

ON A GENERALIZATION OF THE NEUKIRCH-UCHIDA THEOREM

ALEXANDER B. IVANOV

ABSTRACT. In this article we generalize a part of Neukirch-Uchida theorem for number fields from the birational case to the case of curves $\text{Spec } \mathcal{O}_{K,S}$ where S a stable set of primes of a number field K . Such sets have positive but arbitrarily small Dirichlet density, which must be uniformly bounded from below by some $\epsilon > 0$ in the tower K_S/K .

2010 Mathematical Subject Classification: 11R34, 11R37, 14G32.

АБСТРАКТ. В этой статье мы обобщим теорему Нейкирха-Ушиды для числовых полей от бирационального случая к случаю кривых $\text{Spec } \mathcal{O}_{K,S}$, где S стабильное множество простых идеалов в числовом поле K . Такие множества имеют положительную плотность Дирихле, которая равномерно ограничена снизу в башне K_S/K .

1. INTRODUCTION

The anabelian Neukirch-Uchida theorem ([7], [10]) states essentially that each isomorphism of the absolute Galois groups of two global fields comes (up to conjugation) from a unique isomorphism of the fields. In particular, if the absolute Galois groups are isomorphic, then the fields are isomorphic. We restrict attention to the case of two number fields, which we call K_1, K_2 , calling their absolute Galois groups G_{K_1}, G_{K_2} (with respect to chosen algebraic closures). The proof of the theorem proceeds essentially in two steps: first one establish a “local correspondence”, i.e., starting with a given isomorphism $\sigma: G_{K_1} \rightarrow G_{K_2}$, one constructs a well-behaved bijection between the sets of (non-archimedean) primes of K_1 and K_2 , which respects residue characteristics and absolute degrees. From this, it is an exercise in applying the Chebotarev density theorem to deduce the following partial result: if K_1/\mathbb{Q} is normal and $G_{K_1} \cong G_{K_2}$, then $K_1 \cong K_2$. Then in the second (rather technical) step, one deduces from this the general statement of the theorem.

The aim of this paper is to prove the partial statement mentioned above in a setup with restricted ramification. While the situation in positive characteristic is quite well-understood due to the influential works of Tamagawa [9] and Mochizuki [6], the case of arithmetic curves is still remaining completely unclear. We consider schemes of the form $\text{Spec } \mathcal{O}_{K,S}$, where K is a number field, S a set of primes of positive, but arbitrary small Dirichlet density, and $\mathcal{O}_{K,S}$ is the ring of S -integers of K . The striking condition on S will be that the density of S is not only positive, but also uniformly bounded from below in a whole tower of extensions of K : $\delta_L(S) > \epsilon > 0$ for some ϵ independent of the finite subextension $K_S/L/K$ (where K_S/K denote the maximal extension unramified outside S). Essentially, sets satisfying a condition of this kind were introduced in [4], where they were called *stable*. The case of the schemes $\text{Spec } \mathcal{O}_{K,S}$ with S stable, can be seen as lying somewhere between the birational case considering $\text{Spec } K$ and the arithmetic case considering $\text{Spec } \mathcal{O}_{K,S}$ with S a finite set of primes. Clearly, the arithmetic case is much harder, and a strong anabelian result there seems to be out of scope at the moment. Here is our main result (for the precise statement see Theorem 4.1):

Theorem 1.1. *For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i . Assume that K_1 is totally imaginary and normal over \mathbb{Q} and that for $i = 1, 2$, S_i is stable in the above sense and that additionally some mild explicit assumptions hold for S_i (see Theorem 4.1). If $G_{K_1, S_1} \cong G_{K_2, S_2}$ as topological groups, then $K_1 \cong K_2$.*

The first step in the proof of this theorem is again a “local correspondence at the boundary”, which is very similar to the birational case. It is a bijection deduced out of a given isomorphism $\sigma: G_{K_1, S_1} \rightarrow$

The author was partially supported by Mathematical Center Heidelberg and the Mathematical Institute Heidelberg.

G_{K_2, S_2} , between primes of S_1 and S_2 , which respects the residue characteristics and the absolute degrees of primes. In contrast to the original proof of Neukirch, we neither need to know that the decomposition groups of primes in S_i are the full local Galois groups, nor that there is a rational prime p invertible on $\text{Spec } \mathcal{O}_{K, S}$. We emphasize that there are examples of even quite “nice” stable sets S , for which no rational prime is invertible on $\text{Spec } \mathcal{O}_{K, S}$ (cf. [4] Section 3.4).

Now, after establishing a local correspondence in the birational case, the corresponding result follows almost directly by an easy application of the Chebotarev density theorem. In the much more general setup of stable sets a similar argument involving Chebotarev is impossible, since now the Dirichlet density can get arbitrarily small. Thus one needs further arguments to prove the theorem. Those are given in Proposition 4.2 and Proposition 4.5 and make use of the stability of the sets S_i in a quite tricky way.

Notation. In this paper we use the same notations as in [3]. In particular, p denotes a prime number, for a pro-finite group G we denote by $G(p)$ its maximal pro- p quotient and by G_p a p -Sylow subgroup. For a subgroup $H \subseteq G$, we denote by $N_G(H)$ its normalizer in G .

For a Galois extension M/L of fields, $G_{M/L}$ denotes its Galois group. By K we always denote an algebraic number field, that is a finite extension of \mathbb{Q} . If L/K is a Galois extension and $\bar{\mathfrak{p}}$ is a prime of L , then $D_{\bar{\mathfrak{p}}, L/K} \subseteq G_{L/K}$ denotes the decomposition subgroup of $\bar{\mathfrak{p}}$. If $\mathfrak{p} := \bar{\mathfrak{p}}|_K$ is the restriction of $\bar{\mathfrak{p}}$ to K , then we sometimes allow us to write $D_{\bar{\mathfrak{p}}}$ or $D_{\mathfrak{p}}$ instead of $D_{\bar{\mathfrak{p}}, L/K}$, if no ambiguity can occur. We write Σ_K for the set of all primes of K and S, T will usually denote subsets of Σ_K . If L/K is an extension and S a set of primes of K , then we denote the pull-back of S to L by S_L , $S(L)$ or S (if no ambiguity can occur). We write K_S/K for the maximal extension of K , which is unramified outside S and $G_S := G_{K, S}$ for its Galois group. We denote by K_S^T/K the maximal extension of K , which is unramified outside S and completely split in T . Further, for $p \leq \infty$ a (archimedean or non-archimedean) prime of \mathbb{Q} , $S_p = S_p(K)$ denotes the set of all primes of K lying over p and $S_f := S \setminus S_\infty$.

We denote by $\delta_K(S)$ the Dirichlet density of the set S of primes of K .

