Inaugural-Dissertation

zur Erlangung der Doktorwürde der
Naturwissenschaftlich-Mathematischen Gesamtfakultät der
Ruprecht-Karls-Universität Heidelberg

vorgelegt von
Diplom-Mathematiker Alexander Ivanov
aus St.-Petersburg

Tag der mündlichen Prüfung:

_____

Arithmetic and anabelian theorems for stable sets of primes in number fields

Gutachter: PD. Dr. Jakob Stix

Abstract

In this thesis we study arithmetic and anabelian properties of the Galois group $\mathrm{G}_{K,S}$ of the maximal extension of a number field K unramified outside a set of primes S. The work can be divided in two parts: the one part deals with finite and the other with infinite sets S.

The main idea of the part dealing with infinite sets S is to introduce a new class of sets of primes in number fields – stable sets. These sets have positive, but arbitrary small Dirichlet density. We give different examples of stable sets. This can be done in a rather explicit way. For example, Chebotarev sets $P_{M/K}(\sigma)$ with M/K finite Galois and $\sigma \in \mathrm{G}_{M/K}$ are often stable.

Stable sets generalize in some sense sets of density one. In particular, the most arithmetic results, holding for sets with density one, also hold for them. We generalize certain Hasse principles, Grunwald-Wang theorem, Riemann's existence theorem and a statement about the (strict) cohomological dimension from density one sets (cf. [NSW] Chapters IX and X) to stable sets. Then we show that curves $\operatorname{Spec}\mathcal{O}_{K,S}$ with S stable are often $\mathrm{K}(\pi,1)$ (for p). In particular, this gives many (explicit) examples of sets S of positive, but arbitrary small density, such that $\operatorname{Spec}\mathcal{O}_{K,S}$ is an algebraic $\mathrm{K}(\pi,1)$ (for all p simultaneously). Finally, we study anabelian properties of curves $\operatorname{Spec}\mathcal{O}_{K,S}$ with S stable. It turns out that it is possible to generalize a part of the birational anabelian theorem of Neukirch-Uchida to stable sets. More precise, we show that if for $i = 1, 2$, a number field K_i together with a stable set of primes S_i is given, such that $K_1/\mathbb{Q}$ is normal, the groups G_{K_1,S_1} and G_{K_2,S_2} are isomorphic as topological groups and some easy technical conditions are satisfied, then $K_1 \cong K_2$.

In the part concerning finite sets S we consider some anabelian properties of the group $\mathrm{G}_{K,S}$. In contrast to the situation with affine hyperbolic curves over finite fields, for which the Isomform of Grothendieck's Anabelian Conjecture was proven by A. Tamagawa [Ta] some years ago, very little is known about anabelian properties of $\mathrm{G}_{K,S}$ in the number field case. It seems even to be impossible to describe purely group-theoretically (by known methods) the location of the decomposition groups at primes in S inside the group $\mathrm{G}_{K,S}$. We show that this is possible if one has given a bit more information, than simply the group $\mathrm{G}_{K,S}$. We prove that it is equivalent to have the following pieces of information (additionally to $\mathrm{G}_{K,S}$): the location of decomposition groups at primes in S inside $\mathrm{G}_{K,S}$, the p-part χ_p of the cyclotomic character for some prime $p \in \mathcal{O}_{K,S}^*$, the collection of numbers $\sharp S(L)$, where L goes through all finite subextensions of K_S/K, etc. In particular, if $\sigma\colon \mathrm{G}_{K_1,S_1} \xrightarrow{\sim} \mathrm{G}_{K_2,S_2}$ is an isomorphism, such that $\chi_{2,p} \circ \sigma = \chi_{1,p}$, then one obtains a local correspondence at the boundary, i.e., for primes in S_1, S_2.

Zusammenfassung

In der vorliegenden Arbeit studieren wir arithmetische und anabelsche Eigenschaften der Gruppe $\mathrm{G}_{K,S}$, der maximalen außerhalb einer Stellenmenge S unverzweigten Erweiterung eines Zahlkörpers K. Die Arbeit lässt sich in zwei Teile gliedern: der eine Teil beschäftigt sich mit endlichen Mengen S, der andere mit unendlichen.

Die Hauptidee des zweitgenannten Teils besteht darin, eine neue Klasse von Stellenmengen in Zahlkörpern einzuführen – stabile Mengen. Diese haben eine positive, aber beliebig kleine Dirichlet Dichte. Auf eine relativ explizite Weise geben wir dann diverse Beispiele von stabilen Mengen. Zum Beispiel sind Chebotarev Mengen der Form $P_{M/K}(\sigma)$, wobei M/K eine endliche Galois Erweiterung und $\sigma \in \mathrm{G}_{M/K}$ ist, oft stabil.

Stabile Mengen verallgemeinern im bestimmten Sinne Mengen mit Dichte eins. Insbesondere gelten die meisten arithmetischen Sätze, die für Mengen mit Dichte eins gelten, auch für stabile Mengen. Wir werden bestimmte Hasse Prinzipien, den Satz von Grunwald-Wang, den Riemannschen Existenzsatz und eine Aussage über die (strikte) kohomologische Dimension, die allersamt für Mengen mit Dichte eins gelten (vgl. [NSW] Kapitel IX und X) auf stabile Mengen verallgemeinern. Weiterhin zeigen wir, daß die Kurven $\operatorname{Spec}\mathcal{O}_{K,S}$ mit S stabil oft $\mathrm{K}(\pi,1)$ (für p) sind. Außerdem stellt sich heraus, dass man den birationalen anabelschen Satz von Neukirch-Uchida zumindest teilweise auf stabile Mengen verallgemeinern kann. Konkret werden wir fogendes zeigen: angenommen, für $i = 1, 2$ ist ein Zahlkörper K_i mit einer stabilen Stellenmenge S_i gegeben, so dass $K_1/\mathbb{Q}$ normal ist, die Gruppen G_{K_1,S_1} und G_{K_2,S_2} isomorph sind und einige einfache technische Bedingungen erfüllt sind. Dann gilt $K_1 \cong K_2$.

Im Teil der Arbeit, der sich mit endlichen Stellenmengen befasst, werden wir einige anabelsche Eigenschaften der Gruppe $\mathrm{G}_{K,S}$ untersuchen. Im Gegensatz zur Situation mit affinen hyperbolischen Kurven über endlichen Körpern, für welche die Isom-Form der anabelschen Vermutung von Grothendieck, einige Jahre zuvor von A. Tamagawa in [Ta] bewiesen wurde, ist nur sehr wenig über anabelsche Eigenschaften von $\mathrm{G}_{K,S}$ im Zahlköperfall bekannt. Es scheint zum Beispiel unmöglich zu sein, mit Hilfe der bekannten Methoden die Lage der Zerlegungsgruppen der Stellen in S in der Gruppe $\mathrm{G}_{K,S}$ rein gruppentheoretisch zu beschreiben. Wir zeigen, dass dies möglich ist, falls man ein wenig mehr Information als nur die Gruppe $\mathrm{G}_{K,S}$ zur Verfügung hat. Wir werden sehen, dass es equivalent ist, folgende Informationen (zusätzlich zur Gruppe $\mathrm{G}_{K,S}$) zu haben: die Lage der Zerlegungsgruppen von Stellen in S innerhalb der Gruppe $\mathrm{G}_{K,S}$, den p-teil χ_p des zyklotomischen Characters auf $\mathrm{G}_{K,S}$, für eine Primzahl $p \in \mathcal{O}^*_{K,S}$, die Zahlen $\sharp S(L)$, wobei L endliche Untererweiterungen von K_S/K durchläuft, usw. Insbesondere, wenn $\sigma\colon \mathrm{G}_{K_1,S_1} \xrightarrow{\sim} \mathrm{G}_{K_2,S_2}$ ein Isomorphismus ist, für den $\chi_{2,p} \circ \sigma = \chi_{1,p}$ gilt, dann erhält man eine lokale Korrespondenz am Rand, d.h. für Stellen in S_1, S_2.

to my parents

Table of Contents

Introduction

Let K be an algebraic number field[1], i. e. a finite extension of $\mathbb{Q}$. We fix an algebraic closure $\overline{K}$ of K and consider all extensions of K to lie in $\overline{K}$. Let S be a set of primes of K, and assume for simplicity that S contains the set S_∞ of all archimedean primes of K. Let $\mathcal{O}_{K,S}$ be the ring of S-integers of K and $X = \operatorname{Spec} \mathcal{O}_{K,S}$ the corresponding affine scheme. Then the functor sending a finite extension L of K to the normalization of X in $\operatorname{Spec} L$ defines an equivalence of categories between all finite extensions of K, which are unramified outside S and all finite étale connected covers of X. With other words, we have the canonical isomorphism

$$\pi_1(X, \bar{x}) = \mathrm{G}_{K,S},$$

where $\bar{x} = \operatorname{Spec} \overline{K}$ and $\mathrm{G}_{K,S}$ is the Galois group of the maximal extension K_S of K, which is unramified outside S. In this thesis we study various properties of this fundamental group. The work consists of two parts: in the first part (Sections 1,2) we study some anabelian properties of the group $\mathrm{G}_{K,S}$ with S finite. In the second part we introduce a new class of sets of primes of K of positive Dirichlet density, the so called *stable sets* (Section 3) and perform a systematical study of arithmetic (Sections 4, 5) and anabelian (Section 6) properties of the group $\mathrm{G}_{K,S}$ for S lying in this class. These sets generalize in many aspects sets of primes with Dirichlet density 1. Roughly speaking, we aim to generalize the following results, which are known for sets S with Dirichlet density 1 to stable sets:

1. Hasse principles
2. Grunwald-Wang theorem
3. Riemann's existence theorem
4. $\mathrm{cd}_p(\mathrm{G}_{K,S}) = \mathrm{scd}_p(\mathrm{G}_{K,S}) = 2$
5. algebraic $\mathrm{K}(\pi, 1)$-property
6. (a part of) the Neukirch-Uchida theorem

The points 1-5 are closely related with each other. For example, once enough Hasse principles are shown, points 2-4 follow from them in the same way as for sets with density 1. Sections 2 and 6 have much in common, both being of anabelian nature. Section 1, which is devoted to intersections of decomposition groups inside $\mathrm{G}_{K,S}$, can be seen as a technical preparation for them. At first we explain the arithmetic results of Sections 3-5 and postpone the anabelian geometry to the end of this introduction.

The notations in this thesis essentially coincide with the notations in [NSW] and are (at least partially) self-explaining. A list of the most relevant notations can be found after the introduction.

[1] Although we work only with number fields throughout this thesis, many of the statements are also true for global fields in general. Moreover, some of the statements should also be true for arithmetic schemes, i.e., schemes regular, separated and of finite type over $\operatorname{Spec} \mathbb{Z}$.

Hasse principles

A Hasse principle or a local-global principle is a kind of statement which asserts the vanishing of the subgroup of all classes in a global cohomology group, which are locally trivial at a certain collection of closed points. Well-known results in this direction are the classical theorems of Hasse-Minkowski and of Hasse-Brauer-Noether establishing a Hasse principle for quadratic forms and for the Brauer group of global fields respectively.

Let $\mathscr{L}/K$ be a possibly infinite Galois extension and T a set of primes of K. Let $i \geqslant 0$ and let A be a $\mathrm{G}_{\mathscr{L}/K}$-module. We can define the two groups $Ш^i(\mathscr{L}/K, T; A)$ and $\mathrm{coker}^i(\mathscr{L}/K, T; A)$ by exactness of the following sequence

$$0 \to Ш^i(\mathscr{L}/K, T; A) \to \mathrm{H^i}(\mathrm{G}_{\mathscr{L}/\mathrm{K}}, \mathrm{A}) \to \prod\nolimits'_{\mathfrak{p}\in \mathrm{T}} \mathrm{H^i}(\mathscr{L}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}}, \mathrm{A}) \to \mathrm{coker^i}(\mathscr{L}/\mathrm{K}, \mathrm{T}; \mathrm{A}) \to 0,$$

where $\prod'_{\mathfrak{p}\in T}$ means the restricted product with respect to the unramified cohomology groups $\mathrm{H^i_{nr}}(\mathscr{L}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}}, \mathrm{A}) \subseteq \mathrm{H^i}(\mathscr{L}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}}, \mathrm{A})$ and the map in the middle is the product of restriction maps. The **Hasse principle** is said to be satisfied for $\mathscr{L}/K, T, A$ in dimension i if $Ш^i(\mathscr{L}/K, T; A) = 0$. Various situations in which the Hasse principle holds for the extension K_S/K, a set of primes $T \subseteq S$ and a finite $\mathrm{G}_{K,S}$-module A are established in [NSW] chapter IX §1. Here are three representative examples in dimension 1 (similar results in dimension 2 are corollaries of them and Poitou-Tate duality). Let $\delta_K(S)$ denote the Dirichlet density of a set S of primes of K.

Theorem 0.1 ([NSW] 9.1.9, 9.1.15)**.** *Let K be a global field, $T \subseteq S$ sets of primes of K and A a finite $\mathrm{G}_{K,S}$-module. The Hasse principle for $K_S/K, T, A$ in the first dimension holds, i.e.,*

$$Ш^1(K_S/K, T; A) = 0$$

in the following cases:

(i) A is a trivial module and $\delta_K(T) > \frac{1}{p}$, where p is the smallest prime divisor of $\sharp A$.

(ii) $A = \mu_m$ with $m = p_1^{r_1} \dots p_n^{r_n}$, where p_i are pairwise different prime numbers in $\mathbb{N}(S)$, and

$$\delta_K(\mathrm{cs}(K(\mu_{p_i^{r_i}})/K) \cap T) > \frac{1}{p_i[K(\mu_{p_i^{r_i}}) : K]}$$

for all $i = 1, \dots, n$, except, we are in the special case (K, m, T), where $Ш^1(\mathscr{L}/K, T; \mu_m) = \mathbb{Z}/2\mathbb{Z}$.

(iii) A is simple and there is a prime p with $pA = 0$, the minimal extension $K(A)/K$ trivializing A is solvable and $\mathrm{cs}(K(A)/K) \overset{\subseteq}{\sim} T$.

A common assumption in all of them is that the density of T must have some minimal value depending on A, without which nothing can be achieved. The main ingredient in the proofs of all these results is the Chebotarev density theorem. Let us for example prove (i): assume there is some $0 \neq \phi \in Ш^1(K_S/K, T; A)$. Then ϕ can be interpreted as a group homomorphism $\phi\colon \mathrm{G}_{K,S} \to A$ which is trivial on the decomposition groups at all primes in T. Then the extension $L := (K_S)^{\ker(\phi)}/K$ is of degree $[L : K] = \sharp\mathrm{im}(\phi) \geqslant p$ and completely decomposed in T. Hence

$$1 \geqslant \delta_L(T) = [L:K]\delta_K(T \cap \mathrm{cs}(L/K)) = [L:K]\delta_K(T) > p \cdot \frac{1}{p} = 1$$

gives a contradiction, which finishes the proof.

Using various Hasse principles along with Poitou-Tate duality as in [NSW] chapter IX one obtains further facts about the group $\mathrm{G}_{K,S}$, such as Grunwald-Wang theorem, Riemann's existence theorem, a statement about the (strict) cohomological dimension and the algebraic $\mathrm{K}(\pi,1)$-property of $\operatorname{Spec}\mathcal{O}_{K,S}$.

Stable and persistent sets

Now it is time to introduce the main objects of study in this thesis. For simplicity we assume here that all sets we deal with have a Dirichlet density.

Definition 3.7. Let S be a set of primes of K and $\mathscr{L}/K$ any extension.

(i) Let $\lambda > 1$. A finite subextension $\mathscr{L}/L_0/K$ is **λ-stabilizing for S for $\mathscr{L}/K$**, if there exists a subset $S_0 \subseteq S$ and some $a \in (0,1]$, such that $\lambda a > \delta_L(S_0) \geqslant a > 0$ for all finite subextensions $\mathscr{L}/L/L_0$.

(ii) A finite extension $\mathscr{L}/L_0/K$ is **persisting for S for $\mathscr{L}/K$**, if there exists a subset $S_0 \subseteq S$, such that $\delta_L(S_0) = \delta_{L_0}(S_0) > 0$ for all finite subextensions $\mathscr{L}/L/L_0$.

We say that S is **λ-stable** resp. **persistent** for $\mathscr{L}/K$, if it has a λ-stabilizing resp. persisting extension for $\mathscr{L}/K$. We say that S is **stable** for $\mathscr{L}/K$, if it is λ-stable for $\mathscr{L}/K$ for some $\lambda > 1$. Finally, we say that S is **λ-stable** resp. **persistent** if it is λ-stable resp. persistent for K_S/K.

Clearly, persistent implies λ-stable for all $\lambda > 1$. In the applications the stability property is essentially used in three different types of arguments: two times in the proof of the basic Hasse principle (cf. Lemma 4.4, Theorem 4.2 and see also Proposition 4.36) from which all other arithmetic results follow, and once in the anabelian situation (cf. Proposition 6.11). Persistence is not used in these arguments. Nevertheless, the most well-understood examples of stable sets are persistent. But there are also examples of stable sets, for which we can neither prove nor disprove persistence.

Now we show that there are plenty of examples of stable and persistent sets. This is an immediate consequence of the following fact.

Proposition 3.5. *Let M/K be a finite Galois extension, L/K a finite extension and $\sigma \in \mathrm{G}_{M/K}$. Let $L_0 := L \cap M$. Then:*

$$\delta_L(P_{M/K}(\sigma)) = \frac{\sharp C(\sigma; \mathrm{G}_{M/K}) \cap \mathrm{G}_{M/L_0}}{\sharp \mathrm{G}_{M/L_0}}$$

In particular, this value depends only on $L \cap M$, not on L itself. The following corollary is an immediate consequence. For two sets S, T of primes of K, we write $S \backsimeq T$, if S and T differ only in a subset of density zero.

Corollary 3.14. *Let M/K be finite Galois and let $\sigma \in \mathrm{G}_{M/K}$. Let $\mathscr{L}/K$ be any extension and set $L_0 := M \cap \mathscr{L}$. Then a set $S \backsimeq P_{M/K}(\sigma)$ is persisting for $\mathscr{L}/K$ if and only if $C(\sigma; \mathrm{G}_{M/K}) \cap \mathrm{G}_{M/L_0} \neq \varnothing$. If this is the case, L_0 is a persisting field for S for $\mathscr{L}/K$. In particular,*

(i) any set $S \backsimeq \mathrm{cs}(M/K)$ is persistent for any extension $\mathscr{L}/K$,

(ii) any set $S \backsimeq P_{M/K}(\sigma)$ is persistent for any extension $\mathscr{L}/K$ with $\mathscr{L} \cap M = K$.

For example, if M/K is totally ramified in a prime $\mathfrak{p}$ of K, then for any $\sigma \in \mathrm{G}_{M/K}$, the set $S \backsimeq P_{M/K}(\sigma)$ is persistent with persisting field K, provided $\mathfrak{p} \notin S$ (in particular, $P_{M/K}(\sigma)$ itself is).

When one starts to prove arithmetic results, then it is often not enough for S to be stable for K_S/K. One needs the following stronger property, relative to a rational prime $p \leqslant \infty$:

$(*)_p^{\mathrm{stab}}$ $\quad$ S is p-stable for $K_{S \cup S_p \cup S_\infty}/K$ with a stabilizing field contained in K_S

For $p = \infty$, it means that S is stable (i.e., λ-stable with some $\lambda > 1$) for $K_{S \cup S_\infty}/K$ with a stabilizing field contained in K_S (moreover, that a λ-stabilizing field is $\subseteq K_S$ is automatically satisfied for a well-chosen λ; cf. Proposition 3.11). If S satisfies $(*)_p^{\mathrm{stab}}$, then such results as Grunwald-Wang and Riemann's existence theorem *with respect to* p hold for S. Let $E^{\mathrm{stab}}(S)$ denote the set of all rational primes p for which S does not satisfy $(*)_p^{\mathrm{stab}}$. One remarkable fact is the following:

Proposition 3.18. *Let $S \backsimeq P_{M/K}(\sigma)$ for some M/K and $\sigma \in \mathrm{G}_{M/K}$. If $\infty \notin E^{\mathrm{stab}}(S)$, then $E^{\mathrm{stab}}(S)$ is finite.*

From the viewpoint of whether certain arithmetic facts hold, stable sets generalize sets of density 1. But there are also properties of sets of density 1, which stable resp. persistent sets do not share in general (cf. Section 3.5.1). For example, the intersection of two sets of density one again has density one, but the intersection of two persistent sets can be empty. A further difference is that if $\delta_K(S) = 1$, then there are infinitely many rational primes p invertible on $\mathrm{Spec}\, \mathcal{O}_{K,S}$, but one can easily construct persistent sets S such that no rational prime is invertible on $\mathrm{Spec}\, \mathcal{O}_{K,S}$.

Arithmetic of stable sets

Now we turn to the applications of stable sets in the arithmetic context. Let G be a finite group, A a G-module and $i \geqslant 0$. Following Jannsen [Ja], we define the group $\mathrm{H}^{\mathrm{i}}_*(\mathrm{G}, \mathrm{A})$ by exactness of the sequence:

$$0 \to \mathrm{H}^{\mathrm{i}}_*(\mathrm{G}, \mathrm{A}) \to \mathrm{H}^{\mathrm{i}}(\mathrm{G}, \mathrm{A}) \to \prod_{\substack{\mathrm{H} \subseteq \mathrm{G} \\ \text{cyclic}}} \mathrm{H}^{\mathrm{i}}(\mathrm{H}, \mathrm{A}).$$

Then we have the following Hasse principle for stable sets, which is the key result of Section 4.

Theorem 4.2. *Let K be a number field, T a set of primes of K and $\mathscr{L}/K$ a Galois extension with Galois group G. Let A be a finite G-module. Assume that T is p-stable for $\mathscr{L}/K$, where p is the smallest prime divisor of $\sharp A$. Let L be a p-stabilizing field for T for $\mathscr{L}/K$. Write $\Delta := \mathrm{G}_{L(A)/L}$. If $\mathrm{H}^1_*(\Delta, \mathrm{A}) = 0$, then*

$$Ш^1(\mathscr{L}/L, T; A) = 0.$$

Here is an outline of the proof: first one restricts (using p-stability) to the case where A is trivial $\mathrm{G}_{\mathscr{L}/L}$-module. Then one can interpret a non-zero element $0 \neq \phi \in Ш^1(\mathscr{L}/L, T; A)$ as a non-zero homomorphism $\phi\colon \mathrm{G}_{\mathscr{L}/L} \to A$ such that $\ker(\phi)$ contains the decomposition groups of all primes in T. In particular, if $M := \mathscr{L}^{\ker(\phi)}$, then $[M : L] = \sharp\mathrm{im}(\phi) \geqslant p$ and $T \subseteq \mathrm{cs}(M/K)$. This implies

$$\delta_M(T) = [M : L]\delta_L(T \cap \mathrm{cs}(M/L)) \geqslant p\delta_L(T),$$

which is a contradiction to the p-stability property, as M is a subextension of $\mathscr{L}/L$.

In particular, this theorem implies for (p-)stable sets all of the classical Hasse principles holding for sets with Dirichlet density 1 (compare [NSW] chapter IX §1). Using the Hasse principle for μ_n and Poitou-Tate duality, we obtain the following version of the Grunwald-Wang theorem.

Theorem 4.15. *Let K be a number field, S a set of primes of K. Let $T_0, T \subseteq S$ be two disjoint subsets, such that T_0 is finite. Let p be a rational prime and $r > 0$ an integer. Assume $S \setminus T$ is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ with p-stabilizing field L_0, which is contained in K_S. Then for any finite $K_S/L/L_0$, such that we are not in the special case $(L, p^r, S \setminus (T_0 \cup T))$, the canonical map*

$$\mathrm{H}^1(\mathrm{G_{L,S}}, \mathbb{Z}/\mathrm{p^r}\mathbb{Z}) \to \bigoplus_{\mathfrak{p}\in \mathrm{T_0(L)}} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}, \mathbb{Z}/\mathrm{p^r}\mathbb{Z}) \oplus \bigoplus_{\mathfrak{p}\in \mathrm{T(L)}} \mathrm{H}^1(\mathscr{I}_\mathfrak{p}, \mathbb{Z}/\mathrm{p^r}\mathbb{Z})^{\mathscr{G}_\mathfrak{p}}$$

is surjective, where $\mathscr{I}_\mathfrak{p} \subseteq \mathscr{G}_\mathfrak{p} = \mathrm{G}_{K_\mathfrak{p}^{\mathrm{sep}}/L_\mathfrak{p}}$ is the inertia subgroup. If we are in the special case $(L, p^r, S \setminus (T_0 \cup T))$, then $p = 2$ the cokernel of this map is of order 1 or 2.

In particular, if we assume $\delta_K(S) = 1$, $\delta_K(T) = 0$, we obtain [NSW] 9.2.7 as a particular case. Using certain Hasse principles and Grunwald-Wang theorem, one obtains the following form of Riemann's existence theorem for stable sets.

Theorem 4.26. *Let K be a number field, p a rational prime, $T \supseteq S \supseteq R$ sets of primes of K. Assume that R is finite and S is p-stable for $K_{T\cup S_p\cup S_\infty}/K$ and has a p-stabilizing extension contained in $K_S^R(p)$. Then the natural map*

$$\phi_{T,S}^R\colon \mathop{\ast}_{\mathfrak{p}\in R(K_S^R(p))} \mathrm{G}_{K_\mathfrak{p}(p)/K_\mathfrak{p}} * \mathop{\ast}_{\mathfrak{p}\in T\setminus S(K_S^R(p))} I_{K_\mathfrak{p}(p)/K_\mathfrak{p}} \xrightarrow{\sim} \mathrm{G}_{K_T(p)/K_S^R(p)}$$

is an isomorphism, where $I_{K_\mathfrak{p}(p)/K_\mathfrak{p}} = \mathrm{G}_{K_\mathfrak{p}(p)/K_\mathfrak{p}^{\mathrm{nr}}(p)} \subseteq \mathrm{G}_{K_\mathfrak{p}(p)/K_\mathfrak{p}}$ is the inertia subgroup.

When $\delta_K(S) = 1$ we obtain the known version of the theorem.

Finally, there is a statement about the (strict) p-cohomological dimension of $\mathrm{G}_{K,S}$ and $\mathrm{G}_{K,S}(p)$, if S satisfies $(*)_p^{\mathrm{stab}}$ (cf. Corollary 5.15). If K is a p-stabilizing field for S for $K_{S\cup S_p\cup S_\infty}/K$, this statement can be proven directly using all the results above as in [NSW] (cf. Theorem 4.31 and Corollary 4.33). The general case follows from the algebraic $\mathrm{K}(\pi, 1)$-property.

The properties "p-stable" and $(*)_p^{\mathrm{stab}}$ are still too strong for such arithmetic results. For example, let $\mathscr{L}/K$ be a Galois extension, A a trivial p-primary $\mathrm{G}_{\mathscr{L}/K}$-module and T a set of primes of K. Then to obtain the very basic Hasse principle $Ш^1(\mathscr{L}/K, T; A) = 0$, one can require (instead of p-stability of T for $\mathscr{L}/K$ with p-stabilizing field K, as in Theorem 4.2) the weaker condition that there is a subset $T_0 \subseteq T$ with $\delta_*(T_0) > 0$ in the tower $\mathscr{L}/K$ and such that there are no subextensions $\mathscr{L}/L'/L/K$ with $\frac{\delta_{L'}(T_0)}{\delta_L(T_0)} = p$. Thus we can pose the following question.

Question 4.1. What is the most general condition, for which the same results as for p-stable sets resp. sets satisfying $(*)_p^{\mathrm{stab}}$ hold? Are there counterexamples to the Grunwald-Wang theorem or even to the Riemann's existence theorem, among the sets, which do not satisfy this condition?

Concerning this, we conjecture the following two things. Firstly, it is possible to find examples of sets of primes, which do not satisfy $(*)_p^{\mathrm{stab}}$, and for which Grunwald-Wang fails. Secondly, we believe that Riemann's existence theorem still holds for sets of primes, which are only p-stable (or even stable?) and do not satisfy $(*)_p^{\mathrm{stab}}$. Finally, if this last statement would not be true, and one could also find counterexamples to Riemann's existence theorem, this would possibly provide examples of curves $\operatorname{Spec}\mathcal{O}_{K,S}$ which are not $\mathrm{K}(\pi,1)$ for p (cf. Definition 5.2).

$\mathrm{K}(\pi,1)$-property

For the definitions of the (various) $\mathrm{K}(\pi,1)$-properties we refer to Definition 5.2. Let

$$X := \operatorname{Spec}\mathcal{O}_{K,S}$$

with K a number field and S a set of primes of K. The following is well-known:

(i) if $\delta_K(S) = 1$, then X is algebraic $\mathrm{K}(\pi,1)$ and pro-p $\mathrm{K}(\pi,1)$ for each p,

(ii) if $S \supseteq S_p \cup S_\infty$, then X is algebraic $\mathrm{K}(\pi,1)$ for p and pro-p $\mathrm{K}(\pi,1)$

(here we assume that either p is odd K is totally imaginary). Furthermore, there is a powerful recent result of A. Schmidt (cf. [Sch], [Sch2], cf. also [Sch3]) saying the following:

(iii) if $p > 2$ is a prime, S is arbitrary finite and T is a further arbitrary set of primes of K with $\delta_K(T) = 1$, then one can choose a finite subset $T_0 \subseteq T$ such that $X \smallsetminus T_0 = \operatorname{Spec}\mathcal{O}_{K,S\cup T_0}$ is pro-p $\mathrm{K}(\pi,1)$.

We show the algebraic $\mathrm{K}(\pi,1)$-properties for $\operatorname{Spec}\mathcal{O}_{K,S}$ with S stable.

Theorem 5.12. *Let K be a number field, $S \supseteq S_\infty$ a set of primes of K and p a rational prime. Assume that either p is odd or K is totally imaginary.*

(i) Assume that S is p-stable for $K_{S\cup S_p}/K$ and has a p-stabilizing extension contained in $K_S(p)$. Then $\operatorname{Spec}\mathcal{O}_{K,S}$ *is a pro-p* $\mathrm{K}(\pi,1)$.

(ii) Assume that S is stable and satisfies $(*)_p^{\mathrm{stab}}$. Then $\operatorname{Spec}\mathcal{O}_{K,S}$ *is algebraic* $\mathrm{K}(\pi,1)$ *for p.*

In particular, part (ii) of this theorem allows to give explicit examples of schemes $\operatorname{Spec}\mathcal{O}_{K,S}$ which are algebraic $\mathrm{K}(\pi,1)$ *for all* p and such that $\delta_K(S)$ is arbitrary small. The assumption that p is odd or K is totally imaginary is done for convenience.

Further, it is natural to ask, whether in the theorem of Schmidt mentioned above, one can weaken the assumption on T from having density 1 to being p-stable for $K_{S\cup S_p}/K$ and having a p-stabilizing extension contained in $K_S(p)$. We plan to treat this question in a later paper.

Anabelian geometry

Neukirch-Uchida theorem

First we explain the theorem of Neukirch-Uchida (cf. [NSW] chapter XII §2). Let K_1, K_2 be number fields. Choose algebraic closures $\overline{K}_1, \overline{K}_2$ and consider the corresponding absolute Galois groups $\mathrm{G}_{K_1}, \mathrm{G}_{K_2}$. Consider the set

$$\mathrm{Isom}(\mathrm{G}_{K_1}, \mathrm{G}_{K_2})$$

of all (topological) isomorphisms of profinite groups and define

$$\mathrm{OutIsom}(\mathrm{G}_{K_1}, \mathrm{G}_{K_2}) := \mathrm{Isom}(\mathrm{G}_{K_1}, \mathrm{G}_{K_2})/\,\mathrm{G}_{K_2},$$

where the action of G_{K_2} on $\mathrm{Isom}(\mathrm{G}_{K_1}, \mathrm{G}_{K_2})$ is defined by composing with inner automorphisms of G_{K_2}. Now, $\mathrm{OutIsom}(\mathrm{G}_{K_1}, \mathrm{G}_{K_2})$ does not depend on the choice of algebraic closures of K_1, K_2. Then one has a natural map

$$\phi_{K_1,K_2}\colon \mathrm{Isom}(K_2, K_1) \longrightarrow \mathrm{OutIsom}(\mathrm{G}_{K_1}, \mathrm{G}_{K_2}),$$

which is defined as follows: let $\alpha\colon K_2 \to K_1$ be an isomorphism and let $\bar{\alpha}\colon \overline{K_2} \to \overline{K_1}$ be some extension of α to the algebraic closures. Then $g \mapsto \bar{\alpha}^{-1} g \bar{\alpha}$ defines an isomorphism $\mathrm{G}_{K_1} \to \mathrm{G}_{K_2}$. Forgetting the choice of $\bar{\alpha}$ over α corresponds then to the passage from $\mathrm{Isom}(\mathrm{G}_{K_1}, \mathrm{G}_{K_2})$ to $\mathrm{OutIsom}(\mathrm{G}_{K_1}, \mathrm{G}_{K_2})$.

Theorem 0.2 (cf. [Ne], [Ne2], [Uc])**.** *Let K_1, K_2 be number fields. Then ϕ_{K_1,K_2} is bijective.*

This is the theorem of Neukirch-Uchida, which was also independently proven based on results of Neukirch by Ikeda [Ik] and Iwasawa (unpublished). To prove it, one shows first the following intermediate statement.

Claim 0.3. *If K_1 is normal over $\mathbb{Q}$ and $\mathrm{G}_{K_1} \cong \mathrm{G}_{K_2}$, then $K_1 \cong K_2$.*

We give an outline of its proof. First, one establishes the local correspondence. Assume an isomorphism $\sigma\colon \mathrm{G}_{K_1} \xrightarrow{\sim} \mathrm{G}_{K_2}$ is given. Then there is a bijection

$$\sigma_{*,K_1}\colon \Sigma_{K_1,f} \xrightarrow{\sim} \Sigma_{K_2,f}$$

of the sets of all non-archimedean primes of K_1 and of K_2, which respects residue characteristics and absolute degrees of primes and is compatible with taking open subgroups (more on the method of proof of the local correspondence is said below). Let then $P_{\geqslant 1}(K/\mathbb{Q})$ denote the set of primes of $\mathbb{Q}$, having at least one prime of degree 1 in K. From the local correspondence, one obtains the following diagram:

$$\begin{array}{ccc} \mathrm{cs}(K_1/\mathbb{Q}) & = & \mathrm{cs}(K_2/\mathbb{Q}) \\ \| & & \downarrow \\ P_{\geqslant 1}(K_1/\mathbb{Q}) & = & P_{\geqslant 1}(K_2/\mathbb{Q}) \end{array}$$

A posteriori one obtains $\mathrm{cs}(K_2/\mathbb{Q}) = P_{\geqslant 1}(K_2/\mathbb{Q})$, i.e., $K_2/\mathbb{Q}$ is also normal (by Chebotarev density theorem). Finally, by a classical application of Chebotarev density theorem, the equality

$\mathrm{cs}(K_1/\mathbb{Q}) = \mathrm{cs}(K_2/\mathbb{Q})$ implies $K_1 \cong K_2$, as K_1, K_2 are normal over $\mathbb{Q}$. Also the injectivity of ϕ_{K_1,K_2} (for arbitrary K_1, K_2) follows as a corollary from (the proof of) the local correspondence.

There are various extensions and generalizations of Neukirch-Uchida theorem:

- The corresponding result in the function field case was proven by Uchida in [Uc2].
- The result remains true, if one replaces absolute Galois groups by their maximal pro-solvable quotients ([Ne2], [Uc3]).
- The result is still true if one assumes K_1, K_2 to be infinite fields, which are finitely generated over their prime fields. This was done by Pop ([Po1], [Po2], [Po3], cf. also [Sz]).
- The corresponding result for affine curves over finite fields was shown by Tamagawa ([Ta]). Here one considers (instead of K_i) the scheme $X_i = \operatorname{Spec} \mathcal{O}_{K_i,S_i}$, where K_i is a function field in one variable over a finite field and S_i is a *finite* set of primes, and instead of G_{K_i} the étale fundamental group $\pi_1(X_i) = \mathrm{G}_{K_i,S_i}$.

The result of Tamagawa (last one in the above list) for affine curves over finite fields is still out of reach in the number field case: too little is known about the group $\pi_1(\operatorname{Spec} \mathcal{O}_{K,S}) = \mathrm{G}_{K,S\cup S_\infty}$, where K is a number field and S a *finite* set of primes of K. The failure of Tamagawa's proof in the number field case depends mainly on the lack of techniques: there is no everywhere unramified extensions of the field of constants, no geometric fundamental group, etc. Also tools like Grothendieck-Lefschetz trace formula and Weil conjectures are not available.

Neukirch-Uchida for $\operatorname{Spec} \mathcal{O}_{K,S}$ with S stable

Our aim is to generalize Theorem 0.2 to the schemes $\operatorname{Spec} \mathcal{O}_{K,S}$ where K is a number field and S is stable (and so can have arbitrary small positive Dirichlet density). In this thesis, we only generalize Claim 0.3. Further, we believe that the whole theorem can be generalized, at least under an additional technical assumption. To simplify the situation, we consider the following condition:

Dec(K,S) For every $\bar{\mathfrak{p}} \in S_f$, the decomposition group $D_{\bar{\mathfrak{p}}} \subseteq \mathrm{G}_{K,S}$ is the full local group

which is satisfied in several cases (cf. the beginning of Section 6.1), and which is only necessary to simplify the statement of the theorem (cf. Theorem 6.2 in the text for the general case).

