ON SOME ANABELIAN PROPERTIES OF ARITHMETIC CURVES

A. IVANOV

Abstract. In this paper we generalize an argument of Neukirch from birational anabelian geometry to the case of arithmetic curves. In contrast to the function field case, it seems to be more complicated to describe the position of decomposition groups of points at the boundary of the scheme $\operatorname{Spec}\mathcal{O}_{K,S}$, where K is a number field and S a set of primes of K, intrinsically in terms of the fundamental group. We prove that it is equivalent to give the following pieces of information additionally to the fundamental group $\pi_1(\operatorname{Spec}\mathcal{O}_{K,S})$: the location of decomposition groups of boundary points inside it, the p-part of the cyclotomic character, the number of points on the boundary of all finite étale covers, etc. Under a certain finiteness hypothesis on Tate-Shafarevich groups with divisible coefficients, one can reconstruct all these quantities simply from the fundamental group.

1. Introduction

Let K be a number field, $\overline{K}$ a fixed algebraic closure and G_K the absolute Galois group. In [6] Neukirch showed, using an argument involving the Brauer groups of K and its extensions, that the group G_K determines intrinsically, how the decomposition groups $D_{\mathfrak{p}}$ of primes of K lie inside it. In contrast to the case of curves over finite fields, which is now well-understood, in particular, due to Tamagawa [10], there is almost nothing known about the case of arithmetic curves. Not even this Brauer group argument of Neukirch generalizes from the birational to the arithmetic situation, i.e., if one replaces $\operatorname{Spec}K$ by $\operatorname{Spec}\mathcal{O}_{K,S}$, where $S \supseteq S_\infty$ is a finite set of primes of K and considers only the decomposition groups of primes in S. The reason for this failure is the obstruction given by the non-vanishing second Tate-Shafarevich group. We are interested in the question, how much information about the decomposition groups of primes in S is encoded intrinsically in $\mathrm{G}_S := \pi_1(\operatorname{Spec}\mathcal{O}_{K,S})$. It seems to be possible, at least using some additional information, to reconstruct the position of decomposition groups of primes in S inside G_S. Essentially, it turns out that it is equivalent to know one of the following data: the embeddings $D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_S$ for $\bar{\mathfrak{p}} \in S_f := S \smallsetminus S_\infty$; the cyclotomic character on G_S; the S-class number of all finite subfields $K_S/L/K$; the number $\sharp S(L)$ for all these L. The results of this paper are part of author's Ph.D. thesis [4].

Theorem 1.1. *Let K be a number field, $S \supseteq S_\infty$ a finite set of primes. Assume that at least two rational primes lie in $\mathcal{O}^*_{K,S}$, and p is one of them. Assume (G_S, p) are given. The knowledge of one of the following extra structures is equivalent to any other:*

- (i) *The embeddings $\iota_{\bar{\mathfrak{p}}}\colon D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_S$ for $\bar{\mathfrak{p}} \in S_f$.*
- (ii) *The cyclotomic p-character $\chi_p\colon U \to \mathbb{Z}_p^*$ on some open $U \subseteq \mathrm{G}_S$.*
- (iii) *For all open $U \subseteq \mathrm{G}_S$ with totally imaginary fixed field L, the group $\mathrm{Cl}_S(L)$.*
- (iii)' *For all open $U \subseteq \mathrm{G}_S$ with totally imaginary fixed field L, the number $\sharp\mathrm{Cl}_S(L)/p$.*
- (iv) *For all open $U \subseteq \mathrm{G}_S$ with fixed field L, the number $\sharp S(L)$.*

Assume that the decomposition subgroups at primes in S_f are isomorphic to absolute Galois groups of local fields of characteristic zero. Then the knowledge of the above is also equivalent to the knowledge of the following:

- (ii)' *The cyclotomic character on some open subgroup $U \subseteq \mathrm{G}_S$.*

Observe that in the arithmetic situation, to give G_S together with the cyclotomic character, corresponds in some sense in the geometric situation over a finite field, to give the fundamental group of a curve together with the attached outer Galois representation. The assumption in the theorem, that there are at least two rational primes lying under S, implies by the work of Clozel and Chenevier [2] Theorem 5.1, that the decomposition groups in G_S of primes in $S_{p_1} \cup S_{p_2}$ are isomorphic to absolute Galois groups of local fields. It does not imply in general that this holds for all primes in S (but it still does for primes lying in the maximal subset of S, defined over a totally real subfield: cf. [2] Remark 5.3(i)).

Remark 1.2. We make the following observation. If one of the data in the theorem is determined with respect to an open subgroup $U_0 \subseteq \mathrm{G}_S$, then it is also determined for G_S. Indeed, it is enough to see this for (i). So, if the embeddings into U_0 of the decomposition groups at S_f inside U_0 are given, then (using Corollary 2.7(ii) below) the whole projective system of continuous G_S-sets $\varprojlim_{U \subseteq U_0, U \lhd \mathrm{G}_S} S_f(U)$ is determined (here, we write $S_f(U)$ for $S_f(L)$ if $L = K_S^U$), and one obtains the decomposition groups $D_{\bar{\mathfrak{p}}} \subseteq \mathrm{G}_S$ as the stabilizers of points under the action of G_S on it.

Of all the quantities listed in the theorem, the numbers $\sharp S(L)$ seem to be the most accessible ones. First of all, the numbers $\sharp S_\infty(U)$ are determined by (G_S, p) (cf. Proposition 4.1). Proposition 1.3 given below, allow to reconstruct the numbers $\sharp S_f(U)$ for all open $U \subseteq U_0 \subseteq \mathrm{G}_S$ with U_0 small enough, under a certain finiteness assumption. Then Remark 1.2 allows to reconstruct the numbers $\sharp S_f(U)$ for all $U \subseteq \mathrm{G}_S$ open.

Proposition 1.3. *Let K, S be a number field together with a set of primes. Let $p \in \mathcal{O}_{K,S}^*$. Assume that p is odd and $\mu_p \subset K$. Assume, the following holds: for any character $\chi\colon \mathrm{G}_S \to \mathbb{Z}_p^* = \mathrm{Aut}(\mathbb{Q}_p/\mathbb{Z}_p)$ whose restriction to $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$ is trivial, the group $Ш^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi))$ is finite. Then for any such χ, the group $\mathrm{H}^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi))$ is of finite corank and*

$$\sharp S_f(K) = 1 + \max_\chi \mathrm{corank}(\mathrm{H}^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi))). \tag{1.1}$$

This finiteness assumption on $Ш^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi))$ has the following (at least partial) evidence: if χ is the cyclotomic p-character χ_p, then $Ш^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi)) = 0$ is easy to compute and for $\chi = \chi_p^{\otimes k}$ with $k \in \mathbb{Z} \smallsetminus \{1\}$ Soulé showed in [9] using K-theory, that $\mathrm{H}^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi)) = 0$. Compare also [8] 10.3.27 and the discussion preceding it.

Directly from Theorem 1.1 and Proposition 1.3 we get:

Corollary 1.4 (Local correspondence at the boundary)**.** *For $i = 1, 2$, let K_i, S_i be a number field together with a finite set of primes containing S_∞. Assume that at least two rational primes lie completely under S_i, and assume that one of them, denoted p, lies under both. Let $\chi_{i,p}$ denote the p-cyclotomic character on G_{K_i,S_i}. Let*

$$\sigma\colon \mathrm{G}_{K_1,S_1} \xrightarrow{\sim} \mathrm{G}_{K_2,S_2}$$

be a topological isomorphism, such that $\chi_{2,p} \circ \sigma|_{U_1} = \chi_{1,p}|_{U_1}$ for some open subgroup $U_1 \subseteq \mathrm{G}_{K_1,S_1}$ holds. Then for any $\bar{\mathfrak{p}}_1 \in S_f(K_{1,S_1})$, there is a unique prime $\sigma^*(\bar{\mathfrak{p}}_1) \in S_f(K_{2,S_2})$, such that $\sigma(D_{\bar{\mathfrak{p}}_1}) = D_{\sigma^*(\bar{\mathfrak{p}}_1)}$. This defines a G_{K_1,S_1}-equivariant bijection

$$\sigma^*\colon S_{1,f}(K_{1,S_1}) \xrightarrow{\sim} S_{2,f}(K_{2,S_2}),$$

which induces compatible bijections

$$\sigma_{U_1}^*\colon S_{1,f}(L_1) \xrightarrow{\sim} S_{2,f}(L_2),$$

for any L_1/K_1 finite with corresponding subgroup $U_1 \subseteq \mathrm{G}_{K_1,S_1}$ and $U_2 = \sigma(U_1)$ with corresponding field L_2. If the decomposition groups at primes in $S_{1,f}$ are isomorphic to absolute Galois groups of local fields of characteristic zero, then σ_{U_1} preserves the residue characteristics and the absolute degrees of primes.

Moreover, if p is odd and if for $i = 1, 2$, there is an open subgroup $U_i \subseteq \mathrm{G}_{K_i,S_i}$, such that for all characters $\chi\colon U_i \to \mathbb{Z}_p^*$ with torsion-free image, the group $Ш^2(U_i, \mathbb{Q}_p/\mathbb{Z}_p(\chi))$ is finite, then the condition $\chi_{2,p} \circ \sigma|_{U_1} = \chi_{1,p}|_{U_1}$ is automatically satisfied.

Notation. Our notation will essentially coincide with the notations in [8]. We collect some of the most important notations here. 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 $\mathrm{N}_G(H)$ its normalizer in G.

For a Galois extension M/L of fields, $\mathrm{G}_{M/L}$ 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 $D_{\bar{\mathfrak{p}},L/K} \subseteq \mathrm{G}_{L/K}$ 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 $\mathrm{G}_S := \mathrm{G}_{K,S}$ for its Galois group. Further, for $p \leqslant \infty$ 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 $S_f := S \smallsetminus S_\infty$.