An outline of the paper. After recalling necessary definitions and facts about stable sets in Section 2, we will in Section 3 establish the local correspondence at the boundary for a given isomorphism of two Galois groups of the form $G_{K, S}$ with S stable. This is the first step towards a proof of the main Theorem 4.1. In Sections 4.1 and 4.2 we give two further arguments needed in its proof. Finally, in Section 4.3 we prove Theorem 4.1.

Acknowledgements. The results in this paper coincide essentially with a part of author’s Ph.D. thesis [2], which was written under supervision of Jakob Stix at the University of Heidelberg. The author is very grateful to him for the very good supervision, and to Kay Wingberg, Johannes Schmidt and a lot of other people for very helpful remarks and interesting discussions. The work on author’s Ph.D. thesis was partially supported by Mathematical Center Heidelberg and the Mathematical Institute Heidelberg. Also the author is grateful to both of them for their hospitality and the excellent working conditions.

2. STABLE SETS

We briefly recall some definitions and results from [4].

Definition 2.1 (part of [4] Definitions 2.4, 2.7). Let S be a set of primes of K and \mathcal{L}/K any extension.

- (i) Let $\lambda > 1$. A finite subextension $\mathcal{L}/L_0/K$ is **λ -stabilizing for S for \mathcal{L}/K** , if there exists a subset $S_0 \subseteq S$ and some $a \in (0, 1]$, such that $\lambda a > \delta_L(S_0) \geq a > 0$ for all finite subextensions $\mathcal{L}/L/L_0$. We say that S is **λ -stable**, if it has a λ -stabilizing extension for \mathcal{L}/K . We say that S is **stable for \mathcal{L}/K** , if it is λ -stable for \mathcal{L}/K for some $\lambda > 1$. We say that S is **(λ) -stable**, if it is (λ) -stable for K_S/K .
- (ii) Let p be a rational prime. We say that S is **sharply p -stable for \mathcal{L}/K** , if $\mu_p \subseteq \mathcal{L}$ and S is p -stable for \mathcal{L}/K or $\mu_p \not\subseteq \mathcal{L}$ and S is stable for $\mathcal{L}(\mu_p)/K$. We say that S is **sharply p -stable**, if S is sharply p -stable for K_S/K .

Most natural examples of stable sets are given by almost Chebotarev sets: if M/K is a finite Galois extension and $\sigma \in G_{M/K}$, then the associated Chebotarev set is defined as

$$P_{M/K}(\sigma) := \{\mathfrak{p} \in \Sigma_K : \mathfrak{p} \text{ is unramified in } M/K \text{ and } \text{Frob}_{\mathfrak{p}, M/K} \text{ is the conjugacy class of } \sigma\}.$$

We say that a set is almost Chebotarev, if it differs from a Chebotarev set only by a subset of density zero. They are stable in many cases (cf. [4] Corollary 3.4, Corollary 3.6), and even if not, they inherit many properties of stable sets. Also a stable almost Chebotarev set are sharply p -stable for almost all rational primes p (cf. [4] Proposition 3.8(ii)).

Theorem 2.2 ([4], Theorem 5.1(A)). *Let K be a number field, p a rational prime and $S \supseteq R$ sets of primes of K with R finite. Assume that S is sharply p -stable for K_S^R/K . Then*

$$K_{S,p}^R \supseteq \begin{cases} K_{\mathfrak{p}}(p), & \text{if } \mathfrak{p} \in S \setminus R \\ K_{\mathfrak{p}}^{\text{nr}}(p) & \text{if } \mathfrak{p} \notin S. \end{cases}$$

For a Galois extension \mathcal{L}/K , an integer $i \geq 0$ and a $G_{\mathcal{L}/K}$ -module A , let $\text{III}^i(\mathcal{L}/K; A)$ be the Tate-Shafarevich group, which is defined by exactness of the sequence

$$0 \rightarrow \text{III}^i(\mathcal{L}/K; A) \rightarrow H^i(\mathcal{L}/K; A) \rightarrow \prod_{\mathfrak{p} \in \Sigma_K} H^i(\mathcal{L}_{\bar{\mathfrak{p}}}/K_{\mathfrak{p}}; A),$$

where $\bar{\mathfrak{p}}$ is any prime of \mathcal{L} lying over \mathfrak{p} . We also write $\text{III}^i(G_{\mathcal{L}/K}; A)$ instead of $\text{III}^i(\mathcal{L}/K; A)$.

Proposition 2.3 ([4], Proposition 5.13(ii)). *Let K be a number field, S a set of primes of K . Let p be a rational prime, $r > 0$ an integer. Assume that either p is odd or K_S is totally imaginary. Let $K_S/\mathcal{L}/K$ be a normal subextension. Assume S is sharply p -stable for \mathcal{L}/K and $p^\infty | [\mathcal{L} : K]$. Then*

$$\varinjlim_{\mathcal{L}/L/K} \text{III}^2(K_S/L; \mathbb{Z}/p^r\mathbb{Z}) = 0.$$

Remark 2.4. If S contains an almost Chebotarev set, then the global realization result Theorem 2.2 holds for S with respect to all rational primes p (i.e., $(K_S)_{\mathfrak{p}} = \overline{K_{\mathfrak{p}}}$), even if S is not sharply p -stable for some p 's. The proof of this involves further arguments and seems to be much more technical (cf. [5]).

3. LOCAL CORRESPONDENCE AT THE BOUNDARY

Generalizing results of Neukirch, we show that under certain conditions on the set S of primes of K , the decomposition groups of primes in S are intrinsically determined by $G_{K,S}$. Since we in general do not know, whether the decomposition groups are the full local groups, we can not characterize them as absolute Galois groups of local fields and thus we have to deal with p -Sylow subgroups, which are of particularly simple kind.

3.1. Some technical preparations. As in [3] we use the following notational short-cut.

Definition 3.1 ([3] Definition 2.1). A group of p -decomposition type is a non-abelian pro- p Demushkin group of rank 2.

Thus a group of p -decomposition type is of the form $\mathbb{Z}_p \rtimes \mathbb{Z}_p$ with $\mathbb{Z}_p \hookrightarrow \text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^*$ injective (this follows from [8] 3.9.9, 3.9.11). Such groups have an easy structure theory and one easily describes all their subgroups explicitly (cf. [3] Lemma 2.2).