Theorem 6.1. *For $i = 1, 2$ let (K_i, S_i) be a number field and a set of primes of K_i, such that Dec(K_i, S_i) holds and*

- *K_1 is normal over $\mathbb{Q}$,*
- *for $i = 1, 2$ the set S_i is stable and satisfies $(*)^{\mathrm{stab}}_{\ell_i}$ for some odd prime ℓ_i,*
- *there are two odd rational primes under S_1 and $S_\infty \subseteq S_1$,*
- *there is a rational prime under S_2.*

If $\mathrm{G}_{K_1,S_1} \cong \mathrm{G}_{K_2,S_2}$, then $K_1 \cong K_2$.

The first step in the proof is the same as in the proof of Neukirch-Uchida: one establishes a local correspondence at the boundary, i.e., out of an isomorphism $\sigma\colon \mathrm{G}_{K_1,S_1} \xrightarrow{\sim} \mathrm{G}_{K_2,S_2}$, one constructs a bijection

$$\sigma_{*,K_1}\colon S_{1,f}(K_1) \xrightarrow{\sim} S_{2,f}(K_2),$$

which respects the residue characteristic and the local degree of primes (and is compatible with taking subgroups). But now the argument finishing the proof above, can not be used anymore: the sets $S_{1,f}(K_1), S_{2,f}(K_2)$ can simply be too small for an application of Chebotarev as above. An additional obstruction is that sets of the form $P_{M/K}(\sigma)$ (which are in many cases stable) do not determine the field M in general, i.e., there are examples of pairs $(M,\sigma) \neq (N,\tau)$ of a finite Galois extension of K together with an element in the Galois group, such that $P_{M/K}(\sigma) \backsimeq P_{N/K}(\tau)$, but $M \neq N$.

At this point one has to find a new argument, showing that $K_1 \cong K_2$ under the assumptions in the theorem. This argument consists of two parts and is the subject of Sections 6.3 and 6.4, preceding the proof of Theorem 6.1. To describe the idea behind this argument, embed the fields K_{1,S_1}, K_{2,S_2} into a fixed algebraic closure of $\mathbb{Q}$. Then using the local correspondence at the boundary and the stability of S_1, one can show the existence of a certain uniform bound $N > 0$ (depending on K_i, S_i), such that if $K_{1,S_1}/M_1/K_1$ is a (not necessary finite) subextension, which is normal over $\mathbb{Q}$ and M_2 is a subextension corresponding to M_1 via the isomorphism $\sigma\colon \mathrm{G}_{K_1,S_1} \xrightarrow{\sim} \mathrm{G}_{K_2,S_2}$, then one has $[M_1 : M_1 \cap M_2] < N$. Using this bound for the extension $M_1 := K_{1,S_p}(p)$, where p can be one of the primes lying under S_1, one can show that $K_1 \subseteq K_2$. Finally, using the fact that there is a rational prime under S_2, one shows $[K_1 : \mathbb{Q}] \geqslant [K_2 : \mathbb{Q}]$, and hence $K_1 = K_2$.

Anabelian properties of $G_{K,S}$ with S finite

We consider first the birational case (the case of S stable is similar) and review briefly the local correspondence, as needed for the proof of Neukirch-Uchida. Let K be a number field, G_K its absolute Galois group. One shows that if $H \subseteq \mathrm{G}_K$ is a closed subgroup with $H \cong \mathrm{G}_\kappa$, where κ is a non-archimedean local field of characteristic zero, then there is a unique prime $\bar{\mathfrak{p}}$ of $\overline{K}$, such that $H \subseteq D_{\bar{\mathfrak{p}},\overline{K}/K}$. In particular, one characterizes the decomposition groups at non-archimedean primes of K purely group-theoretically as the set of all closed subgroups $H \subseteq \mathrm{G}_K$, which are maximal with the following property:

- $H \cong \mathrm{G}_\kappa$, where κ is a non-archimedean local field of characteristic zero

This property is clearly invariant under topological isomorphisms and one obtains the local correspondence as a corollary from this description.

Now, assume S is finite. Then the use of similar techniques leads only to weaker results. In particular, no general Hasse principle for $Ш^2$ (with constant coefficients) is known, and one can not show that a closed subgroup $H \subseteq \mathrm{G}_{K,S}$, such that $H \cong \mathrm{G}_\kappa$ with κ non-archimedean local field of characteristic zero, must be contained in a decomposition group $D_{\bar{\mathfrak{p}},K_S/K}$. But everything one has to do, to obtain such a description, is to give a bit more information. For example, if one has given the group $\mathrm{G}_{K,S}$ *together with the p-part of the cyclotomic character* $\chi_p\colon \mathrm{G}_{K,S} \to \mathbb{Z}_p^*$, where p is such that $S_p \cup S_\infty \subseteq S$, then one can characterize the decomposition subgroups at primes in S_f only in terms of the group theory of $\mathrm{G}_{K,S}$ and χ_p. This is analogous in the

geometric setup to the situation *relative to a field k*: one considers[2] not simply the fundamental group $\pi_1(X)$ of a k-scheme X, but the pair

$$\pi_1(\overline{X}), \quad \mathrm{G}_k \to \mathrm{Out}(\pi_1(\overline{X}))$$

consisting of the geometric fundamental group $\pi_1(\overline{X})$ together with the corresponding outer Galois representation $\mathrm{G}_k \to \mathrm{Out}(\pi_1(\overline{X}))$, or which is equivalent, the fundamental group sequence

$$1 \to \pi_1(\overline{X}) \to \pi_1(X) \to \mathrm{G}_k \to 1$$

of X/k. In particular, if k is finite, then the projection $\pi_1(X) \twoheadrightarrow \mathrm{G}_k$ describes the cyclotomic character. This explains the motivation for the following main result of Section 2. However, the Isom-form of the Anabelian Conjecture for curves over finite fields, proven by Tamagawa, is an *absolute result*. In particular, the outer representation is encoded in the group theory of $\pi_1(X)$.

Theorem 2.5. *Let K be a number field, $S \supseteq S_\infty$ a finite set of primes. Assume at least two rational primes lie in $\mathcal{O}^*_{K,S}$, and p is one of them. Assume $(\mathrm{G}_{K,S}, p)$ are given. The knowledge of one of the following extra structures is equivalent to any other:*

(i) The embeddings $\iota_{\bar{\mathfrak{p}}} \colon D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_{K,S}$ for $\bar{\mathfrak{p}} \in S_f$.

(ii) The cyclotomic p-character $\chi_p \colon U \to \mathbb{Z}_p^*$ on some open $U \subseteq \mathrm{G}_{K,S}$.

(iii) For all open $U \subseteq \mathrm{G}_{K,S}$ with totally imaginary fixed field, the group $\mathrm{Cl_S(U)}$.

(iii)' For all open $U \subseteq \mathrm{G}_{K,S}$ with totally imaginary fixed field, the number $\sharp\mathrm{Cl_S(U)/p}$.

(iv) For all open $U \subseteq \mathrm{G}_{K,S}$, the number $\sharp S(U)$.

Assume $Dec(K,S)$ holds. Then the knowledge of the above is also equivalent to the knowledge of the following:

(ii)' The cyclotomic character on some open subgroup $U \subseteq \mathrm{G}_{K,S}$.

This theorem allows in particular to state a local correspondence at the boundary for an isomorphism $\sigma \colon \mathrm{G}_{K_1,S_1} \xrightarrow{\sim} \mathrm{G}_{K_2,S_2}$, which satisfies $\chi_{1,p} = \chi_{2,p} \circ \sigma$. However, such a correspondence is by no means so powerful as the local correspondences in the birational resp. stable cases are, since S_i is here only a finite set.

Danksagung

Zuallererst gebührt mein tiefster Dank meinem Betreuer, PD Dr. Jakob Stix. Nur seine kontinuierliche Unterstüzung in allen Fragen, sehr viele produktive Gespräche und die zahlreichen Tipps bezüglich der Vorgehensweise in der Arbeit, haben diese Dissertation in der vorliegenden Form möglich gemacht. Auch möchte ich ihm für die Einführung in die anabelsche Geometrie danken.

Ein weiterer großer Dank gebührt Johannes Schmidt, Dr. Jochen Gärtner, Prof. Dr. Kay Wingberg, Dr. Thanasis Bouganis, Dr. Juan Cerviño, Dr. Dimitry Izychev, Dr. Armin

[2] here and later we suppose that a choice of a geometric point of a scheme X was made, and omit this choice in our notation

Holschbach, Dr. Malte Witte, Martin Sigl, Dr. Johannes Bartels, Dr. Peter Barth, Timo Keller und vielen anderen für viele intessante und lehrreiche mathematische Gespräche, und für eine gute Atmosphäre während des Schreibens meiner Arbeit.

Ein spezieller Dank auch an Natalie Zimmer, sowohl für den glücklichen Vorschlag des Begriffes “persistent”, als auch für die vielen Tassen Tee und die gespielten Spiele Scrabble.

Das Dissertationsprojekt an der Fakultät für Mathematik und Informatik der Universität Heidelberg wurde teilweise vom Mathematical Center Heidelberg (MATCH) und dem Mathematischen Institut Heidelberg unterstützt. Vielen Dank für die sehr guten Arbeitsbedingungen.

Nicht zuletzt möchte ich herzlichst meinen Eltern, meiner Schwester Olga Ivanova und Karima Benimmar für die Unterstützung in allen Fragen und Problemen außerhalb der Mathematik danken.

Notation

Our notation will essentially coincide with the notation of [NSW]. There will be some minor differences, explained in the context. Here we collect all important notations, used in this work. First we have the following group-theoretical notations. Let G be a profinite group, $H \subseteq G$ a closed subgroup and p a rational prime.

- G_p denotes a pro-p-Sylow subgroup of G
- $G(p)$ denotes the maximal pro-p-quotient of G
- G^{solv} denotes the maximal solvable quotient of G
- $C(\sigma; G)$ denotes the conjugacy class of an element σ in G
- $N_G(H)$ is the normalizer of H in G.

Assume G is finite.

- $m_H = m_H^G$ denotes the character of the G-representation $\mathrm{Ind}_H^G \mathbf{1}$. It is a ($\mathbb{Z}$-valued) class function on G.

Let L be any field. We have the following Galois-theoretic notations.

- $\mathrm{G}_{M/L}$ is the Galois group of a Galois extension of fields M/L
- $L(p)/L$ is the maximal pro-p-extension of L

Usually we will denote by K a number field, i.e., a finite extension of $\mathbb{Q}$. We fix an algebraic closure $\overline{K}$ of K and consider all extensions of K to be contained in $\overline{K}$. Let S, R be sets of primes of K.

- K_S/K is the maximal extension of K unramified outside S
- $\mathrm{G}_S = \mathrm{G}_{K,S}$ is the Galois group of K_S/K
- $K_S(p)/K$ is the maximal pro-p-extension of K, contained in K_S/K
- $\mathrm{G}_S(p) = \mathrm{G}_{K,S}(p)$ is the Galois group of $K_S(p)/K$
- K_S^R is the maximal extension of K unramified outside S and completely split in R
- $K_S^R(p)$ is the maximal pro-p extension of K, contained in K_S^R
- if L/K is a Galois extension, $\bar{\mathfrak{p}}$ a prime of L, then $D_{\bar{\mathfrak{p}}} = D_{\bar{\mathfrak{p}},L/K} \subseteq \mathrm{G}_{L/K}$ denotes the decomposition group of $\bar{\mathfrak{p}}$. If $\mathfrak{p} = \bar{\mathfrak{p}}|_K$, the choice of $\bar{\mathfrak{p}}$ over $\mathfrak{p}$ is unimportant and no confusion is possible, we also will write $D_{\mathfrak{p}}$ resp. $D_{\mathfrak{p},L/K}$ instead of $D_{\bar{\mathfrak{p}}}$ resp. $D_{\bar{\mathfrak{p}},L/K}$
- $K_{\mathfrak{p}}^{\mathrm{nr}}$ is the maximal unramified extension of the local field $K_{\mathfrak{p}}$ for $\mathfrak{p}$ a prime of K
- $\mathscr{G}_{\mathfrak{p}}$ denotes the absolute Galois group of the local field $K_{\mathfrak{p}}$
- $\mathscr{I}_{\mathfrak{p}} \subset \mathscr{G}_{\mathfrak{p}}$ is the inertia subgroup

Further, we have the following notations concerning sets of primes of K. Let S be a set of primes of K (it can be either finite or infinite and contain non-archimedean primes as well as archimedean).

- $S_p = S_p(K)$ is the set of primes of K lying over a rational prime p
- $\Sigma_K, \Sigma_{K,f}$, $S_\infty = S_\infty(K)$ is the set of all resp. all finite, resp. all archimedean primes of K
- $S_f := S \setminus S_\infty$
- If $S \subseteq \Sigma_K$ and L/K is an algebraic extension, S_L is the preimage of S under the restriction $\Sigma_L \twoheadrightarrow \Sigma_K$. We write sometimes $S(L)$ or, if L is clear from the context, simply S, instead of S_L.
- If M/K is a finite Galois extension and $\sigma \in \mathrm{G}_{M/K}$, we have the Chebotarev set

  $$P_{M/K}(\sigma) = \{\mathfrak{p} \in \Sigma_K : \mathfrak{p} \text{ is unramified in } M/K \text{ and } (\mathfrak{p}, M/K) = C(\sigma; \mathrm{G}_{M/K})\},$$

  where $(\mathfrak{p}, M/K)$ denotes the conjugacy class of Frobenius elements corresponding to primes of M lying over $\mathfrak{p}$.
- For any finite extension L/K we define:

  $$\begin{aligned} P'(L/K) &:= \{\mathfrak{p} \in \Sigma_L : \mathfrak{p} \text{ is unramified and has degree one over } K\} \\ \mathrm{cs}(L/K) &:= \{\mathfrak{p} \in \Sigma_K : \mathfrak{p} \text{ is completely split in } L\} \\ \mathrm{Ram}(L/K) &:= \{\mathfrak{p} \in \Sigma_K : \mathfrak{p} \text{ is ramified in } L/K\ \}, \end{aligned}$$

  in particular, if L^{gal}/K denotes the normal closure of L over K, then $\mathrm{cs}(L/K) = \mathrm{cs}(L^{gal}/K) = P_{L^{gal}/K}(1)$.
- δ_K is the Dirichlet density defined on suitable subsets of Σ_K
- Let T be a further set of primes of K. Then we define

  $$\begin{aligned} S \overset{\subseteq}{\sim} T &:\Leftrightarrow \delta_K(S \setminus T) = 0 \\ S \backsimeq T &:\Leftrightarrow (S \overset{\subseteq}{\sim} T) \text{ and } (T \overset{\subseteq}{\sim} S). \end{aligned}$$

By a local field we usually mean a non-archimedean local field.

Part I

The group G_S with S finite

1 Intersections of decomposition subgroups

1.1 Overview

The goal of the present section is to study the intersections of decomposition subgroups of points inside arithmetic fundamental groups. In the birational case, there is a well-known result by F.K. Schmidt, which we give here together with a corollary:

Theorem 1.1. *([NSW] 12.1.3) Let K be a global field and $\bar{\mathfrak{p}}$, $\bar{\mathfrak{q}}$ two different primes of K^{sep}. Then $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}} = 1$ in G_K.*

This result can be applied to anabelian geometry: in fact, it provides the starting point to Neukirch's proof of a "local correspondence", which is a functorial bijection between primes of two global fields K_1 and K_2, constructed out of a continuous isomorphism of the corresponding absolute Galois groups. Technically speaking, one needs only the following corollary:

Corollary 1.2. *(cf. [NSW] 12.1.4)*

(i) For all open subgroups $H \subseteq D_{\bar{\mathfrak{p}}}$, one has $N_{\mathrm{G}_K}(H) \subseteq D_{\bar{\mathfrak{p}}}$.

(ii) The intersection of two distinct decomposition subgroups is not open in each of them.

Proof of the corollary. (ii) follows from Theorem 1.1. For (i), let $x \in N_{\mathrm{G}_K}(H)$, then $H = xHx^{-1} \subseteq xD_{\bar{\mathfrak{p}}}x^{-1} = D_{x\bar{\mathfrak{p}}}$, hence $H \subseteq D_{x\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{p}}}$ is non-trivial, hence $x\bar{\mathfrak{p}} = \bar{\mathfrak{p}}$, i.e., $x \in D_{\bar{\mathfrak{p}}}$. □

If one changes from the birational setting to the arithmetic one, i.e., consider the group $\mathrm{G}_{K,S} = \pi_1(\operatorname{Spec} \mathcal{O}_{K,S})$, with $S \supseteq S_\infty$ some *finite* set of primes, an analog of Theorem 1.1 is still unknown. But for an application to anabelian geometry (more precise: to obtain at least a *local correspondence at the boundary*, i.e., for primes in S), it is enough to have a corollary as above. It is possible to obtain such a result using only the maximal solvable quotient of $\mathrm{G}_{K,S}$ and some class field theory. This is the content of Section 1.3.

In Section 1.2 we study some easy properties and introduce a shortcut for the notion of non-abelian pro-p Demushkin groups of rank 2. We call them *groups of p-decomposition type*. In Section 1.4 we consider the intersection of decomposition subgroups at primes outside S ("good" primes). We can not give any definite statement about the intersection of $D_{\bar{\mathfrak{p}}}$ and $D_{\bar{\mathfrak{q}}}$ for any $\bar{\mathfrak{p}}$ and $\bar{\mathfrak{q}}$. But if $\bar{\mathfrak{p}}$ is given, there is, under very mild assumptions, a set of primes of Dirichlet density 1, such that if $\bar{\mathfrak{q}}$ is in this set, $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}} \subseteq D_{\bar{\mathfrak{p}}}$ is not open.

1.2 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 non-archimedean 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. To have a shortcut, we define:

Definition 1.3. 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 $\mathbb{Z}_p \ltimes \mathbb{Z}_p$ with $\mathbb{Z}_p \hookrightarrow \mathrm{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^*$ injective (this follows from [NSW] 3.9.9, 3.9.11). We need a description of all closed subgroups of groups of p-decomposition type:

Lemma 1.4. *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. (i) + (ii): Obviously a closed subgroup of H, which is isomorphic to $\mathbb{Z}_p$, can not be open. Assume now, $N \subseteq H$ is a non-trivial closed subgroup, which is not isomorphic to $\mathbb{Z}_p$. We have to show that it is open and of p-decomposition type. Let $H_n \lhd H$ be a normal subgroup of H, such that $H_n \cong H/H_n \cong \mathbb{Z}_p$. If $N \cap H_n$ would be trivial, then N would inject into $H/H_n \cong \mathbb{Z}_p$, which is impossible due to our assumption. Thus $N \cap H_n \subseteq H_n$ is open, and isomorphic to $\mathbb{Z}_p$. Consider the inclusion $N/(N \cap H_n) \hookrightarrow H/H_n \cong \mathbb{Z}_p$. Since $N \neq N \cap H_n$ (otherwise $N = N \cap H_n \cong \mathbb{Z}_p$), $N/(N \cap H_n)$ is a non-trivial, hence open and isomorphic to $\mathbb{Z}_p$, subgroup of H/H_n. We have the following diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N \cap H_n & \longrightarrow & N & \longrightarrow & N/N \cap H_n & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H_n & \longrightarrow & H & \longrightarrow & H/H_n & \longrightarrow & 1, \end{array}$$

which produces the following equation of supernatural numbers:

$$(H : N) = (H/H_n : N/(N \cap H_n))(H_n : N \cap H_n)$$

Since both numbers on the right side are finite, also $(H : N)$ is finite, i.e., N is open in H. Now, $N \cap H_n$ and $N/N \cap H_n$ are both isomorphic to $\mathbb{Z}_p$. In particular, the upper sequence is split. It remains to show that N is not abelian. Otherwise we would have $N \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and $\mathrm{scd}_p(N) = 3$. But $\mathrm{scd}_p(H) = 2$ and $\mathrm{scd}_p(N) \leqslant \mathrm{scd}_p(H)$. This leads to a contradiction.

(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 $H_2 \not\ni H_n$. 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 $1 \neq N/N \cap H_n \hookrightarrow H/H_n$, hence $N/N \cap H_n$ is infinite pro-cyclic. Thus by (iii), $N \cap H_n = N_n$. □

To a group H of p-decomposition type we can associate a character

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

defining the semi-direct product. We use it only in Section 2.8 below.

1.3 Approach by class field theory

Let K be a number field and $S \supseteq S_\infty$ a set of primes. For a profinite group H, let H^{solv} denote the maximal solvable quotient of H.

Arguments in this section make only use of solvable extensions of K, so we work here with the quotient $\mathrm{G}_S^{\mathrm{solv}}$ of G_S. Therefore, let K_S^{solv} denote the corresponding subfield of K_S. If $\bar{\mathfrak{p}}$ is a prime of K_S^{solv}, we write $D_{\bar{\mathfrak{p}}}$ for the decomposition group $D_{\bar{\mathfrak{p}},K_S^{\mathrm{solv}}/K} \subseteq \mathrm{G}_S^{\mathrm{solv}}$. Throughout this section, except Corollary 1.8, $\bar{\mathfrak{p}}, \bar{\mathfrak{q}}$ will denote primes of K_S^{solv}.

1.3.1 Local situation

Let κ be a non-archimedean local field with residue characteristic ℓ and let $\mathscr{G}_\kappa$ be its absolute Galois group. It is well-known that the maximal tame quotient of $\mathscr{G}_\kappa$ is

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

where the action of $\hat{\mathbb{Z}}$ on $\hat{\mathbb{Z}}^{(\ell')}$ is given by sending the Frobenius element to multiplication by $\sharp\bar{\kappa}$, the cardinality of the residue field. For $p \neq \ell$, the p-Sylow subgroups of $\mathscr{G}_\kappa^{\mathrm{tr}}$ are of p-decomposition type. Consider now a p-Sylow subgroup $\mathscr{G}_{\kappa,p} \subseteq \mathscr{G}_\kappa$. Since $p \neq \ell$, the composition

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

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

1.3.2 Metabelian covers

Lemma 1.5. *Assume $S_p \cup S_\infty \subseteq S$. Let $\bar{\mathfrak{p}} \in (S_f \smallsetminus S_p)(K_S^{\mathrm{solv}})$ 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*

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

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 $\mathscr{I}_{\mathfrak{p},p}$. We show $\ker(\phi) = 1$, i.e., that for any $n > 0$, there is a solvable (moreover, this extension is metabelian) extension of K, which is unramified outside S and whose ramification degree at $\mathfrak{p}$ is p^n (in fact, if then $U_n \subseteq \mathrm{G}_S^{\mathrm{solv}}$ is the corresponding subgroup, then $(\phi|_{\mathscr{I}_{\mathfrak{p},p}})^{-1}(U_n) = p^n\mathscr{I}_{\mathfrak{p},p} \subseteq \mathscr{I}_{\mathfrak{p},p}$, and we get $\ker(\phi) \subseteq \bigcap_n U_n = 1$).

Therefore, let L_0/K be the Hilbert class field of K and set $L := L_0K(\zeta_{p^n})$. 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, one has

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

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. Finally, since L/K and $L(\epsilon^{1/p^n})/L$ are abelian (the second is Galois, since $\mu_{p^n} \subset L$), the successive extension $L(\epsilon^{1/p^n})/L/K$ is metabelian and hence solvable. □

Proposition 1.6. *Let $\bar{\mathfrak{p}} \neq \bar{\mathfrak{q}} \in S_f(K_S^{\mathrm{solv}})$, such that there is a rational prime $p \in \mathcal{O}^*_{K_S^{\mathrm{solv}}, S \smallsetminus \{\bar{\mathfrak{p}}, \bar{\mathfrak{q}}\}}$. 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 1.5, $D_{\bar{\mathfrak{p}},p}$ 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 the Lemma 1.5 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 1.4(ii)). Hence, again by Lemma 1.4(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 1.4(iv) applied to the 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 $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}} \subseteq D_{\bar{\mathfrak{p}}}$ would be 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 also be open in $D_{\bar{\mathfrak{p}},p}$, which contradicts the already proven part of the proposition. □

From this we obtain the following analog of Corollary 1.2 for $\mathrm{G}_S^{\mathrm{solv}}$:

Corollary 1.7.

(i) If $p \in \mathcal{O}^*_{K,S}, \bar{\mathfrak{p}} \in (S_f \smallsetminus S_p)(K_S^{\mathrm{solv}})$ and $H \subseteq D_{\bar{\mathfrak{p}}}$ 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 $N_{\mathrm{G}_S^{\mathrm{solv}}}(H) \subseteq D_{\bar{\mathfrak{p}}}$.

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

Proof. (i): Let $x \in N_{\mathrm{G}_S^{\mathrm{solv}}}(H)$. 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 1.6 implies $x\bar{\mathfrak{p}} = \bar{\mathfrak{p}}$, or equivalently, $x \in D_{\bar{\mathfrak{p}}}$.

(ii): This follows directly from Proposition 1.6, since the condition posed there is automatically satisfied. □

Now consider the whole group G_S. All arguments from above (in particular the lemma and the proposition) also apply, if one replaces $\mathrm{G}_S^{\mathrm{solv}}$ by G_S. Thus we get (in the following $D_{\bar{\mathfrak{p}}} \subseteq \mathrm{G}_S$ means again a decomposition group inside G_S):

Corollary 1.8.

(i) If $p \in \mathcal{O}_{K,S}^*, \bar{\mathfrak{p}} \in (S_f \smallsetminus S_p)(K_S)$ and $H \subseteq D_{\bar{\mathfrak{p}}}$ 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 $N_{\mathrm{G}_S}(H) \subseteq D_{\bar{\mathfrak{p}}}$.

(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 each of them.

Proof. (i) is done as above. (ii): By Proposition 1.6, 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. But by [CC] Theorem 5.1 both groups $D_{\bar{\mathfrak{p}}}$ and $D_{\bar{\mathfrak{q}}}$ are the full local absolute Galois groups, hence also the open subgroup $D_{\bar{\mathfrak{p}}} \cap D_{\bar{\mathfrak{q}}}$ of $D_{\bar{\mathfrak{p}}}$ is. 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. □

1.4 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 $M = K_S^{\mathrm{ab},p}$ denote the corresponding subfield of K_S. For short, we write $D_{\mathfrak{p}}$ for $D_{\mathfrak{p},M/K}$. We consider the intersections of decomposition subgroups at primes outside S. Observe first, that if $\bar{\mathfrak{p}} \in \Sigma_M \smallsetminus S$, 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 (in the following δ_K denotes the Dirichlet density on K). Let $D_{\mathfrak{p},p} \subseteq D_{\mathfrak{p}}$ denote the p-Sylow subgroup.

Proposition 1.9. *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 $\bar{\mathfrak{p}} \in \Sigma_M \smallsetminus S$ 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 each of them.

Proof. Since K is not totally real, the number of complex embeddings of K is $r_2(K) \geqslant 1$ and hence $\mathrm{rk}_{\mathbb{Z}_p} \mathrm{G}_S^{\mathrm{ab,p}} \geqslant 2$ by [NSW] 10.3.20. Let $H \cong \mathbb{Z}_p^2$ be some quotient of $\mathrm{G}_S^{\mathrm{ab},p}$, such that $\mathfrak{p}$ is not completely split in L, the subfield of M corresponding to H (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 density theorem for infinite extensions, the set of primes $T_{\mathfrak{p}}$ of K, lying outside S, whose Frobenius lies in $H \smallsetminus N$ has density 1. Then $T_{\mathfrak{p}}$ satisfies the requirements of the proposition. □

2 Anabelian properties of G_S with S finite

In this section we study which properties of the field K and the set S of primes of K can be reconstructed from the group G_S, if with S finite. Essentially, we find pieces of information, such that the knowledge of each of them, together with the knowledge of the profinite group G_S, determine the other ones.

2.1 Overview

Let K be a number field, $S \supseteq S_\infty$ a set of primes of K. We want to study, which invariants of K can be reconstructed from the group G_S. In Section 2.2 we recall briefly, what can be done in the local case. Then, in Section 2.3, we recover, under the assumption of Leopoldt's conjecture for K and all primes, the degree of $K/\mathbb{Q}$, the number of real and complex embeddings, and the set $\mathbb{Z} \cap \mathcal{O}_{K,S}^*$ of integers invertible in $\mathcal{O}_{K,S}$, if this set is contains at least one rational prime. In Sections 2.4-2.9, we want to study, how the decomposition subgroups at primes in S lie in G_S. Roughly speaking, it turns out that it is equivalent to know one of the following data: the embeddings $(D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_S)_{\bar{\mathfrak{p}} \in S_f}$; 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 L. For the precise result, see Theorem 2.5. Of all these quantities, the numbers $\sharp S(L)$ seem to be the most accessible ones. In Section 2.10 we show how one can reconstruct them from the group G_S, assuming the finiteness of certain Shafarevich groups. The proof of Theorem 2.5 is easier, if one assumes the following condition:

$Dec(K,S)$ For every $\bar{\mathfrak{p}} \in S_f$, the decomposition group $D_{\bar{\mathfrak{p}}} \subseteq \mathrm{G}_S$ is the full local group

on K and S, and requires some additional work in the general case. Further, in the Section 2.11 we show an idea, how one can use the Dedekind zeta function to obtain some information on the location in G_S of the decomposition groups of points of $\operatorname{Spec} \mathcal{O}_{K,S}$ (that is, primes of K lying outside S). Throughout this section we use the following notation:

- n_K, r_1, r_2 degree, the number of real resp. complex embeddings of $K/\mathbb{Q}$,
- $\chi_p \colon \mathrm{G}_S \to \mathbb{Z}_p^*$ the cyclotomic p-character for $p \in \mathcal{O}_{K,S}^*$.

We write $\mathrm{Cl_S(U)}, \sharp\mathrm{S(U)}$, etc. instead of $\mathrm{Cl_S(L)}, \sharp\mathrm{S(L)}$, etc., if $U \subseteq \mathrm{G}_S$ is an open subgroup with $L = (K_S)^U$. We will sometimes assume that there are at least two rational primes $p_1, p_2 \in \mathcal{O}_{K,S}^*$, i.e., that $S_{p_1} \cup S_{p_2} \subseteq S$. This assumption implies by [CC] Theorem 5.1, that the decomposition groups in G_S of primes in $S_{p_1} \cup S_{p_2}$ are the full local groups. 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. [CC] Remark 5.3(i)).

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

2.2 Warm-up: local invariants

In this subsection we recall the anabelian properties of local fields, i.e., which invariants of a local field κ can be recovered from its absolute Galois group G_κ. This material is also covered by [NSW]. A good survey can be found in [SchS]. Local fields are not anabelian (cf. [NSW] Remark before 12.2.7). This means that one can construct two different local fields $\kappa \ncong \kappa'$ with

isomorphic absolute Galois groups: $\mathrm{G}_\kappa \cong \mathrm{G}_{\kappa'}$. Nevertheless, the following data can be recovered from G_κ:

- the characteristic $\operatorname{char}\kappa$
- the characteristic $\operatorname{char}\bar{\kappa}$ of the residue field $\bar{\kappa}$ of κ
- the cardinality $\sharp\bar{\kappa}$ of $\bar{\kappa}$
- the absolute degree $[\kappa : \mathbb{Q}_p]$, if $\operatorname{char}(\kappa) = 0$, $\operatorname{char}(\bar{\kappa}) = p$
- 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. Let us write

$$h_p^i(\mathrm{G}_\kappa) := \dim_{\mathbb{F}_p} \mathrm{H}^{\mathrm{i}}(\mathrm{G}_\kappa, \mathbb{Z}/\mathrm{p}\mathbb{Z}).$$

We have the following standard computations, where $\delta = 1$ if $\mu_p \subset \kappa$ and $\delta = 0$ otherwise:

$$h_p^i(\mathrm{G}_\kappa) = \begin{cases} 1+\delta & \text{if } i = 1, \operatorname{char}(\bar{\kappa}) \neq p, \\ 1+\delta+[\kappa:\mathbb{Q}_p] & \text{if } i = 1, \operatorname{char}(\bar{\kappa}) = p \text{ and } \operatorname{char}(\kappa) = 0, \\ \infty & \text{if } i = 1, \operatorname{char}(\kappa) = p, \\ \delta & \text{if } i = 2. \end{cases}$$

Hence the characteristic of κ equals 0, if $h_p^1(\mathrm{G}_\kappa) < \infty$ for all p and equals p, if $h_p^1(\mathrm{G}_\kappa) = \infty$ (this p is then necessarily unique). The residue characteristic of κ is the unique prime p, such that the set $\{h_p^1(U) : U \subseteq \mathrm{G}_\kappa \text{ open}\}$ is unbounded. We denote it by p in what follows. Further, the norm residue symbol defines an exact sequence:

$$0 \to \kappa^* \to \mathrm{G}_\kappa^{\mathrm{ab}} \to \hat{\mathbb{Z}}/\mathbb{Z} \to 1. \tag{2.1}$$

Let (p') denote the prime-to-p completion. Since $\hat{\mathbb{Z}}/\mathbb{Z}$ is uniquely divisible, we have

$$\bar{\kappa}^* \cong \mu(\kappa)^{(p')} = (\kappa^*)_{\mathrm{tor}}^{(p')} = (\mathrm{G}_\kappa^{\mathrm{ab}})_{\mathrm{tor}}^{(p')},$$

i.e., $\sharp\bar{\kappa} = \sharp(\mathrm{G}_\kappa^{\mathrm{ab}})_{\mathrm{tor}}^{(p')} + 1$. If κ is p-adic, we obtain the absolute degree as the negative of the Euler characteristic of $\mathbb{Z}/p\mathbb{Z}$: $\chi(\mathrm{G}_\kappa, \mathbb{Z}/p\mathbb{Z}) = -[\kappa : \mathbb{Q}_p]$. The above argument also determines the cardinality of the residue field of any finite separable extension of κ, corresponding to an open subgroup $U \subseteq \mathrm{G}_\kappa$. Let us write $q_U := (U^{\mathrm{ab}})_{\mathrm{tor}}^{(p')} + 1$. We obtain the inertia subgroup as

$$I_\kappa = \bigcap_U U,$$

where the intersection is taken over all $U \subseteq \mathrm{G}_\kappa$ open with $q_{\mathrm{G}_\kappa}^{(\mathrm{G}_\kappa:U)} = q_U$, and the wild inertia subgroup V_κ as *the* p-Sylow subgroup of I_κ. Now it is a well-known fact, that as $\mathrm{G}_\kappa/I_\kappa$-modules, we have $I_\kappa/V_\kappa \cong \hat{\mathbb{Z}}^{(p')}(1)$, where 1 denotes the first Tate twist. Thus by injectivity of the cyclotomic character, $\mathrm{Frob}_\kappa \in \mathrm{G}_\kappa/I_\kappa$ is the unique element acting on I_κ/V_κ via multiplication with q_{G_κ}. Finally, the sequence (2.1) determines κ^* as the preimage of the discrete subgroup generated by Frob_κ under the projection $\mathrm{G}_\kappa^{\mathrm{ab}} \twoheadrightarrow \mathrm{G}_\kappa/I_\kappa = \mathrm{G}_{\bar{\kappa}}$. Since the same can be done for any finite Galois extension of κ in a functorial and G_κ-equivariant way, this also determines the G_κ-module $(\kappa^{\mathrm{sep}})^*$. In particular, this gives also the action of G_κ on its torsion $\mu(\kappa^{\mathrm{sep}}) = (\kappa^{\mathrm{sep}})^*_{\mathrm{tor}}$. This determines the cyclotomic character on G_κ.

Further we have a nice lemma, proven by Neukirch (cf. [NSW] proof of 12.1.9).

Lemma 2.1. *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. Since L is p-adic, we have $\mathrm{cd}_\ell(\mathrm{G}_L) = 2$ for all primes ℓ, and therefore $\mathrm{cd}_\ell(\mathrm{G}_M) \geqslant \mathrm{cd}_\ell(\mathrm{G}_L) = 2$ for all ℓ by [NSW] 3.3.5. Hence by [NSW] 6.1.3, $\mathrm{char}\, M = 0$. Since $\mathrm{G}_M \supseteq \mathrm{G}_L$ contains pro-p-subgroups of any finite rank, M is p-adic. Further, for any prime ℓ, we have $\ell^\infty \nmid [\mathrm{G}_M\colon \mathrm{G}_L]$. In fact, if this would not be the case, Lemma 2.2 would imply $2 = \mathrm{cd}_\ell(\mathrm{G}_L) < \mathrm{cd}_\ell(\mathrm{G}_M) = 2$, a contradiction.

Assume $\mathrm{G}_L \subseteq \mathrm{G}_M$ is not open. Let $\mathrm{G}_L \subset U \subseteq \mathrm{G}_M$ be open in G_M, with $p \nmid (U : \mathrm{G}_L)$ (since $p^\infty \nmid (\mathrm{G}_M : \mathrm{G}_L)$, there is a $U_0 \subseteq \mathrm{G}_M$ open, such that this holds for all $\mathrm{G}_L \subseteq U \subseteq U_0$). Then the restriction $\mathrm{H}^1(\mathrm{U}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \to \mathrm{H}^1(\mathrm{G_L}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$ is injective. But as the second group is finite and the order of the first tends to infinity with $(\mathrm{G}_M : U)$, this leads to a contradiction. Thus $\mathrm{G}_L \subseteq \mathrm{G}_M$ is open.

