions of condition (b) in Theorem 3.2. By [8, Lemma 4.1], condition (b) is equivalent to the condition: “for (at least) one \( i \) and for any finite Galois subextension \( L_i \) of \( M_i/K_i \), \( \delta(P_{S_i, f}(L_i)) \neq 0 \).” Further, again by [8, Lemma 4.1], this condition holds if the condition “for (at least) one \( i \) and for some finite extension \( L_i \) of \( K_i \) (not necessary contained in \( K_i(S_i) \), \( \delta_{\text{sup}}(P_{S_i, f}(L_i)) = 1^* \)” is satisfied. In particular, if \( \delta_{\text{sup}}(S_i) = 1 \) for (at least) one \( i \), then \( \delta_{\text{sup}}(S_1(K_1)) = 1 \), and hence \( \delta_{\text{sup}}(P_{S_i, f}(K_1)) = 1 \) by applying [8, Lemma 4.5] to \( K = K_1 \), so that condition (b) holds.

The main result in this paper is the following.

Theorem 3.4. Assume that the following conditions hold:

(a) \( \#P_{S_{i, f}} \geq 2 \) for \( i = 1, 2 \).
(b) For (at least) one \( i \) and for any finite Galois subextension \( L_i \) of \( K_{i, S_i}/K_i \), \( \delta(P_{S_{i, f}}(L_i/\mathbb{Q})) \neq 0 \).
(c) For the \( i \) in condition (b), there exists a prime number \( l \in P_{S_{i, f}} \cap P_{S_{2, f}} \) such that \( S_{3-i} \) satisfies condition \((\star l)\) (see [8, Definition 1.16]).

Let \( \sigma : G_{K_1, S_1} \sim G_{K_2, S_2} \) be an isomorphism. Then, there exists a unique isomorphism \( \tau : K_{2, S_2} \sim K_{1, S_1} \) such that \( K_1 = \tau(K_2) \) and \( \sigma \) coincides with the isomorphism induced by \( \tau \). In other words, the canonical map \( \text{Iso}(K_{2, S_2}/K_2, K_{1, S_1}/K_1) \to \text{Iso}(G_{K_1, S_1}, G_{K_2, S_2}) \) is bijective.
Proof. For \( i = 1, 2 \) and \( l \in P_{S_i,f} \), \( K_i(\mu_2)/K_i \) is unramified outside \( P_{K_i,l} \cup P_{K_i,\infty} \), so that \( K_i(\mu_2) \subset K_i.S_i \) are totally imaginary. Hence, the existence of \( \tau \) in the assertion follows from Theorem 3.2. Let \( \tau', \tau'' \in \text{Iso}(K_2.S_2/K_2, K_1.S_1/K_1) \) induce the same element in \( \text{Iso}(G_{K_1.S_1}, G_{K_2.S_2}) \). Then, the automorphism of \( G_{K_1.S_1} \) induced by the conjugation action of \( \tau''^{-1}\tau' \) is trivial. By Proposition 2.2, \( \tau''^{-1}\tau' \) is trivial. Thus, we obtain the uniqueness of \( \tau \) in the assertion.

□

4 | COROLLARIES

In this section, we prove some applications of the main theorem. First, we see some lemmas as a preparation.

Lemma 4.1. The canonical maps

\[
\begin{align*}
\text{Iso}(\mathcal{O}_{K_2.S_2}, \mathcal{O}_{K_1.S_1}) & \to \text{Iso}((K_2, S_2), (K_1, S_1)), \\
\text{Iso}(\mathcal{O}_{K_2.S_2}/\mathcal{O}_{K_1.S_1}^{(K_2.S_2)/(K_1.S_1)}) & \to \text{Iso}((K_2.S_2/K_2, S_2), (K_1.S_1/K_1, S_1))
\end{align*}
\]

are bijective.

Proof. The inverse maps are induced by restriction. □

Lemma 4.2. Assume \( P_\infty \subset S \) and that \( \# P_{S,f} \geq 1 \). Then, all finite primes in \( S_f \) and all real primes in \( P_\infty \) are ramified in \( K_S/K \).

Proof. Take \( l \in P_{S,f} \). Then, all finite primes in \( P_l \) and all real primes in \( P_\infty \) are ramified in \( K(\mu_\infty)/K \). Further, by the proof of [3, Lemma 2.3], all finite primes in \( S_f \setminus P_l \) are ramified in \( K_S/K \). □

Lemma 4.3. For (at least) one \( i \), assume \( \# P_{S_i,f} \geq 1 \). Then, the canonical inclusion

\[
\text{Iso}((K_2.S_2/(K_2, S_2), (K_1.S_1/K_1, S_1)) \to \text{Iso}((K_2.S_2/K_2, K_1.S_1/K_1))
\]

is bijective.