Lemma 3.2. *Let K be a number field, S a set of primes of K , p a rational prime. Assume S is stable and sharply p -stable. If $\bar{\mathfrak{p}}$ is a prime of K_S , let $D_{\bar{\mathfrak{p}},p} \subseteq D_{\bar{\mathfrak{p}}}$ denote a p -Sylow subgroup. For any $\bar{\mathfrak{p}}_1 \neq \bar{\mathfrak{p}}_2 \in S(K_S)$ with $\bar{\mathfrak{p}}_1$ non-archimedean we have inside $G_{K,S}$:*

$$(D_{\bar{\mathfrak{p}}_1,p} : D_{\bar{\mathfrak{p}}_1,p} \cap D_{\bar{\mathfrak{p}}_2,p}) = \infty$$

and

$$(D_{\bar{\mathfrak{p}}_1} : D_{\bar{\mathfrak{p}}_1} \cap D_{\bar{\mathfrak{p}}_2}) = \infty.$$

Proof. An easy index computation shows that one can go up to a finite extension of K inside K_S . Using this, we can assume that $\bar{\mathfrak{p}}_1|_K \neq \bar{\mathfrak{p}}_2|_K$ and (by [4] Lemma 2.7) that for any subextensions $K_S/\mathcal{L}/L/K$ with L/K finite, S is sharply p -stable for \mathcal{L}/L . Now an application of Theorem 2.2 (with $R = \{\bar{\mathfrak{p}}_2|_K\}$) shows that $D_{\bar{\mathfrak{p}}_2}$ lies in the kernel of the projection

$$G_{K,S} \twoheadrightarrow G_{K,S}^R,$$

whereas $D_{\bar{\mathfrak{p}}_1,p}$ has infinite image. Thus $(D_{\bar{\mathfrak{p}}_1,p} : D_{\bar{\mathfrak{p}}_1,p} \cap D_{\bar{\mathfrak{p}}_2,p}) \geq (D_{\bar{\mathfrak{p}}_1,p} : D_{\bar{\mathfrak{p}}_1,p} \cap V) = \infty$, where $V := \ker(G_{K,S} \twoheadrightarrow G_{K,S}^R)$. The second statement follows from the first. \square

Lemma 3.3. *Let κ be a p -adic field. Let κ'/κ be a Galois extension containing the maximal pro- p -extension of any finite subfield $\kappa'/\lambda/\kappa$. Then $G_{\kappa'/\kappa}$ do not contain any subgroup of p -decomposition type.*

Proof. Is the same as for [3] Lemma 3.2. \square

Lemma 3.4. *Let K be a number field, S a set of primes of K and p a rational prime. Assume S is sharply p -stable.*

- (i) *Let $H_0 \subseteq D_{\bar{\mathfrak{p}}}$ be a subgroup of p -decomposition type, where $\bar{\mathfrak{p}} \in S_f$. Then $N_{G_{K,S}}(H_0) \subseteq D_{\bar{\mathfrak{p}}}$.*
- (ii) *Let H be a subgroup of $G_{K,S}$ of p -decomposition type. Assume there is an open subgroup $H_0 \subseteq H$ such that $H_0 \subseteq D_{\bar{\mathfrak{p}},p}$ for some prime $\bar{\mathfrak{p}} \in S_f$. Then $H \subseteq D_{\bar{\mathfrak{p}}}$.*

Proof. (i): Let $D_{\bar{\mathfrak{p}},p} \subseteq D_{\bar{\mathfrak{p}}}$ be a p -Sylow subgroup, containing H_0 . First of all, by Lemma 3.3 (which assumptions are satisfied by Theorem 2.2), $\bar{\mathfrak{p}}$ does not lie over p . Consequently, $D_{\bar{\mathfrak{p}},p}$ is also of p -decomposition type (it can not be pro-cyclic, since it already contains H_0), and hence by [3] Lemma 2.2, the inclusion $H_0 \subseteq D_{\bar{\mathfrak{p}},p}$ is open. Let $x \in N_{G_{K,S}}(H_0)$. Then $H_0 = xH_0x^{-1} \subseteq xD_{\bar{\mathfrak{p}},p}x^{-1} = D_{x\bar{\mathfrak{p}}}$. Thus $D_{\bar{\mathfrak{p}}} \cap D_{x\bar{\mathfrak{p}}} \supseteq H_0$ contains an open subgroup of $D_{\bar{\mathfrak{p}},p}$. Hence Lemma 3.2 implies $x\bar{\mathfrak{p}} = \bar{\mathfrak{p}}$, i.e., $x \in D_{\bar{\mathfrak{p}}}$.

(ii): Replacing H_0 by the intersection of all its H -conjugates, we can assume that H_0 is normal in H . Since H_0 is also of p -decomposition type, part (i) implies $H \subseteq D_{\bar{\mathfrak{p}}}$. \square

3.2. Characterization of decomposition groups.

Theorem 3.5. *Let K be a number field and S a set of primes of K . Assume there is a rational prime p such that $S \supseteq S_\infty$ is sharply p -stable. Let $H \subseteq G_{K,S}$ be of p -decomposition type and assume that H satisfies the following technical condition: for any intermediate subgroup $H \subseteq U \subseteq G_{K,S}$ with last inclusion open, $p^\infty | (U : \langle\langle H \rangle\rangle_U)$ where $\langle\langle H \rangle\rangle_U$ denotes the minimal closed normal subgroup of U , containing H . Then H is contained in a decomposition subgroup of a unique prime in $(S_f \setminus S_p)(K_S)$.*

Proof. Let first $\bar{\mathfrak{p}}$ be a p -adic prime of K_S contained in $S(K_S)$ and let $\mathfrak{p} = \bar{\mathfrak{p}}|_K$. By [4] Lemma 2.7, S is sharply p -stable for K_S/L for all finite and big enough subextensions $K_S/L/K$. Thus by Theorem 2.2, $(K_S)_{\bar{\mathfrak{p}}}/K_{\mathfrak{p}}$ satisfies the assumptions of Lemma 3.3, and hence $D_{\bar{\mathfrak{p}}}$ contains no subgroups of p -decomposition type. All this shows that if $H \subseteq D_{\bar{\mathfrak{p}}}$ for some prime $\bar{\mathfrak{p}}$ of K_S , then $\bar{\mathfrak{p}}$ is not p -adic.

Assume now $H \subseteq D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}}$ for two different primes $\bar{\mathfrak{p}} \neq \bar{\mathfrak{q}}$ in $S(K_S)$. As shown above, $\bar{\mathfrak{p}}, \bar{\mathfrak{q}}$ are not p -adic. By [3] Lemma 2.2(ii), the inclusions $H \subseteq D_{\bar{\mathfrak{p}},p}$ and $H \subseteq D_{\bar{\mathfrak{q}},p}$ are open (here $D_{\bar{\mathfrak{p}},p}, D_{\bar{\mathfrak{q}},p}$ are some p -Sylow subgroups of $D_{\bar{\mathfrak{p}}}, D_{\bar{\mathfrak{q}}}$). Thus $D_{\bar{\mathfrak{p}},p}$ contains an open subgroup of $D_{\bar{\mathfrak{q}},p}$, which implies $(D_{\bar{\mathfrak{q}},p} : D_{\bar{\mathfrak{q}},p} \cap D_{\bar{\mathfrak{p}},p}) < \infty$. This is a contradiction to Lemma 3.2. This contradiction shows the uniqueness statement in the theorem.