Finally, let M'/M be the finite extension corresponding to the subgroup $\mathrm{G}_L \subseteq \mathrm{G}_M$. Then

$$[M\colon \mathbb{Q}_p] \leqslant [M'\colon \mathbb{Q}_p] = -\chi(\mathrm{G}_L, \mathbb{Z}/p\mathbb{Z}) = [L\colon \mathbb{Q}_p]. \qquad \square$$

Lemma 2.2. *(cf. Exercise 3 in [NSW] III §7) Let G be a Poincaré group at p and $H \subseteq G$ a closed subgroup. Assume that $p^\infty | (G : H)$. Then $\mathrm{cd}_p H < \mathrm{cd}_p G$.*

Proof. Let $n := \mathrm{cd}_p G$ and let I be the dualizing module of G. To show that $\mathrm{cd}_p H < n$, it is enough to show that for any finite H-module A with $pA = 0$ one has $\mathrm{H^n(H, A)} = 0$. Let A be such a module. There is an open subgroup $H \subset U_0 \subseteq G$, such that A lifts to a U_0-module. Then

$$\begin{aligned}
\mathrm{H^n(H, A)} &= \mathrm{H^n}(\varprojlim_{\mathrm{H}\subset\mathrm{U}\subseteq\mathrm{U_0}} \mathrm{U, A}) \\
&= \varinjlim_{H\subset U\subseteq U_0,\mathrm{res}} \mathrm{H^n(U, A)} \\
&= \varinjlim_{H\subset U\subseteq U_0,\mathrm{res}} \mathrm{H^n(G, Ind_U^G\, A)} \\
&= \varinjlim_{H\subset U\subseteq U_0,\mathrm{cor}^\vee} \mathrm{H^0(G, Hom(Ind_U^G\, A, I))}^\vee \\
&= \varinjlim_{H\subset U\subseteq U_0,\mathrm{cor}^\vee} \mathrm{H^0(U, Hom(A, I))}^\vee
\end{aligned}$$

the second to last equality being true, since res is dual to cor with respect to the duality pairing.

Now I is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as an abelian group, hence $\mathrm{Hom}(A, I)$ is still finite. Thus it is enough to show that if M is a finite U_0-module killed by p, then

$$\varinjlim_{H \subset U \subseteq U_0, \mathrm{cor}^\vee} M^U = 0.$$

Since M is finite, we can choose an open $H \subset U_1 \subseteq U$, such that $M^U = M^H$ for all $H \subset U \subseteq U_1$. But by our assumption, for any $H \subseteq U \subseteq U_1$, there is a $H \subseteq V \subseteq U$ with $p|(U : V)$. Then

$$\mathrm{cor}_V^U = N_{U/V} \colon M^V \to M^U \qquad \alpha \mapsto \sum_{g \in U/V} g\alpha$$

is the zero map, since $M^V = M^U$ and in particular $\sum_{g \in U/V} g\alpha = (U : V)\alpha = 0$. Thus also $(\mathrm{cor}_V^U)^\vee$ is the zero map and the claim follows.

□

2.3 Recovering some global invariants under Leopoldt

Proposition 2.3. *Let S be a finite set of primes of K. Assume the Leopoldt conjecture is true for K and for all rational primes. Assume $S_p \cup S_\infty \subseteq S$ for at least one rational prime p. Then G_S determines the set $\mathbb{N}(S) := \mathbb{Z} \cap \mathcal{O}_{K,S}^*$, the degree n of $K/\mathbb{Q}$ and the numbers r_1, r_2 of real resp. complex embeddings of K.*

Proof. First we show that G_S determines the number $r_2 = r_2(K)$ of complex embeddings of K and the set $\mathbb{N}(S)$. For any rational prime p consider the number $r(p) := \mathrm{rk}_{\mathbb{Z}_\mathrm{p}} \mathrm{G}_\mathrm{S}^{\mathrm{ab,p}}$. 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

$$r(p) = \mathrm{rk}_{\mathbb{Z}_\mathrm{p}} \mathrm{G}_\mathrm{S}^{\mathrm{ab,p}} < \mathrm{rk}_{\mathbb{Z}_\mathrm{p}} \mathrm{G}_{\mathrm{S} \cup \mathrm{S}_\mathrm{p}}^{\mathrm{ab,p}} = \mathrm{r}_2 + 1.$$

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 n and r_1 from G_S. Once n is known, r_1 can be recovered as $n - 2r_2$. To recover n, observe that if K is totally imaginary, $n = 2r_2$ can be recovered together with r_2. We find an open subgroup $U \subseteq \mathrm{G}_S$ such that $(K_S)^U$ is totally imaginary. Take a prime $p \in \mathbb{N}(S)$. Let $\pi : \mathrm{G}_S \twoheadrightarrow \mathrm{G}_S^{\mathrm{ab}}$ be the natural projection, and set

$$U := \pi^{-1}(\mathrm{im}([(p-1)p] \colon \mathrm{G}_S^{\mathrm{ab}} \to \mathrm{G}_S^{\mathrm{ab}}))$$

(we take $(p-1)p$ only to cover the case $p = 2$: for all other primes $(p-1)$ would be enough). Then U is open in G_S. Indeed, by class field theory ([NSW] 8.3.21(ii)), the group $\mathrm{G}_S^{\mathrm{ab}}$ is topologically finitely generated, thus the cokernel of the multiplication with $(p-1)p$ on it is finite, and hence $\mathrm{im}(\mathrm{G}_S^{\mathrm{ab}} \xrightarrow{(p-1)p} \mathrm{G}_S^{\mathrm{ab}}) \subseteq \mathrm{G}_S^{\mathrm{ab}}$ is open.

Let L be the subfield of K_S fixed by U. Then L contains every abelian subextension of K_S/K of degree dividing $(p-1)p$. In particular, L contains the p^2-roots of unity, since they are contained in K_S. Hence L is totally imaginary and $[L : \mathbb{Q}] = 2r_2(L)$ can be recovered as above.

Therefore

$$n = [K : \mathbb{Q}] = \frac{[L : \mathbb{Q}]}{(\mathrm{G}_S : U)}$$

can also be recovered from G_S. □

Remark 2.4. Observe that once a prime $p \in \mathbb{Z} \cap \mathcal{O}_{K,S}^*$ is known, one obtains $r_2(K)$ as the negative of the Euler characteristic $-\chi(\mathrm{G}_S, \mathbb{Z}/p\mathbb{Z})$ ([NSW], 8.7.5) and $n(K), r_1(K)$ as in the proof, without assuming Leopoldt.

2.4 The result

Assume the group G_S is given. Then it seems not to be possible in a direct way, still assuming $Dec(K, S)$ (cf. Section 2.1), to extract out of G_S the decomposition subgroups of the primes in S_f. The Brauer group argument of Neukirch (cf. [NSW] 12.1.9) fails because of the S-class group obstruction to the Hasse principle. But with some extra pieces of information, the decomposition subgroups at S_f can be recovered. Moreover, it turns out to be equivalent to give certain extra pieces of information in addition to the profinite group G_S. This is the content of the following theorem.

Theorem 2.5. *Let K be a number field, $S \supseteq S_\infty$ a finite set of primes. Assume 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, the group $\mathrm{Cl_S(U)}$.

(iii)' For all open $U \subseteq \mathrm{G}_S$ with totally imaginary fixed field, the number $\sharp\mathrm{Cl_S(U)/p}$.

(iv) For all open $U \subseteq \mathrm{G}_S$, the number $\sharp S(U)$.

Assume $Dec(K, S)$ holds. Then the knowledge of the above is also equivalent to the knowledge of the following:

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

We will prove Theorem 2.5 in the following sections. The plan is as follows: in Section 2.5 we prove some technical lemmas. In Sections 2.6, 2.7 we prove the theorem under the condition $Dec(K, S)$. In Section 2.8 we give the argument needed in the general case. During the proof of the theorem we will use the notations (x) $\rightsquigarrow$ (y) resp. (x) $\leftrightsquigarrow$ (y) for (x),(y) being from the theorem. They 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.

Remarks 2.6.

(a) By Remark 2.4, the datum (G_S, p) with $p \in \mathcal{O}_{K,S}^*$ determines the numbers $n_K, r_1(K), r_2(K)$.

(b) In the arithmetic situation, to give G_S together with the cyclotomic character, corresponds in the geometric situation over a finite field, in some sense, to give the fundamental group of a curve together with the attached outer Galois representation.

(c) 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 1.8(ii)) the whole projective system of continuous G_S-sets $\varprojlim_{U \subseteq U_0, U \lhd \mathrm{G}_S} S_f(U)$ is determined, 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.

(d) It seems to be impossible to obtain the numbers $\sharp S_f(U)$ from the cohomology of G_S and its subgroups with finite constant coefficients. In fact, let $p \in \mathbb{N}(S)$, and assume for simplicity that $\mu_p \subset K$ and K is totally imaginary if $p = 2$. Then for any $U \subseteq \mathrm{G}_S$ open with corresponding field L, we have the exact sequence:

$$0 \to \mathrm{Cl_S(L)/p} \to \mathrm{H}^2(\mathrm{G_S}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \to \bigoplus_{\mathfrak{p} \in \mathrm{S(L)}} \mathrm{Br(L_\mathfrak{p})[p]} \to \mathbb{Z}/\mathrm{p}\mathbb{Z} \to 0,$$

from which one can obtain only the sum $\dim_{\mathbb{F}_p} \mathrm{Cl_S(L)/p} + \sharp \mathrm{S_f(L)}$. Each of both terms alone (determined for every U) would give enough information to reconstruct the decomposition subgroups.

(e) Of all extra pieces of information in the theorem, the numbers $\sharp S(U)$ seem to be the most accessible ones. In Section 2.10 we give an approach how to reconstruct the numbers $\sharp S_f(U)$ for all $U \subseteq U_0 \subseteq \mathrm{G}_S$ with U_0 small enough, under certain finiteness assumption. Then remark (c) above allows to reconstruct the numbers $\sharp S_f(U)$ for all $U \subseteq \mathrm{G}_S$ open, and the numbers $\sharp S_\infty(U)$ are determined by (G_S, p) by remark (a).

(f) One needs two rational primes in $\mathcal{O}^*_{K,S}$ in the theorem to separate the decomposition groups inside G_S by Corollary 1.8.

As a corollary we get the following local correspondence at S-primes.

Corollary 2.7 (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 $\chi_{2,p} \circ \sigma = \chi_{1,p}$ 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 $Dec(K_1, S_1)$ holds, σ_{U_1} preserves the residue characteristic and the absolute degree 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 $\chi\colon U_i \to \mathbb{Z}_p^*$, the group $Ш^1(U_i, \mathbb{Q}_p/\mathbb{Z}_p(\chi))$ is finite, then the condition $\chi_{2,p} \circ \sigma = \chi_{1,p}$ is automatically satisfied.

Proof. Everything except the last statement follows from the theorem. The last statement follows from Remark 2.6(c) above and Proposition 2.21 below. □

From now on, and until the end of Section 2.9, we permanently assume that at least two rational primes lie in $\mathcal{O}^*_{K,S}$, and that p denotes one of them.

2.5 Some lemmas

As in [NSW] 12.1.10, we have the following lemma.

Lemma 2.8. *Let $H \subseteq \mathrm{G}_S$ be a closed subgroup, which is isomorphic to the absolute Galois group of a local field of characteristic 0. Assume that there is an open subgroup H_0 of H with $H_0 \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}} \in S$. Then $H \subseteq D_{\bar{\mathfrak{p}}}$.*

Proof. Taking the intersection over all H-conjugates of H_0, we can assume H_0 to be normal in H. Now, H_0 being an open subgroup of a local absolute Galois group in characteristic 0, is itself one. By Lemma 2.1, H_0 is thus an open subgroup of $D_{\bar{\mathfrak{p}}}$. Let now $x \in H$. Then x normalizes H_0. By Corollary 1.8(i), $x \in D_{\bar{\mathfrak{p}}}$. □

Unfortunately, Lemma 2.8 with its easy proof can not be applied to the general case, in which the condition $Dec(K, S)$ is not assumed to be true. We need a more precise treatment.

Lemma 2.9. *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 1.4, 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 the full local groups. Hence by Lemma 2.11, $\bar{\mathfrak{p}} \notin S_p$. 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, hence the inclusion is open by Lemma 1.4. Since H normalizes H_0, Corollary 1.8(i) implies now, that $H \subseteq D_{\bar{\mathfrak{p}}}$. □

Finally, we have to answer the following question: let $H \subseteq \mathrm{G}_S$ be a subgroup of p-decomposition type and let $D_{\bar{\mathfrak{p}}} \subseteq \mathrm{G}_S$ be the decomposition group of a prime $\bar{\mathfrak{p}} \in S_p$ (which is the full local group). Can it happen that $H \subseteq D_{\bar{\mathfrak{p}}}$? The answer is negative and given in Lemma 2.11 below.

Lemma 2.10. *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. [De] or [An] 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 Lemma 2.2 implies that $\mathrm{cd}_p H_m < \mathrm{cd}_p H_n$, which is absurd, since both numbers are equal to 2. □

Lemma 2.11. *Let p be a rational prime. Let G_κ be the absolute Galois group of a local field, $H \subset \mathrm{G}_\kappa$ a subgroup of p-decomposition type. Then κ is not p-adic.*

Proof. Suppose κ is p-adic. For an open subgroup U of G_κ, let $U^{(p)}$ denote the maximal pro-p-quotient of U. First of all, we claim that one can choose $H \subset U \subseteq \mathrm{G}_\kappa$ 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 [NSW] 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 1.4, 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 $cd_p(H) = 2$, nor a Demushkin group of rank > 2: this contradicts Lemma 2.10. All together, we get a contradiction, which proves the lemma. □

2.6 Cyclotomic character and the decomposition subgroups

Here we prove the equivalences (i) $\leftsquigarrow$ (ii) $\leftsquigarrow$ (ii)' of Theorem 2.5 under the condition $Dec(K, S)$. The direction (ii)' $\rightsquigarrow$ (ii) is trivial.

Proof of (i) $\rightsquigarrow$ (ii)'. Assume the $(\iota_{\bar{\mathfrak{p}}} \colon D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_S)_{\bar{\mathfrak{p}} \in S_f}$ are given. Since we want to determine the cyclotomic character only on an open subgroup of G_S, we can assume that K is totally imaginary, i.e., the decomposition subgroups of archimedean primes are trivial. The cyclotomic character on $D_{\bar{\mathfrak{p}}}$ is uniquely determined by the full local group $D_{\bar{\mathfrak{p}}}$ (cf. Section 2.2). We have the following exact sequence from class field theory:

$$0 \to \overline{\mathcal{O}^*_{K,S}} \to \prod_{\mathfrak{p} \in S(K)} D^{\mathrm{ab}}_{\bar{\mathfrak{p}}} \to \mathrm{G}^{\mathrm{ab}}_S \to \mathrm{Cl_S(K)} \to 0. \tag{2.2}$$

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

Finally, (ii) $\rightsquigarrow$ (i) follows from the next proposition, which characterizes, which subgroups are the decomposition subgroups of primes in S_f, once the group G_S together with the cyclotomic p-character $\chi_p \colon U \to \mathbb{Z}_p^*$ on an open $U \subseteq \mathrm{G}_S$ is given. We prove it, using a modified argument of Neukirch (cf. [NSW] 12.1.9).

Proposition 2.12. *Let $H \subseteq \mathrm{G}_S$ be a closed subgroup, isomorphic to an absolute Galois group G_κ of a local field κ of characteristic 0. The following are equivalent:*

(a) There is a prime $\bar{\mathfrak{p}} \in S_f$, such that $H \subseteq D_{\bar{\mathfrak{p}}}$.

(b) There is an open subgroup $H_0 \subseteq H$ such that $\chi_p|_{H_0}$ is the p-cyclotomic character on H_0 coming from G_κ.

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

Lemma 2.13. *Assume the following are given:*

- *a filtered category I*
- *for each $i \in I$, a set S_i*
- *for each $i \to j$ in I, a map $\lambda_{ij}\colon S_j \to S_i$ with finite fibres*
- *for each $\mathfrak{p} \in S_i$, an abelian group $A_\mathfrak{p}$*
- *for each pair $\mathfrak{p} \in S_i, \mathfrak{q} \in S_j$, such that $i \to j$ and $\lambda_{ij}(\mathfrak{q}) = \mathfrak{p}$, a homomorphism $m_{\mathfrak{p},\mathfrak{q}}\colon A_\mathfrak{p} \to A_\mathfrak{q}$,*

such that the collection of maps $(\lambda_{ij})_{i,j}$ and $(m_{\mathfrak{p},\mathfrak{q}})_{\mathfrak{p},\mathfrak{q}}$ are compatible in the obvious way. Then the natural homomorphism

$$\phi\colon \varinjlim_{i\in I}\Big(\bigoplus_{\mathfrak{p}\in S_i} A_\mathfrak{p}\Big) \to \prod_{P\in\varprojlim_I S_i}\Big(\varinjlim_{P=(\mathfrak{p}_i)} A_{\mathfrak{p}_i}\Big)$$

is injective.

Proof of Lemma 2.13. For each $i \in I$ and $P = (\mathfrak{p}_j)_{j\in I} \in \varprojlim_I S_i$, there are natural homomorphisms

$$\bigoplus_{\mathfrak{p}\in S_i} A_\mathfrak{p} \to A_{\mathfrak{p}_i} \to \varinjlim_P A_{\mathfrak{p}_j},$$

which induce for each P the homomorphism $\varinjlim_I \bigoplus_{\mathfrak{p}\in S_i} A_\mathfrak{p} \to \varinjlim_P A_{\mathfrak{p}_j}$, which in turn induce ϕ. We have to show injectivity. Let $\alpha \in \varinjlim_{i\in I}(\bigoplus_{\mathfrak{p}\in S_i} A_\mathfrak{p})$ with $\phi(\alpha) = 0$. There is an i, such that α comes from an element $(\alpha_\mathfrak{p})_{\mathfrak{p}\in S_i} \in \bigoplus_{\mathfrak{p}\in S_i} A_\mathfrak{p}$ defined at the level i. As $\alpha_\mathfrak{p} = 0$ for almost all $\mathfrak{p} \in S_i$, we can assume that $\alpha_\mathfrak{p} = 0$ unless $\mathfrak{p} = \mathfrak{p}_0$, where $\mathfrak{p}_0 \in S_i$ is arbitrary. We have to show that there is some $j \in I$ with $i \to j$ such that the image of $(\alpha_\mathfrak{p})_{\mathfrak{p}\in S_i}$ in $\bigoplus_{\mathfrak{p}\in S_j} A_\mathfrak{p}$ vanishes. Assume that there is no such j. For each $i \to j$ define then the set

$$T_j(\mathfrak{p}_0) := \{\mathfrak{p} \in \lambda_{ij}^{-1}(\mathfrak{p}_0)\colon m_{\mathfrak{p}_0,\mathfrak{p}}(\alpha_{\mathfrak{p}_0}) \neq 0\} \subseteq \lambda_{ij}^{-1}(\mathfrak{p}_0) \subseteq S_j,$$

which is finite since $\lambda_{ij}^{-1}(\mathfrak{p}_0)$ is finite and non-empty by our assumption. Then the inverse limit set $\varprojlim_I T_j(\mathfrak{p}_0)$ is non-empty, and thus contains an element P. For this P, the image of $\alpha_{\mathfrak{p}_0}$ in $\varinjlim_{P=(\mathfrak{p}_j)} A_{\mathfrak{p}_j}$ is non-zero by construction, which is a contradiction to the assumption $\phi(\alpha) = 0$. □

Proof of Proposition 2.12. The uniqueness in (a) follows from Lemma 2.1 and Corollary 1.8(ii).

(a) ⇒ (b): Assume $H \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}} \in S_f$. By Lemma 2.1, H is open in $D_{\bar{\mathfrak{p}}}$. There are two cyclotomic characters on H: the one is the cyclotomic character of G_κ, and the other is the restriction of the one on $D_{\bar{\mathfrak{p}}}$. By the discussion in Section 2.2, they must coincide. This proves (b).

(b) $\Rightarrow$ (a): By Lemma 2.8 we can assume that K is totally imaginary. Again by Lemma 2.8 it is enough to show that $H_0 \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}} \in S_f$. Let κ' be the extension of κ corresponding to $H_0 \subseteq \mathrm{G}_\kappa$. For $0 < m \leqslant n$ consider the following commutative exact diagram of G_S-modules (where $\mathcal{O}_S^* := \mathcal{O}_{K_S,S}^*$):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_{p^m} & \longrightarrow & \mathcal{O}_S^* & \xrightarrow{p^m} & \mathcal{O}_S^* & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{=} & & \downarrow{p^{n-m}} & & \\ 0 & \longrightarrow & \mu_{p^n} & \longrightarrow & \mathcal{O}_S^* & \xrightarrow{p^n} & \mathcal{O}_S^* & \longrightarrow & 0. \end{array}$$

Taking the long exact cohomology sequence gives:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{H}^1(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*)/\mathrm{p^m} & \longrightarrow & \mathrm{H}^2(\mathrm{G_S}, \mu_{\mathrm{p^m}}) & \longrightarrow & {}_{p^m}\mathrm{H}^2(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*) & \longrightarrow & 0 \\ & & \downarrow{p^{n-m}} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{H}^1(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*)/\mathrm{p^n} & \longrightarrow & \mathrm{H}^2(\mathrm{G_S}, \mu_{\mathrm{p^n}}) & \longrightarrow & {}_{p^n}\mathrm{H}^2(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*) & \longrightarrow & 0. \end{array}$$

Now ${}_{p^m}\mathrm{H}^2(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*)$ is the p^m-torsion of the Brauer group, and it embeds into the direct sum of the p^m-torsion of the local Brauer groups at S. Hence the above diagram produces the following, which again has exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{H}^1(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*)/\mathrm{p^m} & \longrightarrow & \mathrm{H}^2(\mathrm{G_S}, \mu_{\mathrm{p^m}}) & \longrightarrow & \bigoplus_{\mathfrak{p} \in S(K)} {}_{p^m}\mathrm{H}^2(\mathrm{D}_\mathfrak{p}, \mu_{\mathrm{p^m}}) \\ & & \downarrow{p^{n-m}} & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{H}^1(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*)/\mathrm{p^n} & \longrightarrow & \mathrm{H}^2(\mathrm{G_S}, \mu_{\mathrm{p^n}}) & \longrightarrow & \bigoplus_{\mathfrak{p} \in S(K)} {}_{p^n}\mathrm{H}^2(\mathrm{D}_\mathfrak{p}, \mu_{\mathrm{p^n}}). \end{array}$$

We pass to the direct limit over all n. Since $\mathrm{H}^1(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*) = \mathrm{Cl_S(K)}$ is finite, we have

$$\varinjlim_n \mathrm{H}^1(\mathrm{G_S}, \mathcal{O}_\mathrm{S}^*)/\mathrm{p^n} = \mathrm{Cl_S(K)} \otimes \mathbb{Q}_\mathrm{p}/\mathbb{Z}_\mathrm{p} = 0.$$

Thus we obtain the injection

$$0 \to \mathrm{H}^2(\mathrm{G_S}, \mu_{\mathrm{p}^\infty}) \to \bigoplus_{\mathfrak{p} \in \mathrm{S(K)}} \mathrm{H}^2(\mathrm{D}_\mathfrak{p}, \mu_{\mathrm{p}^\infty}),$$

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 by Lemma 2.13 we obtain:

$$0 \to \mathrm{H}^2(\mathrm{H_0}, \mu_{\mathrm{p}^\infty}) \to \prod_{\mathfrak{p} \in \mathrm{S(M)}} \mathrm{H}^2(\mathrm{D}_{\mathfrak{p}, \mathrm{K_S/M}}, \mu_{\mathrm{p}^\infty}). \tag{2.3}$$

By (b), $\chi_p|_{H_0}$ is the cyclotomic character on H_0 coming from $\mathrm{G}_{\kappa'}$. Thus $\mathrm{H}^2(\mathrm{H_0}, \mu_{\mathrm{p}^\infty}) = \mathbb{Q}_\mathrm{p}/\mathbb{Z}_\mathrm{p}$. From sequence (2.3), there is a prime $\bar{\mathfrak{p}} \in S_f$ with $\mathrm{H}^2(\mathrm{D}_{\bar{\mathfrak{p}}, \mathrm{K_S/M}}, \mu_{\mathrm{p}^\infty}) \neq 0$. As $\mathrm{H}^2(\mathrm{D}_{\bar{\mathfrak{p}}, \mathrm{K_S/M}}, \mu_\mathrm{p})$ maps surjectively onto the p-torsion of $\mathrm{H}^2(\mathrm{D}_{\bar{\mathfrak{p}}, \mathrm{K_S/M}}, \mu_{\mathrm{p}^\infty})$, we obtain $\mathrm{H}^2(\mathrm{D}_{\bar{\mathfrak{p}}, \mathrm{K_S/M}}, \mu_\mathrm{p}) \neq 0$. Now, we can finish the argument as in the original paper of Neukirch. In fact, we show 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 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

$$\mathrm{H}^2(\mathrm{U},\mu_{\mathrm{p}}) \to \bigoplus_{\mathfrak{q}\in \mathrm{T}_{\mathfrak{p},\mathrm{H}'}(\mathrm{U})} \mathrm{H}^2(\mathrm{D}_{\mathfrak{q},\mathrm{K_S/L}},\mu_{\mathrm{p}}) \to 0,$$

which is exact by [NSW] 9.2.1, 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:

$$\mathrm{H}^2(\mathrm{H}',\mu_{\mathrm{p}}) \to \bigoplus_{\mathfrak{p}'\in \mathrm{S}_{\mathfrak{p}}(\mathrm{M}')} \mathrm{H}^2(\mathrm{D}_{\mathfrak{p}',\mathrm{K_S/M}'},\mu_{\mathrm{p}}) \to 0. \tag{2.4}$$

Again, since χ_p is the p-cyclotomic character on $H_0 \cong \mathrm{G}_{\kappa'}$, we have $\mathrm{H}^2(\mathrm{H}',\mu_{\mathrm{p}}) \cong \mathbb{Z}/\mathrm{p}\mathbb{Z}$. Further, $\mathrm{H}^2(\mathrm{D}_{\mathfrak{p}',\mathrm{K_S/M}'},\mu_{\mathrm{p}}) \neq 0$. In fact, $D_{\mathfrak{p}',K_S/M'}$ is conjugate to an open subgroup of $D_{\mathfrak{p},K_S/M}$. But since $\mathrm{H}^2(\mathrm{D}_{\bar{\mathfrak{p}},\mathrm{K_S/M}},\mu_{\mathrm{p}}) \neq 0$, also $\mathrm{H}^2(\mathrm{V},\mu_{\mathrm{p}}) \neq 0$ for any open subgroup $V \subseteq D_{\bar{\mathfrak{p}},K_S/M}$ (this follows from [NSW] 7.1.8 (i),(ii)). Finally, since (2.4) is exact, there is only one prime lying over $\mathfrak{p}$ in any finite extension M'/M. Hence $\bar{\mathfrak{p}}|_M$ is indecomposed. □

Corollary 2.14. *Assume $Dec(K,S)$ is satisfied. A closed subgroup $H \subseteq \mathrm{G}_S$ is a decomposition subgroup of a prime in S_f if and only if H is maximal with the following two properties:*

- *H is isomorphic to an absolute Galois group G_κ of a local field κ of characteristic 0.*
- *The restriction of the p-part of the cyclotomic character of G_S to H is equal to the p-part of the cyclotomic character on an open subgroup $H_0 \subseteq H$, coming from G_κ.*

2.7 Class group obstruction and the decomposition subgroups

Here we proof (i) $\leftsquigarrow$ (iii) $\leftsquigarrow$ (iii)' $\leftsquigarrow$ (iv) of Theorem 2.5, assuming $Dec(K,S)$. The direction (iii) $\rightsquigarrow$ (iii)' is trivial.

Proof of (i) $\rightsquigarrow$ (iii). Assume the $(\iota_{\bar{\mathfrak{p}}}\colon D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_S)_{\bar{\mathfrak{p}}\in S_f}$ 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. By class field theory, we obtain the following exact sequence:

$$\prod_{\mathfrak{p}\in S(U)} D_{\mathfrak{p},L}^{\mathrm{ab}} \to U^{\mathrm{ab}} \to \mathrm{Cl_S(U)} \to 0.$$

Thus the group $\mathrm{Cl_S(U)}$ is equal to 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) $\rightsquigarrow$ (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 known by the Remark 2.6 (a). □

Lemma 2.15. *Assume $\mu_p \subset K$ (and $\mu_4 \subset K$ if $p = 2$) in the theorem. Then (iii)' $\leftsquigarrow$ (iv).*

Proof. Since $\mu_p \subseteq K$, we have for every U the exact sequence

$$0 \to \mathrm{Cl_S(U)/p} \to \mathrm{H^2(U, \mathbb{Z}/p\mathbb{Z})} \to {}_{\mathrm{p}}\mathrm{H^2(U, \mathcal{O}_S^*)} \to 0, \text{ and}$$

$$\dim_{\mathbb{F}_p} {}_p\mathrm{H^2(U, \mathcal{O}_S^*)} = \sharp\mathrm{S_f(U)} - 1,$$

since K is totally imaginary. Thus $\dim_{\mathbb{F}_p} \mathrm{H^2(U, \mathbb{Z}/p\mathbb{Z})} + 1 = \dim_{\mathbb{F}_p} \mathrm{Cl_S(U)/p} + \sharp\mathrm{S_f(U)}$. 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. □

It remains to prove (iii)' $\rightsquigarrow$ (i) and (iv) $\rightsquigarrow$ (i). Since the knowledge of (i) for G_S is by Lemma 2.8 equivalent to the knowledge of (i) for any open $U \subseteq \mathrm{G}_S$, we can assume $\mu_p \subset K$ (and $\mu_4 \subseteq K$, if $p = 2$), i.e., by Lemma 2.15, it is enough to prove that (iv) $\rightsquigarrow$ (i).

Proof of (iv) $\rightsquigarrow$ (i). We can assume $\mu_p \subset K$ (and $\mu_4 \subseteq K$, if $p = 2$). 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 $S(V) = (U : V)S(U)$. 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

$$V_0 := \bigcap_{V \subseteq U} V,$$

where the intersection is taken over all normal open subgroups $V \subseteq U$, such that

$$S(V) = (U : V)S(U)$$

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 $U^{\mathrm{ab}} \to V^{\mathrm{ab}}$.

Proposition 2.16. *Let $H \subseteq \mathrm{G}_S$ be a closed subgroup, isomorphic to an absolute Galois group G_κ of a local field κ of characteristic zero. Assume that $\mu_p \subset \kappa, K$ (or $\mu_4 \subseteq \kappa, K$ if $p = 2$). The following are equivalent:*

(a) $H \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}} \in S_f$.

(b) For H the following condition holds:

$(*)_{p,H}$ For any $U \subseteq \mathrm{G}_S$ open: $H \subseteq U \Rightarrow H \subseteq \ker(\pi_{p,U} \colon U \twoheadrightarrow \mathrm{Cl_S(U)/p})$.

In (a) the prime $\bar{\mathfrak{p}}$ is unique.

Proof. The uniqueness of $\bar{\mathfrak{p}}$ follows from Lemma 2.1 and Corollary 1.8(ii).

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

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

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., $(*)_{p,H}$ holds.

(b) $\Rightarrow$ (a): Assume now $(*)_{p,H}$ holds. For any $U \supseteq H$ open in G_S with corresponding field L, we have $\mu_p \subset L$, and hence $Ш^2(U, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Cl_S(U)/p}$. This gives us the exact sequence:

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

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

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

whose exactness follows from Lemma 2.13. 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 principle ideal theorem (cf. e.g. [Ko] Theorem 8.11; the argument is essentially the same as in the proof of the Hauptidealsatz), 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 $(*)_{p,H}$. Thus $\varinjlim_{H \subseteq U \subseteq \mathrm{G}_S} \mathrm{Cl_S(U)/p} = 0$. Now the proof of (b) $\Rightarrow$ (a) can be finished just as in [NSW] 12.1.9 or in Proposition 2.12. $\square$

Finally, (iv) $\rightsquigarrow$ (i) follows from the Corollary 1.8(i) and the proposition. $\square$

2.8 The general case

In this subsection we prove Theorem 2.5 without the additional assumption $Dec(K, S)$. Recall that in Section 1.2 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

Proposition 2.17. *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) The condition $(*)_{p,H}$ (cf. Proposition 2.16) holds for H.

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 1.4(ii), the last inclusions are open. Proposition 1.6 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): exactly in the same way as in Proposition 2.12, one finds that (b) implies $H_0 \subseteq D_{\bar{\mathfrak{p}}}$ for some $\bar{\mathfrak{p}} \in S_f$. Then Lemma 2.9 implies $H \subseteq D_{\bar{\mathfrak{p}}}$. Since H is of p-decomposition type and the groups $D_{\bar{\mathfrak{q}}}$ with $\bar{\mathfrak{q}} \in S_p$ are the full local groups, Lemma 2.11 implies $\bar{\mathfrak{p}} \notin S_p$.

(a) $\Leftrightarrow$ (c): has the same proof as in Proposition 2.16, except that now we have to argue additionally that $\bar{\mathfrak{p}} \notin S_p$. This is done as in the proof of (b) $\Rightarrow$ (a).

□

Now we prove Theorem 2.5. (i) $\rightsquigarrow$ (iii) $\rightsquigarrow$ (iii)' and (i) $\rightsquigarrow$ (iv) work as before.

Proof of (i) $\rightsquigarrow$ (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 full local group in this case (cf. Section 2.2). 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 (Section 1.3.1); 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 $D_{\bar{\mathfrak{p}}}$. By the same argument as in Section 2.6 (using the exact sequence (2.2)), χ_p is thus determined on an open subgroup of G_S. □

Proof of (ii) $\rightsquigarrow$ (i), (iii)' $\rightsquigarrow$ (i), (iv) $\rightsquigarrow$ (i). Assume (ii), (iii)' or (iv) is given. As we know that the decomposition subgroups of primes over p are the full local groups and as the full local group determines the residue characteristic, Propositions 2.12 resp. 2.16 imply that we can reconstruct them from the given data.

Let $U \subseteq \mathrm{G}_S$ 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 2.17, applied to U, using Corollary 1.8(i) if necessary, we can decide, using the given information, 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 1.5 and Lemma 2.9, 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):

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

which sends H to the (unique by Proposition 1.6!) prime $\bar{\mathfrak{p}}|_L$, 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

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

which is surjective, being equal to the composition

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

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

Lemma 2.18. *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:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Ш^2(U, \mathbb{Z}/p\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(\mathrm{U}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & \longrightarrow & \left(\bigoplus_{\mathfrak{q}\in S(L)} \mathrm{H}^2(\mathrm{D}_{\mathfrak{q},\mathrm{K_S/L}}, \mathbb{Z}/\mathrm{p}\mathbb{Z})\right)^{\Sigma=0} & \longrightarrow & 0 \\ & & & & & \searrow^{\mathrm{res}^U_H} & \downarrow & & \\ & & & & & & \mathrm{H}^2(\mathrm{H}, \mathbb{Z}/\mathrm{p}\mathbb{Z}), & & \end{array}$$

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 $\left(\bigoplus_{\mathfrak{q}\in S(L)\smallsetminus\{\mathfrak{p}\}} \mathrm{H}^2(\mathrm{D}_{\mathfrak{q},\mathrm{K_S/L}}, \mathbb{Z}/\mathrm{p}\mathbb{Z})\right)^{\Sigma=0}$ of the space on the right side by $Ш^2(U, \mathbb{Z}/p\mathbb{Z})$. Two such subspaces of $\mathrm{H}^2(\mathrm{U}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$ corresponding to $\mathfrak{p}$ resp. $\mathfrak{p}'$ are equal if and only if $\mathfrak{p} = \mathfrak{p}'$. This finishes the proof. □

Remark 2.19. The necessity can also be seen in the following way. If $\mathfrak{p} = \psi(H) = \psi(H')$, then H and H' lie in U-conjugate decomposition subgroups $D_{\bar{\mathfrak{p}},K_S/L}$ resp. $D_{\bar{\mathfrak{p}}',K_S/L}$. Say $g\bar{\mathfrak{p}} = \bar{\mathfrak{p}}'$ with $g \in U$ and let c_g denote the isomorphisms induced by conjugation. Then we have the commutative diagram:

$$\begin{array}{ccccc} \mathrm{H}^2(\mathrm{U}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(\mathrm{D}_{\bar{\mathfrak{p}},\mathrm{K_S/L}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & \xrightarrow{\sim} & \mathrm{H}^2(\mathrm{H}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \\ \downarrow{\scriptstyle c_g} & & \downarrow{\scriptstyle c_g} & & \\ \mathrm{H}^2(\mathrm{U}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & \longrightarrow & \mathrm{H}^2(\mathrm{D}_{\bar{\mathfrak{p}}',\mathrm{K_S/L}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & \xrightarrow{\sim} & \mathrm{H}^2(\mathrm{H}', \mathbb{Z}/\mathrm{p}\mathbb{Z}) \end{array}$$

Now, the left vertical arrow is the identity, since $g \in U$, and the second is an isomorphism, hence the kernels of the (compositions of) horizontal maps are equal.