Proof. By symmetry, we may assume that \( \# P_{S_1,f} \geq 1 \). Take \( l \in P_{S_1,f} \). Then, \( \mu_\infty \subset K_1.S_1 \). If \( \text{Iso}(K_2.S_2/K_2, K_1.S_1/K_1) \) is not empty, then \( \mu_\infty \subset K_2.S_2 \), so that \( l \in P_{S_2,f} \). Thus, the assertion follows from Lemma 4.2. □

An element in \( \text{Iso}((K_2, S_2), (K_1, S_1)) \) can be extended to an element in

\[
\text{Iso}((K_2.S_2/K_2, S_2), (K_1.S_1/K_1, S_1)) \subset \text{Iso}((K_2.S_2/K_2, K_1.S_1/K_1),
\]

and therefore induces a well-defined element in \( \text{OutIso}(G_{K_1.S_1}, G_{K_2.S_2}) \). As a corollary of Theorem 3.4, we obtain the following, which is a generalization of [6, (12.2.2) Corollary].

Corollary 4.4. Let notation and assumption be the same as in Theorem 3.4. Then, the canonical map

\[
\text{Iso}((K_2.S_2), (K_1, S_1)) \to \text{OutIso}(G_{K_1.S_1}, G_{K_2.S_2})
\]

is bijective.

Proof. \( G_{K_2.S_2} \) acts on \( \text{Iso}(K_2.S_2/K_2, K_1.S_1/K_1) \) by the rule \( \sigma(\phi) \overset{\text{def}}{=} \phi\sigma^{-1} \), and by Lemma 4.3, we have a bijection \( \text{Iso}(K_2.S_2/K_2, K_1.S_1/K_1)/G_{K_2.S_2} \cong \text{Iso}(K_2.S_2, (K_1.S_1)) \). By Theorem 3.4, we have a bijection \( \text{Iso}(K_2.S_2/K_2, K_1.S_1/K_1) \to \text{Iso}(G_{K_1.S_1}, G_{K_2.S_2}) \), which is easily seen to be \( G_{K_2.S_2} \)-invariant if we let \( G_{K_2.S_2} \) act by inner automorphisms on the right-hand side (cf. Notations). Thus, factoring out the \( G_{K_2.S_2} \)-actions, we obtain the required bijection. □

Corollary 4.5. Assume \( P_\infty \subset S \) and that for any finite Galois subextension \( L \) of \( K_S/K \), \( \delta(P_{S,f} \cap \text{cs}(L/\mathbb{Q})) \neq 0 \). Then, there is a canonical isomorphism \( \text{Aut}(K, S) \cong \text{Out}(G_{K.S}) \).
Proof. By [8, Lemma 4.1] and [8, Proposition 1.20], \( S \) satisfies condition \((\star_l)\) for any \( l \in P_{S,f} \). Therefore, the assertion follows immediately from Corollary 4.4. \( \square \)

The following is a generalization of [6, (12.2.3) Corollary].

**Corollary 4.6.** Let notation and assumption be the same as in Corollary 4.5. Further, assume \( \text{Aut}(K, S) \) is trivial. Then, the canonical homomorphism \( G_{K,S} \to \text{Aut}(G_{K,S}) \) induced by the conjugation action is bijective. In particular, all automorphisms of \( G_{K,S} \) are inner.

**Proof.** By Corollary 4.5, \( \text{Out}(G_{K,S}) \) is trivial. Therefore, \( \text{Inn}(G_{K,S}) = \text{Aut}(G_{K,S}) \). By Proposition 2.2, the canonical homomorphism \( G_{K,S} \to \text{Inn}(G_{K,S}) \) is bijective. \( \square \)

**Remark 4.7.** Assume \( P_{\infty} \subset S \). Write \( \pi_1(\text{Spec} \ O_{K,S}, x) \) for the étale fundamental group of \( \text{Spec} \ O_{K,S} \), where \( x \) is the geometric point defined by the inclusion \( O_{K,S} \subset \overline{Q} \). Then, there exists a canonical isomorphism \( \pi_1(\text{Spec} \ O_{K,S}, x) \cong G_{K,S} \).