Let $H \subseteq G_{K,S}$ be a closed subgroup of p -decomposition type, which satisfies the technical condition in Theorem 3.5. By Lemma 3.4(ii) it is enough to show only that an open subgroup of H is contained in a decomposition group of a prime in $S_f \setminus S_p$. Hence by [4] Lemma 2.7 we can assume that for all subextensions $K_S/\mathcal{L}/K$, S is sharply p -stable for \mathcal{L}/K . Further, if $p = 2$, by Theorem 2.2 K_S is totally imaginary, hence we can assume that K is totally imaginary in this case. For any $H \subseteq U \subseteq G_{K,S}$ with last inclusion open consider the restriction map $H^2(U, \mathbb{Z}/p\mathbb{Z}) \rightarrow \bigoplus_{\mathfrak{p} \in S(K_S^U)} H^2(D_{\mathfrak{p}, K_S/K_S^U}, \mathbb{Z}/p\mathbb{Z})$. The main observation is that

$$\varinjlim_{H \subseteq U \subseteq G_{K,S}} \text{III}^2(U, \mathbb{Z}/p\mathbb{Z}) = 0,$$

as by our assumption and by Proposition 2.3, for any class $\alpha \in \text{III}^2(U, \mathbb{Z}/p\mathbb{Z})$ there is a subgroup $U \supseteq V \supseteq \langle\langle H \rangle\rangle_U \supseteq H$ with first inclusion open, such that the image of α in $\text{III}^2(V, \mathbb{Z}/p\mathbb{Z})$ is zero. Thus passing to the direct limit over all open U containing H we obtain an injection:

$$\mathbb{Z}/p\mathbb{Z} \cong \text{H}^2(H, \mathbb{Z}/p\mathbb{Z}) \hookrightarrow \prod_{\mathfrak{p} \in S(M)} \text{H}^2(D_{\mathfrak{p}, K_S/M}, \mathbb{Z}/p\mathbb{Z}).$$

where $M := K_S^H$. Hence there is a prime $\mathfrak{p} \in S(M)$ with $\text{H}^2(D_{\mathfrak{p}, K_S/M}, \mathbb{Z}/p\mathbb{Z}) \neq 0$, this prime is non-archimedean, since K is totally imaginary if $p = 2$ and the proof can be finished as in the original paper of Neukirch [7] Theorem 1 (also cf. [8] 12.1.9). \square

Corollary 3.6. *Let K be a number field and S a set of primes of K . Assume there is a rational prime p such that the following hold:*

- (i) $S \supseteq S_\infty$ is sharply p -stable,
- (ii) for each $\mathfrak{p} \in S_f$, we have $\mu_p \subseteq K_{S, \mathfrak{p}}$.

Then the topological group $G_{K, S}$ given together with the prime p determines intrinsically the decomposition subgroups of primes in $S_f \setminus S_p$.

Proof. The proof works exactly as in [3] Section 3.4. For convenience we repeat it here (except for some technical details). For a prime \mathfrak{p} of K , let $\mathcal{G}_{\mathfrak{p}}$ denote the absolute Galois group of the local field $K_{\mathfrak{p}}$ and let $\mathcal{G}_{\mathfrak{p}, p}$ be one of its p -Sylow subgroups. First of all, since $\mu_p \subseteq K_{S, \mathfrak{p}}$ for any $\mathfrak{p} \in S_f$, it follows from Theorem 2.2 that for any $\bar{\mathfrak{p}} \in (S_f \setminus S_p)(K_S)$, the composition

$$\mathcal{G}_{\mathfrak{p}, p} \hookrightarrow \mathcal{G}_{\mathfrak{p}} \twoheadrightarrow D_{\bar{\mathfrak{p}}} \hookrightarrow G_{K, S}$$

is injective, or with other words, a p -Sylow subgroup of $D_{\bar{\mathfrak{p}}}$ is of p -decomposition type. For any $U \subseteq G_{K, S}$ open (and small enough) we claim the equality of the following subsets of the set of all subgroups of p -decomposition type inside U :

$$\text{Syl}_p(U, S_f \setminus S_p) = \left\{ \begin{array}{l} H \text{ is a subgroup of } p\text{-decomposition type satisfying} \\ H \subseteq U: \text{ the technical condition in Theorem 3.5} \\ \text{and maximal of this type} \end{array} \right\},$$

where $\text{Syl}_p(U, S_f \setminus S_p)$ denotes the set of all p -Sylow subgroups of decomposition subgroups of primes in $S_f \setminus S_p$ of the field K_S^U . Indeed, Theorem 3.5 assures that any group in the right set is contained in a decomposition group of a prime in $S_f \setminus S_p$, and by maximality it has to be a p -Sylow subgroup. Conversely, any group H lying in the left set is of p -decomposition type, satisfies the technical property from Theorem 3.5 (by Lemma 3.2) and is maximal with these properties. Indeed, to prove maximality assume $H \subseteq H'$ with H' of p -decomposition type. This inclusion has to be open by [3] Lemma 2.2(ii) and thus by Lemma 3.4(ii), H' is contained in the same decomposition group as H . Since both are pro- p -groups and H is a p -Sylow subgroup, we get $H = H'$, proving the maximality of H .

Thus the data $(G_{K, S}, p)$ determine intrinsically the set $\text{Syl}_p(U, S_f \setminus S_p)$ for any $U \subseteq G_{K, S}$ open. U acts on this set by conjugation. We have an U -equivariant surjection

$$\psi: \text{Syl}_p(U, S_f \setminus S_p) \twoheadrightarrow (S_f \setminus S_p)(U)$$

(U acts trivially on the right side), which sends H to the prime $\bar{\mathfrak{p}}|_L$, such that $H \subseteq D_{\bar{\mathfrak{p}}, K_S/L}$, where $L := K_S^U$. By [3] Lemma 3.9 we have a purely group theoretical criterion for two elements on the left side to lie in the same fiber of this surjection, which allows us to reconstruct the set $(S_f \setminus S_p)(U)$. For any inclusion $V \hookrightarrow U$ of open subgroups of $G_{K, S}$, we have (a priori non-canonical) maps $\text{Syl}_p(V, S_f \setminus S_p) \rightarrow \text{Syl}_p(U, S_f \setminus S_p)$, and via ψ they induce the restriction-of-primes maps $(S_f \setminus S_p)(V) \rightarrow (S_f \setminus S_p)(U)$. Finally, if $U \subseteq G_{K, S}$ is normal, the $G_{K, S}$ -action by conjugation on $\text{Syl}_p(U, S_f \setminus S_p)$ induces via ψ the natural $G_{K, S}$ -action on $(S_f \setminus S_p)(U)$ by permuting the primes. In this way we have reconstructed the projective system of $G_{K, S}$ -sets $\{(S_f \setminus S_p)(U): U \subseteq U_0, U \triangleleft G_{K, S}\}$, where $U_0 \subseteq G_{K, S}$ is some open subgroup. Now the decomposition subgroups of primes in $S_f \setminus S_p$ are exactly the stabilizers in $G_{K, S}$ of elements in the $G_{K, S}$ -set $\varprojlim_{U \subseteq U_0, U \triangleleft G_{K, S}} (S_f \setminus S_p)(U)$. \square

Remark 3.7.