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 fibre 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 1.6.

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 an 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 2.5. □

2.9 Further invariants

Assume (G_S, p) and the equivalent data from Theorem 2.5 are given. We investigate, which further information can be recovered from this.

Proposition 2.20. *Assume* $Dec(K, S)$ *holds. Assume the datum* $(\mathrm{G}_S, (D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_S))_{\bar{\mathfrak{p}} \in S_f}$ *are given. 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 inertia and ramification degrees* $f_{\mathfrak{p}, L/K}$ *and* $e_{\mathfrak{p}, L/K}$ *of any* $\mathfrak{p} \in S_f$.

(v) The set $\mathbb{N}(S) := \mathbb{Z} \cap \mathcal{O}^*_{K,S}$.

(vi) The degree $[K : \mathbb{Q}]$.

Proof. (i) + (ii): If K is totally imaginary, one obtains the group $\mathrm{G}_\varnothing = \mathrm{G}_{K_\varnothing/K}$, dividing 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 map in the class field theory.

(iii) follows from (i) $\rightsquigarrow$ (ii)$'$ in Theorem 2.5.

(iv) follows from the discussion in Section 2.2.

(v) + (vi) : 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. Further, $\ell \in \mathbb{N}(S) \Leftrightarrow n(\ell)$ is maximal. If $\ell \in \mathbb{N}(S)$, then $[K : \mathbb{Q}] = n(\ell)$. □

2.10 The numbers $S_f(U)$

Here we present an approach, how the numbers $S_f(U)$ can be reconstructed under a certain finiteness assumption. Recall that we do not assume anymore that two primes lie in $\mathcal{O}_{K,S}^*$.

Proposition 2.21. *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 $\mathrm{H}^2(\mathrm{G_S}, \mathbb{Q}_\mathrm{p}/\mathbb{Z}_\mathrm{p}(\chi))$ is of finite corank and*

$$\sharp S_f(K) = 1 + \max_\chi \mathrm{corank}(\mathrm{H}^2(\mathrm{G_S}, \mathbb{Q}_\mathrm{p}/\mathbb{Z}_\mathrm{p}(\chi))). \tag{2.5}$$

Proof. 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 $\mathrm{G}_S^{\mathrm{ab}}$. By class field theory we have the exact sequence:

$$\prod_{\mathfrak{p} \in S(K)} D_{\mathfrak{p},K}^{\mathrm{ab}} \to \mathrm{G}_S^{\mathrm{ab}} \to \mathrm{Cl_S(K)} \to 0.$$

Thus on the one side, $\chi^{-1} \otimes \chi_p$ factors through a map $\mathrm{Cl_S(K)} \to \mathbb{Z}_\mathrm{p}^*$, 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:

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

where

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

(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 $\mathbb{Z}_p$, i.e., $\chi = \chi_p$). 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. We have the 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, $\chi|_{D_{\bar{\mathfrak{p}}}} \neq \chi_p|_{D_{\bar{\mathfrak{p}}}}$ for at least one $\bar{\mathfrak{p}} \in S_f$. By Lemma 2.22, 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 2.22. *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) $\mathrm{H}^2(\mathrm{G}_\kappa, \mathbb{Q}_\mathrm{p}/\mathbb{Z}_\mathrm{p}(\chi)) \neq 0$.

(ii) χ is the p-part of the cyclotomic character.

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

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

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

2.11 Appendix. Zeta function and primes of small norm

2.11.1 Zeta function and a formula of Landau

For a number field K let $\mathrm{N} := \mathrm{N}_{\mathrm{K}/\mathbb{Q}}$ be the norm of $K/\mathbb{Q}$. For any $s \in \mathbb{C}$ with $\Re(s) > 1$, let

$$\zeta_K(s) = \prod_{\mathfrak{p} \in \Sigma_{K,f}} \frac{1}{1 - \mathrm{N}\mathfrak{p}^{-\mathrm{s}}}.$$

be the Dedekind zeta-function of K. The series defining it converges for any s with $\Re(s) > 1$, and $\zeta_K(s)$ has a meromorphic continuation to the whole complex plain with a unique pole at $s = 1$. We have the following equality for all s with $\Re(s) > 1$:

$$Z_K(s) := -\frac{\zeta_K'(s)}{\zeta_K(s)} = \sum_{\mathfrak{p} \in \Sigma_{K,f}} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^\mathrm{s} - 1},$$

This is (up to a sign) the logarithmic derivative of $\zeta_K(s)$. Set

$$A(K) := \pi^{-r_1(K)/2}(2\pi)^{-r_2(K)}|D_K|^{1/2},$$

where D_K denotes the discriminant of K. There is a fractional decomposition of $Z_K(s)$:

Proposition 2.23 ([La] Satz 179)**.**

$$Z_K(s) = \log A(K) + \frac{r_1(K)}{2}\frac{\Gamma'}{\Gamma}(s/2) + r_2(K)\frac{\Gamma'}{\Gamma}(s) + (\frac{1}{s} + \frac{1}{s-1}) - \sum_\rho{}' \frac{1}{s - \rho},$$

where $\sum_\rho'$ means the sum over the non-trivial zeros of ζ_K and the terms for ρ, $\bar{\rho}$ are summed

together (otherwise the sum must not converge). In particular, if $r_1(K) = 0$, then we have

$$Z_K(s) = \frac{1}{2}\log|D_K| + \frac{n_K}{2}\log(2\pi) + \frac{n_K}{2}\frac{\Gamma'}{\Gamma}(s) + (\frac{1}{s} + \frac{1}{s-1}) - \sum_\rho{}' \frac{1}{s-\rho}. \tag{2.6}$$

We are only interested in totally complex fields, so the second formula is enough for us.

2.11.2 Naive criterion

Let an (infinite) Galois extension $\mathscr{L}$ of K be given. The proposition below describes a relationship between a certain limes involving the Dedekind zeta functions of finite subfields of $\mathscr{L}/K$, and the presence of primes of K of finite norm and finite ramification in $\mathscr{L}$. In this context it makes sense to index extensions of K by their degree. Thus, in particular, we work with an ascending tower $K = L_1 \subsetneq \cdots \subsetneq L_n \subsetneq \ldots$ of extensions of K, denoted $(L_n)_n$, and indexed such that $[L_n : K] = n$, i.e., the index set is an infinite ascending subset of the natural numbers.

Proposition 2.24. *Let $K = L_1 \subsetneq \cdots \subsetneq L_n \subsetneq \cdots \subsetneq \mathscr{L} = \bigcup_n L_n$ be a tower of finite Galois extensions of K, enumerated in the way, such that $[L_n : K] = n$. For any real $s > 1$ the limit*

$$\lambda_{\mathscr{L}}(s) := \lim_{n\to\infty} n^{-1} Z_{L_n}(s)$$

exists. For any $\mathfrak{p} \in \Sigma_{K,f}$, let $f_\mathfrak{p}, e_\mathfrak{p}$ denote the inertia degree resp. the ramification index of $\mathfrak{p}$ in $\mathscr{L}$. Then

$$\lambda_{\mathscr{L}}(s) = \sum_{\substack{\mathfrak{p}\in\Sigma_{K,f} \\ e_\mathfrak{p}, f_\mathfrak{p} < \infty}} \frac{1}{e_\mathfrak{p}} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{\mathrm{f}_\mathfrak{p}\mathrm{s}} - 1}, \tag{2.7}$$

where the sum on the right is absolutely convergent. In particular, $\lambda_{\mathscr{L}}(s)$ depends only on $\mathscr{L}$ and on s, not on the L_n's.

Proof. Fix an $s > 1$. First we show the existence of the limit. For a finite extension L/K, of degree d and a prime $\mathfrak{p} \in \Sigma_{K,f}$ set:

$$B_{L,\mathfrak{p}} = d^{-1} \sum_{\mathfrak{q}\in\Sigma_L^f, \mathfrak{q}|\mathfrak{p}} \frac{\log(N\mathfrak{q})}{N\mathfrak{q}^s - 1}.$$

Then we have: $d^{-1}Z_L(s) = \sum_{\mathfrak{p}\in\Sigma_{K,f}} B_{L,\mathfrak{p}}$, where the series converges absolutely. Assume that L/K is Galois. If r is the number of primes of L, lying over $\mathfrak{p}$, and if each of them has inertia degree f and ramification index e, we have $d = rfe$. Therefore:

$$B_{L,\mathfrak{p}} = d^{-1} \sum_{\mathfrak{q}\in\Sigma_L^f, \mathfrak{q}|\mathfrak{p}} \frac{\log(\mathrm{N}\mathfrak{q})}{N\mathfrak{q}_i^s - 1} = \frac{r}{d}\frac{f\log(N\mathfrak{p})}{N\mathfrak{p}^{fs} - 1} = \frac{1}{e}\frac{\log(N\mathfrak{p})}{N\mathfrak{p}^{fs} - 1} \leqslant \frac{\log(N\mathfrak{p})}{N\mathfrak{p}^s - 1} = B_{K,\mathfrak{p}}.$$

Taking L/K to be L_n/L_m shows that the sequence $(n^{-1}Z_{L_n}(s))_n = (\sum_{\mathfrak{p}\in\Sigma_{K,f}} B_{L_n,\mathfrak{p}})_n$ is monotonically decreasing. On the other hand we have obviously

$$n^{-1}Z_{L_n}(s) > 0$$

for any n, i.e., the sequence is bounded from below. Thus it is convergent. Set

$$B_{L_\infty,\mathfrak{p}} = \begin{cases} \frac{1}{e_\mathfrak{p}} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{f_\mathfrak{p} s}-1} & \text{if } e_\mathfrak{p}, f_\mathfrak{p} < \infty, \\ 0 & \text{if } e_\mathfrak{p} = \infty \text{ or } f_\mathfrak{p} = \infty. \end{cases}$$

Then $\sum_{\mathfrak{p}\in\Sigma_{K,f}, e_\mathfrak{p}, f_\mathfrak{p}<\infty} = \sum_{\mathfrak{p}\in\Sigma_{K,f}} B_{L_\infty,\mathfrak{p}}$. By the same reasoning as above, the series on the right side of (2.7) converges.

Now we have to show the equality (2.7). Let $\epsilon > 0$. Take $C >> 0$ big enough, such that $\sum_{\mathfrak{p}\in\Sigma_{K,f}, \mathrm{N}\mathfrak{p}>\mathrm{C}} B_{K,\mathfrak{p}} < \frac{\epsilon}{4}$. Let now $n_0 >> 0$ be big enough, such that for all $n > n_0$ and for all (finitely many!) $\mathfrak{p} \in \Sigma_{K,f}$ with $\mathrm{N}\mathfrak{p} \leqslant \mathrm{C}$:

$$|B_{L_n,\mathfrak{p}} - B_{L_\infty,\mathfrak{p}}| < \frac{\epsilon}{2C}.$$

and we have

$$\begin{aligned} \left| \sum_\mathfrak{p} B_{L_n,\mathfrak{p}} - \sum_{\mathfrak{p}\colon e_\mathfrak{p}, f_\mathfrak{p}<\infty} \frac{1}{e_\mathfrak{p}} \frac{\log \mathrm{N}\mathfrak{p}}{\mathrm{N}\mathfrak{p}^{f_\mathfrak{p} s}-1} \right| &\leqslant \left| \sum_{\mathrm{N}\mathfrak{p}\leqslant \mathrm{C}} B_{L_n,\mathfrak{p}} - B_{L_\infty,\mathfrak{p}} \right| + \left| \sum_{\mathrm{N}\mathfrak{p}>\mathrm{C}} B_{L_n,\mathfrak{p}} \right| + \left| \sum_{\mathrm{N}\mathfrak{p}>\mathrm{C}} B_{L_\infty,\mathfrak{p}} \right| \\ &< C\frac{\epsilon}{2C} + 2\frac{\epsilon}{4} = \epsilon. \end{aligned}$$

□

Immediately from the proposition we obtain:

Corollary 2.25. *With the assumptions as in the proposition, the following are equivalent:*

(i) $\lambda_\mathscr{L}(s) = 0$.

(ii) There is no non-archimedean prime of $\mathscr{L}$ with finite degree and finite ramification index over K.

We obtain the following criterion, which decides, whether a normal subgroup of G_S has a big intersection with a decomposition subgroup of a prime $\mathfrak{p} \in \Sigma_{K,f}$.

Corollary 2.26. *Let $H \lhd \mathrm{G}_S$ be a closed normal subgroup. Let $\mathrm{G}_S \supseteq \cdots \supseteq U_n \supseteq \ldots$, indexed by $n \to \infty$, such that $(\mathrm{G}_S\colon U_n) = n$ be a series of open normal subgroups of G_S, such that $\bigcap_n U_n = H$. Set $L_n = (K_S)^{U_n}$ and $\mathscr{L} = (K_S)^H$. For any real $s > 1$ the limit*

$$\lambda_H(s) := \lambda_\mathscr{L}(s)$$

exists and is independent of the choice of $(U_n)_n$. Further, the following are equivalent:

(i) $\lambda_H(s) = 0$.

(ii) For any prime in $\Sigma_{\mathscr{L},f}$, its inertia degree or its ramification index over K is infinite.

(iii) For any finite prime $\mathfrak{p}$ of K and any extension $\bar{\mathfrak{p}}/\mathfrak{p}$ to K_S, the inclusion $H \cap D_{\bar{\mathfrak{p}}} \subseteq D_{\bar{\mathfrak{p}}}$ is not open.

Proof. The equivalence of (i) and (ii) is just Corollary 2.25. The equivalence of (ii) and (iii) is evident. □

This corollary shows that if one could obtain information about the number $\lambda_H(s)$ only from the group $\mathrm{G}_{K,S}$, then $\mathrm{G}_{K,S}$ would determine intrinsically, whether H contains an open subgroup of a decomposition group of a finite prime of K_S. However, as stated here, this method would only work for closed subgroups $H \subseteq \mathrm{G}_{K,S}$ with open normalizer in $\mathrm{G}_{K,S}$.

Further, one can hope to obtain some information on $\lambda_H(s)$ by using formula (2.6). Indeed, with the notation as above, $\lambda_H(s)$ is the limit of of the numbers $n^{-1}Z_{L_n}(s)$, and by (2.6), each of this numbers is determined by d_{L_n}, n_{L_n} and (unfortunately) some term coming from the zeta-zeros. One can hope to read off the first two of these three quantities (or at least their growth behavior for $n \to \infty$) from intrinsic properties of G_S, as in the preceding sections. As for the last one, we have no good idea how to obtain this quantity. At least there is a classical result of Landau, giving an estimate of the number of the zeta-zeros: let $N_K(T)$ denote the number of zeros $s = \sigma + it$ of $\zeta_K(s)$ in the region $0 \leqslant \sigma \leqslant 1$, $0 < t \leqslant T$, counted with multiplicity. Then [[La] Satz 171] says that:

$$N(T) = \frac{n_K}{2\pi} T \log T + \frac{\sharp d_K - n_K(1 + 2\pi)}{2\pi} T + O(\log T).$$

Part II

The group G_S with S stable

3 Stable and persistent sets of positive density

In this section we introduce the classes of stable and persistent sets of primes in number fields, study their properties and give examples. The motivation for the definition of stable sets are the arithmetic and anabelian results holding for them, which we prove in the subsequent sections.

3.1 Overview

The first goal of this section is to introduce a new class of sets of primes of positive density in a number field K, which generalize sets of density 1, in the sense that certain arithmetic and anabelian results (cf. Sections 4-6) hold for them. Roughly speaking, we say that a set S of primes of K is *stable* for an extension $\mathscr{L}/K$, if it contains a subset $S_0 \subseteq S$ such that the function of finite subextensions $\mathscr{L}/L/K$, given by $L \mapsto \delta_L(S_0)$ is positive and beginning from some extension, does not oscillate very much. As a stronger version of the above, we call S *persistent*, if this function becomes constant.

A further goal is to find many examples of stable and persistent sets. In particular, for any finite Galois extension M/K, the set $\mathrm{cs}(M/K)$ is persistent for any extension $\mathscr{L}/K$ and for any $\sigma \in \mathrm{G}_{M/K}$, the set $P_{M/K}(\sigma)$ is persistent for any extension $\mathscr{L}/K$ with $\mathscr{L} \cap M = K$ (cf. Corollary 3.14). Also any set containing (up to a density zero subset) a persistent set, is itself persistent. Clearly, if a set is persistent, then it is also stable. Most examples occurring in nature are persistent, but to prove arithmetic and anabelian results, one only needs (p-)stability property of a set. It is still not clear, whether there is a stable set, which is not persistent, cf. Section 3.5.4. Thus both notions have their right to exist.

We have to make the following technical restriction. Let $\mathscr{P}_K$ denote the set of all subsets of Σ_K. The Dirichlet density is not defined for all elements in $\mathscr{P}_K$, and moreover there are examples of finite extensions L/K and $S \in \mathscr{P}_K$, such that S has a density, but the pull-back S_L of S to L has no density. To omit dealing with such sets we make the following convention, which holds until the end of this thesis.

Convention 3.1. *If $S \in \mathscr{P}_K$ is a set of primes of K, then we assume implicitly that for all finite extensions L/K, all finite Galois extensions M/L and all $\sigma \in \mathrm{G}_{M/L}$, the set $S_L \cap P_{M/L}(\sigma)$ has a Dirichlet density.*

In particular, all Chebotarev sets $P_{M/K}(\sigma)$ satisfy this. More on this convention can be found in Section 3.2.2.

Finally, we want to refresh some notations, which will be used in this and the subsequent sections. If G is a finite group and $\sigma \in G$, we write $C(\sigma; G)$ for the conjugacy class of σ in G. If further H is a subgroup, we denote by m_H the character of the G-representation $\mathrm{Ind}_H^G \mathbf{1}$.

If $S, T \subseteq \Sigma_K$ are two sets of primes of a number field K, define

$$\begin{aligned} S \overset{\subseteq}{\sim} T &:\Leftrightarrow \delta_K(S \smallsetminus T) = 0 \\ S \backsimeq T &:\Leftrightarrow (S \overset{\subseteq}{\sim} T) \text{ and } (T \overset{\subseteq}{\sim} S). \end{aligned}$$

In particular, if S and T differ only in a finite set of primes, then $S \backsimeq T$. If M/K is a finite Galois extension and $\sigma \in \mathrm{G}_{M/K}$ we write

$$P_{M/K}(\sigma) = \{\mathfrak{p} \in \Sigma_K \colon \mathfrak{p} \text{ is unramified in } M/K \text{ and } (\mathfrak{p}, M/K) = C(\sigma; \mathrm{G}_{M/K})\}.$$

If L/K is a finite extension, then we write

$$\begin{aligned} P'(L/K) &:= \{\mathfrak{p} \in \Sigma_L : \mathfrak{p} \text{ is unramified and has degree one over } K\} \\ \mathrm{cs}(L/K) &:= \{\mathfrak{p} \in \Sigma_K : \mathfrak{p} \text{ is completely split in } L\} \\ \mathrm{Ram}(L/K) &:= \{\mathfrak{p} \in \Sigma_K : \mathfrak{p} \text{ is ramified in } L/K\ \}. \end{aligned}$$

If L^{gal} denotes the Galois closure of L over K, then $\mathrm{cs}(L/K) = \mathrm{cs}(L^{gal}/K)$.

In Section 3.2 we recall briefly the definition and some properties of the Dirichlet density. In Section 3.3 we compute the density of certain Chebotarev sets (i.e., sets of the form $P_{M/K}(\sigma)$). In Section 3.4 we define and study some properties of stable and persistent sets. Finally, in Section 3.5 we give examples of stable sets. Therefore we use computations from Section 3.3.

3.2 Dirichlet density

In this section we recall briefly the definition and some easy properties of the Dirichlet density, which allow us to compute the density of certain pull-backs of Chebotarev sets in the next section.

3.2.1 Recall of the definition

Definition 3.2. If $S \subseteq \Sigma_K$ is a set of primes, its *Dirichlet-density* is defined as the limit

$$\delta_K(S) = \lim_{s \to 1+} \frac{\sum_{\mathfrak{p} \in S_f} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \in \Sigma_{K,f}} N\mathfrak{p}^{-s}},$$

if this limit exists (if not, the set has no Dirichlet-density).

For $s \to 1+$, the series $\sum_{\mathfrak{p} \in \Sigma_{K,f}} N\mathfrak{p}^{-s}$ behaves like $\log \zeta_K(s)$, which in turn has the same asymptotic behavior as $\log(\frac{1}{s-1})$, i.e., one also can rewrite the limit:

$$\delta_K(S) = \lim_{s \to 1+} \frac{\sum_{\mathfrak{p} \in S_f} N\mathfrak{p}^{-s}}{\log(\frac{1}{s-1})}. \tag{3.1}$$

Since $\log(\frac{1}{s-1}) \to +\infty$ for $s \to 1+$, the Dirichlet density of a set S does not change if one add (or remove) finite subsets of Σ_K to (from) S. If S is a set of primes of K, having a Dirichlet-density, then clearly $0 \leqslant \delta_K(S) \leqslant 1$. A subset of a set with density 0 also has density 0; a superset of a set of density 1 also has density 1. A set S has a Dirichlet density if and only if its complement in Σ_K has. Assume S_1, S_2 have Dirichlet densities. If one of the sets $S_1 \cap S_2$ and $S_1 \cup S_2$ has a density, then also the other one has and the following holds:

$$\delta_K(S_1) + \delta_K(S_2) = \delta_K(S_1 \cap S_2) + \delta_K(S_1 \cup S_2).$$

In particular, if S has a density and T has density 1, then $S \cap T$ has a density and $\delta_K(S \cap T) = \delta_K(S)$.

Let L/K be a finite extension. The set $P'(L/K)$ (cf. Section 3.1) has density 1 in L. Indeed, if $L/K/k$, then $P'(L/k) \subseteq P'(L/K)$, hence it is enough to assume $K = \mathbb{Q}$. Then for any

$\mathfrak{p} \in S := \Sigma_{L,f} \smallsetminus P'(L/\mathbb{Q})$ we have $N\mathfrak{p}^{-s} \leqslant p^{-2s}$, where $\mathfrak{p}$ lies over the rational prime p and hence

$$\delta(S) \leqslant \lim_{s\to 1+} \frac{[L:\mathbb{Q}]\sum_p p^{-2s}}{\sum_p p^{-s}} = 0,$$

as the denominator goes to $+\infty$ and the numerator is bounded, when $s \to 1+$. The most important result involving the Dirichlet density is the Chebotarev density theorem, which says that given a finite Galois extension L/K and an element $\sigma \in G = \mathrm{G}_{L/K}$, one has:

$$\delta_K(P_{L/K}(\sigma)) = \frac{\sharp C(\sigma;G)}{\sharp G}.$$

3.2.2 Measurable sets

We discuss briefly Convention 3.1. Recall that $\mathscr{P}_K$ denotes the set of all subsets of Σ_K, which is a σ-algebra. The optimal way to omit sets having no density would be to find an appropriate sub-σ-algebra of $\mathscr{P}_K$ (for any K), such that the restriction of δ_K to it is a measure (and the pull-back maps $\mathscr{P}_K \to \mathscr{P}_L$ attached to finite extensions L/K restrict to pull-back maps on these sub-σ-algebras). Unfortunately, there is no satisfactory way to find such σ-algebra $\mathscr{B}_K$, at least if one requires that if $S \in \mathscr{B}_K$, then also $T \in \mathscr{B}_K$ for any $T \backsimeq S$, or, which is weaker, that any finite set of primes of K lies in $\mathscr{B}_K$. Indeed, countability of Σ_K would imply $\mathscr{B}_K = \mathscr{P}_K$ in this case, but not all elements of $\mathscr{P}_K$ have a Dirichlet density.

However, Convention 3.1 is satisfied for all sets lying in the following rather big subset of $\mathscr{P}_K$:

$$\mathscr{A}_K := \left\{ \begin{array}{c} S \subseteq \Sigma_K \colon S \backsimeq \bigcup_i P_{L_i/K_i}(\sigma_i)_K \text{ for some } K/K_i/\mathbb{Q} \\ \text{and } L_i/K_i \text{ finite Galois and } \sigma_i \in \mathrm{G}_{L_i/K_i} \end{array} \right\},$$

where the unions are disjoint and countable (or finite or empty). This $\mathscr{A}_K$ can not be closed simultaneously under (arbitrary) unions and complements: otherwise it would be a σ-algebra and hence would be equal to $\mathscr{P}_K$.

3.2.3 Further properties

Let now L/K be a finite extension of degree n (not necessarily Galois). For $0 \leqslant m \leqslant n$, define the following sets:

$$P_m(L/K) := \{\mathfrak{p} \in \Sigma_K \colon \mathfrak{p} \text{ is unramified and has exactly } m \text{ degree-1-factors in } L\}.$$

In particular, $P_n(L/K) = \mathrm{cs}(L/K)$, $P_{n-1}(L/K) = \varnothing$. Recall that if $H \subseteq G$ are finite groups, then m_H denotes the character of the G-representation $\mathrm{Ind}_H^G \mathbf{1}$. One has:

$$m_H(\sigma) = \sharp\{gH \colon \langle\sigma\rangle^g \subseteq H\} = \sharp\{\langle\sigma\rangle gH \colon \langle\sigma\rangle^g \subseteq H\},$$

where $\langle\sigma\rangle \subseteq G$ denotes the subgroup generated by σ and $\langle\sigma\rangle^g := g^{-1}\langle\sigma\rangle g$. The equality on the right follows immediately from the fact that if $\langle\sigma\rangle^g \subseteq H$, then $gH = \langle\sigma\rangle gH$

Lemma 3.3. *Let L/K be a finite extension and N/K a finite Galois extension containing L, with Galois group G, such that L corresponds to a subgroup $H \subseteq G$. Then*

$$P_m(L/K) \backsimeq \{\mathfrak{p} \in P_m(L/K) \colon \mathfrak{p} \text{ is unramified in } N/K\} = \bigcup_{\substack{C(\sigma;G)\subseteq G \\ m_H(\sigma)=m}} P_{N/K}(\sigma)$$

(disjoint union). In particular, $P_m(L/K) \in \mathscr{A}_K$ *and*

$$\delta_K(P_m(L/K)) = \sharp G^{-1} \sum_{\substack{C(\sigma;G)\subseteq G \\ m_H(\sigma)=m}} \sharp C(\sigma;G).$$

Proof. The proof of the first statement is an elementary exercise in Galois theory (if $\mathfrak{p}$ is a prime of K unramified in N, then the primes of L lying over $\mathfrak{p}$ are in one-to-one correspondence with double cosets $\langle\sigma\rangle gH$, where σ is arbitrary in the Frobenius class of $\mathfrak{p}$; the residue field extension of a prime belonging to the coset $\langle\sigma\rangle gH$ over $\mathfrak{p}$ has the Galois group $\langle\sigma\rangle^g/\langle\sigma\rangle^g \cap H$). The second statement follows from the first and the Chebotarev density theorem. □

The following lemma describes how to compute the density of a pull-back of a set of primes.

Lemma 3.4. *Let* L/K *be a finite extension of degree* n *and* S *a set of primes of* K*. Then*

$$\delta_L(S) = \sum_{m=1}^{n} m\delta_K(S \cap P_m(L/K)),$$

or equivalently, if N/K *is a Galois extension containing* L*, such that* $G := \mathrm{G}_{N/K} \supseteq \mathrm{G}_{N/L} =: H$*, then*

$$\delta_L(S) = \sum_{C(\sigma;G)\subseteq G} m_H(\sigma)\delta_K(S \cap P_{N/K}(\sigma)).$$

If, in particular, L/K *is Galois, then*

$$\delta_L(S) = [L:K]\delta_K(S \cap \mathrm{cs}(L/K)).$$

Proof. Let $P_m := P_m(L/K)$, $P' := P'(L/K)$, and $P'_m := P' \cap P_{m,L}$. Then $\delta_L(P') = 1$ and $P' = \bigcup_{m=1}^n P'_m$ (disjoint union). We have:

$$\begin{aligned}
\delta_L(S) &= \delta_L(S \cap P') = \lim_{s\to 1+} \frac{\sum_{S_L \cap P'} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}}{\sum_{P'} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}} \\
&= \lim_{s\to 1+} \frac{\sum_m \sum_{S_L \cap P'_m} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}}{\sum_m \sum_{P'_m} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}} \\
&= \lim_{s\to 1+} \frac{\sum_m m \sum_{S \cap P_m} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}}{\sum_m m \sum_{P_m} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}} \\
&= \lim_{s\to 1+} \frac{\sum_m m \sum_{S \cap P_m} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}}{\sum_{\Sigma_K} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}} \lim_{s\to 1+} \frac{\sum_{\Sigma_K} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}}{\sum_m m \sum_{P_m} \mathrm{N}\mathfrak{p}^{-\mathrm{s}}} \\
&= (\sum_m m\delta_K(S \cap P_m))(\sum_m m\delta_K(P_m))^{-1}.
\end{aligned}$$

It remains to show that $\sum_m m\delta_K(P_m) = 1$. Indeed, let N be the Galois closure of L/K, $G = \mathrm{G}_{N/K}$ and $H = \mathrm{G}_{N/L}$ and let $\langle , \rangle_G$ denote the inner product on the space of class functions

on G. Then by Lemma 3.3 we have:

$$\begin{aligned}\sum_m m\delta_K(P_m) &= \frac{1}{\sharp G}\sum_{C(\sigma;G)\subseteq G} m_H(\sigma)\sharp C(\sigma;G)\\ &= \langle m_H, \mathbf{1}_G\rangle_G = \langle \mathrm{Ind}_H^G \mathbf{1}_H, \mathbf{1}_G\rangle_G = \langle \mathbf{1}_H, \mathbf{1}_H\rangle_H = 1,\end{aligned}$$

by Frobenius reciprocity. □

To prove Lemma 3.4, one does not need Lemma 3.3: one can omit it by using the formula (3.1) and doing the same computation as in the beginning of the proof. However, the author thinks that the given proof is more conceptual. Another treatment (using Dirichlet/Hecke-characters) can be found in [Na]. In particular, [Na] Lemma 7.35(ii) shows $\sum_m m\delta_K(P_m) = 1$.

3.3 Density of certain Chebotarev sets

The goal is to prove the following proposition, which is responsible for all examples of stable and persistent sets we have:

Proposition 3.5. *Let M/K be a finite Galois extension, $\sigma \in \mathrm{G}_{M/K}$ and L/K any finite extension. Let $L_0 := L \cap M$. Then:*

$$\delta_L(P_{M/K}(\sigma)_L) = \frac{\sharp C(\sigma;\mathrm{G}_{M/K}) \cap \mathrm{G}_{M/L_0}}{\sharp \mathrm{G}_{M/L_0}}.$$

Thus $\delta_L(P_{M/K}(\sigma)_L) \neq 0$ if and only if $C(\sigma;\mathrm{G}_{M/K}) \cap \mathrm{G}_{M/L_0} \neq \varnothing$. In particular, this is always the case if $L_0 = K$ or if $\sigma = 1$.

Lemma 3.6 ([Wi] Proposition 2.1)**.** *Let $N/M/K$ be finite Galois extensions and $\sigma \in \mathrm{G}_{M/K}$. Then*

$$P_{M/K}(\sigma) \backsimeq \{\mathfrak{p} \in P_{M/K}(\sigma)\colon \mathfrak{p} \text{ is unramified in } N/K\} = \bigcup_{C(g;\mathrm{G}_{N/K})\mapsto C(\sigma;\mathrm{G}_{M/K})} P_{N/K}(g),$$

where the (disjoint) union is taken over all conjugacy classes of $\mathrm{G}_{N/K}$, which lie over the conjugacy class of σ in $\mathrm{G}_{M/K}$.

Proof of Proposition 3.5. Let N/K be a finite Galois extension with $N \supseteq ML$. Let $H := \mathrm{G}_{N/L}$ and $\overline{H} := \mathrm{G}_{M/L_0}$. We have a natural surjection $H \twoheadrightarrow \overline{H}$. Let $\mathbf{1}_\sigma$ denote the class function on $\mathrm{G}_{M/K}$, which has value 1 on $C(\sigma;\mathrm{G}_{M/K})$ and 0 outside. Finally, let m_H denote the character on $G := \mathrm{G}_{N/K}$ of the induced representation $\mathrm{Ind}_H^G \mathbf{1}_H$. Then we have (the first equality below

follows from Lemma 3.6 and the second from Lemma 3.4):

$$\begin{aligned}
\delta_L(P_{M/K}(\sigma)_L) &= \sum_{C(g;G)\mapsto C(\sigma;\mathrm{G}_{M/K})} \delta_L(P_{N/K}(g)_L) \\
&= \sum_{C(g;G)\mapsto C(\sigma;\mathrm{G}_{M/K})} m_H(g)\delta_K(P_{N/K}(g)) \\
&= \sum_{C(g;G)\mapsto C(\sigma;\mathrm{G}_{M/K})} m_H(g)\frac{\sharp C(g;G)}{\sharp G} \\
&= \frac{1}{\sharp G}\sum_{g\mapsto C(\sigma;\mathrm{G}_{M/K})} m_H(g) \\
&= \langle m_H, \inf^G_{\mathrm{G}_{M/K}} \mathbf{1}_\sigma\rangle_G \\
&= \langle \mathbf{1}_H, \inf^H_{\mathrm{G}_{M/K}} \mathbf{1}_\sigma\rangle_H \\
&= \langle \mathbf{1}_{\overline{H}}, \mathbf{1}_\sigma|_{\overline{H}}\rangle_{\overline{H}} \\
&= \frac{\sharp C(\sigma;\mathrm{G}_{M/K})\cap \overline{H}}{\sharp \overline{H}},
\end{aligned}$$

where the third to last equality sign is Frobenius reciprocity, and the second to last follows from the easy fact that if $H \twoheadrightarrow \overline{H}$ is a surjection of finite groups, χ, ρ are two characters of $\overline{H}$, then $\langle \inf^H_{\overline{H}}\chi, \inf^H_{\overline{H}}\rho\rangle_H = \langle\chi,\rho\rangle_{\overline{H}}$.

□

3.4 Stable and persistent sets

In this section we define stable and persistent sets of primes in a number field, consider some properties of them and give a further characterization of stable sets.

3.4.1 Definition and first properties

Let K be a number field and S a set of primes. Lemma 3.4 implies that if $\delta_K(S) = 0$ resp. $= 1$, then also $\delta_L(S) = 0$ resp. $= 1$ for all finite L/K. Now if $0 < \delta_K(S) < 1$, it can happen that there is some finite L/K with $\delta_L(S) = 0$ (just start with some finite Galois extension L/K and take $S := \Sigma_K \setminus \mathrm{cs}(L/K)$, having the density $1 - [L:K]^{-1}$ in K and density 0 in L). We want to study situations, in which this possibility is excluded, and moreover the density of a subset $S_0 \subseteq S$ considered as a function of extensions of K lies in an interval with logarithmic length bounded by some constant resp. is itself constant.

Definition 3.7. Let S be a set of primes of K and $\mathscr{L}/K$ any extension.

(i) Let $\lambda > 1$. A finite subextension $\mathscr{L}/L_0/K$ is **λ-stabilizing for S for $\mathscr{L}/K$**, if there exists a subset $S_0 \subseteq S$ and some $a \in (0,1]$, such that $\lambda a > \delta_L(S_0) \geqslant a > 0$ for all finite subextensions $\mathscr{L}/L/L_0$.

(ii) A finite subextension $\mathscr{L}/L_0/K$ is **monotone stabilizing for S for $\mathscr{L}/K$**, if there exists a subset $S_0 \subseteq S$, such that $\delta_{L'}(S_0) \geqslant \delta_L(S_0) > 0$ for all finite subextensions $\mathscr{L}/L'/L/L_0$.

(iii) A finite extension $\mathscr{L}/L_0/K$ is **persisting for S for $\mathscr{L}/K$**, if there exists a subset $S_0 \subseteq S$, such that $\delta_L(S_0) = \delta_{L_0}(S_0) > 0$ for all finite subextensions $\mathscr{L}/L/L_0$.

We say that S is **λ-stable** resp. **monotonic stable** resp. **persistent** for $\mathscr{L}/K$, if it has a λ-stabilizing resp. monotone stabilizing resp. persisting extension for $\mathscr{L}/K$. We say that S is **stable** for $\mathscr{L}/K$, if it is λ-stable for $\mathscr{L}/K$ for some $\lambda > 1$.

For short, we say that S is **λ-stable** resp. **monotonic stable** resp. **persistent**, if it is λ-stable resp. monotonic stable resp. persistent for K_S/K. Observe that these notions are not preserved under the equivalence relation $S \simeq T$ on subsets of Σ_K (since $K_S \neq K_T$ in general), whereas the notions from the definition are. Observe also that, apart from our convention that all considered sets have a Dirichlet density, there is no reason to require a stable (resp. persistent) set S to have a density: it is enough, when a stable (resp. persistent) subset $S_0 \subseteq S$ has. If $\mathscr{L}/K, S$ and $\lambda > 1$ are as above, then we have:

$$S \text{ persistent } \Rightarrow S \text{ monotonic stable } \Rightarrow S \ \lambda\text{-stable.}$$

The first implication is trivial. The second is easy (Proposition 3.8 (iv)). We will give another characterization of stable sets in Section 3.4.3. Now we give some basic properties.

Proposition 3.8. *Let $\mathscr{L}/K$ be an extension and S a set of primes of K.*

(i) Let $\lambda \geqslant \mu > 1$. If S is μ-stable with μ-stabilizing field L_0, then S is λ-stable with λ-stabilizing field L_0.