By the canonical isomorphisms in Lemma 4.1 and Lemma 4.3, we can identify the canonical map \( \text{Iso}(K_{2,S_2}/K_2, K_{1,S_1}/K_1) \to \text{Iso}(G_{K_1,S_1}, G_{K_2,S_2}) \) in the assertion of Theorem 3.4 with the canonical map

\[
\text{Iso}(O_{K_2,\bar{S}_2}O_{K_1,\bar{S}_1}) / O_{K_2,\bar{S}_2}O_{K_1,\bar{S}_1}(K_{1,S_1}) / (O_{K_1,S_1}) \to \text{Iso}(\pi_1(\text{Spec} \ O_{K_1,S_1}, x_1), \pi_1(\text{Spec} \ O_{K_2,S_2}, x_2)),
\]

where \( x_i \) is the geometric point defined by the inclusion \( O_{K_i,S_i} \subset \overline{Q} \) for \( i = 1, 2 \). Similarly, we can replace the fields and the Galois groups in the corollaries in this section by the rings and the étale fundamental groups, respectively. Note that there exist canonical maps

\[
\text{Iso}(O_{K_2,S_2}, O_{K_1,S_1}) \to \text{OutIso}(\pi_1(\text{Spec} \ O_{K_1,S_1}, x_1), \pi_1(\text{Spec} \ O_{K_2,S_2}, x_2)), \text{Aut}(O_{K,S}) \to \text{Out}(\pi_1(\text{Spec} \ O_{K,S}, x))
\]

for any base points \( x_1, x_2, x \), and that these maps do not depend essentially on the choice of the base points.

**ACKNOWLEDGMENTS**

The author would like to thank Professor Akio Tamagawa for helpful advice and carefully reading preliminary versions of this paper. The author would also like to thank Professor Florian Pop for comments on the proofs of Lemma A.2 and Lemma A.3 in a former version of this paper. The author would also like to thank the referees for the improvement of presentations. This work was supported by JSPS KAKENHI Grant Number 21J11879.

**ORCID**

Ryoji Shimizu https://orcid.org/0000-0002-6655-1548

**REFERENCES**

[1] T. T. Allen, Introduction to discrete event simulation and agent-based modeling: voting systems, health care, military, and manufacturing, Springer, New York, 2011.

[2] T. T. Ballen, Introduction to discrete event simulation and agent-based modeling: voting systems, health care, military, and manufacturing, 2nd ed., Springer, New York, 2011.

[3] G. Blanchard and R. Loubere, High-order conservative remapping with a posteriori MOOD stabilization on polygonal meshes, http://www.emn.fr/z-info/choco-solver/, 2015.

[4] R. Boggs, J. Bozman, and R. Perry, Reducing downtime and business loss: Adressing business risk with effective technology, Technical report 91-18, International Data Corporation (IDC), Sernageomin, 2002.

[5] S. Elbaum, A. G. Malishevsky, and G. Rothermel, Test case prioritization: a family of empirical studies, IEEE T. Software Eng. 28 (2002), no. 2, 159–182.

[6] G. Rothermel, A safe efficient regression test selection technique, ACM T. Softw. Eng. Meth. 6 (1997), no. 2, 173–210.

[7] G. Rothermel et al., A safe efficient regression test selection technique, ACM T. Softw. Eng. Meth. 6 (1998), no. 2, 173–210.

[8] A. Schulz and G. Dobhammer, Aktueller und zukünftiger Krankenbestand von Demenz in Deutschland auf basis der outinedaten der AOK. (Current and future number of people suffering from dementia in Germany based on routine data from the AOK.), C. Gnster, J. Klose, and N. Schmacke, eds.), Versorgungs-Report, IEEE Press, Piscataway, NJ, USA, pp. 161–175.

[9] S. Yoo and M. Harman, Pareto efficient multi-objective test case selection, Proceedings of the International Conference on Software Testing and Analysis, London, UK, pp. 140–150.
APPENDIX A: INTERSECTIONS OF DECOMPOSITION GROUPS

In this section, we study intersections of decomposition groups in \( G_{K,S} \). The results not only are interesting in themselves, but also give a proof of a little weaker version of Proposition 2.2 without Lemma 2.1 (cf. Proposition A.6).

**Lemma A.1.** Assume that \( P_\infty \subset S \) and that \( \#P_{S,f} \geq 2 \). Let \( \overline{p}, \overline{q} \in S_f(K_S) \). Then, \( D_{\overline{p}}(K_S/K) = D_{\overline{q}}(K_S/K) \) if and only if \( \overline{p} = \overline{q} \).

**Proof.** The assertion follows immediately from [3, Corollary 2.7(ii)]. \( \square \)

**Lemma A.2.** Let \( p \) be a prime number, \( \kappa \) a \( p \)-adic field, and \( N \) a nontrivial closed normal subgroup of \( G_\kappa \). Then, \( V_\kappa \cap N \) is a topologically infinitely generated pro-\( p \) subgroup.

**Proof.** The assertion follows immediately from [7, (1.4) Satz]. \( \square \)

**Lemma A.3.** Let \( p, l \) be distinct prime numbers, \( \kappa / \mathbb{Q}_p \) a (possibly infinite) algebraic extension, and \( \lambda / \kappa \) a Galois extension. Then, \( G(\lambda/\kappa) \) does not have a topologically infinitely generated pro-\( l \) subgroup.