- (i) It is remarkable that Theorem 3.5 and Corollary 3.6 hold even if $\mathbb{N}(S) = \{1\}$, i.e, if there is no rational prime invertible on $\text{Spec } \mathcal{O}_{K,S}$. Indeed, there are examples of stable sets with arbitrarily small density which are sharply p -stable for all p and $\mathbb{N}(S) = \{1\}$ ([4] Section 3.4)
- (ii) Observe that sharp 2-stability is equivalent to 2-stability. In particular, the assumptions of Corollary 3.6 in the case $p = 2$ reduce to ' S is 2-stable and $S \supseteq S_\infty$ '.

3.3. Local correspondence at the boundary.

Definition 3.8. For $i = 1, 2$, let K_i be a number field, S_i a set of primes of K_i and let

$$\sigma: G_{K_1, S_1} \xrightarrow{\sim} G_{K_2, S_2}$$

be a (topological) isomorphism. If U_1 is a closed subgroup of G_{K_1, S_1} with fixed field L_1 , we write U_2 for $\sigma(U_1)$ and L_2 for its fixed field, etc. We say that the **local correspondence at the boundary** holds for σ , if the following conditions are satisfied:

- (i) For $i = 1, 2$, there is a finite exceptional set $S_i^{\text{ex}} \subseteq S_i$, such that for any $\bar{\mathfrak{p}}_1 \in (S_{1,f} \setminus S_1^{\text{ex}})(K_{1,S_1})$, there is a unique prime $\sigma_*(\bar{\mathfrak{p}}_1) \in (S_{2,f} \setminus S_2^{\text{ex}})(K_{2,S_2})$, with $\sigma(D_{\bar{\mathfrak{p}}_1}) = D_{\sigma_*(\bar{\mathfrak{p}}_1)}$, such that σ induces a bijection

$$\sigma_*: (S_{1,f} \setminus S_1^{\text{ex}})(K_{1,S_1}) \xrightarrow{\sim} (S_{2,f} \setminus S_2^{\text{ex}})(K_{2,S_2})$$

which is Galois-equivariant, i.e.,

$$\sigma_*(g\bar{\mathfrak{p}}_1) = \sigma(g)\sigma_*(\bar{\mathfrak{p}}_1)$$

for each $g \in G_{K_1, S_1}$ and $\bar{\mathfrak{p}}_1 \in (S_{1,f} \setminus S_1^{\text{ex}})(K_{1,S_1})$. In particular, for any finite subextension L_1 of $K_{1,S_1}/K_1$ with corresponding open subgroup $U_1 \subseteq G_{K_1, S_1}$, if two primes $\bar{\mathfrak{p}}_1, \bar{\mathfrak{q}}_1 \in S_{1,f}(K_{1,S_1})$ restrict to the same prime of L_1 , then also $\sigma_*(\bar{\mathfrak{p}}_1), \sigma_*(\bar{\mathfrak{q}}_1)$ restrict to the same prime of L_2 , and hence σ_* induces a bijection

$$\sigma_{*,U_1}: (S_{1,f} \setminus S_1^{\text{ex}})(L_1) \xrightarrow{\sim} (S_{2,f} \setminus S_2^{\text{ex}})(L_2).$$

- (ii) For all $K_{1,S_1}/L_1/K_1$ finite with corresponding subgroup $U_1 \subseteq G_{K_1, S_1}$ and for all but finitely many primes $\mathfrak{p}_1 \in (S_{1,f} \setminus S_1^{\text{ex}})(L_1)$, the residue characteristics and the local degrees of \mathfrak{p}_1 and $\sigma_{*,U_1}(\mathfrak{p}_1)$ are equal.

Proposition 3.9. For $i = 1, 2$, let K_i be a number field and S_i a stable set of primes. Assume that K_{i,S_i} is totally imaginary and that S_i is sharply p -stable for almost all rational primes p and in particular for $p = 2$. Let

$$\sigma: G_{K_1, S_1} \xrightarrow{\sim} G_{K_2, S_2}$$

be an isomorphism. Then the local correspondence at the boundary holds for σ and moreover, one can choose S_i^{ex} to be the set of 2-adic primes in S_i . More precisely, for any open subgroup $U_1 \subseteq G_{K_1, S_1}$, σ_{*,U_1} preserves the residue characteristic and the absolute degree of all primes $\mathfrak{p} \in S_1(U_1)$, whose residue characteristic ℓ is odd and such that S_i is sharply ℓ -stable for $i = 1, 2$.

Proof. To avoid notational problems, let us exceptionally denote by $S_{2\text{-adic}}(L)$ the set of 2-adic primes of a number field L . We apply Corollary 3.6 to $(K_i, S_i, p = 2)$ for $i = 1, 2$. It shows that σ maps decomposition groups of primes in $S_{1,f} \setminus S_{2\text{-adic}}$ to decomposition groups of primes in $S_{2,f} \setminus S_{2\text{-adic}}$. Thus we can define $\sigma_*(\bar{\mathfrak{p}}_1)$ by the equality

$$D_{\sigma_*(\bar{\mathfrak{p}}_1)} = \sigma(D_{\bar{\mathfrak{p}}_1}).$$

The prime $\sigma_*(\bar{\mathfrak{p}}_1)$ satisfying this equality is unique by Lemma 3.2. The Galois-equivariance of σ_* is straightforward. It remains to show that for any finite subextension $K_{1,S_1}/L_1/K_1$ with corresponding open subgroup U_1 and for any $\mathfrak{p}_1 \in S_{1,f}(L_1)$ with residue characteristic ℓ , which is odd and such that S_i is sharply ℓ -stable for $i = 1, 2$, the map σ_{*,U_1} preserves the residue characteristic and the local absolute degree. For any such ℓ and any $\bar{\mathfrak{p}} \in S_{1,f}(K_{1,S_1})$ with residue characteristic ℓ , Theorem 2.2 implies that the maximal pro- ℓ -extension of $K_{i,\bar{\mathfrak{p}}}$ is realized by K_{i,S_i} . Let $\mathfrak{p} \in S_i(L_i)$ be a prime with

residue characteristic ℓ and $\bar{\mathfrak{p}}$ an extension to K_{i,S_i} . Lemma 3.10 shows that $D_{\bar{\mathfrak{p}},K_S/L_i}$ encodes the information about the residue characteristic and the absolute degree of \mathfrak{p} . Thus σ_{*,U_1} preserves the residue characteristic and the absolute degree of all primes in $S_{1,f}$ with residue characteristic ℓ being odd and such that S_i is sharply ℓ -stable for $i = 1, 2$. \square