(ii) If L_0 is λ-stabilizing resp. monotone stabilizing resp. persisting field for S for $\mathscr{L}/K$, then any finite subextension $\mathscr{L}/L_1/L_0$ has the same property.

(iii) Let S' be a further set of primes of K. If $S \overset{\subseteq}{\sim} S'$, and S is λ-stable resp. monotonic stable resp. persistent for $\mathscr{L}/K$, then S' also has this property. Any λ-stabilizing resp. monotone stabilizing resp. persisting field for S has the same property for S'.

(iv) If S is monotonic stable for $\mathscr{L}/K$, then it is λ-stable for $\mathscr{L}/K$ for any $\lambda > 1$.

(v) Let $\mathscr{L}/\mathscr{N}/M/K$ be subextensions. If S is λ-stable (resp. monotonic stable resp. persistent) for $\mathscr{L}/K$ with λ-stabilizing (resp. monotone stabilizing, resp. persisting) field $L_0 \subseteq \mathscr{N}$, then S_M is λ-stable (resp. monotonic stable resp. persistent) for $\mathscr{N}/M$.

Proof. (i) - (iii) are immediate.

(iv): Let S be monotonic stable for $\mathscr{L}/K$ and let L_0 be monotone stabilizing for S for $\mathscr{L}/K$ with respect to a subset $S_0 \subseteq S$. Consider the set $\{\delta_L(S_0)\colon \mathscr{L}/L/L_0 \text{ finite}\} \subset [0,1]$. This is a bounded set of real numbers, which thus has a supremum, and we have $\delta_{L'}(S_0) \geqslant \delta_L(S_0) > 0$ for all finite $\mathscr{L}/L'/L/L_0$. Let $\mathscr{L}/L_1/L_0$ be finite and such that $a := \delta_{L_1}(S_0) > \frac{1}{\lambda}\sup_{\mathscr{L}/L/L_0}\{\delta_L(S_0)\}$. This L_1 is λ-stabilizing for S (with respect to the subset S_0 and the real number a).

(v): Let S be λ-stable for $\mathscr{L}/K$ with λ-stabilizing field $L_0 \subseteq \mathscr{N}$. Then S_M is λ-stable for $\mathscr{L}/M$ with stabilizing field L_0M, and hence also λ-stable for $\mathscr{N}/M$ with stabilizing field $L_0M \subseteq \mathscr{N}$. For monotonic stable and persistent sets the proof is the same. □

Remark 3.9. In the definition of stable/persisting sets we used the Dirichlet density, which is a measure on $\mathscr{A}_L$ for any finite subextension $\mathscr{L}/L/K$. For arithmetic applications there is in fact no reason, why one should use exactly δ_L. It is not clear, whether functions essentially different from δ_L can be constructed. Such a construction should work as follows: one considers

an appropriate subset $\mathscr{B}_L \subseteq \mathscr{P}_L$ for each $\mathscr{L}/L/K$, such that the pull-back map $\mathscr{P}_L \to \mathscr{P}_{L'}$ restricts to a pull-back $\mathscr{B}_L \to \mathscr{B}_{L'}$ for any $\mathscr{L}/L'/L/K$ and replace the formation $(\delta_L)_{\mathscr{L}/L/K}$ in the Definition 3.7 by any formation of functions

$$\mu_L \colon \mathscr{B}_L \longrightarrow [0,1]$$

such that the following three conditions hold:

(i) $\mu_L(\Sigma_L) = 1$,

(ii) $\mu_L(S \cup T) = \mu_L(S) + \mu_L(T)$ for any disjoint $S, T \in \mathscr{B}_L$,

(iii) (pull-back formula for Galois extensions) For any finite Galois subextension N of $\mathscr{L}/L$ one has

$$\mu_N(S) = [N : L]\mu_L(S \cap \mathrm{cs}(N/K)),$$

resp.

(iii') (general pull-back formula) For any finite Galois subextension N of $\mathscr{L}/L$ and any subextension $N/L'/L$, with $G := \mathrm{G}_{N/L}$, $H := \mathrm{G}_{N/L'}$, one has:

$$\mu_{L'}(S) = \sum_{C(\sigma;G)\subseteq G} m_H(\sigma)\mu_L(S \cap P_{L'/L}(\sigma)).$$

There are only few places in this and the following chapters, where we use the stability property of a set directly. They are essentially in Proposition 3.11, Theorem 4.2, Lemma 4.4 and Proposition 4.36. By posing conditions (i),(ii) and (iii)' on μ_L one would have enough to use μ_L instead of δ_L in all cases. By posing (i),(ii) and the weaker condition (iii), one would abandon Lemma 4.4 and (the most general form of) Proposition 3.11, but still have enough for (a slightly weaker version of) Theorem 4.2 and consequently all of the important results.

The conditions above are restrictive. In particular, μ_L is determined by (i),(ii) and (iii)' on each set of the form $P_{M/L}(\sigma)$ for M being a finite Galois subextension of $\mathscr{L}/L$, and coincides with δ_L there. However, it is not clear, whether there are interesting choices of $(\mathscr{B}_L, \mu_L)_L$ such that μ_L does not coincide with δ_L on the whole set $\mathscr{B}_L$. For example, one could try to define μ_L as the limit

$$\mu_L(S) := \lim_{s \to s_0^+} \frac{\sum_{\mathfrak{p}\in S_f, \deg\mathfrak{p}>k} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}\in\Sigma_{L,f}, \deg\mathfrak{p}>k} N\mathfrak{p}^{-s}},$$

where $\deg\mathfrak{p} = \log_p \mathrm{N}\mathfrak{p}$ (p is the residue characteristic of $\mathfrak{p}$) and the positive real s_0 is chosen in a way such that denominator has a pole at s_0.

3.4.2 Properties $(*)$

The first property which gets important in the arithmetic applications is the p-stability of a set for some rational prime p. But it turns out that also the following refinement is important (in particular for the Grunwald-Wang theorem):

Definition 3.10. Let S be a set of primes of K and p a (finite or infinite) prime of $\mathbb{Q}$.

(i) Assume S is persistent (i.e., persistent for K_S/K). We say that S satisfies **property** $(*)_p^{\mathrm{pers}}$, if S is persistent for $K_{S\cup S_p\cup S_\infty}/K$ with a persisting field contained in K_S.

(i)' Assume S is persistent. We say that S satisfies **property** $(*)^{\mathrm{pers}}$, if S satisfies $(*)_p^{\mathrm{pers}}$ for almost all p.

(ii) Assume S is stable. We say that S satisfies **property** $(*)_p^{\mathrm{stab}}$, if S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ with a p-stabilizing field contained in K_S (if $p=\infty$, then this means that S is stable for $K_{S\cup S_\infty}/K$).

(ii)' Assume S is stable. We say that S satisfies **property** $(*)^{\mathrm{stab}}$, if S satisfies $(*)_p^{\mathrm{stab}}$ for almost all p.

For S persistent resp. stable, define the **exceptional set** by

$$E^{\mathrm{pers}}(S) := \{p\colon S \text{ does not satisfy } (*)_p^{\mathrm{pers}}\},$$

resp. by

$$E^{\mathrm{stab}}(S) := \{p\colon S \text{ does not satisfy } (*)_p^{\mathrm{stab}}\},$$

Clearly, $(*)_p^{\mathrm{pers}}$ resp. $(*)^{\mathrm{pers}}$ is stronger than $(*)_p^{\mathrm{stab}}$ resp. $(*)^{\mathrm{stab}}$. Further a stable set S satisfies $(*)^{\mathrm{stab}}$ if and only if $E^{\mathrm{stab}}(S)$ is finite (and similarly for $(*)^{\mathrm{pers}}$). In practice most of the occurring stable sets are persistent and satisfy $(*)^{\mathrm{pers}}$ (cf. Section 3.5), but to prove things, we only use the stability property resp. $(*)_p^{\mathrm{stab}}$ for various p.

3.4.3 Other characterization of stable sets

The following proposition gives another characterization of stable sets and shows in particular, that if S is stable for $\mathscr{L}/K$, then any finite subfield $\mathscr{L}/L/K$ is λ-stabilizing for S with a certain $\lambda > 1$ depending on L.

Proposition 3.11. *Let S be a set of primes of K and $\mathscr{L}/K$ any extension. The following are equivalent:*

(i) S is stable for $\mathscr{L}/K$.

(ii) There exists some $\lambda > 1$, such that S is λ-stable for $\mathscr{L}/K$ with λ-stabilizing field K.

(iii) There exist some $\epsilon > 0$ such that $\delta_L(S) > \epsilon$ for all finite $\mathscr{L}/L/K$.

Proof. (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) are trivial. We prove (i) $\Rightarrow$ (iii). Let $\lambda > 1$ and let S be λ-stable for $\mathscr{L}/K$ with λ-stabilizing field L_0. Then there is some $a > 0$ and a subset $S_0 \subseteq S$ such that $a \leqslant \delta_L(S_0) < \lambda a$ for all $\mathscr{L}/L/L_0$. We want to find some $\epsilon > 0$ such that $\delta_L(S_0) > \epsilon$ for all $\mathscr{L}/L/K$. Suppose there is no such $\epsilon > 0$. This implies that there is a family $(M_i)_{i=1}^{\infty}$ of finite subextensions of $\mathscr{L}/K$ with $\delta_{M_i}(S_0) \to 0$ as $i \to \infty$. Then $d_i = [L_0M_i : M_i] = [L_0 : L_0 \cap M_i]$ is bounded from above by $[L_0 : K]$ and hence

$$\delta_{L_0M_i}(S_0) = \sum_{m=1}^{d_i} m\delta_{M_i}(S_0 \cap P_m(L_0M_i/M_i)) \leqslant [L_0 : K]\delta_{M_i}(S_0) \to 0$$

for $i \to \infty$. This contradicts to the λ-stability of S_0 with respect to the λ-stabilizing field L_0. $\square$

If S is stable for $\mathscr{L}/K$, then $\delta_L(S) > 0$ for all finite $\mathscr{L}/L/K$. The converse is not true, as an example in Section 3.5.4 shows.

3.5 Examples

Finally we consider examples of stable resp. persistent sets. There are plenty of examples of persistent sets, but on the other side it is not really clear, whether there is a stable set, which is not persistent. A construction which goes in this direction is also done here.

3.5.1 Sets of density one

Stable and persistent sets generalize sets of density one. In particular, every set of primes of K of density one is persisting for any extension $\mathscr{L}/K$ with persisting field K and satisfies $(*)_p^{\mathrm{pers}}$ for each p. Nevertheless, sets of density one have some properties, which stable resp. persistent sets do not have in general:

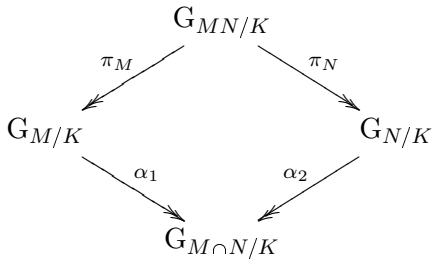
(i) the intersection of two sets of density one has again density one, which is not true for stable and persistent sets: the intersection of two sets persistent for $\mathscr{L}/K$ can be empty (cf. Corollary 3.14 and explicit examples below).

(ii) if $S \subseteq \Sigma_K$ has density one, then there are infinitely many primes $p \in \Sigma_{\mathbb{Q}}$, such that $S_p \subseteq S$ (otherwise, for all primes $p \in \mathrm{cs}(K/\mathbb{Q})$ one could choose a prime $\mathfrak{p} \in S_p \setminus S$ of K and we would have $\delta(S) \leqslant 1 - [K : \mathbb{Q}]^{-1}$). On the other side, it is easy to construct a persistent set $S \subseteq \Sigma_K$ with $S_p \nsubseteq S$ for all $p \in \Sigma_{\mathbb{Q}}$ (cf. Section 3.5.5 for an explicit example).

3.5.2 Almost Chebotarev sets

Definition 3.12. Let K be a number field. A **Chebotarev set** is a set of primes of K of the form $P_{M/K}(\sigma)$, where M/K is a finite Galois extension and $\sigma \in \mathrm{G}_{M/K}$. An **almost Chebotarev set** is a set S of primes of K, such that there is a Chebotarev set $P_{M/K}(\sigma)$ with $S \backsimeq P_{M/K}(\sigma)$.

Remark 3.13. It is natural to ask, whether M and $C(\sigma; \mathrm{G}_{M/K})$ are unique in the definition. This is false even in the easiest case: let N/K be an extension having as its Galois group the permutation group S_3 and let M be the subextension corresponding to the kernel of the quotient $\pi\colon S_3 \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$. Let $g \in S_3$ denote any odd permutation. Then one has $\pi^{-1}(\pi(g)) = C(g; S_3)$ and hence $P_{M/K}(\pi(g)) \backsimeq P_{N/K}(g)$ by Proposition 3.6. To study this question in general, let (M, σ) and (N, τ) be two finite Galois extensions of K together with an element in the Galois group. Then we claim that $P_{M/K}(\sigma) \backsimeq P_{N/K}(\tau)$ if and only if in the diagram



we have $\alpha_1^{-1}(\alpha_2(\tau)) \subseteq C(\sigma; \mathrm{G}_{M/K})$ and $\alpha_2^{-1}(\alpha_1(\sigma)) \subseteq C(\tau; \mathrm{G}_{M/K})$. Indeed, by Lemma 3.6, $P_{M/K}(\sigma) \subseteq P_{N/K}(\tau)$ is equivalent to $\pi_M^{-1}(C(\sigma; \mathrm{G}_{M/K})) \subseteq \pi_N^{-1}(C(\tau; \mathrm{G}_{N/K}))$. But this is equivalent to $\alpha_2^{-1}(\alpha_1(\sigma)) \subseteq C(\tau; \mathrm{G}_{M/K})$, which follows from the fact that the above diagram of groups is a pull-back diagram, and the underlying diagram of sets is also a pull-back diagram, and from the following general fact: if $\alpha_X \colon X \twoheadrightarrow Z, \alpha_Y \colon Y \twoheadrightarrow Z$ are maps of sets, $X \times_Z Y$ is the pull-back with projections denoted by π_X, π_Y, and $X_1 \subseteq X$, $Y_1 \subseteq Y$ are subsets, then $\pi_X^{-1}(X_1) \subseteq \pi_Y^{-1}(Y_1)$ if and only if $\alpha_Y^{-1}(\alpha_X(X_1)) \subseteq Y_1$. This proves our claim.

Let (M, σ), (N, τ) are given, and assume that $h := \alpha_M(\sigma) = \alpha_N(\tau) \in \mathrm{G}_{M\cap N/K}$ (otherwise $P_{M/K}(\sigma) \backsimeq P_{N/K}(\tau)$ is impossible). We can reformulate the above criterion:

$$P_{M/K}(\sigma) \backsimeq P_{N/K}(\tau) \Leftrightarrow \alpha_M^{-1}(h) \subseteq C(\sigma; \mathrm{G}_{M/K}) \text{ and } \alpha_N^{-1}(h) \subseteq C(\tau; \mathrm{G}_{N/K})$$

This group-theoretic criterion allows to construct many further examples in which one has $P_{M/K}(\sigma) \backsimeq P_{N/K}(\tau)$ but $M \neq N$. For example, take any surjection of finite groups $\pi \colon G \twoheadrightarrow H$ and an element $x \in H$, such that for some preimage g of h in G, one has $\pi^{-1}(h) \subseteq C(g, G)$ (cf. for example the first paragraph of this remark). Then any extensions $M, N/K$ such that $\mathrm{G}_{M/K} \cong \mathrm{G}_{N/K} \cong G$ (they have in particular the same degree over K), $\mathrm{G}_{M\cap N/K} \cong H$ gives such an example.

On the other side, assume $(M, \sigma), (N, \tau)$ are given, such that σ resp. τ are central in $\mathrm{G}_{M/K}$ resp. $\mathrm{G}_{N/K}$. Then $P_{M/K}(\sigma) \backsimeq P_{N/K}(\tau) \Leftrightarrow (M, \sigma) = (N, \tau)$. Indeed, in this situation one has $\sharp C(\sigma; \mathrm{G}_{M/K}) = \sharp C(\tau; \mathrm{G}_{N/K}) = 1$ and hence $P_{M/K}(\sigma) \backsimeq P_{N/K}(\tau)$ implies that $\sharp\ker(G \twoheadrightarrow \mathrm{G}_{M/K}) = \sharp\ker(G \twoheadrightarrow \mathrm{G}_{N/K}) = 1$, i.e., $M = N$ and hence also $C(\sigma; \mathrm{G}_{M/K})) = C(\tau; \mathrm{G}_{N/K})$. This generalizes the classical application of Chebotarev, which is the special case with $\sigma = \tau = 1$ ([Ne3] Corollary 13.10).

Proposition 3.5 shows that almost Chebotarev sets are often persistent:

Corollary 3.14. *Let M/K be finite Galois and let $\sigma \in \mathrm{G}_{M/K}$. Let $\mathscr{L}/K$ be any extension and set $L_0 := M \cap \mathscr{L}$. Then a set $S \backsimeq P_{M/K}(\sigma)$ is persistent for $\mathscr{L}/K$ if and only if*

$$C(\sigma; \mathrm{G}_{M/K}) \cap \mathrm{G}_{M/L_0} \neq \emptyset.$$

If this is the case, L_0 is a persistent field for S for $\mathscr{L}/K$. In particular,

(i) any set $S \backsimeq \mathrm{cs}(M/K)$ is persistent for any extension $\mathscr{L}/K$,

(ii) any set $S \backsimeq P_{M/K}(\sigma)$ is persistent for any extension $\mathscr{L}/K$ with $\mathscr{L} \cap M = K$.

We collect some properties of almost Chebotarev sets.

Proposition 3.15. *Let S be an almost Chebotarev set and $\mathscr{L}/K$ an extension. Then the following are equivalent:*

(i) S *is stable for* $\mathscr{L}/K$.

(ii) S *is persistent for* $\mathscr{L}/K$.

(iii) $\delta_L(S) > 0$ *for all finite* $\mathscr{L}/L/K$.

Proof. Let $S \backsimeq P_{M/K}(\sigma)$ with a finite Galois M/K and $\sigma \in \mathrm{G}_{M/K}$. By Proposition 3.5, the density of S is constant and equal to some $d \geqslant 0$ in the tower $\mathscr{L}/L_0$ with $L_0 = \mathscr{L} \cap M$. There are two cases: either $d = 0$ or $d > 0$. If $d = 0$, then S is not stable and hence also not persistent for $\mathscr{L}/K$ by Proposition 3.11, i.e., (i), (ii) and (iii) do not hold in this case. If $d > 0$, then S is obviously persistent for $\mathscr{L}/K$ with persisting field L_0 and hence also stable, i.e., (i),(ii),(iii) hold.

□

Example 3.16 (A persistent set)**.** Let K be a number field, M/K a finite Galois extension, which is totally ramified in a prime $\mathfrak{p}$ of K. Let $\sigma \in \mathrm{G}_{M/K}$ and let S be a set of primes of K, such that

- $S \backsimeq P_{M/K}(\sigma)$
- $\mathfrak{p} \notin S$.

Then S is persistent with persisting field K. Indeed, we have $K_S \cap M = K$ by construction, and the claim follows from Corollary 3.14.

Example 3.17 (Unramified extensions)**.** Let M/K be a finite unramified Galois extension. Let $\sigma \in \mathrm{G}_{M/K}$ and let S be a set of primes of K with $S \backsimeq P_{M/K}(\sigma)$. If $\sigma \neq 1$, then S is never stable. Indeed, one has $M \subseteq K_S$ and the density of S is zero for all fields in the tower K_S/M (cf. Proposition 3.15).

3.5.3 Finiteness of $E^{\mathrm{stab}}(S)$ and properties $(*)$

Proposition 3.18. *Let* S *be an almost Chebotarev set.*

(i) If $\infty \in E^{\mathrm{stab}}(S)$*, then* $E^{\mathrm{stab}}(S)$ *contains all rational primes. If* $\infty \notin E^{\mathrm{stab}}(S)$*, then* S *satisfies property* $(*)^{\mathrm{stab}}$*, i.e., the set* $E^{\mathrm{stab}}(S)$ *is finite.*

(ii) If $\infty \in E^{\mathrm{pers}}(S)$*, then* $E^{\mathrm{pers}}(S)$ *contains all rational primes. If* $\infty \notin E^{\mathrm{pers}}(S)$ *and one has* $K_{S\cup S_\infty} \cap M \subseteq K_S$*, then* $E^{\mathrm{pers}}(S)$ *is finite.*

Proof. (i): If $\infty \in E^{\mathrm{stab}}(S)$, then S does not have a stabilizing field for $K_{S\cup S_\infty}/K$, which is contained in K_S. This is by Proposition 3.11 equivalent to the fact that S is not stable for $K_{S\cup S_\infty}/K$, which in turn is equivalent by Proposition 3.15 to the fact that $\delta_L(S) = 0$ for all $K_{S\cup S_\infty}/L/L_0$ where L_0 is some fixed subextension of $K_{S\cup S_\infty}/K$. From this immediately follows that $p \in E^{\mathrm{stab}}(S)$ for any rational prime p.

Now we prove that if $\infty \in E^{\mathrm{stab}}(S)$, then $E^{\mathrm{stab}}(S)$ is finite. Let $S \backsimeq P_{M/K}(\sigma)$ with $\sigma \in \mathrm{G}_{M/K}$. Let $L_0 := M \cap K_{S\cup S_\infty}$ and $L_p := M \cap K_{S\cup S_p\cup S_\infty}$. By Proposition 3.5, the density of S is constant in the towers $K_{S\cup S_\infty}/L_0$ and $K_{S\cup S_p\cup S_\infty}/L_p$ and equal to some real numbers d_0 and d_p respectively. Since S is stable for $K_{S\cup S_\infty}/K$, we have $d_0 > 0$.

We claim that for almost all p's we have $L_p = L_0$. More precise, this is true for all p's, such that the set

$$\{\mathfrak{p} \in (S_p \smallsetminus S)_{L_0} : \mathfrak{p} \text{ is ramified in } M/L_0\}.$$

is empty. In fact, if this set is empty for p, then the extension L_p/L_0 is unramified in $S_p \smallsetminus S(L_0)$, since contained in M/L_0. But being contained in $K_{S\cup S_p\cup S_\infty}$ and unramified in $S_p \smallsetminus S(L_0)$, it is contained in $K_{S\cup S_\infty}$, and hence also in $M \cap K_{S\cup S_\infty} = L_0$, which proves our claim.

Let now p be such that $L_p = L_0$. Then we claim that S is $([L_0 : K]d_0^{-1})$-stable for $K_{S\cup S_p\cup S_\infty}/K$ with $([L_0 : K]d_0^{-1})$-stabilizing field K. Indeed, as $L_p = L_0$, we have $d_p = d_0 > 0$. Let $K_{S\cup S_p\cup S_\infty}/N/K$ be any finite subextension. We have

$$d_0 = \delta_{L_0N}(S) = [L_0N : N]\delta_N(S \cap \mathrm{cs}(L_0N/N)) \leqslant [L_0 : K]\delta_N(S),$$

i.e., $\delta_N(S) \geqslant [L_0 : K]^{-1}d_0$ for all N, and in particular our claim follows.

Finally, almost all primes satisfy $p > [L_0 : K]d_0^{-1}$ and $L_p = L_0$ and for them S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ with stabilizing field K.

(ii): First, $\infty \in E^{\mathrm{pers}}(S)$ is equivalent to the following fact: for all $S_0 \subseteq S$ and for all $K_S/L'/K$, the density $\delta_*(S_0)$ does not get positive and constant in the tower $K_{S\cup S_\infty}/L'$. In particular, for all such S_0 and L', the density $\delta_*(S_0)$ does not get constant and positive in the bigger tower $K_{S\cup S_p\cup S_\infty}/L'$ for any rational prime p. Hence $p \in E^{\mathrm{pers}}(S)$.

Let now L_0, L_p, d_0, d_p be as in the proof of (i) and assume that $\infty \notin E^{\mathrm{pers}}(S)$ and $L_0 = K_{S\cup S_\infty} \cap M \subseteq K_S$. As in the proof of (i), we have $L_p = L_0$ for almost all p's. For such p's we have $\delta_L(S) = d_p = d_0 > 0$ for all finite subextensions $K_{S\cup S_p\cup S_\infty}/L/L_p$, i.e. $p \notin E^{\mathrm{pers}}(S)$. □

Remark 3.19. The proof also indicates which primes lie in $E^{\mathrm{stab}}(S)$ for $S \backsimeq P_{M/K}(\sigma)$, and in which cases $E^{\mathrm{stab}}(S)$ is empty. If $E^{\mathrm{stab}}(S) = \varnothing$, then $\operatorname{Spec}\mathcal{O}_{K,S}$ is an algebraic $K(\pi, 1)$-space (cf. Corollary 5.14).

Example 3.20 (Persistent sets with $E^{\mathrm{stab}}(S)$ finite but non-empty)**.** Let K be a totally imaginary number field and let M/K be a finite Galois extension extension, which satisfies the following conditions:

- M/K is totally ramified in a prime $\mathfrak{p} \in S_p(K)$,
- $d := [M : K] > p$.

Let $\sigma \in \mathrm{G}_{M/K}$ and let S be a set of primes of K, such that

- $S \backsimeq P_{M/K}(\sigma)$,
- $\mathrm{Ram}(M/K) \smallsetminus S = \{\mathfrak{p}\}$.

Then S is persistent ($\delta_L(S) = d^{-1}$ for all $K_S/L/K$) with persisting field K and does not satisfy $(*)_p^{\mathrm{stab}}$, i.e., $p \in E^{\mathrm{stab}}(S)$ (and $\infty \notin E^{\mathrm{stab}}(S)$, i.e., $E^{\mathrm{stab}}(S)$ is finite). Indeed, $M \subseteq K_{S\cup S_p\cup S_\infty}$ and there are two cases $\sigma = 1$ or $\sigma \neq 1$. In the second case, the density of S in $K_{S\cup S_p\cup S_\infty}/K$ is zero beginning from M, hence S is non-stable for this extension, and $(*)_p^{\mathrm{stab}}$ is not satisfied. In the first case, we have $\delta_L(S) = 1$ for all $K_{S\cup S_p\cup S_\infty}/L/M$. Assume there is a p-stabilizing field $N \subseteq K_S$ for S for $K_{S\cup S_p\cup S_\infty}/K$, i.e., there is some $S_0 \subseteq S$ and some $a \in (0, 1]$ with $a \leqslant \delta_L(S_0) < pa$ for all $K_{S\cup S_p\cup S_\infty}/L/N$. But this leads to a contradiction. Indeed,

$$\delta_{MN}(S_0) = [MN : N]\delta_N(S_0 \cap \mathrm{cs}(MN/N)) = [M : K]\delta_N(S_0) \geqslant p\delta_N(S_0),$$

since $N \cap M = K$ and $S_0 \subseteq S \backsimeq \mathrm{cs}(M/K)$.

Example 3.21 (Persistent sets with $E^{\mathrm{pers}}(S) = \varnothing$)**.** Let M/K be a finite Galois extension of degree d with K totally imaginary, which is totally ramified in at least two primes $\mathfrak{p}$ resp. $\mathfrak{l}$ with different residue characteristics ℓ_1 resp. ℓ_2. Let $S \backsimeq P_{M/K}(\sigma)$ for some $\sigma \in \mathrm{G}_{M/K}$, such that $\mathfrak{p}, \mathfrak{l} \notin S$. Then $M \cap K_S = K$, hence S is persistent with persisting field K. Let p be a rational prime. Then $M \cap K_{S \cup S_p \cup S_\infty} = K$, since M/K is totally ramified over primes with *different* residue characteristics ℓ_1 and ℓ_2. Hence S satisfies $(*)_p^{\mathrm{pers}}$ for every prime p and K is a persisting field for S for $K_{S \cup S_p \cup S_\infty}/K$.

Example 3.22 (Persistent sets with $E^{\mathrm{pers}}(S) = \varnothing$)**.** There is also another possibility to construct sets S with $E^{\mathrm{pers}}(S) = \varnothing$, using the same idea as in the preceding example. Assume for simplicity that K is totally imaginary. Let $M_1, M_2/K$ be two Galois extensions of K, and $\sigma_1 \in \mathrm{G}_{M_1/K}, \tau \in \mathrm{G}_{M_2/K}$. Assume M_i/K is totally ramified in a non-archimedean prime $\mathfrak{p}_i$ of K, such that the residue characteristics of $\mathfrak{p}_1, \mathfrak{p}_2$ are unequal. Then let S be a set of primes of K, such that

- $S \supsetneq P_{M_1/K}(\sigma_1) \cup P_{M_2/K}(\sigma_2)$,
- $\{\mathfrak{p}_1, \mathfrak{p}_2\} \notin S$.

Then, by the same reasoning as in the preceding example, S is persistent with persisting field K and $E^{\mathrm{pers}}(S) = \varnothing$. Moreover for each rational prime p, the field K is persisting for S for $K_{S \cup S_p \cup S_\infty}/K$.

Example 3.23 (Persistent set S with $p \in E^{\mathrm{pers}}(S) \smallsetminus E^{\mathrm{stab}}(S)$)**.** Let K be totally imaginary and M/K a finite extension of degree $d := [M : K] < p$, which is totally ramified in a prime $\mathfrak{p} \in S_p$. Let $S \backsimeq \mathrm{cs}(M/K)$, such that $\mathfrak{p} \notin S$. Then S is persistent with persisting field K, since $M \cap K_S = K$. Further, $p \notin E^{\mathrm{stab}}(S)$, as K is p-stabilizing field for S for $K_{S \cup S_p \cup S_\infty}/K$ (with respect to $S_0 = S$ and $a = d^{-1}$). Moreover, $p \in E^{\mathrm{pers}}(S)$. Indeed, assume $L_0 \subseteq K_S$ would be a persisting field for S for $K_{S \cup S_p \cup S_\infty}/K$. I.e., there would be a subset $S_0 \subseteq S$ with $\delta_L(S_0) = \delta_{L_0}(S_0) > 0$ for all finite subextensions $K_{S \cup S_p \cup S_\infty}/L/L_0$. In particular, this must hold for $L := ML_0$, which is a proper extension of L_0, since $M \cap K_S = K$. But then we have

$$\delta_{ML_0}(S_0) = [ML_0 : L_0]\delta_{L_0}(S_0 \cap \mathrm{cs}(ML_0/L_0)) > \delta_{L_0}(S_0),$$

as $[ML_0 : L_0] > 1$ and $S_0 \subseteq S \backsimeq \mathrm{cs}(M/K)$.

3.5.4 Stable but not persistent sets

It is not clear to the author how to construct a stable but not persistent set. The following example goes in this direction, and by the way provides an example of a set S, such that $\delta_L(S) > 0$ for all finite $\mathscr{L}/L/K$ but S not stable (i.e., S satisfies satisfies property (iii) of Proposition 3.15, but does not satisfy (i)).

Let $\mathscr{L}/K$ be normal and infinite, let $\mathscr{L} = \bigcup_{i=1}^{\infty} L_i \supsetneq \cdots \supsetneq L_i \supsetneq \cdots \supsetneq L_1 \supsetneq K$ be an infinite tower of finite Galois subextensions. Write $d_i := [L_i : K]$. Let $S_i \subseteq \mathrm{cs}(L_i/K) \smallsetminus \mathrm{cs}(L_{i+1}/K)$ be

a subset with some density $\delta_K(S_i) = a_i \geqslant 0$ (one can choose S_i such that a_i is arbitrary small). Let $S := \bigcup_{i=1}^{\infty} S_i$. Then

$$\delta_{L_i}(S) = d_i \delta_K(S \cap \mathrm{cs}(L_i/K)) = d_i \sum_{m=i}^{\infty} a_m.$$

Notice however, that if we still choose the a_i above such that S is stable, but $\delta_{L_i}(S)$ never gets constant, it is still unclear, whether S is persistent or not (because of the freedom of choosing $S_0 \subseteq S$).

To find a set with $\delta_L(S) > 0$ for all $\mathscr{L}/L/K$, but S not stable, consider in the previous example numbers $a_i > 0$, such that $\sum_{m=i}^{\infty} a_m < \frac{1}{id_i}$, which is clearly possible (e.g. take $a_i \leqslant \frac{1}{2^i i d_i}$). This gives $0 < \delta_{L_i}(S) < \frac{1}{i}$. Since $\mathscr{L} = \bigcup_{i=1}^{\infty} L_i$, it is easy to see that $\delta_L(S) > 0$ for all finite $\mathscr{L}/L/K$. The constructed set does not satisfy part (iii) of Proposition 3.11, hence is not stable for $\mathscr{L}/K$.

3.5.5 Stable sets with $\mathbb{N}(S) = \{1\}$

Let $M/K/K_0$ be two finite Galois extensions of a number field K_0. Then the natural map $\mathrm{G}_{M/K_0} \to \mathrm{Aut}(\mathrm{G}_{M/K})$ induces an exterior action

$$\mathrm{G}_{K/K_0} \to \mathrm{Out}(\mathrm{G}_{M/K}),$$

thus inducing a natural action of G_{K/K_0} on the set of all conjugacy classes of $\mathrm{G}_{M/K}$. For any $g \in \mathrm{G}_{K/K_0}$ and $\sigma \in \mathrm{G}_{M/K}$, we choose a representative of the conjugacy class $g.C(\sigma; \mathrm{G}_{M/K})$ and denote it by $g.\sigma$. Further, G_{K/K_0} acts naturally on Σ_K, and we have

$$g.P_{M/K}(\sigma) = P_{M/K}(g.\sigma).$$

Let $K_0 = \mathbb{Q}$ and let $\sigma \in \mathrm{G}_{M/K}$ be an element, such that $C(\sigma; \mathrm{G}_{M/K})$ is not a fixed point of the action of $\mathrm{G}_{K/\mathbb{Q}}$. Let then

$$S := \mathrm{cs}(K/\mathbb{Q})_K \cap P_{M/K}(\sigma).$$

If $p \in \Sigma_{\mathbb{Q},f} \smallsetminus \mathrm{cs}(K/\mathbb{Q})$, then $S \cap S_p = \varnothing$. If $p \in \mathrm{cs}(K/\mathbb{Q})$ such that $S_p \cap S \neq \varnothing$, then the action of $g \in \mathrm{G}_{K/K_0}$, chosen such that $C(\sigma; \mathrm{G}_{M/K}) \neq C(g.\sigma; \mathrm{G}_{M/K})$, defines an isomorphism between the disjoint sets $S_p \cap P_{M/K}(\sigma)$ and $S_p \cap P_{M/K}(g.\sigma)$, hence the last of these two sets is non-empty. From this we obtain $S_p \nsubseteq S$. Thus $\mathbb{N}(S) = 1$. Moreover, if we choose σ such that the stabilizer of $C(\sigma; \mathrm{G}_{M/K})$ in $\mathrm{G}_{K/\mathbb{Q}}$ is trivial, then for any p the intersection $S_p \cap S$ is either empty or contains exactly one element.

Now we have to choose M in a way such that S is stable. This is easy: for example take M/K to be totally ramified in a fixed prime, which is (by definition of S) not contained in S. Then $K_S \cap M = K$, i.e., S is stable for K_S/K with stabilizing field K, as $\delta_K(\mathrm{cs}(K/\mathbb{Q})_K) = 1$ and hence $S \backsimeq P_{M/K}(\sigma)$.

4 Arithmetic applications

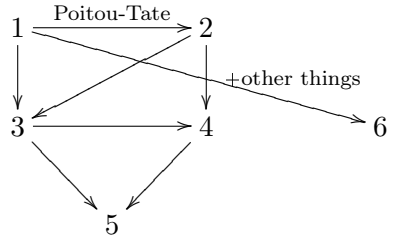
In this section we prove certain arithmetic results for stable sets. Most of them are generalizations of theorems shown in [NSW] Chapters IX and X for sets with density one to stable sets.

4.1 Overview

Our main result is Theorem 4.2, which is a Hasse principle for $Ш^1$. All other results in this section make an essential use of this theorem (along with other inputs). Here are the theorems we want to generalize.

1. Hasse principles
2. Grunwald-Wang theorem
3. Riemann's existence theorem
4. $\mathrm{cd}_p \mathrm{G}_S = \mathrm{scd}_p \mathrm{G}_S = 2$
5. algebraic $\mathrm{K}(\pi, 1)$-property
6. (a part of) the Neukirch Uchida theorem

Here is a rough scheme, how these statements depend on each other:



Essentially, in the pro-p case, 3 and 4 are equivalent to 5.

The two properties of a set S of primes of K, which deserve the most interest here, are the p-stability of S and the property $(*)_p^{\mathrm{stab}}$. Roughly speaking, p-stability is enough for some Hasse principles for $Ш^1$ and $(*)_p^{\mathrm{stab}}$ is necessary for all further results, such as Hasse principles for $Ш^2$, the Grunwald-Wang theorem with respect to the rational prime p, etc.