Let K, S be a number field and a set of primes. Then $n_K, r_1(K), r_2(K)$ is the degree, the number of real and of conjugate pairs of complex embeddings of $K/\mathbb{Q}$ and $\mathbb{N}(S) := \mathbb{N} \cap \mathcal{O}_{K,S}^*$, i.e., $p \in \mathbb{N}(S)$ if and only if $S_p \subseteq S$. Further, $\chi_p\colon \mathrm{G}_S \to \mathbb{Z}_p^*$ denotes the cyclotomic p-character for $p \in \mathbb{N}(S)$ and $\mathrm{Cl}_S(K)$ the S-class group of K. If $U \subseteq \mathrm{G}_S$ is an open subgroup and $L = (K_S)^U$, then we sometimes write $\mathrm{Cl}_S(U), \sharp S(U)$, etc. instead of $\mathrm{Cl}_S(L), \sharp S(L)$, etc.

If (x),(y) are some sets of invariants of K, S (like, for example, (i),(ii) in Theorem 1.1), then (x) $\rightsquigarrow$ (y) resp. (x) $\leftrightsquigarrow$ (y) will have the following meaning: if the data in (x) are known, then we can deduce the data in (y) from them resp. the knowledge of (x) and (y) is equivalent. In particular, (x) $\rightsquigarrow$ (y) implies that if two pairs $(K_i, S_i), i = 1, 2$ are given, with $\mathrm{G}_{K_1,S_1} \cong \mathrm{G}_{K_2,S_2}$ and such that the data in (x) coincide for $i = 1, 2$, then also the data in (y) are coincide.

A local field means always a non-archimedean local field.

Outline of the paper. In Section 2 we study intersections of decomposition subgroups of different primes inside G_S, which is the first step towards a proof of Theorem 1.1. Section 3 is devoted to the proof of Theorem 1.1. In Section 4 we prove Proposition 1.3 and discuss which invariants of K, S can be recovered from G_S (plus possibly some further information).

2. Intersections of decomposition subgroups

Let S be a finite set of primes of K and let $\bar{\mathfrak{p}}, \bar{\mathfrak{q}}$ be two primes of K_S lying over S_f. In this section we investigate, under the assumption that $S_p \cup S_\infty \subseteq S$, how big the intersection of the decomposition groups $D_{\bar{\mathfrak{p}}}, D_{\bar{\mathfrak{q}}}$ inside G_S is. If S is the set of all primes of K, then this intersection is trivial by a theorem of F.K. Schmidt [8] 12.1.3. Its proof does not generalize to the case of restricted ramification, so we use different arguments, all of which are simple applications of class field theory. The main result of this section, which will be used later in the text is Corollary 2.7. It is an analog of [8] 12.1.4 in the case of G_S. Finally, in Section 2.4 we consider the case of primes $\bar{\mathfrak{p}}, \bar{\mathfrak{q}}$ not lying over S.

2.1. **Groups of p-decomposition type.** One of the most frequently used objects in our investigations will be the p-Sylow subgroup of an absolute Galois group of a local field with residue characteristic $\neq p$. Such a group has a very special and easy structure: it is a non-abelian pro-p-Demushkin group of rank two. Recall (cf. [8] 3.9.9) that a pro-p-group is called a Demushkin group, if $\mathrm{H}^1(G, \mathbb{Z}/p\mathbb{Z})$ is finite, $\mathrm{H}^2(G, \mathbb{Z}/p\mathbb{Z})$ is one-dimensional over $\mathbb{F}_p$ and the cup-product from the first degree into the second is non-degenerate. To have a shortcut, we define:

Definition 2.1. A group of *p-decomposition type* is a non-abelian pro-p Demushkin group of rank 2.

By a theorem of Demushkin (cf. [8] 3.9.11) a one-relator pro-p-group G is a Demushkin group, if and only if for some integers $n \geqslant 1, q \geqslant 0$ (assume for simplicity that $q \neq 2$; for the case $q = 2$, cf. [8] 3.9.19), G is generated by $x_1, \ldots, x_n$ subject to one relation:

$$x_1^q (x_1, x_2)(x_3, x_4) \ldots (x_{n-1}, x_n) = 1,$$

where $(x, y) = x^{-1}y^{-1}xy$. The numbers n, q are the rank and the invariant of G respectively. For a group G of p-decomposition type we have $n = 2$ and hence $q \neq 0$ (otherwise G would be abelian). Thus G is of the form $\mathbb{Z}_p \ltimes \mathbb{Z}_p$ with $\mathbb{Z}_p \hookrightarrow \mathrm{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^*$ injective. We need a description of all closed subgroups of groups of p-decomposition type.

Lemma 2.2. *Let H be a group of p-decomposition type.*

(i) *A non-trivial closed subgroup of H is either isomorphic to $\mathbb{Z}_p$ or is of p-decomposition type.*
(ii) *The open subgroups of H are exactly the subgroups of p-decomposition type.*
(iii) *H has a unique maximal closed normal pro-cyclic subgroup, denoted H_n. It is also the unique closed normal subgroup, such that H/H_n is infinite pro-cyclic.*
(iv) *If $N \subseteq H$ is open, then $N_n = N \cap H_n$.*

Proof. Let H be a group of p-decomposition type.
(i)+(ii): one verifies immediately that a closed subgroup $N \subseteq H$ is either $\cong \mathbb{Z}_p$ or open. It remains to show that an open subgroup $N \subseteq H$ is of p-decomposition type. Let $H_n \lhd H$ be a closed normal subgroup of H, such that $H/H_n \cong \mathbb{Z}_p$. One obtains an exact sequence:

$$1 \to N \cap H_n \to N \to N/N \cap H_n \to 1$$

with the first and the last term isomorphic to $\mathbb{Z}_p$. Hence this sequence splits and $N \cong \mathbb{Z}_p \ltimes_\phi \mathbb{Z}_p$ for some $\phi\colon \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_p)$. Either the image of ϕ is $\{1\}$ or ϕ is injective. In the first case $N \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and in the second N is of p-decomposition type. The first case can not occur, as otherwise one would have the contradiction $3 = \mathrm{scd}_p(N) \leqslant \mathrm{scd}_p(H) = 2$. (iii): Let H_n be as above. Assume $\mathbb{Z}_p \cong H_1 \lhd H$ is normal and $H_1 \nsubseteq H_n$. Then

$$H_1/(H_1 \cap H_n) \hookrightarrow H/H_n \cong \mathbb{Z}_p,$$

i.e., $H_1 \cap H_n = 1$. Now H_n, H_1 are two normal subgroups of H with trivial intersection, i.e., $H_n \times H_1 \subseteq H$. But $H_n \times H_1 \ncong \mathbb{Z}_p$ is not of p-decomposition type. This is a contradiction to (i). Hence H_n is the unique maximal normal closed pro-cyclic subgroup of H.

Assume now, $H_2 \lhd H$ is normal with $H/H_2 \cong \mathbb{Z}_p$ and $H_2 \not\supseteq H_n$. As $H_n/H_2 \cap H_n \hookrightarrow H/H_2 \cong \mathbb{Z}_p$, we get $H_n \cap H_2 = 1$. The same reasoning as above gives a contradiction. Thus $H_2 \supseteq H_n$. Then $H_2 = H_n$ follows easily.

(iv): Since $N \subseteq H$ is open, $N \nsubseteq H_n$ and we have an inclusion $1 \neq N/N \cap H_n \hookrightarrow H/H_n$, we obtain that $N/N \cap H_n$ is infinite pro-cyclic. Thus by (iii), $N \cap H_n = N_n$. □

To a group H of p-decomposition type we can associate the character defining the semi-direct product:

$$\chi_H \colon H \twoheadrightarrow H/H_n \hookrightarrow \mathbb{Z}_p^* = \mathrm{Aut}(H_n).$$

2.2. **Local situation.** Let κ be a local field with residue characteristic ℓ and let G_κ be its absolute Galois group. For $p \neq \ell$, the p-Sylow subgroups of the maximal tame quotient

$$\mathrm{G}_\kappa^{\mathrm{tr}} \cong \hat{\mathbb{Z}} \ltimes \hat{\mathbb{Z}}^{(\ell')}$$

of G_κ are of p-decomposition type, which can easily be seen directly. Consider now a p-Sylow subgroup $\mathrm{G}_{\kappa,p} \subseteq \mathrm{G}_\kappa$. The composition

$$\mathrm{G}_{\kappa,p} \hookrightarrow \mathrm{G}_\kappa \twoheadrightarrow \mathrm{G}_\kappa^{\mathrm{tr}}$$

is injective, since $p \neq \ell$ and the kernel of the second map is a pro-ℓ-subgroup. Thus $\mathrm{G}_{\kappa,p}$ is isomorphic to a p-Sylow subgroup of $\mathrm{G}_\kappa^{\mathrm{tr}}$, and hence is of p-decomposition type.

2.3. **Metabelian covers.**

Lemma 2.3. *Let K be a number field and $S \supseteq S_p \cup S_\infty$ a set of primes of K. Let $\bar{\mathfrak{p}} \in (S_f \smallsetminus S_p)(K_S)$ and $\mathfrak{p} = \bar{\mathfrak{p}}|_K$. Let $\mathscr{G}_\mathfrak{p}$ denote the absolute Galois group of $K_\mathfrak{p}$ and $\mathscr{G}_{\mathfrak{p},p}$ a p-Sylow subgroup. Then the composition*

$$\phi \colon \mathscr{G}_{\mathfrak{p},p} \hookrightarrow \mathscr{G}_\mathfrak{p} \twoheadrightarrow D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_S$$

is injective. In particular, any p-Sylow subgroup of $D_{\bar{\mathfrak{p}}}$ is of p-decomposition type.

Proof. Since $\mathfrak{p} \notin S_p$, we have $\mathscr{G}_{\mathfrak{p},p} \cong (\mathscr{G}_{\mathfrak{p},p}/\mathscr{I}_{\mathfrak{p},p}) \ltimes \mathscr{I}_{\mathfrak{p},p}$, where both factors are isomorphic to $\mathbb{Z}_p$ and the second is the inertia subgroup. Due to the cyclotomic p-extension, which realizes the maximal unramified p-extension at $\mathfrak{p}$ and is unramified outside $S_p \subseteq S$, the kernel of ϕ is contained in $\mathscr{I}_{\mathfrak{p},p}$. To show that $\ker(\phi) = 1$, it is enough to show that for any $n > 0$, there is a finite subextension of K_S/K, whose ramification degree at $\mathfrak{p}$ is p^n.