Lemma 3.10. *Let κ be a local field with characteristic zero and some residue characteristic ℓ and λ/κ a Galois extension with Galois group D , which contains the maximal pro- ℓ -extension of κ . Then the quantities ℓ and $[\kappa : \mathbb{Q}_\ell]$ can be recovered from the pro-finite group D (i.e., if ℓ_i -adic fields λ_i/κ_i for $i = 1, 2$ as above are given, and if there is a continuous isomorphism $D_1 \cong D_2$, then $\ell_1 = \ell_2$ and $[\kappa_1 : \mathbb{Q}_{\ell_1}] = [\kappa_2 : \mathbb{Q}_{\ell_2}]$).*

Proof. Let \mathcal{G}_κ be the absolute Galois group of κ . We have a surjection $\pi: \mathcal{G}_\kappa \twoheadrightarrow D$, and for any open $U \subseteq \mathcal{G}_\kappa$ with \mathcal{G}_κ/U an ℓ -group, surjections $U \twoheadrightarrow \pi(U) \twoheadrightarrow U^{(\ell)}$, which for any rational prime p induce injections

$$H^1(U^{(\ell)}, \mathbb{Z}/p\mathbb{Z}) \hookrightarrow H^1(\pi(U), \mathbb{Z}/p\mathbb{Z}) \hookrightarrow H^1(U, \mathbb{Z}/p\mathbb{Z}).$$

For all primes $p \neq \ell$, the \mathbb{F}_p -dimension of the space on the right (and hence also in the middle) is bounded by 2, and for $p = \ell$, the dimension of the space on the left gets arbitrary big, if U gets arbitrary small among all subgroups $U \subseteq \mathcal{G}_\kappa$ such that \mathcal{G}_κ/U is an ℓ -group. Thus the residue characteristic ℓ is equal to the unique prime p , such that $\dim_{\mathbb{F}_p} H^1(V, \mathbb{Z}/p\mathbb{Z})$ is unbounded as V varies over all open subgroups of D , such that D/V is a p -group. Further,

$$[\kappa : \mathbb{Q}_\ell] = \chi_\ell(\mathcal{G}_\kappa(\ell), \mathbb{Z}/\ell\mathbb{Z}) = \chi_\ell(D(\ell), \mathbb{Z}/\ell\mathbb{Z}). \quad \square$$

Remark 3.11. The proofs (of Theorem 3.5, Corollary 3.6 and Proposition 3.9) would be less technical if one would assume the stronger condition: ' K_S realize the maximal local extension at each $\mathfrak{p} \in S_f$ ' on the involved stable sets S . It is satisfied in the following cases.

- (i) If S is defined over a totally real subfield, (not necessarily stable), and $S \supseteq S_\infty \cup S_{p_1} \cup S_{p_2}$ for two different rational primes p_1, p_2 (by [1] Remark 5.3(i)).
- (ii) If S is strongly p -stable for all rational p 's (by [4]).
- (iii) If S contains an almost Chebotarev set (by [5]).

We conjecture that it is true in general if S is stable.

4. ANABELIAN GEOMETRY OF CURVES $\text{Spec } \mathcal{O}_{K,S}$ WITH S STABLE

Now we state and prove our main result.

Theorem 4.1. *For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i , such that*

- (a) K_1 is totally imaginary and Galois over \mathbb{Q} ,
- (b) for $i = 1, 2$, the set S_i is 2-stable and is sharply p -stable for almost all p ,
- (c) there are two odd rational primes under S_1 ,
- (d) there is an odd rational prime p with $S_p \subseteq S_2$ and S_i is sharply p -stable for $i \in \{1, 2\}$.

If $G_{K_1, S_1} \cong G_{K_2, S_2}$ as topological groups, then $K_1 \cong K_2$.

4.1. Uniform bound. Besides the local correspondence on the boundary, the following argument plays a central role in the proof of Theorem 4.1. From now on, we consider all occurring fields to be subfields of a fixed algebraic closure $\bar{\mathbb{Q}}$ of \mathbb{Q} .

Proposition 4.2 (Uniform bound). *For $i = 1, 2$, let K_i be a number field, S_i a set of primes of K_i and let*

$$\sigma: G_{K_1, S_1} \xrightarrow{\sim} G_{K_2, S_2}$$

be an isomorphism. Assume that the local correspondence at the boundary holds. Assume that S_1 is stable. Then there is some $N > 0$, such that for all (not necessarily finite) intermediate subfields $K_{1, S_1}/M_1/K_1$, such that M_1 is normal over \mathbb{Q} , one has $[M_1 : M_1 \cap M_2] < N$, where M_2/K_2 corresponds to M_1/K_1 via σ .

Lemma 4.3. *Let κ be a field. If $(V_i)_{i \in I}$ is a cofiltered system of κ -vector spaces, such that $\dim_{\kappa} V_i < n$, and $V := \varinjlim_I V_i$, then $\dim_{\kappa} V < n$.*

Proof of Lemma 4.3. For any n vectors in V there is an $i \in I$, such that these vectors has preimages in V_i . These preimages are linearly dependent. Hence their images in V are linearly dependent. \square

Proof of Proposition 4.2. Since S_1 is stable, by [4] Proposition 2.6, there is some $N > 0$, such that $\delta_{L_1}(S_1) > N^{-1}$ for all finite subfields $K_{1,S_1}/L_1/K_1$. Let M_1 be a subextension of $K_{1,S_1}/K_1$, such that M_1/\mathbb{Q} is normal. By Lemma 4.3 and since M_1 is a union of finite extensions of K_1 , which are normal over \mathbb{Q} , we can assume that M_1/K_1 finite. Let

$$S'_1 := (S_1 \setminus S_1^{\text{ex}})(M_1) \cap \text{cs}(M_1/\mathbb{Q})(M_1).$$

Since M_1/\mathbb{Q} is normal, $\delta_{M_1}(\text{cs}(M_1/\mathbb{Q})(M_1)) = 1$ and hence

$$\delta_{M_1}(S'_1) = \delta_{M_1}(S_1) > N^{-1}.$$

Lemma 4.4. *Let $S'_2 := \sigma_{*,U_1}(S'_1)$, where U_1 corresponds to M_1 . Then*

- (i) $\delta_{M_2}(S'_2) = \delta_{M_1}(S'_1)$.
- (ii) $S'_2 \stackrel{\subset}{\sim} \text{cs}(M_1 M_2/M_2)$.