The properties "p-stable" and $(*)_p^{\mathrm{stab}}$ are still too strong for the results of this section, i.e., they can be weakened further, without changing the results. For example, let $\mathscr{L}/K$ be a Galois extension, A a trivial p-primary $\mathrm{G}_{\mathscr{L}/K}$-module and T a set of primes of K. Then to obtain the very basic Hasse principle $Ш^1(\mathscr{L}/K, T; A) = 0$, one can require (instead of p-stability of T for $\mathscr{L}/K$ with p-stabilizing field K, as in Theorem 4.2) the weaker condition that there is a subset $T_0 \subseteq T$ with $\delta_*(T_0) > 0$ in the tower $\mathscr{L}/K$ and such that there are no subextensions $\mathscr{L}/L'/L/K$ with $\frac{\delta_{L'}(T_0)}{\delta_L(T_0)} = p$. Thus we can pose the following question.

Question 4.1. What is the most general condition, for which the same results as for p-stable sets resp. sets satisfying $(*)_p^{\mathrm{stab}}$ hold? Are there counterexamples to the Grunwald-Wang theorem or even to the Riemann's existence theorem, among the sets, which do not satisfy this condition?

A positive answer to the second part of the question (it is by no means clear, whether one should expect it) could possibly provide examples of curves $\mathrm{Spec}\, \mathcal{O}_{K,S}$ which are not $\mathrm{K}(\pi, 1)$ for p (cf. Definition 5.2).

In Section 4.2 we prove our key result. In Sections 4.3,4.4 resp. 4.6 we apply it to obtain certain Hasse principles, the Grunwald-Wang theorem resp. Riemann's existence theorem for stable sets. In Section 4.5 we deal with the realization of local extensions by global ones. In Section 4.7 we consider the (strict) cohomological dimension of the groups $\mathrm{G}_{K,S}$ resp. $\mathrm{G}_{K,S}(p)$. Up to here we generalized results from [NSW] for density 1 sets to stable sets. Further, in Section 4.8 we prove a Hasse principle in dimension 2, which is needed in the anabelian setting in the Section 6 to prove the local correspondence. We must postpone this Hasse principle to Section 4.8 and do not prove it in Section 4.3, since the proof uses all results shown so far. Finally, in Section 4.9, we prove the finiteness of Shafarevich groups with divisible coefficients for stable sets.

4.2 Stable sets and $Ш^1$: key result

Let K be a number field and $\mathscr{L}/K$ a (possibly infinite) Galois extension with Galois group $\mathrm{G}_{\mathscr{L}/K}$. Let A be a finite $\mathrm{G}_{\mathscr{L}/K}$-module. Let $\mathfrak{p}$ be a prime of K and let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ to $\mathscr{L}$. Let

$$\mathscr{L}_{\mathfrak{P}} := \bigcup_{\mathscr{L}/K'/K \text{ finite}} K'_{\mathfrak{P}|_{K'}}.$$

Choose an algebraic closure $\overline{\mathscr{L}}_{\mathfrak{P}}$ of $\mathscr{L}_{\mathfrak{P}}$, which is also an algebraic closure of $K_{\mathfrak{p}}$. Then one has natural homomorphisms

$$\mathscr{G}_{\mathfrak{p}} := \mathrm{G}_{\overline{\mathscr{L}}_{\mathfrak{P}}/K_{\mathfrak{p}}} \twoheadrightarrow D_{\mathfrak{P},\mathscr{L}/K} \hookrightarrow \mathrm{G}_{\mathscr{L}/K},$$

giving A a natural structure of $\mathscr{G}_{\mathfrak{p}}$-module, and hence giving rise to a restriction homomorphism

$$\mathrm{res}^*_{\mathfrak{P},\mathscr{L}/K} \colon \mathrm{H}^*(\mathscr{L}/\mathrm{K}, \mathrm{A}) \to \mathrm{H}^*(\mathscr{G}_{\mathfrak{p}}, \mathrm{A}).$$

The group $\mathrm{H}^{\mathrm{i}}(\mathscr{G}_{\mathfrak{p}}, \mathrm{A})$ depends on the choice of $\mathfrak{P}$ over $\mathfrak{p}$ and on the choice of an algebraic closure of $\mathscr{L}_{\mathfrak{P}}$ only up to a canonical isomorphism: assume $\mathfrak{P}_1, \mathfrak{P}_2$ are two primes of $\mathscr{L}$ lying over $\mathfrak{p}$ and $\overline{\mathscr{L}}_{\mathfrak{P}_i}$ is some algebraic closure of $\mathscr{L}_{\mathfrak{P}_i}$ $(i = 1, 2)$. Then $\mathfrak{P}_1, \mathfrak{P}_2$ are conjugate over K, hence $\overline{\mathscr{L}}_{\mathfrak{P}_1}, \overline{\mathscr{L}}_{\mathfrak{P}_2}$ are isomorphic. Let γ_1, γ_2 be two isomorphisms of $\overline{\mathscr{L}}_{\mathfrak{P}_1}, \overline{\mathscr{L}}_{\mathfrak{P}_2}$ over $K_{\mathfrak{p}}$. Then homomorphisms induced by them in the cohomology are equal:

$$\gamma_1^* = \gamma_2^* \colon \mathrm{H}^*(\overline{\mathscr{L}}_{\mathfrak{P}_1}/\mathrm{K}_{\mathfrak{p}}, \mathrm{A}) \to \mathrm{H}^*(\overline{\mathscr{L}}_{\mathfrak{P}_2}/\mathrm{K}_{\mathfrak{p}}, \mathrm{A}),$$

since inner automorphisms act trivial on the cohomology (indeed, consider $\gamma_2^{-1}\gamma_1 \in \mathrm{G}_{\overline{\mathscr{L}}_{\mathfrak{P}_1}/K_{\mathfrak{p}}}$). It is immediate, that $\mathrm{res}^*_{\mathfrak{P}_1,\mathscr{L}/K}, \mathrm{res}^*_{\mathfrak{P}_2,\mathscr{L}/K}$ commute with this canonical isomorphism. From now on, we suppress the choice of the prime $\mathfrak{P}$ over $\mathfrak{p}$ and of the algebraic closure $\overline{\mathscr{L}}_{\mathfrak{P}}$ in our notation.

Let now T be a set of primes of K. Consider the **i-th Shafarevich group** with respect to T:

$$Ш^i(\mathscr{L}/K, T; A) := \ker(\mathrm{res}^i \colon \mathrm{H}^{\mathrm{i}}(\mathscr{L}/\mathrm{K}, \mathrm{A}) \to \prod_{\mathfrak{p} \in \mathrm{T}} \mathrm{H}^{\mathrm{i}}(\mathscr{G}_{\mathfrak{p}}, \mathrm{A})),$$

where $\mathscr{G}_{\mathfrak{p}} = \mathrm{G}_{K_{\mathfrak{p}}^{\mathrm{sep}}/K_{\mathfrak{p}}}$ is the local absolute Galois group. We denote by $K(A)$ the **trivializing extension** for A, i.e., the smallest field between K and $\mathscr{L}$, such that the subgroup $\mathrm{G}_{\mathscr{L}/K(A)}$ of

$\mathrm{G}_{\mathscr{L}/K}$ acts trivially on A. It is a finite Galois extension of K.

Let G be a finite group and A a G-module. Following [Ja], let $\mathrm{H}^{\mathrm{i}}_*(\mathrm{G},\mathrm{A})$ be defined by exactness of the following sequence:

$$0 \to \mathrm{H}^{\mathrm{i}}_*(\mathrm{G},\mathrm{A}) \to \mathrm{H}^{\mathrm{i}}(\mathrm{G},\mathrm{A}) \to \prod_{\substack{\mathrm{H}\subseteq\mathrm{G}\\ \text{cyclic}}} \mathrm{H}^{\mathrm{i}}(\mathrm{H},\mathrm{A}).$$

We have the following key result.

Theorem 4.2. *Let K be a number field, T a set of primes of K and $\mathscr{L}/K$ a Galois extension with Galois group G. Let A be a finite G-module. Assume that T is p-stable for $\mathscr{L}/K$, where p is the smallest prime divisor of $\sharp A$. Let L be a p-stabilizing field for T for $\mathscr{L}/K$. Then:*

$$Ш^1(\mathscr{L}/L, T; A) \subseteq \mathrm{H}^1_*(\mathrm{L}(\mathrm{A})/\mathrm{L},\mathrm{A}).$$

In particular, if $\mathrm{H}^1_*(\mathrm{L}(\mathrm{A})/\mathrm{L},\mathrm{A}) = 0$, then $Ш^1(\mathscr{L}/L, T; A) = 0$.

All results in the following make use of this theorem in a crucial way.

Lemma 4.3. *Let $\mathscr{L}/L/K$ be two Galois extensions of K and T a set of primes of K. Let A be a $\mathrm{G}_{\mathscr{L}/K}$-module, such that for any $\mathfrak{p} \in T$ one has $A^{\mathrm{G}_{\mathscr{L}/L}} = A^{D_{\mathfrak{p},\mathscr{L}/L}}$. Then there is an exact sequence*

$$0 \to Ш^1(L/K, T; A^{\mathrm{G}_{\mathscr{L}/L}}) \to Ш^1(\mathscr{L}/K, T; A) \to Ш^1(\mathscr{L}/L, T(L); A)$$

Proof. Recall that for a prime $\mathfrak{p}$ of K the set $S_{\mathfrak{p}}(L)$ consists of all primes lying over $\mathfrak{p}$ in L. Let $\mathfrak{P}$ be any extension of $\mathfrak{p}$ to L, and let $\tilde{\mathfrak{P}}$ be an extension of $\mathfrak{P}$ to $\mathscr{L}$. The sequence

$$0 \to \mathrm{H}^1(\mathrm{L}_{\mathfrak{P}}/\mathrm{K}_{\mathfrak{p}}, \mathrm{A}^{\mathrm{D}_{\mathfrak{P},\mathscr{L}/\mathrm{L}}}) \to \mathrm{H}^1(\mathscr{L}_{\tilde{\mathfrak{P}}}/\mathrm{K}_{\mathfrak{p}},\mathrm{A}) \to \mathrm{H}^1(\mathscr{L}_{\tilde{\mathfrak{P}}}/\mathrm{L}_{\mathfrak{P}},\mathrm{A}),$$

is exact and the right map does not depend on the choice of $\mathfrak{P}$ over $\mathfrak{p}$ (cf. the beginning of this section). Hence also the sequence

$$0 \to \mathrm{H}^1(\mathrm{L}_{\mathfrak{P}}/\mathrm{K}_{\mathfrak{p}}, \mathrm{A}^{\mathrm{D}_{\mathfrak{P},\mathscr{L}/\mathrm{L}}}) \to \mathrm{H}^1(\mathscr{L}_{\tilde{\mathfrak{P}}}/\mathrm{K}_{\mathfrak{p}},\mathrm{A}) \to \prod_{\mathfrak{Q}\in \mathrm{S}_{\mathfrak{p}}(\mathrm{L})} \mathrm{H}^1(\mathscr{L}_{\tilde{\mathfrak{Q}}}/\mathrm{L}_{\mathfrak{Q}},\mathrm{A}),$$

is exact, where the map on the right is the restriction into each component. Thus we obtain the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{H}^1(\mathrm{L}/\mathrm{K}, \mathrm{A}^{\mathrm{G}_{\mathscr{L}/\mathrm{L}}}) & \longrightarrow & \mathrm{H}^1(\mathscr{L}/\mathrm{K},\mathrm{A}) & \longrightarrow & \mathrm{H}^1(\mathscr{L}/\mathrm{L},\mathrm{A}) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \prod_{\mathfrak{p}\in T} \mathrm{H}^1(\mathrm{L}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}}, \mathrm{A}^{\mathrm{D}_{\mathfrak{p},\mathscr{L}/\mathrm{L}}}) & \longrightarrow & \prod_{\mathfrak{p}\in T} \mathrm{H}^1(\mathscr{L}_{\mathfrak{p}}/\mathrm{K}_{\mathfrak{p}},\mathrm{A}) & \longrightarrow & \prod_{\mathfrak{p}\in T(L)} \mathrm{H}^1(\mathscr{L}_{\mathfrak{p}}/\mathrm{L}_{\mathfrak{p}},\mathrm{A}).
\end{array}$$

The lemma follows by taking kernels of the vertical maps. □

Lemma 4.4. *Let L/K be a finite Galois extension, T a set of primes of K, and A a finite $\mathrm{G}_{L/K}$-module. Assume that T is p-stable for L/K with p-stabilizing field K, where p is the smallest prime divisor of $\sharp A$. Then*

$$Ш^i(L/K, T; A) \subseteq \mathrm{H}^{\mathrm{i}}_*(\mathrm{L}/\mathrm{K},\mathrm{A}).$$

Proof. We can assume that A is p-primary. Indeed, decompose A into ℓ-primary components, and observe that any p-stable set is ℓ-stable for any $\ell \geqslant p$. We have to show that any cyclic p-subgroup of $\mathrm{G}_{L/K}$ is a decomposition subgroup of a prime in T. This is content of the next lemma. □

Lemma 4.5. *Let L/K be a finite Galois extension, T a set of primes of K and p a rational prime, such that T is p-stable for L/K with p-stabilizing field K. Then any cyclic p-subgroup of $\mathrm{G}_{L/K}$ is the decomposition group of a prime in T.*

Notice that this shows automatically that there are infinitely many primes in T, for which the given cyclic group is a decomposition group.

Proof. Assume that the cyclic p-subgroup $H \subseteq \mathrm{G}_{L/K}$ is not a decomposition group of a prime in T. Let $pH \subseteq H$ be the subgroup of index p. Then one computes directly $m_{pH}(\sigma) = pm_H(\sigma)$ for any $\sigma \in pH$. Since H is not a decomposition subgroup of a prime $\mathfrak{p} \in T$, no generator of H is a Frobenius at T, i.e., $P_{L/K}(\sigma) \cap T = \varnothing$ for any $\sigma \in H \smallsetminus pH$. By p-stability of T, there is a subset $T_0 \subseteq T$ and an $a > 0$, such that $pa > \delta_{L'}(T_0) \geqslant a$ for all $L/L'/K$. Let $L_0 = L^H$ and $L_1 = L^{pH}$. Then

$$\begin{aligned}
\delta_{L_0}(T_0) &= \sum_{\sigma \in H} m_H(\sigma)\delta_K(P_{L/K}(\sigma) \cap T_0) \\
&= \sum_{\sigma \in pH} m_H(\sigma)\delta_K(P_{L/K}(\sigma) \cap T_0) \\
&= p^{-1} \sum_{\sigma \in pH} m_{pH}(\sigma)\delta_K(P_{L/K}(\sigma) \cap T_0) \\
&= p^{-1}\delta_{L_1}(T_0).
\end{aligned}$$

This contradicts our assumption on T_0.

□

Proof of the theorem. We can assume $L = K$. By applying Lemma 4.3 to $\mathscr{L}/K(A)/K$ and using Lemma 4.4, we are reduced to showing that if A is a trivial G-module, then $Ш^1(\mathscr{L}/K, T; A) = 0$. Let $T_0 \subseteq T$ and $a > 0$ be such that $pa > \delta_{L'}(T_0) \geqslant a$ for all $\mathscr{L}/L'/L$. Let G^T be the quotient of G, corresponding to the maximal subextension of $\mathscr{L}/K$, which is completely split in T. We have then

$$Ш^1(\mathscr{L}/K, T; A) = \ker(\mathrm{Hom}(G, A) \to \prod_{\mathfrak{p} \in T} \mathrm{Hom}(\mathscr{G}_\mathfrak{p}, A)) = \mathrm{Hom}(G^T, A).$$

If $0 \neq \phi \in \mathrm{Hom}(G^T, A)$, then $M := \mathscr{L}^{\ker(\phi)}/K$ is a finite extension inside $\mathscr{L}/K$ with Galois group $\mathrm{im}(\phi) \neq 0$ and completely decomposed in T, and in particular in T_0. Thus

$$pa > \delta_M(T_0) = [M : K]\delta_K(T_0 \cap \mathrm{cs}(M/K)) = \sharp\mathrm{im}(\phi)\delta_K(T_0) \geqslant pa,$$

since $\delta_K(T_0) \geqslant a$. This is a contradiction, and hence we obtain

$$Ш^1(\mathscr{L}/K, T; A) = \mathrm{Hom}(G^T, A) = 0.$$

This finishes the proof. □

4.3 Some Hasse principles

Now we give first applications of Theorem 4.2. Consider the case $\mathscr{L} = K_S$, where S is some further set of primes of K. Then we have the usual Shafarevich group (A is a $\mathrm{G}_{K,S}$-module and T is a set of prime of K, not necessarily contained in S):

$$Ш^i(K_S/K, T; A) := \ker(\mathrm{res}^i \colon \mathrm{H^i(K_S/K, A)} \to \prod_{\mathfrak{p}\in T} \mathrm{H^i}(\mathscr{G}_\mathfrak{p}, \mathrm{A})).$$

If $S = T$, we also write $Ш^i(K_S/K; A)$ instead of $Ш^i(K_S/K, S; A)$. The Hasse principle for A (in the i-th dimension, with respect to S and T) is said to be satisfied, if

$$Ш^i(K_S/K, T; A) = 0.$$

Various conditions on S, T, A which imply the Hasse principle in dimensions 1 and 2 are considered in [NSW] chapter IX, §1. We prove a generalization for stable sets.

Corollary 4.6. *Let K be a number field, T, S sets of primes of K, A a finite $\mathrm{G}_{K,S}$-module. Assume that T is p-stable for K_S/K, where p is the smallest prime divisor of $\sharp A$. Let L_0 be a p-stabilizing field for T for K_S/K, which trivializes A. Then*

$$Ш^1(K_S/L, T; A) = 0$$

for any finite $K_S/L/L_0$.

Proof. Since L_0 is a p-stabilizing field which trivializes A, any L lying between K_S/L_0 is too. Thus the corollary follows immediately from Theorem 4.2. □

Let $\mathfrak{c}$ be a full class of finite groups, in the sense of [NSW] 3.5.2. Let $K_S(\mathfrak{c})/K$ denote the maximal pro-$\mathfrak{c}$-extension of K in K_S, and $\mathrm{G}_{K,S}(\mathfrak{c})$ its Galois group over K, i.e., the maximal pro-$\mathfrak{c}$-quotient of $\mathrm{G}_{K,S}$. We have the pro-$\mathfrak{c}$-version of Corollary 4.6:

Corollary 4.7. *Let $\mathfrak{c}$ be a full class of finite groups, K a number field, T, S sets of primes of K, A a finite $\mathrm{G}_{K,S}(\mathfrak{c})$-module. Assume that T is p-stable for $K_S(\mathfrak{c})/K$, where p is the smallest prime divisor of $\sharp A$. Let L_0 be a p-stabilizing field for T for $K_S(\mathfrak{c})/K$, which trivializes A. Then*

$$Ш^1(K_S(\mathfrak{c})/L, T; A) = 0$$

for any finite $K_S(\mathfrak{c})/L/L_0$.

A further consequence of Theorem 4.2 is Corollary 4.9 below, which is, besides Poitou-Tate duality, the key ingredient in the Grunwald-Wang theorem for stable sets. Before stating it, we recall from [NSW] 9.1.5, 9.1.7 the definitions of the special cases:

Definition 4.8. Let k be a field, $n = 2^r n'$ be a natural number prime to $\mathrm{char}(k)$ with n' odd.

(i) We say that we are in the **special case** (k, n), if $r \geqslant 2$ and -1 is in the image of the cyclotomic character $\chi_{\mathrm{cycl}} \colon \mathrm{G}_{k(\mu_{2^r})/k} \to (\mathbb{Z}/2^r\mathbb{Z})^*$.

(ii) Let further T be a set of primes of k. We say that we are in the **special case** (k, n, T), if we are in the special case (k, n) and all primes $\mathfrak{p} \in T$ decompose in $k(\mu_{2^r})/k$.

Corollary 4.9. *Let K be a number field, $S \supseteq S_\infty$ a set of primes, $n \in \mathbb{N}(S)$ and let p be the smallest prime divisor of n. Let T be a further set of primes of K, which is p-stable for K_S/K, and let L_0 be a p-stabilizing field for T for K_S/K. Then*

$$Ш^1(K_S/L, T; \mu_n) = 0$$

for any finite $K_S/L/L_0$, such that we are not in the special case (L, n, T). In the special case (L, n, T) we have $Ш^1(K_S/L, T; \mu_n) = \mathbb{Z}/2\mathbb{Z}$.

Before proving this, we quote the following proposition:

Proposition 4.10 ([NSW] 9.1.6)**.** *Let p be a prime, $r \in \mathbb{N}$ and let k be any field with $\mathrm{char}(k) \neq p$. Then*

$$\hat{\mathrm{H}}^i(k(\mu_{p^r})/k, \mu_{p^r}) = 0 \qquad \text{for all } i \in \mathbb{Z},$$

except, when $p = 2$, $r \geqslant 2$ and we are in the special case $(k, 2^r)$. In this case

$$\hat{\mathrm{H}}^i(k(\mu_{2^r})/k, \mu_{2^r}) = \mathbb{Z}/2\mathbb{Z} \qquad \text{for all } i \in \mathbb{Z}.$$

Let $p = 2$, $r \geqslant 2$. Then the special case $(k, 2^r)$ occurs if and only if

$$\mathrm{char}(k) = 0 \text{ and } \mathbb{Q}(\mu_{2^r}) \cap k \text{ is real,}$$
$$\text{or } \mathrm{char}(k) = \ell \equiv -1 \mod 2^r \text{ and } \mathbb{F}_\ell(\mu_{2^r}) \cap k = \mathbb{F}_\ell.$$

Proof of Corollary 4.9. We can assume $n = p^r$. If we are not in the special case (L, p^r), Proposition 4.10 implies $\mathrm{H}^1(\mathrm{L}(\mu_{\mathrm{p^r}})/\mathrm{L}, \mu_{\mathrm{p^r}}) = 0$, i.e., we are done by Theorem 4.2. Assume we are in the special case (L, p^r). In particular, $p = 2$. Then $\mathrm{H}^1(\mathrm{L}(\mu_{2^{\mathrm{r}}})/\mathrm{L}, \mu_{2^{\mathrm{r}}}) = \mathbb{Z}/2\mathbb{Z}$. Since

$$Ш^1(K_S/L(\mu_{2^r}), T; \mu_{2^r}) = 0$$

by Theorem 4.2, we see from Lemma 4.3

$$Ш^1(K_S/L, T; \mu_{2^r}) = Ш^1(L(\mu_{2^r})/L, T; \mu_{2^r}).$$

If there is a prime $\mathfrak{p} \in T(L)$, which is not decomposed in $L(\mu_{2^r})/L$, then $\mathrm{G}_{L(\mu_{2^r})/L} = \mathrm{G}_{L_\mathfrak{p}(\mu_{2^r})/L_\mathfrak{p}}$, and hence $Ш^1(L(\mu_{2^r})/L, T; \mu_{2^r}) = 0$. Otherwise, we are in the special case $(L, 2^r, T)$ and for any $\mathfrak{p} \in T(L)$, the restriction homomorphism

$$\mathbb{Z}/2\mathbb{Z} \cong \mathrm{H}^1(\mathrm{L}(\mu_{2^{\mathrm{r}}})/\mathrm{L}, \mu_{2^{\mathrm{r}}}) \to \mathrm{H}^1(\mathrm{L}_\mathfrak{p}(\mu_{2^{\mathrm{r}}})/\mathrm{L}_\mathfrak{p}, \mu_{2^{\mathrm{r}}})$$

is zero, as the argument in the proof of [NSW] 9.1.9(ii) shows. Hence in this case one obtains $Ш^1(L(\mu_{2^r})/L, T; \mu_{2^r}) \cong \mathbb{Z}/2\mathbb{Z}$. □

Now we turn to $Ш^2$. For a $\mathrm{G}_{K,S}$-module A, such that $\sharp A \in \mathbb{N}(S)$, we denote by

$$A' := \mathrm{Hom}(A, \mathcal{O}^*_{K_S,S})$$

the dual of A. As in [NSW] 9.1.10, we obtain the following corollary.

Corollary 4.11. *Let K be a number field, $S \supseteq S_\infty$ a set of primes of K, A a finite $\mathrm{G}_{K,S}$-module with $\sharp A \in \mathbb{N}(S)$. Assume that S is p-stable (i.e., p-stable for K_S/K), where p is the smallest prime divisor of $\sharp A$. Let L be a p-stabilizing field for S for K_S/K, such that $\mathrm{H}^1_*(\mathrm{L}(\mathrm{A}')/\mathrm{L}, \mathrm{A}') = 0$. Then*

$$Ш^2(K_S/L; A) = 0.$$

In particular:

(i) If A' is trivial $\mathrm{G}_{K,S}$-module, then $Ш^2(K_S/L; A) = 0$ for all fields L, which are p-stabilizing for S.

(ii) Let $n \in \mathbb{N}(S)$ with smallest prime divisor p. If L is a p-stabilizing field for S and we are not in the special case (L, n, S), then $Ш^2(K_S/L, \mathbb{Z}/n\mathbb{Z}) = 0$. In the special case, we have $Ш^2(K_S/L; \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$.

Remark 4.12. The condition $\sharp A \in \mathbb{N}(S)$ is not necessary if A is trivial: we postpone the proof of this until all necessary ingredients (in particular Grunwald-Wang theorem, Riemann's existence theorem and $\mathrm{cd}_p \mathrm{G}_{K,S} = 2$) are proven. Cf. Proposition 4.34.

Proof. By Poitou-Tate duality (this is the reason, why we need $S \supseteq S_\infty$ and $\sharp A \in \mathbb{N}(S)$) we have:

$$Ш^2(K_S/L, A) \cong Ш^1(K_S/L, A')^\vee,$$

where $X^\vee := \mathrm{Hom}(X, \mathbb{R}/\mathbb{Z})$ is the Pontrjagin dual. An application of Theorem 4.2 to K_S/K, the sets $S = T$ and the module A' gives the desired result. (i) and (ii) follow from Corollaries 4.6 and 4.9 respectively. □

4.4 On the Grunwald-Wang theorem

In this section we consider the cokernel of the global-to-local restriction homomorphism

$$\mathrm{coker}^i(K_S/K, T; A) := \mathrm{coker}(\mathrm{res}^i \colon \mathrm{H}^i(\mathrm{K_S/K}, \mathrm{A}) \to \prod\nolimits'_{\mathfrak{p} \in \mathrm{T}} \mathrm{H}^i(\mathscr{G}_\mathfrak{p}, \mathrm{A})),$$

where A is a finite $\mathrm{G}_{K,S}$-module and $T \subseteq S$. If A is a trivial $\mathrm{G}_{K,S}$-module, then the vanishing of this cokernel is equivalent to the existence of global extensions unramified outside S, which realize given local extensions at primes in T. If S has density 1, the set T is finite, A is constant and we are not in a special case, this vanishing is essentially the statement of the Grunwald-Wang theorem. Certain conditions on S, T, A, under which this cokernel vanishes are considered in [NSW] chapter IX §2. All of them require S to have certain minimal density. We prove analogous results for stable resp. persistent sets.

Corollary 4.13. *Let K be a number field, $T \subseteq S$ sets of primes of K with $S_\infty \subseteq S$. Let A be a finite $\mathrm{G}_{K,S}$-module with $\sharp A \in \mathbb{N}(S)$. Assume that T is finite and S is p-stable, where p is the smallest prime divisor of $\sharp A$. For any p-stabilizing field L for S for K_S/K, such that $\mathrm{H}^1_*(\mathrm{L}(\mathrm{A}')/\mathrm{L}, \mathrm{A}') = 0$, we have:*

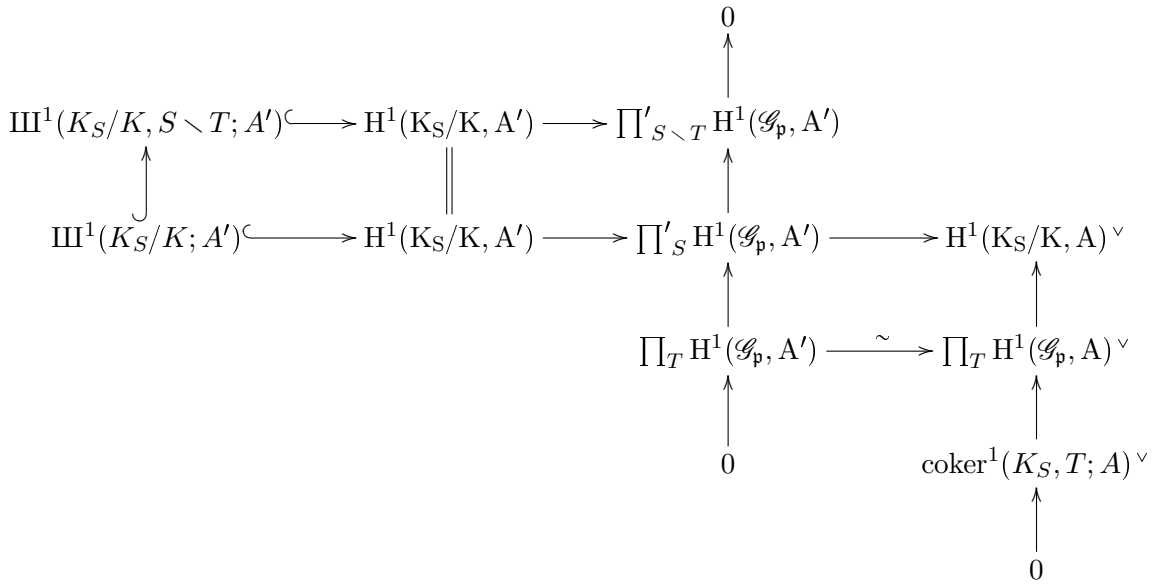
$$\mathrm{coker}^1(K_S/L, T; A) = 0.$$

First we reprove the following lemma:

Lemma 4.14 ([NSW] 9.2.2)**.** *Let K be a number field and S a set of primes of K. Assume $S_\infty \subseteq S$ and $\sharp A \in \mathbb{N}(S)$. For any finite subextension $K_S/L/K$ and any finite subset $T \subseteq S$, there is an exact sequence*

$$0 \to Ш^1(K_S/L; A') \to Ш^1(K_S/L, S \smallsetminus T; A') \to \mathrm{coker}^1(K_S/L, T; A)^\vee \to 0.$$

Proof of the lemma. Since $L_S = K_S$, we can assume $L = K$. We have the following commutative exact diagram:



where $\prod'$ denotes the restricted product, with respect to the unramified cohomology subgroups $\mathrm{H}^*_{\mathrm{nr}}(\mathscr{G}_\mathfrak{p}, \cdot)$. The two horizontal arrows on the right are given by Poitou-Tate and local duality theorems. All other arrows follow from the definitions. Now the claim follows from the snake lemma, applied to the second and the third columns in the diagram (the second column has to be extended by zeros).

□

Proof of the Corollary 4.13. Since T is finite and S is p-stable for K_S/K, $S \smallsetminus T$ also is p-stable for K_S/K, and the p-stabilizing fields for S and $S \smallsetminus T$ are equal. Let L be as in the corollary. By Theorem 4.2, applied to K_S/L, $S \smallsetminus T$ and A', we obtain $Ш^1(K_S/L, S \smallsetminus T; A') = 0$. Then Lemma 4.14 implies $\mathrm{coker}^1(K_S/L, T; A) = 0$. □

Now we give a generalization of [NSW] 9.2.7.

Theorem 4.15. *Let K be a number field, S a set of primes of K. Let $T_0, T \subseteq S$ be two disjoint subsets, such that T_0 is finite. Let p be a rational prime and $r > 0$ an integer. Assume $S \smallsetminus T$ is p-stable for $K_{S \cup S_p \cup S_\infty}/K$ with p-stabilizing field L_0, which is contained in K_S. Then for any finite $K_S/L/L_0$, such that we are not in the special case $(L, p^r, S \smallsetminus (T_0 \cup T))$, the canonical map*

$$\mathrm{H}^1(\mathrm{K_S/L}, \mathbb{Z}/\mathrm{p^r}\mathbb{Z}) \to \bigoplus_{\mathfrak{p} \in \mathrm{T_0(L)}} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}, \mathbb{Z}/\mathrm{p^r}\mathbb{Z}) \oplus \bigoplus_{\mathfrak{p} \in \mathrm{T(L)}} \mathrm{H}^1(\mathscr{I}_\mathfrak{p}, \mathbb{Z}/\mathrm{p^r}\mathbb{Z})^{\mathscr{G}_\mathfrak{p}}$$

is surjective, where $\mathscr{I}_\mathfrak{p} \subseteq \mathscr{G}_\mathfrak{p} = \mathrm{G}_{K_\mathfrak{p}^{\mathrm{sep}}/L_\mathfrak{p}}$ *is the inertia subgroup. If we are in the special case* $(L, p^r, S \smallsetminus (T_0 \cup T))$*, then* $p = 2$ *and the cokernel of this map is of order 1 or 2.*

Remarks 4.16.

(i) Observe that if $\delta_K(T) = 0$, the condition "$S \smallsetminus T$ is p-stable for $K_{S \cup S_p \cup S_\infty}/K$ with a p-stabilizing field contained in K_S" is equivalent to "S stable and satisfies $(*)_p^{\mathrm{stab}}$".

(ii) If $\delta_K(S) = 1$ and $\delta_K(T) = 0$, then $L_0 = K$ is a persisting field for $S \smallsetminus T$ for any $\mathscr{L}/K$ and the condition in the theorem is automatically satisfied. Thus our result is a generalization of [NSW] 9.2.7.

(iii) To show that Theorem 4.15 is a proper generalization of [NSW] 9.2.7, we give the following example. Let $N/M/K$ be finite Galois extensions of K, such that N/K (and hence also M/K) is totally ramified in a non-archimedean prime $\mathfrak{p}$ of K, lying over the rational prime ℓ. Let $\sigma \in \mathrm{G}_{M/K}$ and let $\tilde{\sigma} \in \mathrm{G}_{N/K}$ be a preimage of σ. Let $S \supseteq T$ be such that

- $S \backsimeq P_{M/K}(\sigma)$,
- $\mathfrak{p} \notin S$ and
- $T \backsimeq P_{M/K}(\sigma) \smallsetminus P_{N/K}(\tilde{\sigma})$.

Then $S \smallsetminus T \backsimeq P_{N/K}(\tilde{\sigma})$ is persistent for $K_{S \cup S_p \cup S_\infty}/K$ for any $p \neq \ell$, and moreover K is a persisting field (indeed, this follows from $K_{S \cup S_p \cup S_\infty} \cap N = K$). Hence the sets $S \supseteq T$ satisfies the conditions of the theorem with respect to each $p \neq \ell$. Observe that in this example T is itself persistent $K_{S \cup S_p \cup S_\infty}/K$, with persisting field contained in K_S. In [NSW] 9.2.7, the set T must have density zero.

Proof. We omit $\mathbb{Z}/p^r\mathbb{Z}$ coefficients from the notation. Let L_0 be as in the theorem. Let $K_S/L/L_0$ be a finite subextension, and $S_0 \subseteq S \smallsetminus T$ a subset, such that there is an $a > 0$ for which $pa > \delta_M(S_0) \geqslant a$ holds for any finite $K_{S \cup S_p \cup S_\infty}/M/L$. Since T_0 is finite, we can assume $S_0 \cap T_0 = \varnothing$. We follows the same steps as in the proof of [NSW] 9.2.7. The unique non-trivial extension of archimedean local fields is totally ramified, hence $\mathrm{H}^1(\mathscr{G}_\mathfrak{p}) = \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}}$ for archimedean primes. For all non-archimedean primes $\mathfrak{p}$, the group $\mathscr{G}_\mathfrak{p}/\mathscr{I}_\mathfrak{p} \cong \hat{\mathbb{Z}}$ is of cohomological dimension one, and Hochschild-Serre spectral sequence shows the surjectivity of the natural map $\mathrm{H}^1(\mathscr{G}_\mathfrak{p}) \twoheadrightarrow \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}}$. Thus we can move the finitely many primes of $T \cap (S_p \cup S_\infty)$ to T_0, and thus assume $T \cap (S_p \cup S_\infty) = \varnothing$. We first treat the

Case $S \supseteq S_p \cup S_\infty$. Let $T_1 \subseteq T$ be a finite subset. $S \smallsetminus T$ is p-stable for K_S/L with p-stabilizing field L, hence the same is true for the subextension $L_{(S \smallsetminus T) \cup T_1}/L$.

We claim that $\mathrm{coker}^1(L_{(S \smallsetminus T) \cup T_1}/L, T_1 \cup T_0; \mathbb{Z}/p^r\mathbb{Z}) = 0$, i.e., the localization map

$$\mathrm{H}^1(\mathrm{L}_{(\mathrm{S} \smallsetminus \mathrm{T}) \cup \mathrm{T}_1}/\mathrm{L}) \to \bigoplus_{\mathfrak{p} \in \mathrm{T}_0 \cup \mathrm{T}_1} \mathrm{H}^1(\mathscr{G}_\mathfrak{p})$$

is surjective, if we are not in the special case $(L, p^r, S \smallsetminus (T_0 \cup T_1))$, and is of order 2 in the special case. Indeed, Corollary 4.9 implies

$$Ш^1(L_{(S \smallsetminus T) \cup T_1}/L, S \smallsetminus (T \cup T_0); \mu_{p^r}) = 0$$

if we are not in the special case, since L is a p-stabilizing field field for $S \setminus (T \cup T_0)$ for $L_{(S \setminus T) \cup T_1}/L$ (resp. $Ш^1(L_{(S \setminus T) \cup T_1}/L, S \setminus (T_0 \cup T); \mu_{p^r}) \cong \mathbb{Z}/2\mathbb{Z}$ if we are in the special case) and Lemma 4.14 implies the claim.