Therefore, let L_0/K be the Hilbert class field of K and set $L := L_0 K(\zeta_{p^n})$. This is an abelian extension of K, unramified outside S_p. The ideal $\mathfrak{p}$ is on the one side unramified in L, and on the other side principal (being principal already in L_0). Thus we can write

$$\mathfrak{p}\mathcal{O}_L = (\epsilon) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r,$$

with $\epsilon \in \mathcal{O}_L$, and $\mathfrak{p}_i$ unequal prime ideals of $\mathcal{O}_L$. We can assume that $\bar{\mathfrak{p}}|_L = \mathfrak{p}_1$. Since $\mathfrak{p} \in S$, we have $\epsilon \in \mathcal{O}_{L,S}^*$, and the extension $L(\epsilon^{1/p^n})$ is unramified outside $S_p \cup S_\mathfrak{p} \subseteq S$. But since $\mathfrak{p}_1|\mathfrak{p}$ is unramified, we have

$$v_{\mathfrak{p}_1}(\epsilon) = 1,$$

where $v_{\mathfrak{p}_1}$ denotes the valuation corresponding to $\mathfrak{p}_1$. Thus the local extension $L_{\mathfrak{p}_1}(\epsilon^{1/p^n})/L_{\mathfrak{p}_1}$ is tamely ramified of degree p^n. □

Proposition 2.4. *Let $\bar{\mathfrak{p}} \neq \bar{\mathfrak{q}} \in S_f(K_S)$, such that there is a rational prime $p \in \mathcal{O}_{K_S, S \smallsetminus \{\bar{\mathfrak{p}}, \bar{\mathfrak{q}}\}}^*$. Choose some p-Sylow subgroups $D_{\bar{\mathfrak{p}},p} \subseteq D_{\bar{\mathfrak{p}}}$ resp. $D_{\bar{\mathfrak{q}},p} \subseteq D_{\bar{\mathfrak{q}}}$. Then $D_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}},p}$ is not open in $D_{\bar{\mathfrak{p}},p}$. In particular, $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}}$ is not open in $D_{\bar{\mathfrak{p}}}$.*

Proof. By Lemma 2.3, $D_{\bar{\mathfrak{p}},p}$ resp. $D_{\bar{\mathfrak{q}},p}$ are groups of p-decomposition type. Let $\mathfrak{p} = \bar{\mathfrak{p}}|_K$, $\mathfrak{q} = \bar{\mathfrak{q}}|_K$. By going up to a finite extension, we can assume $\mathfrak{p} \neq \mathfrak{q}$. Observe that the extension constructed in the proof of Lemma 2.3 is Galois and unramified in $\mathfrak{q}$, as $\mathfrak{q} \notin S_p \cup \{\mathfrak{p}\}$. Thus if $I_{\cdot,p} \subseteq D_{\cdot,p}$ denotes the corresponding inertia subgroup, we have $I_{\bar{\mathfrak{p}},p} \cap I_{\bar{\mathfrak{q}},p} = 1$.

Now, assume $D_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}},p} \subseteq D_{\bar{\mathfrak{p}},p}$ is open. The second group is of p-decomposition type, hence the first also is (Lemma 2.2(ii)). Hence, again by Lemma 2.2(ii), the inclusion $D_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}},p} \subseteq D_{\bar{\mathfrak{q}},p}$

is also open. The maximal normal pro-cyclic subgroup of $D_{\cdot,p}$ is $I_{\cdot,p}$. Thus by Lemma 2.2(iv) applied to both inclusions, the maximal normal pro-cyclic subgroup of $D_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}},p}$ is equal to $I_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}},p}$ and to $D_{\bar{\mathfrak{p}},p} \cap I_{\bar{\mathfrak{q}},p}$ simultaneously, i.e., these two intersections are equal. This implies $D_{\bar{\mathfrak{p}},p} \cap I_{\bar{\mathfrak{q}},p} = I_{\bar{\mathfrak{p}},p} \cap I_{\bar{\mathfrak{q}},p} = 1$. But this group, being the maximal normal pro-cyclic subgroup of a group of p-decomposition type must be isomorphic to $\mathbb{Z}_p$. This is a contradiction.

Finally, if $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}} \subseteq D_{\bar{\mathfrak{p}}}$ were open, then also $D_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}}} \subseteq D_{\bar{\mathfrak{p}},p}$. But $D_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}}}$ is a pro-p-subgroup of $D_{\bar{\mathfrak{q}}}$, hence contained in a p-Sylow subgroup $D'_{\bar{\mathfrak{q}},p}$ of it. Thus the intersection $D_{\bar{\mathfrak{p}},p} \cap D'_{\bar{\mathfrak{q}},p} = D_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}}}$ would be open in $D_{\bar{\mathfrak{p}},p}$, which contradicts to the already proven part of the proposition. □

Observe that all arguments up to now made only use of solvable extensions of K, thus we could also replace G_S by its maximal solvable quotient. Before going on, we quote the following recent result of Clozel and Chenevier:

Theorem 2.5 (Clozel-Chenevier, [2] Theorem 5.1)**.** *Let S_f be a set of finite primes of $\mathbb{Q}$. Let $S := S_f \cup \{\infty\}$. If $\sharp S_f \geqslant 2$, then for any $p \in S$ and $\bar{\mathfrak{p}} \in S(\mathbb{Q}_S)$ lying over p, the map*

$$\mathrm{G}_{\overline{\mathbb{Q}_p}/\mathbb{Q}_p} \twoheadrightarrow D_{\bar{\mathfrak{p}},\mathbb{Q}_S/\mathbb{Q}} \subseteq \mathrm{G}_{\mathbb{Q},S}$$

is injective.

Its proof is rather involved and uses proven cases of the automorphic base change and results of Harris-Taylor on local Langlands correspondence. We also remark that to prove this result it is necessary to work with the full group $\mathrm{G}_{\mathbb{Q},S}$ and not with its maximal solvable quotient. We deduce an immediate corollary:

Corollary 2.6. *Let K be a number field, p, ℓ two different rational primes, S a set of primes of K, such that $S \supseteq S_p \cup S_\ell \cup S_\infty$. Then for any $\mathfrak{p} \in S_p$ and $\bar{\mathfrak{p}} \in S_p(K_S)$ lying over $\mathfrak{p}$, the map*

$$\mathrm{G}_{\overline{K_\mathfrak{p}}/K_\mathfrak{p}} \twoheadrightarrow D_{\bar{\mathfrak{p}},K_S/K} \subseteq \mathrm{G}_{K,S}$$

is injective.

Proof. Let $S_0 := \{p, \ell, \infty\}$. Then $S_0(K) \subseteq S$ and $\mathbb{Q}_{S_0} \subseteq K_{S_0(K)} \subseteq K_S$. By Theorem 2.5 of Clozel-Chenevier, $\mathbb{Q}_{S_0}/\mathbb{Q}$ realizes the maximal local extensions at p, i.e., for any extension $\bar{\mathfrak{p}}_0$ of p to $\mathbb{Q}_{S_0}$, the field $\mathbb{Q}_{S_0,\bar{\mathfrak{p}}_0}$ is algebraically closed. Hence for any $\bar{\mathfrak{p}} \in S_p(K_S)$ with restriction $\bar{\mathfrak{p}}_0$ to the subfield $\mathbb{Q}_{S_0}$, the field $K_{S,\bar{\mathfrak{p}}} \supseteq \mathbb{Q}_{S_0,\bar{\mathfrak{p}}_0}$ is also algebraically closed. This finishes the proof. □

Using this, we deduce from Proposition 2.4 the following analog of [8] 12.1.4 for G_S:

Corollary 2.7.

(i) *If $p \in \mathcal{O}^*_{K,S}, \bar{\mathfrak{p}} \in (S_f \smallsetminus S_p)(K_S)$ and $H \subseteq D_{\bar{\mathfrak{p}}}$ is a closed subgroup, such that $H \cap D_{\bar{\mathfrak{p}},p} \subseteq D_{\bar{\mathfrak{p}},p}$ is open for some p-Sylow subgroup $D_{\bar{\mathfrak{p}},p} \subseteq D_{\bar{\mathfrak{p}}}$, then $\mathrm{N}_{\mathrm{G}_S}(H) \subseteq D_{\bar{\mathfrak{p}}}$.*

(ii) *Assume that at least two rational primes lie in $\mathcal{O}^*_{K,S}$. Then the intersection of two distinct decomposition subgroups in G_S of primes in $S_f(K_S)$ is not open in any of them.*

Proof. (i): Let $x \in \mathrm{N}_{\mathrm{G}_S}(H)$. Then $H = xHx^{-1} \subseteq xD_{\bar{\mathfrak{p}}}x^{-1} = D_{x\bar{\mathfrak{p}}}$. Thus $D_{\bar{\mathfrak{p}}} \cap D_{x\bar{\mathfrak{p}}} \supseteq H$ contains an open subgroup of a p-Sylow subgroup of $D_{\bar{\mathfrak{p}}}$. Proposition 2.4 implies $x\bar{\mathfrak{p}} = \bar{\mathfrak{p}}$, i.e., $x \in D_{\bar{\mathfrak{p}}}$.