Proof of Lemma 4.4. (i) The local correspondence at the boundary implies that there is a subset $S''_1 \subseteq S'_1$ with a finite complement, such that $S''_2 := \sigma_{*,U_1}(S''_1) \subseteq S'_2$ has finite complement and such that for any $\mathfrak{p}_1 \in S''_1$, the residue characteristic and the absolute degree of \mathfrak{p}_1 and $\sigma_{*,U_1}(\mathfrak{p}_1)$ coincide. In particular, $N\mathfrak{p}_1 = N\sigma_{*,U_1}(\mathfrak{p}_1)$ for all $\mathfrak{p}_1 \in S''_1$, where $N\mathfrak{p}$ denotes the norm of the prime \mathfrak{p} over \mathbb{Q} . Hence

$$\delta_{M_1}(S'_1) = \delta_{M_1}(S''_1) = \lim_{s \rightarrow 1+0} \frac{\sum_{\mathfrak{p}_1 \in S''_1} N\mathfrak{p}_1^{-s}}{\log \frac{1}{s-1}} = \lim_{s \rightarrow 1+0} \frac{\sum_{\mathfrak{p}_2 \in S''_2} N\mathfrak{p}_2^{-s}}{\log \frac{1}{s-1}} = \delta_{M_2}(S''_2) = \delta_{M_2}(S'_2).$$

(ii): Let $\mathfrak{p}_1 \in S'_1$ be such that σ_{*,U_1} preserves the residue characteristic and the absolute degree of \mathfrak{p}_1 . Let $\mathfrak{p}_2 := \sigma_{*,U_1}(\mathfrak{p}_1) \in S'_2$ and $\mathfrak{p} := \mathfrak{p}_2|_{M_1 \cap M_2}$. The fiber $\mathcal{O}_{M_1 M_2} \otimes_{\mathcal{O}_{M_2}} \kappa(\mathfrak{p}_2)$ over \mathfrak{p}_2 in $\text{Spec } \mathcal{O}_{M_1 M_2}$ is isomorphic to $(\mathcal{O}_{M_1} \otimes_{\mathcal{O}_{M_1 \cap M_2}} \kappa(\mathfrak{p})) \otimes_{\kappa(\mathfrak{p})} \kappa(\mathfrak{p}_2)$. By assumption, we have $\mathfrak{p}_2|_{\mathbb{Q}} = \mathfrak{p}_1|_{\mathbb{Q}} \in \text{cs}(M_1/\mathbb{Q})$ and hence $\mathfrak{p} \in \text{cs}(M_1/\mathbb{Q})(M_1 \cap M_2) \subseteq \text{cs}(M_1/M_1 \cap M_2)$. This implies that $\mathcal{O}_{M_1} \otimes_{\mathcal{O}_{M_1 \cap M_2}} \kappa(\mathfrak{p})$ is isomorphic to a product of copies of $\kappa(\mathfrak{p})$. Thus we obtain

$$\mathcal{O}_{M_1 M_2} \otimes_{\mathcal{O}_{M_1}} \kappa(\mathfrak{p}_2) \cong \prod \kappa(\mathfrak{p}_2),$$

i.e., \mathfrak{p}_2 is completely decomposed in $M_1 M_2$. \square

Using Lemma 4.4 and the normality of $M_1 M_2/M_2$, we obtain:

$$\begin{aligned} [M_1 : M_1 \cap M_2]^{-1} &= [M_1 M_2 : M_2]^{-1} \\ &= \delta_{M_2}(\text{cs}(M_1 M_2/M_2)) \\ &\geq \delta_{M_2}(S'_2) \\ &= \delta_{M_1}(S'_1) \\ &> N^{-1}. \end{aligned}$$

This proves Proposition 4.2. \square

4.2. Non-existence of lifts. Last but not least, Proposition 4.5 proven in this section provides the last argument which we need in the proof of Theorem 4.1. Let L/K be a Galois extension of global fields. We want to study, under which conditions there is no Galois extension L_0/K_0 , such that L/K is a base change of L_0/K_0 , i.e., $K_0 = K \cap L_0$ and $L = KL_0$.

Proposition 4.5. *Let K, L_0 be two linearly disjoint Galois extensions of a global field K_0 , and set $L = KL_0$. Assume one of the following holds:*

- (a) – K is a totally imaginary number field and
- $L = K_{S_p}(p)$ for some prime number p , or

- (b) *There is a prime \mathfrak{p} of K_0 , which is completely split in K , such that for any $\bar{\mathfrak{p}}_1, \bar{\mathfrak{p}}_2 \in S_{\mathfrak{p}}(L)$ with $\bar{\mathfrak{p}}_1|_K \neq \bar{\mathfrak{p}}_2|_K$, we have $D_{\bar{\mathfrak{p}}_1, L/K} \neq D_{\bar{\mathfrak{p}}_2, L/K}$.*

Then $K = K_0$.

We will only use part (a) of this proposition.

Proof. Assume (a) holds. Then L/K and L_0/K_0 are both Galois with Galois group isomorphic to $G_{K, S_p}(p)$. By [8] 10.3.20, the number of independent \mathbb{Z}_p -extensions of K satisfies

$$\mathrm{rk}_{\mathbb{Z}_p} G_{K, S_p}^{\mathrm{ab}}(\mathfrak{p}) \geq r_2(K) + 1.$$

Since $G_{L/K} \cong G_{L_0/K_0}$, the field K_0 has at least $r_2(K) + 1$ independent \mathbb{Z}_p -extensions. Assume $K \neq K_0$. Then $[K : K_0] \geq 2$, and since K is totally imaginary, we obtain:

$$r_2(K) + 1 = \frac{[K : \mathbb{Q}]}{2} + 1 \geq [K_0 : \mathbb{Q}] + 1 > [K_0 : \mathbb{Q}].$$

But by [8] 10.3.20, the number of independent \mathbb{Z}_p -extensions of K_0 is $\leq [K_0 : \mathbb{Q}]$. This is a contradiction, hence $K = K_0$ (notice that we nowhere made use of Leopoldt's conjecture!).

Assume (b) holds. Let $\psi: G_{L/K} \xrightarrow{\sim} G_{L_0/K_0}$ denote the canonical isomorphism. Assume there are two different primes $\mathfrak{p}_1 \neq \mathfrak{p}_2$ in K over \mathfrak{p} . Let \mathfrak{q} be some prime of L_0 over \mathfrak{p} . One can choose primes $\bar{\mathfrak{p}}_i \in S_{\mathfrak{p}}(L)$, such that $\bar{\mathfrak{p}}_i|_K = \mathfrak{p}_i$ and $\bar{\mathfrak{p}}_i|_{L_0} = \mathfrak{q}$. As $\mathfrak{p}_1, \mathfrak{p}_2$ are split over K_0 , we obtain that ψ maps $D_{\bar{\mathfrak{p}}_i, L/K}$ isomorphically to $D_{\mathfrak{q}, L_0/K_0}$. But by assumption $D_{\bar{\mathfrak{p}}_1, L/K} \neq D_{\bar{\mathfrak{p}}_2, L/K}$, hence $D_{\mathfrak{q}, L_0/K_0} = \psi(D_{\bar{\mathfrak{p}}_1, L/K}) \neq \psi(D_{\bar{\mathfrak{p}}_2, L/K}) = D_{\mathfrak{q}, L_0/K_0}$, which is a contradiction. Thus there is only one prime over \mathfrak{p} in K , and since \mathfrak{p} is completely split, we obtain $[K : K_0] = 1$. \square