Since the map $\mathrm{H}^1(\mathscr{G}_\mathfrak{p}) \twoheadrightarrow \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}}$ is surjective, the natural map

$$\mathrm{H}^1(\mathrm{L}_{(\mathrm{S} \setminus \mathrm{T}) \cup \mathrm{T}_1}/\mathrm{L}) \to \bigoplus_{\mathfrak{p} \in \mathrm{T}_0} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}) \oplus \bigoplus_{\mathfrak{p} \in \mathrm{T}_1} \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}}$$

is also surjective if we are not in the special case (resp. has cokernel of order 1 or 2 otherwise). For $T_1 \subseteq T_2 \subseteq T$ we obtain a commutative diagram, where the vertical arrows are the inflation maps:

$$\begin{array}{ccc} \mathrm{H}^1(\mathrm{L}_{(\mathrm{S} \setminus \mathrm{T}) \cup \mathrm{T}_2}/\mathrm{L}) & \longrightarrow & \bigoplus_{T_0} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}) \oplus \bigoplus_{\mathrm{T}_2} \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}} \\ \uparrow & & \uparrow \\ \mathrm{H}^1(\mathrm{L}_{(\mathrm{S} \setminus \mathrm{T}) \cup \mathrm{T}_1}/\mathrm{L}) & \longrightarrow & \bigoplus_{T_0} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}) \oplus \bigoplus_{\mathrm{T}_1} \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}} \end{array}$$

Passing to the direct limit over all finite $T_1 \subseteq T$ we obtain the claim of the theorem.

General case. Let $V = (S_p \cup S_\infty) \setminus S$. By assumption, $S \setminus T$ is p-stable for $K_{S \cup V}/L$ with p-stabilizing field L. In particular, the assumptions of the theorem are satisfied for the extension $K_{S \cup V} = L_{S \cup V}/L$, and sets $T_0 \cup V, T \subseteq S \cup V$. Then the already proven case implies that the map

$$\mathrm{H}^1(\mathrm{L}_{\mathrm{S} \cup \mathrm{V}}/\mathrm{L}) \to \bigoplus_{\mathrm{T}_0 \cup \mathrm{V}} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}) \oplus \bigoplus_{\mathrm{T}} \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}}$$

is surjective (resp. has cokernel of order 1 or 2 in the special case). Since $L \subseteq K_S$, we have $L_S = K_S$ and since any class $\alpha \in \mathrm{H}^1(\mathrm{L}_{\mathrm{S} \cup \mathrm{V}}/\mathrm{L})$ for which $\alpha_\mathfrak{p} \in \mathrm{H}^1_{\mathrm{nr}}(\mathscr{G}_\mathfrak{p})$ for all $\mathfrak{p} \in V$, lies already in $\mathrm{H}^1(\mathrm{L}_\mathrm{S}/\mathrm{L}) = \mathrm{H}^1(\mathrm{K}_\mathrm{S}/\mathrm{L})$, we obtain the same statement for the map

$$\mathrm{H}^1(\mathrm{K}_\mathrm{S}/\mathrm{L}) \to \bigoplus_{\mathrm{T}_0} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}) \oplus \bigoplus_{\mathrm{V}} \mathrm{H}^1_{\mathrm{nr}}(\mathscr{G}_\mathfrak{p}) \oplus \bigoplus_{\mathrm{T}} \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}}.$$

This finishes the proof.

□

From this we obtain the following form of the Grunwald-Wang theorem. The proof is the same as in [NSW] 9.2.8.

Corollary 4.17. *Let $T \subseteq S$ be sets of primes of a number field K. Let A be a finite abelian group. Assume that T is finite and that for any prime divisor p of $\sharp A$, S is p-stable for $K_{S \cup S_p \cup S_\infty}/K$ with stabilizing field K. For all $\mathfrak{p} \in T$, let $L_\mathfrak{p}/K_\mathfrak{p}$ be a finite abelian extension, such that its Galois group can be embedded into A. Assume that we are not in the special case $(K, \exp(A), S \setminus T)$. Then there exists a global abelian extension L/K with Galois group A, unramified outside S, such that L has completion $L_\mathfrak{p}$ at $\mathfrak{p} \in T$.*

Finally, we have two corollaries generalizing [NSW] 9.2.4 and 9.2.9 to stable sets.

Corollary 4.18. *Let K be a number field, $T \subseteq S$ sets of primes of K with T finite. Let $K_S/L/K$ be a finite Galois subextension with Galois group G. Let p be a prime and $A = \mathbb{F}_p[G]^n$ a $\mathrm{G}_{K,S}$-module. Assume S is p-stable for $K_{S \cup S_p \cup S_\infty}/K$ with p-stabilizing field L. Then the restriction map*

$$\mathrm{H}^1(\mathrm{K_S/K, A}) \to \bigoplus_{\mathfrak{p}\in \mathrm{T}} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}, \mathrm{A})$$

is surjective.

Proof (cf. [NSW] 9.2.4). We have the commutative diagram, in which the vertical maps are Shapiro-isomorphisms:

$$\begin{array}{ccc} \mathrm{H}^1(\mathrm{K_S/K, A}) & \longrightarrow & \bigoplus_{\mathfrak{p}\in T} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}, \mathrm{A}) \\ \downarrow \sim & & \downarrow \sim \\ \mathrm{H}^1(\mathrm{K_S/L}, \mathbb{F}_\mathrm{p}^\mathrm{n}) & \longrightarrow & \bigoplus_{\mathfrak{P}\in T(L)} \mathrm{H}^1(\mathscr{G}_\mathfrak{P}, \mathbb{F}_\mathrm{p}^\mathrm{n}) \end{array}$$

The lower map is surjective by Theorem 4.15, and so is the upper. □

Corollary 4.19. *Let K be number field, S a set of primes of K. Let $K_S/L/K$ be a finite Galois subextension with Galois group G. Let p be a prime and $A = \mathbb{F}_p[G]^n$ a $\mathrm{G}_{K,S}$-module. Assume that S is p-stable for $K_{S\cup S_p\cup S_\infty}/L$ with p-stabilizing field L. Then the embedding problem*

$$\begin{array}{ccccccccc} & & & & & & \mathrm{G}_{K,S} & & \\ & & & & & & \downarrow & & \\ 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

is properly solvable.

Proof (cf. [NSW] 9.2.9). We have $\mathrm{H}^2(\mathrm{G, A}) = 0$, and hence the sequence in the lemma is split. In particular, the embedding problem is solvable (cf. also [NSW] 3.5.9). Let $\psi_0\colon \mathrm{G}_{K,S} \to E$ denote a solution. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathrm{cs}(L/K) \cap S$ (observe that $\mathrm{cs}(L/K) \cap S$ has positive density and, in particular, is infinite) be primes of K and let $\phi_i\colon \mathscr{G}_{\mathfrak{p}_i} \to A$ be homomorphisms, the images of which generate A. By Corollary 4.18, the restriction homomorphism

$$\mathrm{H}^1(\mathrm{K_S/K, A}) \to \bigoplus_{\mathrm{i}=1}^{\mathrm{r}} \mathrm{H}^1(\mathscr{G}_{\mathfrak{p}_\mathrm{i}}, \mathrm{A})$$

is surjective. Let $\phi \in \mathrm{H}^1(\mathrm{K_S/K, A})$ be a preimage of $(\phi_i - \psi_0|_{G_{\mathfrak{p}_i}})_{i=1}^r$. Then

$$\psi := \phi \cdot \psi_0\colon \mathrm{G}_{K,S} \to E,$$

defined by $\psi(g) = \phi(g)\psi_0(g)$ (cf. [NSW] 3.5.11) is a proper solution of the embedding problem. □

4.5 Realizing local extensions

If $\mathfrak{p}$ is any prime of K, one can ask, how big the local extensions $(K_S)_\mathfrak{p}/K_\mathfrak{p}$ and $(K_S(p))_\mathfrak{p}/K_\mathfrak{p}$ are. Motivated by the treatment in [NSW] 9.4.3, we study these questions in the case, when S is stable. If $R \subseteq S$ is a subset, we write K_S^R for the maximal subextension of K_S/K, which is completely split in R and $K_S^R(p)$ for the maximal pro-p-subextension of K_S^R/K. The next proposition is a generalization of [NSW] 10.5.9.

Proposition 4.20. *Let K be a number field, $R \subseteq S$ sets of primes of K, p a rational prime. Assume R is finite and S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ and has a p-stabilizing extension contained in $K_S^R(p)$. Then*

$$(K_S^R(p))_{\mathfrak{p}} = \begin{cases} K_{\mathfrak{p}}(p) & \text{if } \mathfrak{p} \in S \smallsetminus R, \\ K_{\mathfrak{p}} & \text{if } \mathfrak{p} \in R. \end{cases}$$

If, moreover, $\mathfrak{p} \notin S$ and S is p-stable for $K_{S\cup S_p\cup S_\infty\cup\{\mathfrak{p}\}}/K$ with a p-stabilizing field contained in $K_S^R(p)$, then also

$$(K_S^R(p))_{\mathfrak{p}} = K_{\mathfrak{p}}^{\mathrm{nr}}(p).$$

Proof. For $\mathfrak{p} \in R$ there is nothing to prove. Let $L_0 \subseteq K_S^R(p)$ be a p-stabilizing field for S for $K_{S\cup S_p\cup S_\infty}/K$. By Theorem 4.15, for each finite subset $T \subseteq S \smallsetminus R$ and each finite subextension $K_S^R(p)/L/L_0$, the restriction map

$$\mathrm{H}^1(\mathrm{K_S^R(p)/L}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \to \bigoplus_{\mathrm{T(L)}} \mathrm{H}^1(\mathrm{L_{\mathfrak{p}}}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$$

is surjective (since $\mathrm{H}^1(\mathrm{K_S^R(p)/L}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) = \mathrm{H}^1(\mathrm{K_S^R/L}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$). For $\mathfrak{p} \in S \smallsetminus R$ and $T = \{\mathfrak{p}\}$, this means that we can realize any local class $\alpha_{\mathfrak{p}} \in \mathrm{H}^1(\mathrm{L_{\mathfrak{p}}}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$ by an element $\alpha \in \mathrm{H}^1(\mathrm{K_S^R(p)/L}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$. This means that the field $K_S^R(p)_{\mathfrak{p}}$ has no p-extensions, and hence is equal to $K_{\mathfrak{p}}(p)$. The proof in the case $\mathfrak{p} \notin S$ is similar. □

Corollary 4.21. *Let K be a number field, $R \subseteq S$ sets of primes of K, p a rational prime. Assume R is finite and S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ and has a p-stabilizing extension contained in K_S^R (if $R = \varnothing$, then this condition is equivalent to "S is stable and satisfies $(*)_p^{\mathrm{stab}}$"). Then for any $\mathfrak{p} \in S \smallsetminus R$:*

$$(K_S^R)_{\mathfrak{p}} \supseteq K_{\mathfrak{p}}(p)$$

If, moreover, $\mathfrak{p} \notin S$ and S is p-stable for $K_{S\cup S_p\cup S_\infty\cup\{\mathfrak{p}\}}/K$ with a p-stabilizing field contained in K_S^R, then also

$$(K_S^R)_{\mathfrak{p}} \supseteq K_{\mathfrak{p}}^{\mathrm{nr}}(p).$$

Proof. Apply Proposition 4.20 to a p-stabilizing field L_0 of S for $K_{S\cup S_p\cup S_\infty}/K$, which is contained in K_S^R. □

Remarks 4.22.

(i) Observe that in the Corollary 4.21 the assumption is weaker than in Proposition 4.20: the p-stabilizing field of S for $K_{S\cup S_p\cup S_\infty}$ must only lie in K_S^R, and not in $K_S^R(p)$. We will use it in Proposition 4.25, which is in turn used in Section 6.2 to prove a local correspondence at the boundary.

(ii) The above techniques also allow to construct some examples of sets of density 0, for which the assertion of Proposition 4.20 holds. Indeed, let S be a set of primes of K, with p-stabilizing field K for $K_{S\cup S_p\cup S_\infty}/K$, and let M/K be a Galois extension of p-power

degree, such that $\delta_M(S) = 0$ and $M \cap K_S = K$ (such K, M, S exist - take for example M/K Galois of p-power degree and totally ramified in exactly one prime $\mathfrak{p} \notin S \cup S_p \cup S_\infty$, and let $S \backsimeq P_{M/K}(\sigma)$ with $1 \neq \sigma \in \mathrm{G}_{M/K}$). Then

$$\mathrm{G}^R_{M,S}(p) \twoheadrightarrow \mathrm{G}_{M.K^R_S(p)/M} \xrightarrow{\sim} \mathrm{G}^R_{K,S}(p),$$

and for any prime $\mathfrak{q} \in S \smallsetminus R$ of K with extension $\mathfrak{q}'$ to M, one has $K_\mathfrak{q}(p) = M_{\mathfrak{q}'}(p)$, since M/K has p-power degree. Hence $M^R_S(p)_{\mathfrak{q}'} = M_{\mathfrak{q}'}(p)$ for each $\mathfrak{q}' \in (S \smallsetminus R)(M)$.

Now we consider the following concrete situation, which we need later on (cf. proof of Proposition 4.34). Let p be a rational prime, S a set of primes of K and $V := (S_p \cup S_\infty) \smallsetminus S$. Let $\mathfrak{p} \in V$ be a prime of K over p. Assume S is p-stable for $K_{S\cup V}/K$ with a p-stabilizing field contained in K_S. Let $K'_{S\cup V}(p)$ be the maximal pro-p subextension of $K_{S\cup V}/K_S$. Let further $K'_\mathfrak{p}(p)$ be the maximal pro-p-extension of $K_{S,\mathfrak{p}}$, and define

$$I'_\mathfrak{p}(p) := \mathrm{G}_{K'_\mathfrak{p}(p)/K_{S,\mathfrak{p}}}.$$

Lemma 4.23. *We have $(K'_{S\cup V}(p))_\mathfrak{p} = K'_\mathfrak{p}(p)$. In particular, there is a natural isomorphism $D_{\mathfrak{p},K'_{S\cup V}(p)/K_S} \cong I'_\mathfrak{p}(p)$ and $(K'_{S\cup V}(p))_\mathfrak{p}$ is p-closed.*

Proof. The inclusion '$\subseteq$' is trivial. We show the inclusion '$\supseteq$'. Since $(K'_{S\cup V}(p))_\mathfrak{p} \supseteq K_{S,\mathfrak{p}}$, it is enough to show that $(K'_{S\cup V}(p))_\mathfrak{p}$ is p-closed. Let $L_0 \subseteq K_S$ be a p-stabilizing field for S for $K_{S\cup V}/K$. Then any finite subextension $K'_{S\cup V}(p)/L/L_0$ is a p-stabilizing field for $S \cup V$ for $K_{S\cup V}/K$. By Proposition 4.20, we have for any such L:

$$L_\mathfrak{p}(p) = (L_{S\cup V}(p))_\mathfrak{p} \subseteq (K'_{S\cup V}(p))_\mathfrak{p}.$$

This implies that $(K'_{S\cup V}(p))_\mathfrak{p}$ is p-closed. □

Consider now the following extensions:

$$\begin{array}{ccccc}
K'_{S\cup V}(p) & & K'_\mathfrak{p}(p) & \subseteq & \overline{K_\mathfrak{p}} \\
\Big| & & \Big| I'_\mathfrak{p}(p) & & \Big| \mathscr{I}_\mathfrak{p} \\
K_S & & K_{S,\mathfrak{p}} & \subseteq & K^{\mathrm{nr}}_\mathfrak{p} \\
\Big| & & \Big| D_{\mathfrak{p},K_S/K} & & \Big| \mathscr{G}^{\mathrm{nr}}_\mathfrak{p} \\
K & & K_\mathfrak{p} & & K_\mathfrak{p}
\end{array}$$

By Lemma 4.23 we have the commutative diagram with exact rows of local Galois groups:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathscr{I}_\mathfrak{p} & \longrightarrow & \mathscr{G}_\mathfrak{p} & \longrightarrow & \mathscr{G}^{\mathrm{nr}}_\mathfrak{p} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & I'_\mathfrak{p}(p) & \longrightarrow & D_{\mathfrak{p},K'_{S\cup V}(p)/K} & \longrightarrow & D_{\mathfrak{p},K_S/K} & \longrightarrow & 1
\end{array}$$

Since $K_{S,\mathfrak{p}}$ contains the maximal unramified p-extension of $K_\mathfrak{p}$, the extension $K'_\mathfrak{p}(p)/K_{S,\mathfrak{p}}$ is purely ramified and in particular, the vertical arrow on the left is also surjective. In this situation we have the following comparison of cohomology.

Lemma 4.24. *Let $i \geqslant 0$ and $r \geqslant 1$ be two integers. We have canonical isomorphisms:*

$$\begin{aligned} \mathrm{H}^{\mathrm{i}}(\mathrm{D}_{\mathfrak{p},\mathrm{K}'_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})/\mathrm{K}}, \mathbb{Z}/\mathrm{p}^{\mathrm{r}}\mathbb{Z}) &= \mathrm{H}^{\mathrm{i}}(\mathscr{G}_{\mathfrak{p}}, \mathbb{Z}/\mathrm{p}^{\mathrm{r}}\mathbb{Z}) \\ \mathrm{H}^{\mathrm{i}}(\mathrm{D}_{\mathfrak{p},\mathrm{K}_{\mathrm{S}}/\mathrm{K}}, \mathbb{Z}/\mathrm{p}^{\mathrm{r}}\mathbb{Z}) &= \mathrm{H}^{\mathrm{i}}(\mathscr{G}_{\mathfrak{p}}^{\mathrm{nr}}, \mathbb{Z}/\mathrm{p}^{\mathrm{r}}\mathbb{Z}) \end{aligned}$$

Furthermore, $\mathrm{cd}_p I'_{\mathfrak{p}}(p) = \mathrm{cd}_p \mathscr{I}_{\mathfrak{p}} = 1$ *and* $\mathrm{cd}_p D_{\mathfrak{p},K_S/K} = \mathrm{cd}_p \mathscr{G}_{\mathfrak{p}}^{\mathrm{nr}} = 1$.

Proof. Proof of the first equality is similar to the proof of [NSW] 7.5.8. Let H denote the kernel of $\mathscr{G}_{\mathfrak{p}} \twoheadrightarrow D_{\mathfrak{p},K'_{S\cup V}(p)/K}$. Then $\mathrm{cd}_p H \leqslant 1$ by [NSW] 7.1.8 (i). Moreover, we have $\mathrm{H}^1(\mathrm{H}, \mathbb{Z}/\mathrm{p}^{\mathrm{r}}\mathbb{Z}) = 0$. Indeed, $(K'_{S\cup V}(p))_{\mathfrak{p}}$ is p-closed by Lemma 4.23 and hence H has no non-trivial p-quotients. Thus the first equality follows from the Hochschild-Serre spectral sequence for H and $D_{\mathfrak{p},K'_{S\cup V}(p)/K}$.

By Corollary 4.21, K_S/K realizes the maximal unramified pro-p-extension at $\mathfrak{p}$. Thus the order of the kernel of $\mathscr{G}_{\mathfrak{p}}^{\mathrm{nr}} \twoheadrightarrow D_{\mathfrak{p},K_S/K}$ is prime to p and the second equality again follows from the associated spectral sequence. The statement about the p-cohomological dimension follows from the fact that the p-Sylow subgroups of $D_{\mathfrak{p},K_S/K}$ and of $\mathscr{G}_{\mathfrak{p}}^{\mathrm{nr}}$ are isomorphic to $\mathbb{Z}_p$.

Finally, $\mathrm{cd}_p \mathscr{I}_{\mathfrak{p}} = 1$ holds by [NSW] 7.1.8 (i). The group $I'_{\mathfrak{p}}(p)$ is the inverse limit of pro-p intertia groups:

$$I'_{\mathfrak{p}}(p) = \varprojlim_{K_{S,\mathfrak{p}}/L/K_{\mathfrak{p}}} \mathrm{G}_{L(p)/L^{\mathrm{nr}}(p)},$$

which are free pro-p-groups as follows for example from [NSW] 7.5.11 using Lemma 2.2, as the index of $\mathrm{G}_{L(p)/L^{\mathrm{nr}}(p)}$ in $\mathrm{G}_{L(p)/L}$ is p^∞. In particular, we obtain $\mathrm{cd}_p I'_{\mathfrak{p}}(p) = 1$ by [NSW] 3.3.2. □

Using the Grunwald-Wang theorem we can easily deduce that the intersections of decomposition subgroups inside $\mathrm{G}_{K,S}$ are small (we will need this in Section 6.2, to deduce a local correspondence at the boundary):

Proposition 4.25. *Let K be a number field, S a set of primes of K, p a rational prime. Assume S is stable and satisfies $(*)_p^{\mathrm{stab}}$. 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 $\bar{\mathfrak{p}}_1 \neq \bar{\mathfrak{p}}_2 \in S(K_S)$ we have inside $\mathrm{G}_{K,S}$:*

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

and

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

Proof. Write $D_{i,p} := D_{\bar{\mathfrak{p}}_i,p}$. Assume for $i = 1, 2$, we have $U_i \subseteq D_{i,p}$ an open subgroup, and we have shown that $(U_1 \colon U_1 \cap U_2) = \infty$. We show that also $(D_{1,p} \colon D_{1,p} \cap D_{2,p}) = \infty$. In fact, we have $(D_{i,p} \colon U_i) < \infty$, hence $(D_{1,p} \cap D_{2,p} \colon D_{1,p} \cap U_2), (D_{1,p} \cap D_{2,p} \colon U_1 \cap D_{2,p}) < \infty$. Hence also $(D_{1,p} \cap D_{2,p} \colon U_1 \cap U_2) < \infty$. Now $(U_1 \colon U_1 \cap U_2) = \infty$ implies

$$(D_{1,p} \colon D_{1,p} \cap D_{2,p})(D_{1,p} \cap D_{2,p} \colon U_1 \cap U_2) = (D_{1,p} \colon U_1 \cap U_2) = \infty,$$

and the second factor in the product is finite, hence we get $(D_{1,p} \colon D_{1,p} \cap D_{2,p}) = \infty$.

Using this, we can go up to a finite extension of K inside K_S, and thus assume that S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ with stabilizing field K and that $\bar{\mathfrak{p}}_1|_K \neq \bar{\mathfrak{p}}_2|_K$. Now an application of Corollary 4.21 with $\mathfrak{p} = \bar{\mathfrak{p}}_1|_K$ and $R = \{\bar{\mathfrak{p}}_2|_K\}$ shows that $D_{2,p}$ lies in the kernel of the projection

$$\mathrm{G}_{K,S} \twoheadrightarrow \mathrm{G}_{K,S}^R,$$

whereas $D_{1,p}$ has infinite image. Thus $(D_{1,p}\colon D_{1,p}\cap D_{2,p}) \geqslant (D_{1,p}\colon D_{1,p}\cap V) = \infty$, where $V := \ker(\mathrm{G}_{K,S} \twoheadrightarrow \mathrm{G}_{K,S}^R)$. The second statement follows from the first in the same way as in Proposition 1.6. □

4.6 Riemann's Existence Theorem

The results from sections 4.3-4.5 allow us to show the following version of Riemann's existence theorem, which generalizes [NSW] 10.5.8. The proof follows the same steps as in *loc. cit.*

Theorem 4.26. *Let K be a number field, p a rational prime, $T \supseteq S \supseteq R$ sets of primes of K. Assume that R is finite and S is p-stable for $K_{T\cup S_p\cup S_\infty}/K$ and has a p-stabilizing extension contained in $K_S^R(p)$. Then the natural map*

$$\phi_{T,S}^R\colon \mathop{\ast}_{\mathfrak{p}\in R(K_S^R(p))} \mathrm{G}_{K_\mathfrak{p}(p)/K_\mathfrak{p}} * \mathop{\ast}_{\mathfrak{p}\in(T\smallsetminus S)(K_S^R(p))} I_{K_\mathfrak{p}(p)/K_\mathfrak{p}} \xrightarrow{\sim} \mathrm{G}_{K_T(p)/K_S^R(p)}$$

is an isomorphism, where $I_{K_\mathfrak{p}(p)/K_\mathfrak{p}} = \mathrm{G}_{K_\mathfrak{p}(p)/K_\mathfrak{p}^{\mathrm{nr}}(p)} \subseteq \mathrm{G}_{K_\mathfrak{p}(p)/K_\mathfrak{p}}$ is the inertia subgroup.

In particular, since the groups $I_{K_\mathfrak{p}(p)/K_\mathfrak{p}}$ are free pro-p groups, we obtain the following corollary.

Corollary 4.27. *Under the assumptions as in Theorem 4.26, if $R = \varnothing$, then the group $\mathrm{G}_{K_T(p)/K_S(p)}$ is a free pro-p group.*

Proof of Theorem 4.26. It suffices to show the theorem in the case $T \supseteq S_p \cup S_\infty$. Indeed, assume this is done and T is arbitrary. Then the condition is still satisfied for T replaced by $T\cup S_p\cup S_\infty$, and the theorem in this case implies that $\phi^R_{T\cup S_p\cup S_\infty,S}$ is bijective. Then the bijectivity of $\phi^R_{T,S}$ follows by dividing out the inertia subgroups at primes in $(S_p\cup S_\infty)\smallsetminus T$ on both sides.

From now on we assume $T \supseteq S_p \cup S_\infty$. All cohomology groups in the proof have $\mathbb{Z}/p\mathbb{Z}$-coefficients and we omit them from the notation. Consider the maps induced by $\phi^R_{T,S}$ in the cohomology

$$\mathrm{H}^{\mathrm{i}}(\phi^{\mathrm{R}}_{\mathrm{T,S}})\colon \mathrm{H}^{\mathrm{i}}(\mathrm{K_T(p)/K_S^R(p)}) \to \mathrm{H}^{\mathrm{i}}(\mathop{\ast}_{\mathfrak{p}\in\mathrm{R}(\mathrm{K_S^R(p)})} \mathrm{G}_{\mathrm{K_\mathfrak{p}(p)/K_\mathfrak{p}}} * \mathop{\ast}_{\mathfrak{p}\in(\mathrm{T}\smallsetminus\mathrm{S})(\mathrm{K_S^R(p)})} \mathrm{I}_{\mathrm{K_\mathfrak{p}(p)/K_\mathfrak{p}}})$$

By [NSW] 1.6.15 it is enough to show that this map is bijective for $i = 1$ and injective for $i = 2$. By [NSW] 4.3.14, we have

$$\begin{aligned}\mathrm{H}^{\mathrm{i}}(\mathop{\ast}_{\mathfrak{p}\in\mathrm{R}(\mathrm{K_S^R(p)})} \mathrm{G}_{\mathrm{K_\mathfrak{p}(p)/K_\mathfrak{p}}} * \mathop{\ast}_{\mathfrak{p}\in(\mathrm{T}\smallsetminus\mathrm{S})(\mathrm{K_S^R(p)})} \mathrm{I}_{\mathrm{K_\mathfrak{p}(p)/K_\mathfrak{p}}}) &= \\ \bigoplus\nolimits'_{\mathfrak{p}\in R(K_S^R(p))} \mathrm{H}^{\mathrm{i}}(\mathrm{G}_{\mathrm{K_\mathfrak{p}(p)/K_\mathfrak{p}}}) &\oplus \bigoplus\nolimits'_{\mathfrak{p}\in(T\smallsetminus S)(K_S^R(p))} \mathrm{H}^{\mathrm{i}}(\mathrm{I}_{\mathrm{K_\mathfrak{p}(p)/K_\mathfrak{p}}}),\end{aligned}$$

where $\bigoplus'$ means the restricted direct sum in the sense of the definition [NSW] 4.3.13. Now, $\mathrm{H}^1(\phi^{\mathrm{R}}_{\mathrm{T,S}})$ is injective since $\phi^R_{T,S}$ is surjective: $\mathrm{G}_{K_T(p)/K^R_S(p)}$ is generated by the inertia subgroups of primes in $T \smallsetminus S$ and the decomposition subgroups in R.

To show the surjectivity of $\mathrm{H}^1(\phi^{\mathrm{R}}_{\mathrm{T,S}})$, let $K^R_S(p)/L_0/K$ be a p-stabilizing field for S for the extension K_T/K. Let $K^R_S(p)/L/L_0$ be any finite subextension. Since $T \supseteq S_p \cup S_\infty$, the natural maps $\mathrm{H^i(K_T(p)/L)} \to \mathrm{H^i(K_T/L)}$ are isomorphisms for all $i \geqslant 0$ by [NSW] 10.4.8 (for $i = 1$, this is obvious; we need this later also for $i = 2$). Analogously, $\mathrm{H^i(K_\mathfrak{p}(p)/L_\mathfrak{p}) \to H^i(L_\mathfrak{p})}$ are isomorphisms for all $i \geqslant 0$ by [NSW] 7.5.8.

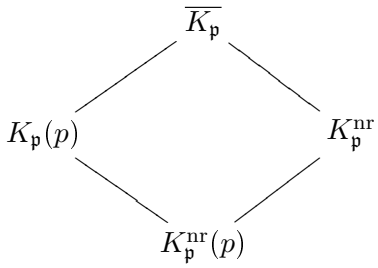
By Grunwald-Wang Theorem 4.15 the restriction map

$$\mathrm{H}^1(\mathrm{K_T/L}) \to \bigoplus_{\mathfrak{p}\in \mathrm{R(L)}} \mathrm{H}^1(\mathrm{L}_\mathfrak{p}) \oplus \bigoplus_{\mathfrak{p}\in(\mathrm{T}\smallsetminus\mathrm{S})(\mathrm{L})} \mathrm{H}^1(\mathrm{I}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{L}_\mathfrak{p}})^{\mathrm{G}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{L}_\mathfrak{p}}} \tag{4.1}$$

is surjective (observe that for the module $\mathbb{Z}/p\mathbb{Z}$ the special case, where the cokernel can be non-trivial, never occurs). By the above considerations, we have $\mathrm{H}^1(\mathrm{K_T/L}) = \mathrm{H}^1(\mathrm{K_T(p)/L})$ and $\mathrm{H}^1(\mathrm{L}_\mathfrak{p}) = \mathrm{H}^1(\mathrm{K}_\mathfrak{p}(\mathrm{p})/\mathrm{L}_\mathfrak{p})$. For the last term we have $L_\mathfrak{p} \subseteq K^{\mathrm{nr}}_\mathfrak{p}(p)$ if $\mathfrak{p} \in T \smallsetminus S(L)$ and the following computation:

$$\begin{aligned} \mathrm{H}^1(\mathrm{I}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{K}_\mathfrak{p}})^{\mathrm{G}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{K}^{\mathrm{nr}}_\mathfrak{p}(\mathrm{p})}} = \mathrm{H}^1(\mathrm{G}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{K}^{\mathrm{nr}}_\mathfrak{p}})^{\mathrm{G}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{K}^{\mathrm{nr}}_\mathfrak{p}(\mathrm{p})}} & \\ \cong \mathrm{H}^1(\mathrm{G}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{K}^{\mathrm{nr}}_\mathfrak{p}(\mathrm{p})}) & \\ \cong \mathrm{H}^1(\mathrm{G}_{\mathrm{K}_\mathfrak{p}(\mathrm{p})/\mathrm{K}^{\mathrm{nr}}_\mathfrak{p}(\mathrm{p})}) & \\ \cong \mathrm{H}^1(\mathrm{I}_{\mathrm{K}_\mathfrak{p}(\mathrm{p})/\mathrm{K}_\mathfrak{p}}), & \end{aligned} \tag{4.2}$$

which follows by considering the Hochschild-Serre spectral sequences of the extensions of Galois groups occurring in the following diagram:



Finally, by Proposition 4.20, the limit over $K^R_S(p)/L/L_0$ of $L_\mathfrak{p}$ for $\mathfrak{p} \in T \smallsetminus S$ is equal to $K^{\mathrm{nr}}_\mathfrak{p}(p)$, and hence the limit over L of the right summand of the term on the right in (4.1) is equal to

$$\bigoplus\nolimits'_{\mathfrak{p}\in T\smallsetminus S(K^R_S(p))} \mathrm{H}^1(\mathrm{I}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{K}_\mathfrak{p}})^{\mathrm{G}_{\overline{\mathrm{K}_\mathfrak{p}}/\mathrm{K}^{\mathrm{nr}}_\mathfrak{p}(\mathrm{p})}} = \bigoplus\nolimits'_{\mathfrak{p}\in \mathrm{T}\smallsetminus \mathrm{S}(\mathrm{K}^{\mathrm{R}}_{\mathrm{S}}(\mathrm{p}))} \mathrm{H}^1(\mathrm{I}_{\mathrm{K}_\mathfrak{p}(\mathrm{p})/\mathrm{K}_\mathfrak{p}}).$$

Thus $\mathrm{H}^1(\phi^{\mathrm{R}}_{\mathrm{T,S}})$ is surjective. Finally, we show the injectivity of $\mathrm{H}^2(\phi^{\mathrm{R}}_{\mathrm{T,S}})$. Since S (and hence also T) is p-stable for K_T/K with p-stabilizing field L_0 contained in $K^R_S(p)$, we obtain by Corollary 4.11 for any finite $K^R_S(p)/L/L_0$:

$$\mathrm{H}^2(\mathrm{K_T(p)/L}) \hookrightarrow \bigoplus_{\mathfrak{p}\in\mathrm{T}} \mathrm{H}^2(\mathrm{K}_\mathfrak{p}(\mathrm{p})/\mathrm{L}_\mathfrak{p})$$

is injective. After passing to the direct limit over all $K_S^R(p)/L/L_0$ over restriction maps, only the entries for $\mathfrak{p} \in R$ on the right survive, as Proposition 4.20 shows. Since $\varinjlim$ is exact on abelian groups, the obtained map, which is exactly $\mathrm{H}^2(\phi^{\mathrm{R}}_{\mathrm{T,S}})$, is injective. □

We can also replace $K_S^R(p)$ by K_S^R:

Corollary 4.28. *Let K be a number field, p a rational prime, $T \supseteq S \supseteq R$ sets of primes of K. Assume that R is finite and S is p-stable for $K_{T\cup S_p\cup S_\infty}/K$ and has a p-stabilizing extension contained in K_S^R. Let $K_T'(p)$ be the maximal pro-p-subextension of K_T/K_S^R. For $\mathfrak{p}$ a prime of K, let $I_\mathfrak{p}'(p)$ denote the Galois group of the maximal pro-p extension $K_\mathfrak{p}'(p)$ of $K_{S,\mathfrak{p}}^R$. Then the natural map*

$$\phi_{T,S}^R\colon \mathop{\ast}_{\mathfrak{p}\in R(K_S^R)} \mathrm{G}_{K_\mathfrak{p}(p)/K_\mathfrak{p}} * \mathop{\ast}_{\mathfrak{p}\in T\smallsetminus S(K_S^R)} I_\mathfrak{p}'(p) \xrightarrow{\sim} \mathrm{G}_{K_T'(p)/K_S^R}$$

is an isomorphism.

Remark 4.29. If $\mathfrak{p} \in T \smallsetminus S_p$, then $I_\mathfrak{p}'(p) = I_{K_\mathfrak{p}(p)/K_\mathfrak{p}}$, the inertia group of $K_\mathfrak{p}(p)/K_\mathfrak{p}$, but if $\mathfrak{p} \in T \cap S_p$, then $I_{K_\mathfrak{p}(p)/K_\mathfrak{p}}$ is in general a proper quotient of the group $I_\mathfrak{p}'(p)$, as the rank of $I_{K_\mathfrak{p}(p)/K_\mathfrak{p}}$ grows with K.

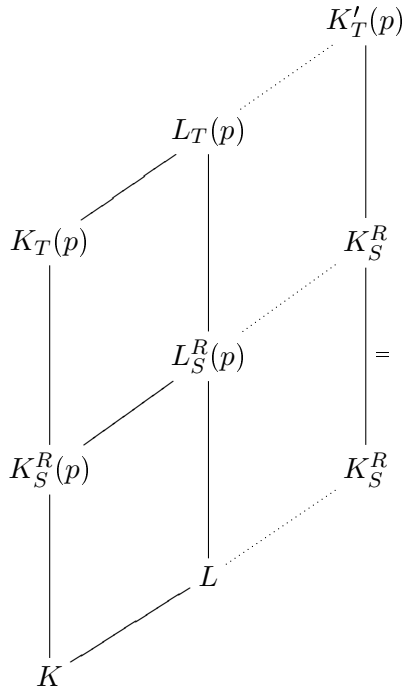
Proof. We have

$$I_\mathfrak{p}'(p) = \varprojlim_{K_S/L/K} I_{L_\mathfrak{p}(p)/L_\mathfrak{p}}.$$

and

$$\mathrm{G}_{K_T'(p)/K_S^R} = \varprojlim_{K_S^R/L/K} \mathrm{G}_{L_T(p)/L_S^R(p)}$$

with natural transition maps coming from the diagram:



Thus the corollary follows from Theorem 4.26.

□

Since the groups $I'_{\mathfrak{p}}(p)$ are free pro-p groups by Lemma 4.24, we obtain the following corollary.