(ii): By Proposition 2.4, the only case to consider, is $S_p \cup S_\ell \subseteq S$, $\bar{\mathfrak{p}} \in S_p$, $\bar{\mathfrak{q}} \in S_\ell$ with $p \neq \ell$ (and there is no further prime to compare $D_{\bar{\mathfrak{p}}}$ with $D_{\bar{\mathfrak{q}}}$). Assume $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}} \subseteq D_{\bar{\mathfrak{p}}}$ is open. By Corollary 2.6, $D_{\bar{\mathfrak{p}}}$ resp. $D_{\bar{\mathfrak{q}}}$ is isomorphic to the absolute Galois group of a p-adic resp. ℓ-adic field. Hence also the open subgroup $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}}$ of $D_{\bar{\mathfrak{p}}}$ is isomorphic to a Galois group of a p-adic field. Hence $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}}$ contains free pro-p-subgroups of any finite rank. But $D_{\bar{\mathfrak{q}}}$ does not, and we get a contradiction. □

2.4. **Intersection of decomposition subgroups at good primes.** Let K be a number field and $S \supseteq S_p \cup S_\infty$ a finite set of primes. Arguments in this section make only use of abelian p-extensions, so we work with $\mathrm{G}_S^{\mathrm{ab}}(p)$ instead of G_S. Let $K_S^{\mathrm{ab}}(p)$ denote the corresponding subfield of K_S. For short, we write $D_{\bar{\mathfrak{p}}}$ for $D_{\bar{\mathfrak{p}},K_S^{\mathrm{ab}}(p)/K}$. We consider the intersections of decomposition subgroups at primes outside S. Observe first that if $\bar{\mathfrak{p}} \in \Sigma_{K_S^{\mathrm{ab}}(p)} \smallsetminus S$, then we have natural surjections:

$$\hat{\mathbb{Z}} \twoheadrightarrow D_{\bar{\mathfrak{p}}} \twoheadrightarrow \mathbb{Z}_p.$$

Indeed, the first surjection holds, since $\bar{\mathfrak{p}}|_K$ is unramified with finite residue field and the second due to the assumption on S and the existence of the cyclotomic p-extension. We will use the infinite version of the Chebotarev density theorem to prove the following result. Let δ_K denote the Dirichlet density on K.

Proposition 2.8. *Let p be a rational prime, S a finite set of primes of K with $S_p \cup S_\infty \subseteq S$. Assume that K is not totally real. Let $\bar{\mathfrak{p}} \in \Sigma_{K_S^{\mathrm{ab}}(p)} \smallsetminus S$ and $\mathfrak{p} = \bar{\mathfrak{p}}|_K$. Then there is a set $T_{\mathfrak{p}} \subseteq \Sigma_K \smallsetminus S$ with $\delta_K(T_{\mathfrak{p}}) = 1$, such that for all $\mathfrak{q} \in T_{\mathfrak{p}}$ and all extensions $\bar{\mathfrak{q}}$ of $\mathfrak{q}$ to M, the following holds:*

$$D_{\bar{\mathfrak{p}},p} \cap D_{\bar{\mathfrak{q}},p} = 1.$$

In particular, the intersection of $D_{\bar{\mathfrak{p}}}$ and $D_{\bar{\mathfrak{q}}}$ is not open in any of them.

Proof. Since K is not totally real, $r_2(K) \geqslant 1$ and hence $\mathrm{rk}_{\mathbb{Z}_p} \mathrm{G}_S^{ab,p} \geqslant 2$ by [8] 10.3.20. Let $H \cong \mathbb{Z}_p^2$ be some quotient of $\mathrm{G}_S^{\mathrm{ab}}(p)$ with corresponding field $L \subseteq K_S^{\mathrm{ab}}(p)$, such that $\mathfrak{p}$ is not completely split in L (such quotient exists due to the cyclotomic extension). Since H is torsion-free, this implies that the composition $D_{\bar{\mathfrak{p}},p} \hookrightarrow \mathrm{G}_S^{\mathrm{ab}}(p) \twoheadrightarrow H$ is injective, i.e., $D_{\bar{\mathfrak{p}},p} \twoheadrightarrow D_{\bar{\mathfrak{p}},L/K}$ is an isomorphism.

We have $\mathbb{Z}_p \cong D_{\bar{\mathfrak{p}},L/K} \subseteq H$. Consider $H \hookrightarrow H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and let $N := H \cap (D_{\bar{\mathfrak{p}},L/K} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$, the intersection taken in $H \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then N being compact and closed subgroup of $D_{\bar{\mathfrak{p}},L/K} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p$ is isomorphic to $\mathbb{Z}_p$. Let μ be the Haar measure on H, such that $\mu(H) = 1$. Then $\mu(N) = 0$ and hence $\mu(H \smallsetminus N) = 1$ and $\mu(\partial(H \cap N)) = \mu(N) = 0$. By Chebotarev's density theorem for infinite extensions, the set $T_{\mathfrak{p}}$ of primes of K, lying outside S, whose Frobenius lies in $H \smallsetminus N$ has density 1, and thus satisfies the requirements of the proposition. □

3. Modified argument of Neukirch

In this section we prove Theorem 1.1. Therefore we use a modification of Neukirch's argument involving Brauer groups (cf. [6] Theorem 1). From now on until the end of this section, we permanently assume that K is a number field, $S \supseteq S_\infty$ is a finite set of primes of K, that there are at least two rational primes under S and that p denotes one of them.

3.1. **Local invariants.** For convenience we recall briefly the local situation. Local fields are not anabelian (cf. [8] Remark before 12.2.7). This means that one can construct two non-isomorphic local fields $\kappa \ncong \kappa'$ with isomorphic absolute Galois groups: $\mathrm{G}_\kappa \cong \mathrm{G}_{\kappa'}$. Nevertheless, the following invariants of κ can be recovered from G_κ: the characteristics $\mathrm{char}\,\kappa$ of κ and $\mathrm{char}\,\bar{\kappa}$ of the residue field $\bar{\kappa}$, the cardinality $\sharp\bar{\kappa}$ of $\bar{\kappa}$, the absolute degree $[\kappa : \mathbb{Q}_p]$, if κ is p-adic, the inertia and the wild inertia subgroups $V_\kappa \subset I_\kappa \subset \mathrm{G}_\kappa$, the Frobenius class $\mathrm{Frob}_\kappa \in \mathrm{G}_\kappa / I_\kappa$, the multiplicative group λ^* of any finite extension λ/κ, the cyclotomic character χ_{cycl} on G_κ.

These invariants can be recovered using the cohomology with finite coefficients of G_κ, the local reciprocity law and the structure of the tame quotient of G_κ. This material is essentially covered by [8]. Further we have a (reformulation of a) nice lemma, proven by Neukirch:

Lemma 3.1 (cf. [6] Korollar 1)**.** *Let L, M be two local fields with L p-adic, and assume an injection $\mathrm{G}_L \subseteq \mathrm{G}_M$ is given. Then M is p-adic too, and G_L is of finite index in G_M. Further $[M\colon \mathbb{Q}_p] \leqslant [L\colon \mathbb{Q}_p]$.*

Proof. A proof can be found at the end of the proof of [8] 12.1.9. □

3.2. **Some lemmas.**

Lemma 3.2. *Let p be a rational prime. Let G_κ be the absolute Galois group of a local field κ, $H \subset \mathrm{G}_\kappa$ a subgroup of p-decomposition type. Then κ is not p-adic.*

Proof. Suppose κ is p-adic. First, we choose some $H \subset U \subseteq \mathrm{G}_\kappa$ with last inclusion open, such that the image of H in $U(p)$ is not (pro-)cyclic. Indeed, choose an open normal subgroup $V \lhd \mathrm{G}_\kappa$ such that $H/H \cap V$ is not (pro-)cyclic. Then let U be the preimage under $\mathrm{G}_\kappa \twoheadrightarrow \mathrm{G}_\kappa/V$ of the p-subgroup $H/H \cap V$.

Now, by [8] 7.5.11, $U(p)$ is either free or a Demushkin group of rank $[\lambda : \mathbb{Q}_p] + 2 > 2$, where λ is the local field corresponding to U. In both cases $U(p)$, being of finite cohomological dimension, is torsion-free, hence the image of H in $U(p)$ is torsion-free, hence H embeds into $U(p)$ (using Lemma 2.2, one sees that the kernel of the map $H \to U(p)$ can only be the trivial subgroup of H). Now, $U(p)$ can neither be free: this contradicts $\mathrm{cd}_p H = 2$, nor a Demushkin group of rank > 2: this contradicts Lemma 3.3. This finishes the proof. □

Lemma 3.3. *Assume H_m, H_n are two Demushkin pro-p-groups of ranks $m, n \geqslant 2$ respectively. If there is an inclusion $H_m \subseteq H_n$, then it is automatically open and $m = (H_n : H_m)(n-2) + 2$. In particular, $m \geqslant n$.*

Proof. If $H_m \subseteq H_n$ is open, then $m = (H_n : H_m)(n-2) + 2 \geqslant n$, which is well-known (cf. [3] or [1] for a purely group-theoretic proof). If $H_m \subseteq H_n$ is not open, then p^∞ divides the index $(H_n : H_m)$ and [8] Chap. III §7 Ex.3 implies that $\mathrm{cd}_p H_m < \mathrm{cd}_p H_n$, which is absurd, since both numbers are equal to 2. □

In the original proof Neukirch used the following fact: let $H \subseteq G_S$ be a closed subgroup, which is isomorphic to the absolute Galois group of a local field of characteristic 0. If an open subgroup of H is contained in a decomposition subgroup $D_{\bar{\mathfrak{p}}}$ of a prime $\bar{\mathfrak{p}} \in S$, then also $H \subseteq D_{\bar{\mathfrak{p}}}$. Unfortunately, this easy fact can not be applied to Theorem 1.1, since we do not know in general, whether the groups $D_{\bar{\mathfrak{p}}}$ are isomorphic to absolute Galois groups of local fields for $\bar{\mathfrak{p}} \in S_f$. However, a more precise treatment involving p-Sylow subgroups of decomposition subgroups is available.