**Proof.** We may assume that \( \kappa \) is a \( p \)-adic field and that \( \lambda = \overline{\kappa} \). Let \( G_{\kappa,f} \) be any \( l \)-Sylow subgroup of \( G_\kappa \). Then, there exists an exact sequence \( 1 \to \mathbb{Z}_l \to G_{\kappa,f} \to \mathbb{Z}_l \to 1 \), and hence all subgroups of \( G_{\kappa,f} \) are topologically generated by at most two elements (cf. [3, 2.2, Local situation and Lemma 2.2]). \( \square \)

**Proposition A.4.** Let \( \overline{p} \in S_f(K_S) \) and \( q \in P_K \setminus \{ \overline{p} | Q \} \). Assume that \( \overline{p} | Q \neq q | Q \) if \( q \in S_f \), and that \( D_{\overline{p}}(K_S/K) \) is full (cf. Notations). Then, \( D_{\overline{p}}(K_S/K) \cap (\cap_{q \in \{q \}(K_S)} D_q(K_S/K)) \) is trivial.

**Proof.** Let \( p = [\overline{p}]_Q \) and \( N = D_{\overline{p}}(K_S/K) \cap (\cap_{q \in \{q \}(K_S)} D_q(K_S/K)) \). Assume that \( N \) is nontrivial. By the fullness of \( D_{\overline{p}}(K_S/K) \) and Lemma A.2, \( N \) has a topologically infinitely generated pro-\( p \) subgroup. Assume \( q \notin S_f \). Then, \( q \) is unramified in \( K_S/K \) or an archimedean prime. Therefore, for any \( \overline{q} \in \{q \}(K_S) \), \( D_{\overline{q}}(K_S/K) \) is pro-cyclic, so that all subgroups of \( D_{\overline{q}}(K_S/K) \) are also pro-cyclic, a contradiction. Assume \( q \in S_f \). Then, \( p \neq q | Q \) by assumption. By Lemma A.3, for any \( \overline{q} \in \{q \}(K_S) \), \( D_{\overline{q}}(K_S/K) \) does not have a topologically infinitely generated pro-\( p \) subgroup, a contradiction. \( \square \)

**Corollary A.5.** Assume that \( P_\infty \subset S \) and that \( \#P_{S,f} \geq 2 \). Then, \( \cap_{\overline{p} \in S_f(K_S)} D_{\overline{p}}(K_S/K) \) is trivial.

**Proof.** Take \( \overline{p} \in P_{S,f}(K_S) \) and \( q \in S_f \) with \( \overline{p} | Q \neq q | Q \). By [1, Théorème 5.1], \( D_{\overline{p}}(K_S/K) \) is full (see [3, Corollary 2.6]). By Proposition A.4, we have \( D_{\overline{p}}(K_S/K) \cap (\cap_{q \in \{q \}(K_S)} D_q(K_S/K)) = 1 \). Thus, we obtain \( \cap_{\overline{p} \in S_f(K_S)} D_{\overline{p}}(K_S/K) = 1 \). \( \square \)

**Proposition A.6.** Assume that \( P_\infty \subset S \) and that \( \#P_{S,f} \geq 2 \). Let \( \tau \in \text{Aut}(K_S) \). Assume \( \tau(K) = K \) and that the automorphism of \( G_{K,S} \) induced by the conjugation action of \( \tau \) is trivial. Then, \( \tau \) is trivial.

**Proof.** Write \( K_0 \) for the \( \text{Aut}(K_S) \)-invariant subfield of \( K_S \). Then, \( K_S/K_0 \) is Galois. Let \( \overline{p} \in S_f(K_S) \). Then, we have \( D_{\overline{p}}(K_S/K) = \tau^{-1} D_{\overline{p}}(K_S/K) \tau = D_{\overline{p}}(K_S/K) \) in \( \text{Aut}(K_S) \). By Lemma 4.3, \( \tau \overline{p} \in S_f(K_S) \). Therefore, by Lemma A.1, we obtain \( \tau \overline{p} = \overline{p} \), and hence \( \tau \in D_{\overline{p}}(K_S/K_0) \). Thus, \( \tau \in N \) by \( \cap_{\overline{p} \in S_f(K_S)} D_{\overline{p}}(K_S/K_0) \).

By Corollary A.5, \( N \cap G_{K,S} = \cap_{\overline{p} \in S_f(K_S)} D_{\overline{p}}(K_S/K) \) is trivial. Hence, \( N \) is finite. As in the proof of Corollary A.5, for \( \overline{p} \in P_{S,f}(K_S) \), \( D_{\overline{p}}(K_S/K) \) is full, and hence \( D_{\overline{p}}(K_S/K_0) \) is also full, so that \( D_{\overline{p}}(K_S/K_0) \) is torsion-free by [6, (7.1.8) Theorem (i)]. Therefore, \( N \) is trivial. Thus, \( \tau \) is trivial. \( \square \)