4.3. Proof of Theorem 4.1. By assumption (b) in Theorem 4.1 and Proposition 3.9 the local correspondence at the boundary holds for σ : for any open subgroup $U_1 \subseteq G_{K_1, S_1}$ with fixed field L_1 , σ induces a functorial bijection

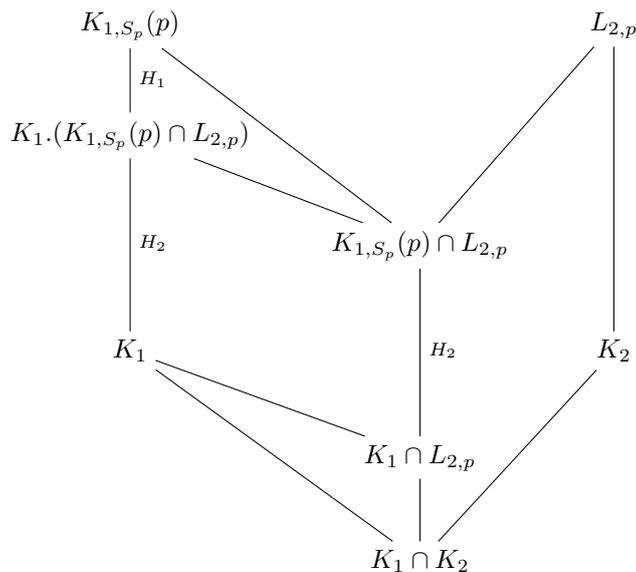
$$\sigma_{U_1}^*: (S_{1, f} \setminus S_{2\text{-adic}})(L_1) \xrightarrow{\sim} (S_{2, f} \setminus S_{2\text{-adic}})(L_2),$$

which preserves the residue characteristic and the absolute degree of all primes in

$(S_{1, f} \setminus (S_{2\text{-adic}} \cup T))(L_1)$, with $T := \{\ell : S_1 \text{ or } S_2 \text{ is not sharply } \ell\text{-stable}\}$. We obtain $[K_2 : \mathbb{Q}] \leq [K_1 : \mathbb{Q}]$ from this. Indeed, by assumption (d) there is an odd prime p with $S_p \subseteq S_2$ and $p \notin T$, and hence σ_* preserves the residue characteristic and the absolute degree of primes in $S_p(K_1) \cap S_1$ by Proposition 3.9. Hence $\sigma_*(S_1 \cap S_p(K_1)) = S_p(K_2)$ and

$$\begin{aligned} [K_2 : \mathbb{Q}] &= \dim_{\mathbb{Q}_p} K_2 \otimes_{\mathbb{Q}} \mathbb{Q}_p = \sum_{\mathfrak{p} \in S_p(K_2)} [K_{2, \mathfrak{p}} : \mathbb{Q}_p] = \sum_{\mathfrak{p} \in (S_p \cap S_1)(K_1)} [K_{1, \sigma_*^{-1}(\mathfrak{p})} : \mathbb{Q}_p] \\ (4.1) \quad &\leq \sum_{\mathfrak{p} \in S_p(K_1)} [K_{1, \sigma_*^{-1}(\mathfrak{p})} : \mathbb{Q}_p] = [K_1 : \mathbb{Q}]. \end{aligned}$$

By (c) we have two rational primes p_1, p_2 , such that $S_{p_j} \subseteq S_1$, $p_j > 2$. Let $p \in \{p_1, p_2\}$. The quotient $G_{K_1, S_p}(p)$ of G_{K_1, S_1} is torsion-free (cf. [8] 8.3.18 and 10.4.8). Since K_1 is normal over \mathbb{Q} , S_p is defined over \mathbb{Q} and the maximal pro- p -quotient of a profinite group is characteristic, we deduce that the field $K_{1, S_p}(p)$ is normal over \mathbb{Q} . Let $L_{2, p}$ be the field corresponding to $K_{1, S_p}(p)$ via σ (a priori, $L_{2, p}$ must not be equal $K_{2, S_p}(p)$). We have the following situation:



In this diagram the group H_1 is a subgroup of $G_{K_{1,S_p}(p)/K_{1,S_p}(p) \cap L_{2,p}}$ and of $G_{K_{1,S_p}(p)}$. But the first of these two groups is finite by Proposition 4.2 and the second is torsion-free. Hence $H_1 = 1$, i.e., $H_2 = G_{K_{1,S_p}(p)}$. By Proposition 4.5(a) we get $K_1 = K_1 \cap L_{2,p}$, i.e., $K_1 \subseteq L_{2,p}$. Doing this for $p = p_1, p_2$, we get: $K_1 \subseteq L_{2,p_1} \cap L_{2,p_2} = K_2$, the last equality being true, since $L_{2,p_j}/K_2$ is a pro- p_j -extension for $j = 1, 2$. By (4.1) we conclude that $K_1 = K_2$. \square

REFERENCES

- [1] Chenevier G., Clozel L.: *Corps de nombres peu ramifiés et formes automorphes autoduales*, J. of the AMS, vol. 22, no. 2, 2009, p. 467-519.
- [2] Ivanov A.: *Arithmetic and anabelian theorems for stable sets in number fields*, Dissertation, Universität Heidelberg, 2013.
- [3] Ivanov A.: *On some anabelian properties of arithmetic curves*, Manuscripta Math., vol. 144 (2014), no. 3, 545-564.
- [4] Ivanov A.: *Stable sets of primes in number fields*, to appear in Algebra and Number Theory J., arXiv:1309.2800.
- [5] Ivanov A.: *Densities of primes and realization of local extensions*, preprint, arXiv:1309.78532013, 2013.
- [6] Mochizuki S.: *Absolute anabelian cuspidalizations of proper hyperbolic curves*, J. Math. Kyoto Univ., 47-3 (2007), 451-539.
- [7] Neukirch J.: *Kennzeichnung der p -adischen und der endlich algebraischen Zahlkörper*, Invent. Math. 6 (1969) 296-314.
- [8] Neukirch J., Schmidt A., Wingberg K.: *Cohomology of number fields*, Springer, 2008, second edition.
- [9] Tamagawa A.: *The Grothendieck conjecture for affine curves*, Comp. Math. 109 (1997), 135-194.
- [10] Uchida K.: *Isomorphisms of Galois groups*, J. Math. Soc. Japan 28 (1976), 617-620.

ALEXANDER B. IVANOV, TECHNISCHE UNIVERSITÄT MÜNCHEN, ZENTRUM MATHEMATIK - M11, BOLTZMANNSTR. 3, 85748 GARCHING BEI MÜNCHEN
E-mail address: ivanov@ma.tum.de