Lemma 3.4. *Let $H \subseteq \mathrm{G}_S$ be a closed subgroup of p-decomposition type. Assume that there is an open subgroup H_0 of H with $H_0 \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}} \in S_f$. Then $H \subseteq D_{\bar{\mathfrak{p}}}$.*

Proof. Taking the intersection over all conjugates of H_0 in H, we can assume H_0 to be normal in H. By Lemma 2.2, H_0 is of p-decomposition type. Since two rational primes lie in $\mathcal{O}^*_{K,S}$, the decomposition groups of primes in $S_p \subset S$ are isomorphic to absolute Galois groups of local p-adic fields. Hence by Lemma 3.2, $\bar{\mathfrak{p}} \notin S_p$. Further, H_0 is a pro-p-subgroup of $D_{\bar{\mathfrak{p}}}$, hence contained in a pro-p-Sylow subgroup $D_{\bar{\mathfrak{p}},p}$, which is again of p-decomposition type, since $\bar{\mathfrak{p}} \notin S_p$. Thus, $H_0 \subseteq D_{\bar{\mathfrak{p}},p}$ are both of p-decomposition type and the inclusion is open by Lemma 2.2. Since H normalizes H_0, Corollary 2.7(i) implies $H \subseteq D_{\bar{\mathfrak{p}}}$. □

3.3. **Characterization of decomposition subgroups.** Recall that in Section 2.1 we associated to any group $H \cong \mathbb{Z}_p \ltimes \mathbb{Z}_p$ of p-decomposition type a character $\chi_H\colon H \to \mathbb{Z}_p^*$, which

describes the action of the first $\mathbb{Z}_p$ on the second. Recall that χ_p denotes the p-cyclotomic character on G_S. For any open subgroup $U \subseteq G_S$, let $\pi_{p,U}$ denote the natural projection

$$\pi_{p,U} \colon U \twoheadrightarrow \mathrm{Cl}_S(U)/p. \tag{3.1}$$

Then we have the following criteria for a subgroup of p-decomposition type of G_S to lie in a decomposition subgroup of a prime.

Proposition 3.5. *Let $H \subseteq \mathrm{G}_S$ be a closed subgroup of p-decomposition type. The following are equivalent:*

(a) *$H \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}} \in S_f \smallsetminus S_p$.*
(b) *For some open subgroup $H_0 \subseteq H$, $\chi_p|_{H_0} = \chi_{H_0}$.*

If moreover $\mu_p \subset K$, then they are also equivalent to

(c) *For H the following condition holds:*
$(*)_H$ *For any $U \subseteq \mathrm{G}_S$ open: $H \subseteq U \Rightarrow H \subseteq \ker(\pi_{p,U} \colon U \twoheadrightarrow \mathrm{Cl}_S(U)/p)$.*

The prime $\bar{\mathfrak{p}}$ in (a) is unique.

Proof. If $H \subseteq D_{\bar{\mathfrak{p}}}, D_{\bar{\mathfrak{q}}}$ with $\bar{\mathfrak{p}}, \bar{\mathfrak{q}} \in S_f \smallsetminus S_p$, then $H \subseteq D_{\bar{\mathfrak{p}},p}, D_{\bar{\mathfrak{q}},p}$ for some p-Sylow-subgroups, which are again of p-decomposition type. Hence by Lemma 2.2(ii), the last inclusions are open. Proposition 2.4 implies then $\bar{\mathfrak{p}} = \bar{\mathfrak{q}}$. This proves the uniqueness of $\bar{\mathfrak{p}}$ in (a).

(a) $\Rightarrow$ (b): After replacing G_S by an appropriate open subgroup containing H, we can assume $H = D_{\bar{\mathfrak{p}},p} \cong \mathbb{Z}_p \ltimes \mathbb{Z}_p$ is a p-Sylow subgroup of $D_{\bar{\mathfrak{p}}}$. Then the first $\mathbb{Z}_p$ acts on the second as the unramified quotient on the inertia subgroup, i.e., by the p-cyclotomic character. This means $\chi_H = \chi_p|_H$.

(b) $\Rightarrow$ (a): By Lemma 3.4 we can assume that K is totally imaginary. Again by Lemma 3.4 it is enough to show that $H_0 \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}} \in S_f$. First we claim that the restriction map

$$\mathrm{H}^2(\mathrm{G}_S, \mu_{p^\infty}) \to \bigoplus_{\mathfrak{p} \in S(K)} \mathrm{H}^2(D_{\mathfrak{p}}, \mu_{p^\infty}),$$

is injective. Interpreting elements of $Ш^1(\mathrm{G}_S, \mathbb{Z}/p^n\mathbb{Z})$ as homomorphisms $\mathrm{G}_S \to \mathbb{Z}/p^n\mathbb{Z}$, which are trivial on the decomposition groups at S, we see from [8] 8.3.21(ii) that $Ш^1(\mathrm{G}_S, \mathbb{Z}/p^n\mathbb{Z}) \cong (\mathrm{Cl}_S/p^n)^\vee$. Hence the kernel of the map which is claimed to be injective is by Poitou-Tate duality equal to:

$$\begin{aligned} Ш^2(\mathrm{G}_S, \mu_{p^\infty}) &= \varinjlim_n Ш^2(\mathrm{G}_S, \mu_{p^n}) = \varinjlim_n [Ш^1(\mathrm{G}_S, \mathbb{Z}/p^n\mathbb{Z})^\vee] \\ &= [\varprojlim_n Ш^1(\mathrm{G}_S, \mathbb{Z}/p^n\mathbb{Z})]^\vee \cong [\varprojlim_n (\mathrm{Cl}_S/p^n)^\vee]^\vee = 0, \end{aligned}$$

the last equality being true by finiteness of the Hilbert class field and as the transition maps in the inverse limit are multiplications by p. This proves our claim.

Now we can do the same for any open subgroup $U \subseteq \mathrm{G}_S$, and pass to the direct limit over all open U containing H_0. Let M denote the fixed field of H_0. By exactness of $\varinjlim$ and some straightforward abstract nonsense we obtain:

$$0 \to \mathrm{H}^2(H_0, \mu_{p^\infty}) \to \prod_{\mathfrak{p} \in S(M)} \mathrm{H}^2(D_{\mathfrak{p},K_S/M}, \mu_{p^\infty}). \tag{3.2}$$

By (b), $\chi_p|_{H_0} = \chi_{H_0}$. Thus $\mathrm{H}^2(H_0, \mu_{p^\infty}) = \mathbb{Q}_p/\mathbb{Z}_p$. From the sequence (3.2), there is a prime $\bar{\mathfrak{p}} \in S_f$ with $\mathrm{H}^2(D_{\bar{\mathfrak{p}},K_S/M}, \mu_{p^\infty}) \neq 0$. We claim that the prime $\mathfrak{p} = \bar{\mathfrak{p}}|_M$ is indecomposed in K_S/M, i.e., that $H_0 = D_{\bar{\mathfrak{p}},K_S/M} \subseteq D_{\bar{\mathfrak{p}}}$. Therefore, consider an open subgroup $H' \subseteq H_0$ with

corresponding fixed field M'. For any open $H' \subseteq U \subseteq \mathrm{G}_S$ with corresponding fixed field L, let $T_{\mathfrak{p},H'}(U)$ be the (finite) set of all primes of L lying under a prime $\mathfrak{p}' \in S_{\mathfrak{p}}(M')$. Then we have the sequence

$$\mathrm{H}^2(U, \mu_{p^\infty}) \to \bigoplus_{\mathfrak{q} \in T_{\mathfrak{p},H'}(U)} \mathrm{H}^2(D_{\mathfrak{q},K_S/L}, \mu_{p^\infty}) \to 0,$$

which is exact by [8] 9.2.1 (after passing to the limit over all finite submodules), since there are still non-archimedean primes in $S(L)$, which do not enter the index set of the direct sum. Passing to the limit over all open U containing H' gives the exact sequence:

$$\mathrm{H}^2(H', \mu_{p^\infty}) \to \bigoplus_{\mathfrak{p}' \in S_{\mathfrak{p}}(M')} \mathrm{H}^2(D_{\mathfrak{p}',K_S/M'}, \mu_{p^\infty}) \to 0. \tag{3.3}$$

Since $\chi_p|_{H'} = \chi_{H_0}|_{H'} = \chi_{H'}$, we have $\mathrm{H}^2(H', \mu_{p^\infty}) \cong \mathbb{Q}_p/\mathbb{Z}_p$. Further, $\mathrm{H}^2(D_{\mathfrak{p}',K_S/M'}, \mu_{p^\infty}) \neq 0$. In fact, $D_{\mathfrak{p}',K_S/M'}$ is conjugate to an open subgroup of $D_{\bar{\mathfrak{p}},K_S/M}$. But since $\mathrm{H}^2(D_{\bar{\mathfrak{p}},K_S/M}, \mu_{p^\infty}) \neq 0$, also $\mathrm{H}^2(V, \mu_{p^\infty}) \neq 0$ for any open subgroup $V \subseteq D_{\bar{\mathfrak{p}},K_S/M}$ (this is an easy fact on p-decomposition groups). By counting the coranks in (3.3) it follows that there is only one prime lying over $\mathfrak{p}$ in any finite extension M'/M. Hence $\bar{\mathfrak{p}}|_M$ is indecomposed.

Since H is of p-decomposition type and the groups $D_{\bar{\mathfrak{q}}}$ with $\bar{\mathfrak{q}} \in S_p$ are isomorphic to absolute Galois groups of local p-adic fields by Corollary 2.6 (since two rational primes lie under S), Lemma 3.2 implies $\bar{\mathfrak{p}} \notin S_p$.

(a) $\Rightarrow$ (c): Let $H \subseteq U \subseteq \mathrm{G}_S$ with last inclusion open. Consider the commutative diagram:

$$\begin{array}{ccccc} H & \hookrightarrow & D_{\bar{\mathfrak{p}}} \cap U & \hookrightarrow & U \\ & & \downarrow & & \downarrow \\ & & (D_{\bar{\mathfrak{p}}} \cap U)^{\mathrm{ab}} & \longrightarrow & U^{\mathrm{ab}} \twoheadrightarrow \mathrm{Cl}_S(U)/p. \end{array}$$

Since the composition of the maps in the lower row is zero by class field theory,

$$H \subseteq D_{\bar{\mathfrak{p}}} \cap U \subseteq \ker(U \twoheadrightarrow \mathrm{Cl}_S(U)/p),$$

i.e., $(*)_H$ holds.

(c) $\Rightarrow$ (a): Assume now $(*)_H$ holds. For any $U \supseteq H$ open in G_S with corresponding field L, we have $\mu_p \subset L$, and hence by Poitou-Tate duality:

$$Ш^2(U, \mathbb{Z}/p\mathbb{Z}) = Ш^1(U, \mu_p)^\vee \cong Ш^1(U, \mathbb{Z}/p\mathbb{Z})^\vee = (\mathrm{Cl}_S(U)/p)^{\vee\vee} = \mathrm{Cl}_S(U)/p.$$

This gives us the exact sequence:

$$0 \to \mathrm{Cl}_S(U)/p \to \mathrm{H}^2(U, \mathbb{Z}/p\mathbb{Z}) \to \bigoplus_{\mathfrak{p} \in S(U)} \mathrm{H}^2(D_{\mathfrak{p},K_S/L}, \mathbb{Z}/p\mathbb{Z}).$$

Set $M = (K_S)^H$ and consider the limit of these sequences over all open $U \supseteq H$:

$$0 \to \varinjlim_{H \subseteq U \subseteq \mathrm{G}_S} \mathrm{Cl}_S(U)/p \to \mathrm{H}^2(H, \mathbb{Z}/p\mathbb{Z}) \to \prod_{\mathfrak{p} \in S(M)} \mathrm{H}^2(D_{\mathfrak{p},K_S/M}, \mathbb{Z}/p\mathbb{Z}).$$

This sequence is exact. We claim that $\varinjlim_{H \subseteq U \subseteq \mathrm{G}_S} \mathrm{Cl}_S(U)/p = 0$. For an open $H \subseteq U \subseteq \mathrm{G}_S$, let $U' := \ker(U \twoheadrightarrow \mathrm{Cl}_S(U)/p)$. By the S-version of the principal ideal theorem, which states that any ideal class in $\mathrm{Cl}_S(U)/p$ gets trivial in the subfield of the Hilbert class field corresponding to the quotient $\mathrm{Cl}(U) \twoheadrightarrow \mathrm{Cl}_S(U)/p$ (cf. e.g. [5] Theorem 8.11), the map $\mathrm{Cl}_S(U)/p \to \mathrm{Cl}_S(U')/p$, induced by inclusion on ideals, is zero. On the other side, U' appears in the index set of the limit due to $(*)_H$. Thus $\varinjlim_{H \subseteq U \subseteq \mathrm{G}_S} \mathrm{Cl}_S(U)/p = 0$. Now we can conclude as in the (b) $\Rightarrow$ (a) part

(with μ_{p^∞}-coefficients replaced by $\mathbb{Z}/p\mathbb{Z}$), exactly as in the original argument of Neukirch [6] Theorem 1. □

Remark 3.6. With exactly the same proof (except for the uniqueness statements, which follow from Lemma 3.1 and Corollary 2.7(ii) instead from Lemma 3.4 as above), the same criteria as in the proposition hold for H if one assumes it to be a closed subgroup of G_S, which is isomorphic to the absolute Galois group of a local field of characteristic zero instead of a group of p-decomposition type.

3.4. **Proof of Theorem 1.1.**

Proof of (i) ⇝ (ii). Since we want to reconstruct the p-cyclotomic character χ_p only on an open subgroup of G_S, we can assume $\mu_p \subset K$ and K totally imaginary. Observe that χ_p on the local groups $D_{\bar{\mathfrak{p}}}$ with $\bar{\mathfrak{p}} \in S_p$ is determined by the group structure, since $D_{\bar{\mathfrak{p}}}$ is the absolute Galois group of a local field in this case (cf. Section 3.1). If $\bar{\mathfrak{p}} \in S_f \smallsetminus S_p$, then $D_{\bar{\mathfrak{p}},p} \hookrightarrow D_{\bar{\mathfrak{p}}} \twoheadrightarrow D_{\bar{\mathfrak{p}}}(p)$ is bijective; χ_p is determined on $D_{\bar{\mathfrak{p}},p}$ (in fact, it is equal to the character associated to the p-decomposition group $D_{\mathfrak{p},p}$); and χ_p factors through $D_{\bar{\mathfrak{p}}} \twoheadrightarrow D_{\bar{\mathfrak{p}}}(p)$. Thus χ_p is in this case also determined on $D_{\bar{\mathfrak{p}}}$. We have the following exact sequence from class field theory ([8] 8.3.21(ii)):

$$0 \to \overline{\mathcal{O}^*_{K,S}} \to \prod_{\mathfrak{p}\in S(K)} D_{\bar{\mathfrak{p}}}^{\mathrm{ab}} \to \mathrm{G}_S^{\mathrm{ab}} \to \mathrm{Cl}_S(K) \to 0. \tag{3.4}$$

The data given by (i) determine this sequence, since they determine the map in the middle. Since the global cyclotomic character factorizes through $\mathrm{G}_S^{\mathrm{ab}}$, it is determined by the local ones on the open subgroup $\ker(\mathrm{G}_S \twoheadrightarrow \mathrm{Cl}_S(K))$ of G_S. □

Under the additional assumption that the decomposition groups at S_f are isomorphic to absolute Galois groups of local fields of characteristic zero, the proof of (i) ⇝ (ii)' works similarly and (ii)' ⇝ (ii) and (iii) ⇝ (iii)' are immediate.

Proof of (i) ⇝ (iii). Assume the embeddings $(\iota_{\bar{\mathfrak{p}}} \colon D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_S)_{\bar{\mathfrak{p}}\in S_f}$ are given. Then they are also given for any open subgroup $U \subseteq \mathrm{G}_S$. Let U be such that the corresponding field L is totally imaginary, i.e., the decomposition groups of archimedean primes are trivial. Then the sequence (3.4) for U determines $\mathrm{Cl}_S(U)$ as the quotient of U by the closure of the normal subgroup generated by the commutator and the images of $\iota_{\bar{\mathfrak{p}},L}$ for $\bar{\mathfrak{p}} \in S_f$. □

Proof of (i) ⇝ (iv). For any U, $\sharp S_f(U)$ is equal to the number of the U-conjugacy classes of the subgroups $D_{\bar{\mathfrak{p}}} \cap U$ and $\sharp S_\infty(U)$ is given by the number of real/complex embeddings, which is deduced from (G_S, p) by Proposition 4.1. □

Finally, we show the remaining directions, using criteria from Proposition 3.5.

Proof of (ii) ⇝ (i), (iii)' ⇝ (i), (iv) ⇝ (i). Assume (ii), (iii)' or (iv) is given. As we know that the decomposition subgroups of primes over p are isomorphic to absolute Galois groups of local p-adic fields and as such groups determine the residue characteristic, Remark 3.6 implies that we can reconstruct them from the given data.

Lemma 3.7. *Assume $\mu_p \subset K$ (and $\mu_4 \subset K$ if $p = 2$) in Theorem 1.1. Then (iii)' ⇜⇝ (iv).*

Proof. Since $\mu_p \subseteq K$, we have for every U the exact sequence ($_pA$ means the p-torsion of the abelian group A):

$$0 \to \mathrm{Cl}_S(U)/p \to \mathrm{H}^2(U, \mathbb{Z}/p\mathbb{Z}) \to {}_p\,\mathrm{H}^2(U, \mathcal{O}_S^*) \to 0, \text{ and}$$
$$\dim_{\mathbb{F}_p} {}_p\,\mathrm{H}^2(U, \mathcal{O}_S^*) = \sharp S_f(U) - 1,$$

since K is totally imaginary. Thus $\dim_{\mathbb{F}_p} \mathrm{H}^2(U, \mathbb{Z}/p\mathbb{Z}) + 1 = \dim_{\mathbb{F}_p} \mathrm{Cl}_S(U)/p + \sharp S_f(U)$. Since the number on the left is known, the knowledge of one of the summands on the right is equivalent to the knowledge of the other. □

Lemma 3.8. *From the data in (iv) one can reconstruct the maps $\pi_{p,U}$ (cf. (3.1)) and for any $V \subseteq U \subseteq \mathrm{G}_S$ open, the maps $\mathrm{Cl}_S(U)/p \to \mathrm{Cl}_S(V)/p$, which are induced by inclusion on ideals.*

Proof. For any open U with corresponding field L, we can describe the Galois group of the maximal abelian unramified extension of L, which is completely decomposed in S. By class field theory, it is canonically isomorphic to $\mathrm{Cl}_S(U)$. In fact, an extension of L, corresponding to an open subgroup $V \subseteq U$ is completely decomposed in S, if and only if $\sharp S(V) = (U : V)\sharp S(U)$. Observe that such extension is automatically unramified, since it is unramified outside S, as all groups are subquotients of G_S, and also unramified in S, being completely decomposed there. Thus if we set $V_0 := \bigcap_V V$, where the intersection is taken over all open normal subgroups $V \subseteq U$, such that $\sharp S(V) = (U : V)\sharp S(U)$ and the quotient U/V is abelian, then $U/V_0 \cong \mathrm{Cl}_S(U)$. Thus (iv) gives us the surjections $U \twoheadrightarrow \mathrm{Cl}_S(U)$ and in particular the surjections

$$\pi_{p,U} \colon U \twoheadrightarrow \mathrm{Cl}_S(U)/p$$

(notice that (iii)' contains this information only implicitly!). Furthermore, for $V \subseteq U \subseteq \mathrm{G}_S$ open, the map $\mathrm{Cl}_S(U) \to \mathrm{Cl}_S(V)$ induced by inclusion on ideals, is encoded in the group theory as the map induced by the transfer map $U^{\mathrm{ab}} \to V^{\mathrm{ab}}$ (cf. e.g. [7], after Proposition 6.13). □

Let now $U \subseteq \mathrm{G}_S$ be an open (normal) subgroup, small enough, such that the corresponding fixed field L contains the p-roots of unity and is totally imaginary. By Proposition 3.5, applied to U, using Corollary 2.7(i) if necessary, we can decide, using the information given by (ii), (iii)' or (iv) and Lemmas 3.7 and 3.8, whether a closed subgroup $H \subseteq U$ of p-decomposition type is contained in a decomposition subgroup of a prime in $S_f \smallsetminus S_p$. By Lemma 2.3 and Lemma 3.4, the maximal subgroups with this property are exactly the p-Sylow subgroups of the groups $D_{\bar{\mathfrak{p}},K_S/L}$ with $\bar{\mathfrak{p}} \in S_f \smallsetminus S_p$. Thus we have reconstructed the set

$$\mathrm{Syl}_p(U, S_f \smallsetminus S_p) := \{H \subseteq U \colon H \text{ is a } p\text{-Sylow-subgroup of } D_{\bar{\mathfrak{p}},K_S/L} \text{ with } \bar{\mathfrak{p}} \in S_f \smallsetminus S_p\}.$$

Now, U acts on this set by conjugation. We have an U-equivariant surjection (U acts trivially on the right side):

$$\psi \colon \mathrm{Syl}_p(U, S_f \smallsetminus S_p) \twoheadrightarrow (S_f \smallsetminus S_p)(U),$$

which sends H to the prime $\bar{\mathfrak{p}}|_L$ (unique by Proposition 2.4!), such that $H \subseteq D_{\bar{\mathfrak{p}},K_S/L}$. We want to determine, when two elements have the same image under ψ. For $H \in \mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ such that $H \subseteq D_{\bar{\mathfrak{p}},K_S/L}$ is a p-Sylow subgroup, consider the restriction map

$$\mathrm{res}^U_H \colon \mathrm{H}^2(U, \mathbb{Z}/p\mathbb{Z}) \twoheadrightarrow \mathrm{H}^2(H, \mathbb{Z}/p\mathbb{Z}),$$

which is surjective, being equal to the composition

$$\mathrm{H}^2(U, \mathbb{Z}/p\mathbb{Z}) \twoheadrightarrow \mathrm{H}^2(D_{\bar{\mathfrak{p}},K_S/L}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\sim} \mathrm{H}^2(H, \mathbb{Z}/p\mathbb{Z}),$$

in which the first map is surjective by [8] 9.2.1, since $\sharp S_f(U) > 1$, and the second is an isomorphism, since $\mu_p \subset L$.

Lemma 3.9. *Let $H, H' \in \mathrm{Syl}_p(U, S_f \smallsetminus S_p)$. Then:*

$$\psi(H) = \psi(H') \Leftrightarrow \ker(\mathrm{res}^U_H) = \ker(\mathrm{res}^U_{H'}).$$

Proof. Consider the commutative diagram with exact row:

$$0 \longrightarrow Ш^2(U, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{H}^2(U, \mathbb{Z}/p\mathbb{Z}) \longrightarrow (\bigoplus_{\mathfrak{q}\in S(L)} \mathrm{H}^2(D_{\mathfrak{q},K_S/L}, \mathbb{Z}/p\mathbb{Z}))^{\Sigma=0} \longrightarrow 0$$
$$\mathrm{res}^U_H \searrow \quad \downarrow$$
$$\mathrm{H}^2(H, \mathbb{Z}/p\mathbb{Z})$$

where $\Sigma = 0$ means that we take the subspace of trace zero elements. The diagonal map factors through the vertical one, since $H \in \mathrm{Syl}_p(U, S_f \smallsetminus S_p)$. From this sequence we see that if $\mathfrak{p} = \psi(H)$, then the kernel of res^U_H is the extension of the subspace $(\bigoplus_{\mathfrak{q}\in S(L)\smallsetminus\{\mathfrak{p}\}} \mathrm{H}^2(D_{\mathfrak{q},K_S/L}, \mathbb{Z}/p\mathbb{Z}))^{\Sigma=0}$ of the space on the right side by $Ш^2(U, \mathbb{Z}/p\mathbb{Z})$. Two such subspaces of $\mathrm{H}^2(U, \mathbb{Z}/p\mathbb{Z})$ corresponding to $\mathfrak{p}$ resp. $\mathfrak{p}'$ are equal if and only if $\mathfrak{p} = \mathfrak{p}'$ (since we can assume $S_{p_1} \cup S_{p_2} \subsetneq S_f(U)$ and hence $\sharp S_f(U) \geqslant 3$). This finishes the proof. □

The lemma gives a purely group-theoretical criterion to decide, whether two elements of $\mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ lie in the same fiber of ψ. If we define an equivalence relation on $\mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ by $H \sim H' :\Leftrightarrow \ker(\mathrm{res}^U_H) = \ker(\mathrm{res}^U_{H'})$, we get a bijective map induced by ψ:

$$\mathrm{Syl}_p(U, S_f \smallsetminus S_p)/\sim \quad \xrightarrow{\sim} \quad (S_f \smallsetminus S_p)(U).$$

If $U' \subseteq U \subseteq \mathrm{G}_S$, then we get a (non-canonical!) mapping

$$\alpha\colon \mathrm{Syl}_p(U', S_f \smallsetminus S_p) \to \mathrm{Syl}_p(U, S_f \smallsetminus S_p),$$

which sends $H' \in \mathrm{Syl}_p(U', S_f \smallsetminus S_p)$ to some $H \in \mathrm{Syl}_p(U, S_f \smallsetminus S_p)$, such that $H' \subseteq H$ (there is at least one by construction). If $H' \subseteq H_1, H_2$, then $H_1, H_2 \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}}$ by Proposition 2.4. In particular, α induces a map

$$\overline{\alpha}\colon \mathrm{Syl}_p(U', S_f \smallsetminus S_p)/\sim \to \mathrm{Syl}_p(U, S_f \smallsetminus S_p)/\sim,$$

which is independent of the above choices. We obtain the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Syl}_p(U', S_f \smallsetminus S_p)/\sim & \xrightarrow{\sim} & (S_f \smallsetminus S_p)(U') \\ \downarrow{\scriptstyle \overline{\alpha}} & & \downarrow \\ \mathrm{Syl}_p(U, S_f \smallsetminus S_p)/\sim & \xrightarrow{\sim} & (S_f \smallsetminus S_p)(U), \end{array}$$

where horizontal maps are bijections induced by ψ, and the vertical map on the right is the restriction of primes.

If $U \lhd \mathrm{G}_S$ is normal, then G_S acts on $\mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ by conjugation. It is easy to see that this action induces via ψ a G_S-action on $(S_f \smallsetminus S_p)(U)$ and that this last action coincides with the action of G_S on this set by permuting the primes. *In this way we have reconstructed the projective system of* G_S*-sets* $\{(S_f \smallsetminus S_p)(U)\colon U \subseteq U_0, U \lhd \mathrm{G}_S\}$, where $U_0 \subseteq \mathrm{G}_S$ is some open subgroup. Now the decomposition subgroups of primes in $S_f \smallsetminus S_p$ are exactly the stabilizers in G_S of elements in the G_S-set $\varprojlim_{U\subseteq U_0, U\lhd \mathrm{G}_S} (S_f \smallsetminus S_p)(U)$. This finishes the proof of Theorem 1.1. □

4. Invariants encoded in G_S

In this section we discuss easy consequences of Theorem 1.1 and prove Proposition 1.3.

4.1. **Recovering some global invariants.** Let K, S be a number field together with a finite set of primes. Assume there is a rational prime p with $S \supseteq S_p \cup S_\infty$. Which invariants of K are encoded in G_S resp. (G_S, p) resp. $(\mathrm{G}_S, p, \chi_p)$? The next two propositions determine some of these invariants.

Proposition 4.1. *Let S be a finite set of primes of K. Assume there is a rational prime p with $S_p \cup S_\infty \subseteq S$. Then $(G_S, p) \rightsquigarrow [K:\mathbb{Q}], r_1(K), r_2(K)$. If the Leopoldt conjecture is true for K and for all rational primes, then $\mathrm{G}_S \rightsquigarrow [K:\mathbb{Q}], r_1(K), r_2(K), \mathbb{N}(S)$.*

Proof. First we show the last statement. So, assume Leopoldt is true for K and all rational primes. We show that G_S determines $r_2 = r_2(K)$ and the set $\mathbb{N}(S)$. For any rational prime p consider the number $r(p) := \mathrm{rk}_{\mathbb{Z}_p} \mathrm{G}_S^{\mathrm{ab}}(p)$. The Leopoldt conjecture says that $r_2 + 1 = r(p)$ if $S_p \cup S_\infty \subseteq S$. If $S_p \nsubseteq S$, then at least the cyclotomic $\mathbb{Z}_p$-extension is not contained in K_S/K, thus in this case

$$r(p) = \mathrm{rk}_{\mathbb{Z}_p} \mathrm{G}_S^{\mathrm{ab}}(p) < \mathrm{rk}_{\mathbb{Z}_p} \mathrm{G}_{S\cup S_p}^{\mathrm{ab},p} = r_2 + 1.$$

Since $S_p \subseteq S$ for at least one p, we obtain $r_2 = \max_p\{r(p)\} - 1$, and a prime lies in $\mathbb{N}(S)$ if and only if $r(p)$ is maximal.

Now it remains to recover $[K:\mathbb{Q}]$ and r_1. Once $[K:\mathbb{Q}]$ is known, r_1 can be recovered as $[K:\mathbb{Q}] - 2r_2$. To recover $[K:\mathbb{Q}]$, observe that if K is totally imaginary, $[K:\mathbb{Q}] = 2r_2$ can be recovered together with r_2. If $\pi : \mathrm{G}_S \twoheadrightarrow \mathrm{G}_S^{\mathrm{ab}}$ denotes the natural surjection, and $U := \pi^{-1}(\mathrm{im}([(p-1)p]\colon \mathrm{G}_S^{\mathrm{ab}} \to \mathrm{G}_S^{\mathrm{ab}}))$, then $U \subseteq \mathrm{G}_S$ is open and $L := K_S^U$ is totally imaginary. Indeed, L contains the p^2-roots of unity, since they are contained in K_S (p^2 and not simply p is needed to cover the case $p = 2$). Thus

$$[K:\mathbb{Q}] = (\mathrm{G}_S : U)^{-1}[L:\mathbb{Q}] = 2(\mathrm{G}_S : U)^{-1} r_2(L).$$

To show the first (unconditional) statement of the proposition, notice that once a prime $p \in \mathbb{N}(S)$ is known, one obtains $r_2(K)$ as the negative of the Euler characteristic $-\chi(\mathrm{G}_S, \mathbb{Z}/p\mathbb{Z})$ ([8] 8.7.5) and $[K:\mathbb{Q}], r_1(K)$ as above, without assuming Leopoldt. □

Proposition 4.2. *Let K, S be a number field together with a set of primes, such that the decomposition groups at primes in S_f are isomorphic to absolute Galois groups of local fields of characteristic zero. Assume G_S is given together with any one (or, equivalently, all) pieces of information from Theorem 1.1. Then one can recover the following invariants of K and its extensions:*

(i) *For any $U \subseteq \mathrm{G}_S$ open with corresponding field totally imaginary, the class number $\mathrm{Cl}(U)$.*
(ii) *For every $U' \subseteq U \subseteq \mathrm{G}_S$ open, with corresponding fields totally imaginary, the natural maps $\mathrm{Cl}(U) \to \mathrm{Cl}(U')$.*
(iii) *For $U \subseteq \mathrm{G}_S$ small enough, with $L = (K_S)^U$, the roots of unity $\mu(L)$.*
(iv) *For any $U \subseteq \mathrm{G}_S$ open with $L = (K_S)^U$, the absolute inertia and ramification degrees $f_{\mathfrak{p},L/\mathbb{Q}_\ell}$ and $e_{\mathfrak{p},L/\mathbb{Q}_\ell}$ of any $\mathfrak{p} \in S_f(L)$ ($\mathfrak{p}$ lies over ℓ).*
(v) *The set $\mathbb{N}(S)$.*
(vi) *The numbers $[K:\mathbb{Q}], r_1(K), r_2(K)$.*

Proof. (i) + (ii): If K is totally imaginary, one obtains the group $\mathrm{G}_\varnothing = \mathrm{G}_{K_\varnothing/K}$ as the quotient of G_S by the closure of the normal subgroup generated by the inertia subgroups of all $D_{\bar{\mathfrak{p}}}$, $\bar{\mathfrak{p}} \in S_f$. Then canonically $\mathrm{G}_\varnothing^{\mathrm{ab}} \cong \mathrm{Cl}(K)$. The maps between two class groups are given by the transfer maps in the class field theory.

(iii) follows from (i) $\leftrightsquigarrow$ (ii)$'$ in Theorem 1.1.

(iv) follows from the anabelian properties of local fields listed in Section 3.1.

(v): for any rational prime ℓ, let $n(\ell) := \sum_{\mathfrak{p}\in S\cap S_\ell} [K_\mathfrak{p} : \mathbb{Q}_\ell]$. This number can be reconstructed from the given data. Thus, $\ell \in \mathbb{N}(S) \Leftrightarrow n(\ell)$ is maximal. Finally (vi) follows from (v) and Proposition 4.1. □

4.2. **The numbers $\sharp S_f(U)$.**

Proof of Proposition 1.3. Recall that χ_p denotes the p-cyclotomic character, and that $\mu_p \subset K$ implies that its image lies in $\ker(\mathrm{Aut}(\mathbb{Q}_p/\mathbb{Z}_p) \twoheadrightarrow \mathrm{Aut}(\frac{1}{p}\mathbb{Z}/\mathbb{Z}))$. Assume $\chi\colon \mathrm{G}_S \to \mathbb{Z}_p^*$ induces the trivial action on $\frac{1}{p}\mathbb{Z}/\mathbb{Z}$. We claim first that if $\chi|_{D_{\bar{\mathfrak{p}}}} = \chi_p|_{D_{\bar{\mathfrak{p}}}}$ for all $\bar{\mathfrak{p}} \in S$, then $\chi = \chi_p$ on G_S. Indeed, χ, χ_p factor both through $\mathrm{G}_S^{\mathrm{ab}}$. Using sequence (3.4), $\chi^{-1} \otimes \chi_p$ factors through a map $\mathrm{Cl}_S(K) \to \mathbb{Z}_p^*$, i.e., its image is finite, and on the other side the images of χ and χ_p lie in the subgroup $\ker(\mathrm{Aut}(\mathbb{Q}_p/\mathbb{Z}_p) \twoheadrightarrow \mathrm{Aut}(\frac{1}{p}\mathbb{Z}/\mathbb{Z})) \cong \mathbb{Z}_p$, i.e., the image of $\chi^{-1} \otimes \chi_p$ does too, and hence is torsion-free. Thus $\chi^{-1} \otimes \chi_p$ is the trivial character of G_S, or with other words $\chi = \chi_p$ on G_S.

The last part of the Tate-Poitou sequence for the G_S-modules $\mathbb{Z}/p^n\mathbb{Z}(\chi)$ gives, after changing to the limit over all $n > 0$, the following exact sequence:

$$0 \to Ш^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi)) \to \mathrm{H}^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi)) \to \bigoplus_{\mathfrak{p}\in S(K)} \mathrm{H}^2(D_{\mathfrak{p},K}, \mathbb{Q}_p/\mathbb{Z}_p(\chi)) \to \mathrm{coker} \to 0,$$

where

$$\begin{aligned}\mathrm{coker} &= \varinjlim_n [\mathrm{H}^0(\mathrm{G}_S, \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}(\chi^{-1} \otimes \chi_p))^\vee] = [\varprojlim_n \mathrm{H}^0(\mathrm{G}_S, \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}(\chi^{-1} \otimes \chi_p))]^\vee = \\ &= [\mathrm{H}^0(\mathrm{G}_S, \mathbb{Z}_p(\chi^{-1} \otimes \chi_p))]^\vee = \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p & \text{if } \chi = \chi_p, \\ 0 & \text{if } \chi \neq \chi_p \end{cases}\end{aligned}$$

(the last equality holds, since the restriction map $\mathrm{Aut}(\mathbb{Z}_p) \to \mathrm{Aut}(p^n\mathbb{Z}_p)$ is an isomorphism; thus if $\chi^{-1} \otimes \chi_p$ is trivial on some open subgroup of $\mathbb{Z}_p$, then it is also trivial on $\mathbb{Z}_p$). By our assumption, the corank (i.e., the $\mathbb{Z}_p$-rank of the Pontrjagin-dual) of the first term in the sequence is zero. Thus the corank of the third term is equal to the sum of the coranks of the second and the last terms. There are two cases:
Case $\chi = \chi_p$. Then the corank of the third term is $\sharp S_f(K)$ and the corank of the last term is 1. Thus the corank of the second term is $\sharp S_f(K) - 1$.
Case $\chi \neq \chi_p$. Then by the claim above, $\chi|_{D_{\bar{\mathfrak{p}}}} \neq \chi_p|_{D_{\bar{\mathfrak{p}}}}$ for at least one $\bar{\mathfrak{p}} \in S_f$. By Lemma 4.3, the corank of the third term is $\leqslant \sharp S_f(K) - 1$, and the corank of the last term is 0. Thus the corank of the second term is $\leqslant \sharp S_f(K) - 1$. The proposition follows. □

Lemma 4.3. *Let κ be a local field, $p \neq \mathrm{char}(\kappa)$ an odd prime. Let $\chi\colon \mathrm{G}_\kappa \to \mathbb{Z}_p^* = \mathrm{Aut}(\mathbb{Q}_p/\mathbb{Z}_p)$ be a character. The following are equivalent:*

(i) $\mathrm{H}^2(\mathrm{G}_\kappa, \mathbb{Q}_p/\mathbb{Z}_p(\chi)) \neq 0$.
(ii) *χ is the p-part of the cyclotomic character.*

Proof. Let χ_p denote the p-part of the cyclotomic character of G_κ. The local duality gives:

$$\begin{aligned}\mathrm{H}^2(\mathrm{G}_\kappa, \mathbb{Q}_p/\mathbb{Z}_p(\chi)) &= \varinjlim_n \mathrm{H}^2(\mathrm{G}_\kappa, \mathbb{Z}/p^n\mathbb{Z}(\chi)) = \varinjlim_n [\mathrm{H}^0(\mathrm{G}_\kappa, \mathbb{Z}/p^n\mathbb{Z}(\chi^{-1} \otimes \chi_p))^\vee] \\ &= [\varprojlim_n \mathrm{H}^0(\mathrm{G}_\kappa, \mathbb{Z}/p^n\mathbb{Z}(\chi^{-1} \otimes \chi_p))]^\vee = [\mathrm{H}^0(\mathrm{G}_\kappa, \mathbb{Z}_p(\chi^{-1} \otimes \chi_p))]^\vee \\ &= \begin{cases} \mathbb{Q}_p/\mathbb{Z}_p & \text{if } \chi = \chi_p \\ 0 & \text{if } \chi \neq \chi_p. \end{cases}\end{aligned}$$

The last equality holds by the same reasoning as in the proposition. □

Remark 4.4. Observe that the proof of Proposition 1.3 does not determine χ_p directly as *the* character with the maximal corank of $\mathrm{H}^2(\mathrm{G}_S, \mathbb{Q}_p/\mathbb{Z}_p(\chi))$, but only intrinsically by determining the numbers $\sharp S(U)$ and using Theorem 1.1.

Acknowledgements

The results in this paper coincide with a part of author's Ph.D. thesis [4], which was written under the 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.

References

[1] Andozhskii I. V.: *Demushkin groups*, Mat. Zametki, 14:1 (1973), 121-126.

[2] 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.

[3] Demushkin S. P.: *The group of the maximal p-extension of a local field*, Izv. Akad. Nauk SSSR, Ser. Matem., **25** (1961), 326-346.

[4] Ivanov A.: *Arithmetic and anabelian theorems for stable sets in number fields*, Dissertation, Universität Heidelberg, 2013.

[5] Koch H.: *Galois theory of p-extensions*, Springer, 2002, first edition.

[6] Neukirch J.: *Kennzeichnung der p-adischen und der endlich algebraischen Zahlkörper*, Invent. Math. **6** (1969) 296-314.

[7] Neukirch J.: *Klassenkörpertheorie*, Mannheim, 1969.

[8] Neukirch J., Schmidt A., Wingberg K.: *Cohomology of number fields*, Springer, 2008, second edition.

[9] Soulé C.: *K-theorie des anneaux d'entiers de corps de nombres et cohomologie étale*, Invent. Math. **55** (1979) 251-295.

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

Alexander B. Ivanov, Fakultät für Mathematik der Technischen Universität München - M11, Boltzmannstr. 3, 85748 Garching, Germany

E-mail address: ivanov@math.uni-bonn.de