Corollary 4.30. *Under the assumptions as in Corollary 4.28, if $R = \varnothing$, then the group $\mathrm{G}_{K'_T(p)/K_S}$ is a free pro-p group.*

4.7 Cohomological dimension

Theorem 4.31. *Let K be a number field, $S \supseteq R$ sets of primes of K and p a rational prime. Assume p is odd or K is totally imaginary. If R is finite and S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ with K as a p-stabilizing extension, then*

$$\mathrm{cd}(\mathrm{G}^R_{K,S}(p)) = \mathrm{scd}(\mathrm{G}^R_{K,S}(p)) = 2.$$

Remark 4.32. In Section 5 we will remove the assumption that K is a p-stabilizing field for S for $K_{S\cup S_p\cup S_\infty}/K$ if $R = \varnothing$.

Proof. We follow the same steps as in the proof of [NSW] 10.5.10. We omit the coefficients $\mathbb{Z}/p\mathbb{Z}$ from the notation. Let $V := (S_p \cup S_\infty) \setminus S$. If $\mathfrak{p}$ is non-archimedean, then $\mathrm{G}_{K_{\mathfrak{p}}(p)/K^{\mathrm{nr}}_{\mathfrak{p}}(p)}$ and $\mathrm{G}_{K^{\mathrm{nr}}_{\mathfrak{p}}(p)/K_{\mathfrak{p}}}$ are free. Thus Hochschild-Serre spectral sequence gives us a canonical isomorphism

$$\mathrm{H}^1(\mathrm{K}^{\mathrm{nr}}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}, \mathrm{H}^1(\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}^{\mathrm{nr}}_{\mathfrak{p}}(\mathrm{p}))) \xrightarrow{\sim} \mathrm{H}^2(\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}). \tag{4.3}$$

Next consider the Hochschild-Serre sequence $(E^{i,j}_n, \delta^{i,j}_n)$ for the Galois groups of the global extensions $K_{S\cup V}(p)/K_S(p)/K$. By [NSW] 8.3.18 and 10.4.8, we have:

$$\mathrm{cd}\,\mathrm{G}_{K,S\cup V}(p) \leqslant \mathrm{cd}_p\,\mathrm{G}_{K,S\cup V} \leqslant 2.$$

By Riemann's existence theorem (cf. Corollary 4.27) the group $\mathrm{G}_{K_{S\cup V}(p)/K_S(p)}$ is free. In particular, we have

$$\mathrm{coker}(\delta^{1,1}_2) = E^{3,0}_3 = E^{3,0}_\infty \subseteq \mathrm{H}^3(\mathrm{G}_{\mathrm{K,S\cup V}}(\mathrm{p})) = 0.$$

I.e., $\delta^{1,1}_2$ is surjective.

Cohomological dimension, case $R = \varnothing$. By Riemann's existence theorem 4.26 we have

$$\mathrm{H}^1(\mathrm{K}_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})/\mathrm{K}_{\mathrm{S}}(\mathrm{p})) \cong \bigoplus_{\mathfrak{p}\in\mathrm{V}} \mathrm{Ind}^{\mathrm{G_{K,S}(p)}}_{\mathrm{D}_{\mathfrak{p},\mathrm{K_S(p)/K}}} \mathrm{H}^1(\mathrm{I}_{\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}}). \tag{4.4}$$

This and Shapiro's lemma imply:

$$\begin{aligned} E^{1,1}_2 &= \mathrm{H}^1(\mathrm{K_S(p)/K}, \mathrm{H}^1(\mathrm{K_{S\cup V}(p)/K_S(p)})) \\ &= \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^1(\mathrm{K}^{\mathrm{nr}}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}, \mathrm{H}^1(\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}^{\mathrm{nr}}_{\mathfrak{p}}(\mathrm{p}))) \\ &= \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^2(\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}), \end{aligned} \tag{4.5}$$

where the last equality is (4.3). Further we have the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccc}
 & & \bigoplus_{\mathfrak{p}\in S} \mathrm{H}^2(\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}) & \twoheadrightarrow & \mathrm{H}^0(\mathrm{K}_{\mathrm{S}\cup\mathrm{V}}/\mathrm{K},\mu_{\mathrm{p}})^{\vee} \\
 & & \downarrow & & \downarrow = \\
\mathrm{H}^2(\mathrm{K}_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})/\mathrm{K}) & \hookrightarrow & \bigoplus_{\mathfrak{p}\in S\cup V} \mathrm{H}^2(\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}) & \twoheadrightarrow & \mathrm{H}^0(\mathrm{K}_{\mathrm{S}\cup\mathrm{V}}/\mathrm{K},\mu_{\mathrm{p}})^{\vee} \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{H}^1(\mathrm{K}_{\mathrm{S}}(\mathrm{p})/\mathrm{K},\mathrm{H}^1(\mathrm{K}_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})/\mathrm{K}_{\mathrm{S}}(\mathrm{p}))) & \xrightarrow{\sim} & \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^2(\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}) & \longrightarrow & 0 \\
\downarrow{\scriptstyle \delta_2^{1,1}} & & & & \\
\mathrm{H}^3(\mathrm{K}_{\mathrm{S}}(\mathrm{p})/\mathrm{K}) & & & &
\end{array}$$

in which the second row comes from the Poitou-Tate long exact sequence. The first map in the second row is injective by Corollary 4.11(ii) applied to K and $S \cup V$ and from [NSW] 10.4.8. The first map in the third row is an isomorphism by (4.5). The map in the first row is surjective, since the dual map

$$\mu_p(K) = \mathrm{H}^0(\mathrm{K}_{\mathrm{S}\cup\mathrm{V}}/\mathrm{K},\mu_{\mathrm{p}}) \to \bigoplus_{\mathfrak{p}\in\mathrm{S}} \mathrm{H}^2(\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}})^{\vee} = \bigoplus_{\mathfrak{p}\in\mathrm{S}} \mu_{\mathrm{p}}(\mathrm{K}_{\mathfrak{p}})$$

is injective. The Snake lemma for the second and the third row in the above diagram implies $\mathrm{H}^3(\mathrm{K}_{\mathrm{S}}(\mathrm{p})/\mathrm{K}) = 0$, and hence $\mathrm{cd}(\mathrm{G}_{K,S}(p)) \leqslant 2$ by [NSW] 3.3.2.

Cohomological dimension, general case. Now consider the Hochschild-Serre spectral sequence for the Galois groups of $K_S(p)/K_S^R(p)/K$. By Riemann's existence theorem 4.26 applied to $T := S \supseteq R$, it follows that $\mathrm{H}^{\mathrm{j}}(\mathrm{K}_{\mathrm{S}}(\mathrm{p})/\mathrm{K}_{\mathrm{S}}^{\mathrm{R}}(\mathrm{p}))$ are induced $\mathrm{G}_{K,S}^R(p)$-modules for $j \geqslant 1$. Hence $E_2^{i,j} = 0$ for $i, j \geqslant 1$. Then

$$\mathrm{H}^3(\mathrm{K}_{\mathrm{S}}^{\mathrm{R}}(\mathrm{p})/\mathrm{K}) = \mathrm{E}_2^{3,0} \hookrightarrow \mathrm{H}^3(\mathrm{K}_{\mathrm{S}}(\mathrm{p})/\mathrm{K}) = 0,$$

and hence $\mathrm{H}^3(\mathrm{K}_{\mathrm{S}}^{\mathrm{R}}(\mathrm{p})/\mathrm{K}) = 0$. Again by [NSW] 3.3.2 we conclude that $\mathrm{cd}(\mathrm{G}_{K,S}^R(p)) \leqslant 2$.

Now we show equality. Since S is stable for $K_{S\cup S_p\cup S_\infty}/K$, we have

$$\delta_K(S \cap \mathrm{cs}(K(\mu_p)/K)) = [K(\mu_p) : K]^{-1}\delta_{K(\mu_p)}(S) > 0,$$

hence there is a prime $\mathfrak{p} \in S \smallsetminus (R \cup S_p \cup S_\infty)$ with $\mu_p \subset K_{\mathfrak{p}}$. By Proposition 4.20, the subgroup $D_{\mathfrak{p},K_S^R(p)/K}$ of $\mathrm{G}_{K,S}^R(p)$ is of cohomological dimension 2. Hence $\mathrm{cd}(\mathrm{G}_{K,S}^R(p)) = 2$.

Now we turn to the strict cohomological dimension.

Strict cohomological dimension, case $S \supseteq S_p \cup S_\infty$ and $R = \varnothing$ (cf. [NSW] 10.2.3).
Since $\mathrm{cd}\,\mathrm{G}_S(p) = 2$, by [NSW] 3.3.4 it is enough to show that $\mathrm{H}^2(\mathrm{U},\mathbb{Q}_{\mathrm{p}}/\mathbb{Z}_{\mathrm{p}}) = 0$ for all open $U \subseteq \mathrm{G}_{K,S}(p)$. Since the assumptions carry over from $\mathrm{G}_{K,S}(p)$ to U, we can assume $U = \mathrm{G}_{K,S}(p)$. Except in the special case, we obtain from [NSW] 10.4.8 and from Corollary 4.11 the injection

$$\mathrm{H}^2(\mathrm{G}_{\mathrm{K,S}}(\mathrm{p}),\mathbb{Z}/\mathrm{p}^{\mathrm{r}}\mathbb{Z}) \cong \mathrm{H}^2(\mathrm{G}_{\mathrm{K,S}},\mathbb{Z}/\mathrm{p}^{\mathrm{r}}\mathbb{Z}) \hookrightarrow \bigoplus_{\mathfrak{p}\in\mathrm{S}} \mathrm{H}^2(\mathscr{G}_{\mathfrak{p}},\mathbb{Z}/\mathrm{p}^{\mathrm{r}}\mathbb{Z})$$

for any r (recall that by our assumption, S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ and not only for $K_{S\cup S_p\cup S_\infty}(p)/K$). Passing to the limit over all $r > 0$ and using $\mathrm{scd}_p(\mathscr{G}_{\mathfrak{p}}) = 2$, we obtain

the result. If we are in the special case, then $p = 2$ and $i \notin K$. Then by the same argument as above, we get $\mathrm{H}^2(\mathrm{G}_{\mathrm{K(i),S}}, \mathbb{Q}_2/\mathbb{Z}_2) = 0$ and by [NSW] 3.3.11, the corestriction

$$0 = \mathrm{H}^2(\mathrm{G}_{\mathrm{K(i),S}}(2), \mathbb{Q}_2/\mathbb{Z}_2) \to \mathrm{H}^2(\mathrm{G}_{\mathrm{K,S}}(2), \mathbb{Q}_2/\mathbb{Z}_2)$$

is surjective. This finishes the proof in the first case.

Strict cohomological dimension, general case. We omit the coefficients $\mathbb{Q}_p/\mathbb{Z}_p$ from the notation. From the Hochschild-Serre spectral sequence associated to the extension

$$1 \to \mathrm{G}_{K_{S\cup V}(p)/K_S^R(p)} \to \mathrm{G}_{K,S\cup V}(p) \to \mathrm{G}_{K,S}^R(p) \to 1,$$

and using $\mathrm{scd}_p(\mathrm{G}_{K,S\cup V}(p)) = 2$, which implies $\mathrm{H}^2(\mathrm{K_{S\cup V}(p)/K}, \mathbb{Q}_\mathrm{p}/\mathbb{Z}_\mathrm{p}) = 0$, we get an exact sequence

$$\mathrm{H}^1(\mathrm{K_{S\cup V}(p)/K}) \to \mathrm{H}^1(\mathrm{K_{S\cup V}(p)/K_S^R(p)})^{\mathrm{G_{K,S}^R(p)}} \to \mathrm{H}^2(\mathrm{K_S^R(p)/K}) \to 0. \tag{4.6}$$

But by Riemann's existence theorem 4.26,

$$\mathrm{H}^1(\mathrm{K_{S\cup V}(p)/K_S^R(p)})^{\mathrm{G_{K,S}^R(p)}} \cong \bigoplus_{\mathrm{R}} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}) \oplus \bigoplus_{\mathrm{V}} \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}},$$

and hence by Grunwald-Wang theorem 4.15 the map on the left in the sequence (4.6) is surjective, except we are in the special case, in which the cokernel, which is isomorphic to $\mathrm{H}^2(\mathrm{G_{K,S}^R(p)})$ is annihilated by 2. But since $\mathrm{cd}\,\mathrm{G}_{K,S}^R(p) = 2$, the group $\mathrm{H}^2(\mathrm{G_{K,S}^R(p)})$ is divisible, and hence trivial. This is true for any extension of K in $K_S^R(p)$, hence we are done by [NSW] 3.3.4. □

As in [NSW] 10.5.11, we obtain have the following corollary.

Corollary 4.33. *Let K be a number field, $S \supseteq R$ sets of primes of K and p a rational prime. Assume that either p is odd or K is totally imaginary. If R is finite and S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ with stabilizing field K, then*

$$\mathrm{cd}_p\,\mathrm{G}_{K,S}^R = \mathrm{scd}_p\,\mathrm{G}_{K,S}^R = 2.$$

Proof. Write $G = \mathrm{G}_{K,S}^R$. Since the assumptions carry over from K to any finite subextension $K_S^R/L/K$, by Theorem 4.31 we have $\mathrm{cd}_p U(p) = 2$ for any open subgroup $U \subseteq G$. Let $G_p \subseteq G$ be a p-Sylow subgroup. Then

$$G_p = \varprojlim_{G_p \subseteq U \subseteq G} U(p).$$

Hence by [NSW] 3.3.6 we have $\mathrm{cd}_p G = \mathrm{cd}_p G_p \leqslant 2$ and $\mathrm{scd}_p G = \mathrm{scd}_p G_p \leqslant 2$. Since G contains (exactly as in the proof of Theorem 4.31) subgroups of cohomological dimension 2, we obtain $\mathrm{cd}_p G = \mathrm{scd}_p G = 2$. □

4.8 Vanishing of $Ш^2(G_S; \mathbb{Z}/p\mathbb{Z})$ without $p \in \mathcal{O}_{K,S}^*$

We generalize Corollary 4.11 for $A = \mathbb{Z}/p\mathbb{Z}$. The proof makes use of many facts proven before: we will need Grunwald-Wang theorem, Riemann's existence theorem and $\mathrm{cd}_p\,\mathrm{G}_S = 2$ along with

the result of Neumann showing the vanishing of certain cohomology groups.

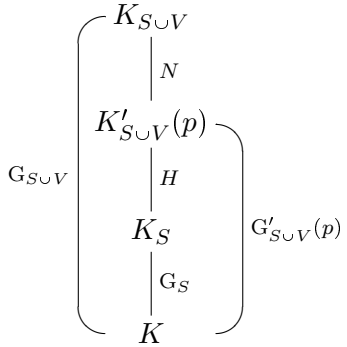
Proposition 4.34. *Let K be a number field, S a set of primes of K. Let p be a rational prime, $r > 0$ an integer and assume that S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ and has a p-stabilizing extension L_0 contained in K_S (i.e., S satisfies $(*)_p^{\mathrm{stab}}$). Assume p is odd or L_0 totally imaginary. Then*

$$Ш^2(K_S/L;\mathbb{Z}/p^r\mathbb{Z}) = 0$$

for any finite $K_S/L/L_0$, such that we are not in the special case (L, p^r, S).

This result has one important consequence for anabelian geometry of schemes $\operatorname{Spec}\mathcal{O}_{K,S}$ with S stable: to obtain a local correspondence at the boundary out of an isomorphism of étale fundamental groups $\sigma\colon \mathrm{G}_{K_1,S_1} \xrightarrow{\sim} \mathrm{G}_{K_2,S_2}$, one does not need to assume existence of a prime p with $S_p \subseteq S_i$ (cf. Section 6.2).

Proof. We can assume $K = L$. Let $V := (S_p \cup S_\infty) \smallsetminus S$. Let $K'_{S\cup V}(p)$ be the maximal pro-p-subextension of $K_{S\cup V}/K_S$. Consider the following tower of extensions:



with $N := \mathrm{G}_{K_{S\cup V}/K'_{S\cup V}(p)}$, $H := \mathrm{G}_{K'_{S\cup V}(p)/K_S}$ and $\mathrm{G}'_{S\cup V}(p) := \mathrm{G}_{K'_{S\cup V}(p)/K}$. In the following, we write $\mathrm{H}^*(\cdot)$ instead of $\mathrm{H}^*(\cdot, \mathbb{Z}/\mathrm{p}^\mathrm{r}\mathbb{Z})$ and $Ш^*(\cdot,\cdot)$ instead of $Ш^*(\cdot,\cdot;\mathbb{Z}/p^r\mathbb{Z})$. First of all we claim that

$$Ш^2(K'_{S\cup V}(p)/K, S\cup V) = Ш^2(K_{S\cup V}/K, S\cup V). \tag{4.7}$$

Once we know that the infation map $\mathrm{H}^2(\mathrm{G}'_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})) \to \mathrm{H}^2(\mathrm{G}_{\mathrm{S}\cup\mathrm{V}})$ is an isomorphism, the claim follows from the definition of $Ш^2$. To show this last assertion, consider the Hochschild-Serre spectral sequence

$$E_2^{ij} = \mathrm{H}^\mathrm{i}(\mathrm{G}'_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p}), \mathrm{H}^\mathrm{j}(\mathrm{N})) \Rightarrow \mathrm{H}^{\mathrm{i}+\mathrm{j}}(\mathrm{G}_{\mathrm{S}\cup\mathrm{V}}).$$

A result of Neumann ([NSW] 10.4.2) applied to $K_{S\cup V}/K'_{S\cup V}(p)$ (the upper field is $p-(S\cup V)$-closed, the lower is $p-(S_p\cup S_\infty)$-closed and $K_{S\cup V} = (K_S)_{S\cup V}$) implies $E_2^{ij} = 0$ for $j > 0$, hence the sequence degenerates in the second tableau and

$$\mathrm{H}^\mathrm{i}(\mathrm{G}'_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})) = \mathrm{H}^\mathrm{i}(\mathrm{G}_{\mathrm{S}\cup\mathrm{V}}),$$

for $i \geqslant 0$, proving our claim.

For $\mathfrak{p} \in V$, let $K'_{\mathfrak{p}}(p)$ denote the maximal pro-p extension of $K_{S,\mathfrak{p}}$. Let

$$I'_{\mathfrak{p}}(p) := \mathrm{G}_{K'_{\mathfrak{p}}(p)/K_{S,\mathfrak{p}}}$$

(observe that if $\mathfrak{p} \in S_\infty$, then $I'_{\mathfrak{p}}(p) = 1$. Indeed, if $p > 2$, this is always the case, and if $p = 2$, then $K_{S,\mathfrak{p}} = \mathbb{C}$ using the assumption that L_0 is totally imaginary). By Lemma 4.23 we have $I'_{\mathfrak{p}}(p) = D_{\mathfrak{p},K'_{S\cup V}(p)/K_S}$. By Riemann's existence theorem (Corollary 4.28 applied to $K'_{S\cup V}(p)/K_S/K$), we have

$$H \cong \mathop{\ast}_{\mathfrak{p}\in V(K_S)} I'_{\mathfrak{p}}(p).$$

In particular, H is a free pro-p-group by Corollary 4.30. Thus $\mathrm{cd}_p H \leqslant 1$. Consider the exact sequence

$$1 \to H \to \mathrm{G}'_{S\cup V}(p) \to \mathrm{G}_S \to 1,$$

and the corresponding Hochschild-Serre spectral sequence

$$E_2^{ij} = \mathrm{H}^{\mathrm{i}}(\mathrm{G_S}, \mathrm{H}^{\mathrm{j}}(\mathrm{H})) \Rightarrow \mathrm{H}^{\mathrm{i+j}}(\mathrm{G'_{S\cup V}(p)})$$

Since by Corollary 4.33, we know that $\mathrm{cd}_p \mathrm{G}_S = 2$, we have $E_2^{ij} = 0$ if $i > 2$ or $j > 1$. Let us compute the terms of this sequence. First of all, we have

$$\mathrm{H}^1(\mathrm{H}) = \bigoplus\nolimits'_{\mathrm{V(K_S)}} \mathrm{H}^1(\mathrm{I'_{\mathfrak{p}}(p)}) = \bigoplus_{\mathrm{V(K)}} \mathrm{Ind}_{\mathrm{D_{\mathfrak{p},K_S/K}}}^{\mathrm{G_S}} \mathrm{H}^1(\mathrm{I'_{\mathfrak{p}}(p)}),$$

as G_S-modules, where $D_{\mathfrak{p},K_S/K} \subseteq \mathrm{G}_S$ is the decomposition group at $\mathfrak{p}$, which is in particular pro-cyclic and has an infinite p-Sylow subgroup (by Corollary 4.21). Frobenius reciprocity resp. Shapiro's lemma imply:

$$\begin{aligned} E_2^{01} &= \bigoplus_{V(K)} \mathrm{H}^1(\mathrm{I'_{\mathfrak{p}}(p)})^{\mathrm{D_{\mathfrak{p},K_S/K}}}, \\ E_2^{11} &= \bigoplus_{V(K)} \mathrm{H}^1(\mathrm{D_{\mathfrak{p},K_S/K}}, \mathrm{H}^1(\mathrm{I'_{\mathfrak{p}}(p)})) = \bigoplus_{\mathrm{V(K)}} \mathrm{H}^2(\mathrm{D_{\mathfrak{p},K'_{S\cup V}(p)/K}}) = \bigoplus_{\mathrm{V(K)}} \mathrm{H}^2(\mathscr{G}_{\mathfrak{p}}), \end{aligned}$$

where the second line follows from Lemma 4.24.

Let $\delta := \delta_2^{01} \colon E_2^{01} \to E_2^{20}$ denote the differential in the second tableau. We obtain the following exact sequence (the first five terms of which are the five-term long exact sequence of Hochschild-Serre):

$$0 \longrightarrow \mathrm{H}^1(\mathrm{G_S}) \longrightarrow \mathrm{H}^1(\mathrm{G'_{S\cup V}(p)}) \longrightarrow \bigoplus_{V(K)} \mathrm{H}^1(\mathrm{I'_{\mathfrak{p}}(p)})^{\mathrm{D_{\mathfrak{p},K_S/K}}} \longrightarrow$$

$$\xrightarrow{\delta} \mathrm{H}^2(\mathrm{G_S}) \longrightarrow \mathrm{H}^2(\mathrm{G'_{S\cup V}(p)}) \xrightarrow{d} \bigoplus_{V(K)} \mathrm{H}^2(\mathscr{G}_{\mathfrak{p}}) \longrightarrow 0.$$

We show that the map in the sequence preceding δ is surjective. Indeed, we have

$$\mathrm{H}^1(\mathrm{G}'_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})) = \mathrm{H}^1(\mathrm{G}_{\mathrm{S}\cup\mathrm{V}}) \twoheadrightarrow \bigoplus_{\mathfrak{p}\in\mathrm{V}(\mathrm{K})} \mathrm{H}^1(\mathscr{G}_\mathfrak{p}) = \bigoplus_{\mathfrak{p}\in\mathrm{V}(\mathrm{K})} \mathrm{H}^1(\mathrm{D}_{\mathfrak{p},\mathrm{K}'_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})/\mathrm{K}}) \twoheadrightarrow \mathrm{H}^1(\mathrm{I}'_\mathfrak{p}(\mathrm{p}))^{\mathrm{D}_{\mathfrak{p},\mathrm{K}_\mathrm{S}/\mathrm{K}}},$$

where the second map is surjective by Grunwald-Wang theorem 4.15, and the second and the third maps follow from Lemma 4.24. Hence $\delta = 0$ and we obtain the short exact sequence:

$$0 \longrightarrow \mathrm{H}^2(\mathrm{G}_\mathrm{S}) \longrightarrow \mathrm{H}^2(\mathrm{G}'_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})) \xrightarrow{d} \bigoplus_{V(K)} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}) \longrightarrow 0,$$

which in turn gives the short exact sequence

$$0 \longrightarrow Ш^2(K_S/K, S) \longrightarrow Ш^2(K'_{S\cup V}(p)/K, S) \xrightarrow{d} \bigoplus_{V(K)} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}),$$

Finally, by definition of the Shafarevich group, we have the short exact sequence

$$0 \longrightarrow Ш^2(K'_{S\cup V}(p)/K, S\cup V) \longrightarrow Ш^2(K'_{S\cup V}(p)/K, S) \xrightarrow{d} \bigoplus_{V(K)} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}),$$

which shows that

$$Ш^2(K_S/K, S) \cong Ш^2(K'_{S\cup V}(p)/K, S\cup V) = Ш^2(K_{S\cup V}/K, S\cup V) = 0$$

the second equality being equation (4.7), and the last equality following from Corollary 4.11. □

We have the same statement in the pro-p case:

Proposition 4.35. *Let K be a number field, S a set of primes of K. Let p be a rational prime, $r > 0$ an integer and assume that S is p-stable for $K_{S\cup S_p\cup S_\infty}/K$ and has a p-stabilizing extension L_0 contained in $K_S(p)$. Assume p is odd or L_0 totally imaginary. Then*

$$Ш^2(K_S(p)/L; \mathbb{Z}/p^r\mathbb{Z}) = 0$$

for any finite $K_S(p)/L/L_0$, such that we are not in the special case (L, p^r, S).

Proof. We can assume $K = L$. We omit the coefficients $\mathbb{Z}/p^r\mathbb{Z}$ from the notation. Let us write $V := (S_p \cup S_\infty) \smallsetminus S$. Consider Galois groups of the extensions $K_{S\cup V}(p)/K_S(p)/K$:

$$1 \to \mathrm{G}_{K_{S\cup V}(p)/K_S(p)} \to \mathrm{G}_{S\cup V}(p) \to \mathrm{G}_S(p) \to 1.$$

Using the corresponding Hochschild-Serre spectral sequence, $\operatorname{cd} \mathrm{G}_{K,S}(p) = 2$, Grunwald-Wang theorem and Riemann's existence theorem, one obtains exactly as in the proof of Proposition 4.34 the following short exact sequence:

$$0 \to \mathrm{H}^2(\mathrm{G}_\mathrm{S}(\mathrm{p})) \to \mathrm{H}^2(\mathrm{G}_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})) \to \bigoplus_{\mathrm{V(K)}} \mathrm{H}^2(\mathrm{D}_{\mathfrak{p},\mathrm{K}_{\mathrm{S}\cup\mathrm{V}}(\mathrm{p})/\mathrm{K}}) \to 0. \tag{4.8}$$

Further one has:

$$Ш^2(K_S(p)/K, S) \cong Ш^2(K_{S\cup V}(p)/K, S\cup V) = Ш^2(K_{S\cup V}/K, S\cup V) = 0,$$

where the first isomorphism follows from the sequence (4.8) in the same way as in the proof of Proposition 4.34, the second follows form [NSW] 7.5.8 and 10.4.8 and the the last is Corollary 4.11. □

4.9 Stability and the order of $Ш^1$.

Now we generalize the results from Section 4.3, and study the connection between stability and the order of the first Shafarevich group with trivial coefficients.

Proposition 4.36. *Let K be a number field, $\mathscr{L}/K$ a Galois extension, p^m some rational prime power ($m \geqslant 1$). Let T be a set of primes of K, which is p^m-stable for $\mathscr{L}/K$, with p^m-stabilizing field L_0. Then*

$$\sharp Ш^1(\mathscr{L}/L, T; \mathbb{Z}/p^r\mathbb{Z}) < p^m$$

for any $r > 0$ and any finite $\mathscr{L}/L/L_0$.

Proof. Let $T_0 \subseteq T$ and $a > 0$ be such that $a \leqslant \delta_L(T_0) < p^m a$ for all finite $\mathscr{L}/L/L_0$. Let $\mathscr{L}/L/L_0$ be a finite extension. Assume that $\sharp Ш^1(\mathscr{L}/L, T; \mathbb{Z}/p^r\mathbb{Z}) \geqslant p^m$. Then also

$$\sharp Ш^1(\mathscr{L}/L, T_0; \mathbb{Z}/p^r\mathbb{Z}) \geqslant p^m$$

and we have:

$$Ш^1(\mathscr{L}/L, T_0; \mathbb{Z}/p^r\mathbb{Z}) \cong \mathrm{Hom}(\mathrm{G}^{T_0}_{\mathscr{L}/L}(p), \mathbb{Z}/p^r\mathbb{Z}) = (\mathrm{G}^{T_0}_{\mathscr{L}/L}(p)^{\mathrm{ab}}/p^r)^\vee.$$

Thus $\sharp Ш^1(\mathscr{L}/L, T_0; \mathbb{Z}/p^r\mathbb{Z}) \geqslant p^m$ implies $\sharp \mathrm{G}^{T_0}_{\mathscr{L}/L}(p)^{\mathrm{ab}}/p^r \geqslant p^m$, and if M/L is the subextension of $\mathscr{L}/L$, corresponding to $\mathrm{G}^{T_0}_{\mathscr{L}/L}(p)^{\mathrm{ab}}/p^r$, then it has a finite subextension M_1 of degree $\geqslant p^m$, which is completely split in T_0, hence $\delta_{M_1}(T_0) \geqslant p^m\delta_L(T_0)$, which is a contradiction to p^m-stability of T_0. □

Corollary 4.37. *Let K be a number field, $\mathscr{L}/K$ a Galois extension, and T a set of primes of K stable for $\mathscr{L}/K$. Then $Ш^1(\mathscr{L}/K, T; \mathbb{Q}_p/\mathbb{Z}_p)$ is finite for any p.*

Proof. Since $\varinjlim$ is exact and commutes with cohomology, we have

$$Ш^1(\mathscr{L}/K, T; \mathbb{Q}_p/\mathbb{Z}_p) = \varinjlim_r Ш^1(\mathscr{L}/K, T; \mathbb{Z}/p^r\mathbb{Z}).$$

It is enough to show that $\sharp Ш^1(\mathscr{L}/K, T; \mathbb{Z}/p^r\mathbb{Z})$ is uniformly bounded for $r > 0$.

By Proposition 3.11, there is some $m \geqslant 1$, such that K is a p^m-stabilizing field for T for $\mathscr{L}/K$. Then Proposition 4.36 implies $\sharp Ш^1(\mathscr{L}/K, T; \mathbb{Z}/p^r\mathbb{Z}) < p^m$, which gives the required uniform bound. □

Corollary 4.38. *Let K be a number field, $\mathscr{L}/K$ a Galois extension, T a set of primes of K stable for $\mathscr{L}/K$. Then $Ш^1(\mathscr{L}/K, T; \mathbb{Q}/\mathbb{Z})$ is finite.*

Proof. Clearly, $Ш^1(\mathscr{L}/K, T; \mathbb{Q}/\mathbb{Z}) \cong \bigoplus_p Ш^1(\mathscr{L}/K, T; \mathbb{Q}_p/\mathbb{Z}_p)$. Previous corollary shows that each of the summands is finite. Moreover, almost all are zero: there is some $\lambda > 1$, such that K is λ-stabilizing field for T for $\mathscr{L}/K$. Thus for any $p \geqslant \lambda$, the group $Ш^1(\mathscr{L}/K, T; \mathbb{Q}_p/\mathbb{Z}_p)$ vanishes. □

5 K$(\pi, 1)$-property of rings of integers

In this section we consider the K$(\pi, 1)$ property of schemes $\operatorname{Spec} \mathcal{O}_{K,S}$ where K is a number field and S is a set of primes. Essentially, we prove that if S satisfies $(*)_p^{\mathrm{stab}}$, then $\operatorname{Spec} \mathcal{O}_{K,S}$ is K$(\pi, 1)$ for p.

5.1 Overview

Let K be a number field, S a set of primes of K and p a rational prime. Assume that either p is odd or K is totally imaginary and let

$$X = \operatorname{Spec} \mathcal{O}_{K,S}.$$

We study under which conditions X is an algebraic K$(\pi, 1)$ space (for p). While it is well known that X is algebraic K$(\pi, 1)$ for p if either

- $S \supseteq S_p \cup S_\infty$ ("wild case"), or
- $\delta_K(S) = 1$,

it is a challenging problem to determine whether X is K$(\pi, 1)$ if S is finite and not necessarily contains $S_p \cup S_\infty$. There are no (non-trivial) examples of K, S such that X is not a K$(\pi, 1)$ for p, and until recently there were also no examples of (K, S) such that X is K$(\pi, 1)$ for p or pro-p K$(\pi, 1)$. Recent results of A. Schmidt ([Sch], [Sch2], cf. also [Sch3]) show that the finite sets S, such that X is a pro-p K$(\pi, 1)$ are in some sense cofinal in the set of all primes of K. That means, given K, S and p and any set T of primes of K of density 1, one can find a finite subset $T_1 \subseteq T$ such that $X \smallsetminus T_1$ is pro-p K$(\pi, 1)$. The main ingredient in the proof is the theory of mild pro-p groups, developed by Labute. Since stable sets generalize sets of density 1 in many arithmetic aspects, the following question is quite natural.

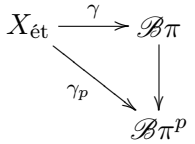
Question 5.1. Can one replace the condition $\delta_K(T) = 1$ in Schmidt's work by the weaker condition that T is stable (or p-stable or satisfies $(*)_p^{\mathrm{stab}}$)?

In the present section we enlarge the examples of such pairs (K, S), for which X is algebraic K$(\pi, 1)$ for p and prove essentially that if S satisfies $(*)_p^{\mathrm{stab}}$, then X is algebraic K$(\pi, 1)$ for p. In particular, if S is almost Chebotarev set and $\infty \notin E^{\mathrm{stab}}(S)$ (cf. Proposition 3.18 and Example 3.20), then X is algebraic K$(\pi, 1)$ for almost all primes p, and if $E^{\mathrm{stab}}(S) = \varnothing$ (cf. Examples 3.21 and 3.22), then X algebraic K$(\pi, 1)$.

5.2 Definitions

There are many equivalent ways to define algebraic K$(\pi, 1)$-spaces (cf. [St] Appendix A, where they are discussed in detail). Without repeating all of them, we want to introduce a small refinement of terminology, such that it is better adapted to formulate our results.

To begin with, let X be a connected scheme, $X_{\text{ét}}$ the étale site on X. Fix a geometric point $\bar{x} \in X$ and let $\pi := \pi_1(X, \bar{x})$ be the étale fundamental group of X. Let $\mathscr{B}\pi$ denote the site of continuous π-sets endowed with the canonical topology. Let further p be a rational prime, and let $\mathscr{B}\pi^p$ denote the site of continuous $\pi^{(p)}$-sets, where $\pi^{(p)}$ is the pro-p completion of π. As in [St] A.1, we have natural continuous maps of sites



For a site Y, let $\mathscr{S}(Y)$ denote the category of sheaves of abelian groups on Y, let $\mathscr{S}(Y)_f$ be the subcategory of locally constant torsion sheaves, and $\mathscr{S}(Y)_p$ the subcategory of locally constant p-primary torsion sheaves. Let $A \in \mathscr{S}(\mathscr{B}\pi)_f$ resp. $B \in \mathscr{S}(\mathscr{B}\pi^p)_p$. Then we have the natural transformations of functors $\mathrm{id} \to \mathrm{R}\,\gamma_*\gamma^*$ resp. $\mathrm{id} \to \mathrm{R}\,\gamma_{p,*}\gamma_p^*$, which induce maps in the cohomology:

$$\begin{aligned} c_A^i\colon &\quad \mathrm{H^i}(\pi, \mathrm{A}) &&\longrightarrow \mathrm{H^i}(\mathrm{X_{\acute{e}t}}, \gamma^*\mathrm{A}) \\ c_{p,B}^i\colon &\quad \mathrm{H^i}(\pi^{(\mathrm{p})}, \mathrm{B}) &&\longrightarrow \mathrm{H^i}(\mathrm{X_{\acute{e}t}}, \gamma_{\mathrm{p}}^*\mathrm{B}) \end{aligned}$$

Let $\tilde{X}$ resp. $\tilde{X}(p)$ denote the universal resp. the universal pro-p covering of X. Since

$$\mathrm{H}^1(\tilde{\mathrm{X}}_{\mathrm{et}}, \mathrm{A}) = \mathrm{H}^1(\tilde{\mathrm{X}}(\mathrm{p})_{\mathrm{et}}, \mathrm{B}) = 0$$

for each A, B, the maps c_A^i and $c_{p,B}^i$ are isomorphisms for $i = 0, 1$ and are injective for $i = 2$.

Definition 5.2. Let X be a connected scheme.

(i) X is *algebraic* $\mathrm{K}(\pi, 1)$ if c_A^i is an isomorphism for all $A \in \mathscr{S}(\mathscr{B}\pi)_f$ for all $i \geqslant 0$.

(ii) X is *algebraic* $\mathrm{K}(\pi, 1)$ *for* p if c_A^i is an isomorphism for all $A \in \mathscr{S}(\mathscr{B}\pi)_p$ for all $i \geqslant 0$.

(iii) X is *pro-*p $\mathrm{K}(\pi, 1)$ if $c_{p,B}^i$ is an isomorphism for all $B \in \mathscr{S}(\mathscr{B}\pi^p)_p$ for all $i \geqslant 0$.

Notice that we use a shift in the definitions compared with [Sch] or [Wi2]: what there is called algebraic $\mathrm{K}(\pi, 1)$ for p, we call here pro-p $\mathrm{K}(\pi, 1)$. Parts (i) and (iii) of our definition coincide with the definition of $K(\pi, 1)$ in [St] A.1.2. By decomposing any sheaf into p-primary components we obtain:

Lemma 5.3. *X is algebraic $\mathrm{K}(\pi, 1)$ if and only if it is algebraic $\mathrm{K}(\pi, 1)$ for all p.*

A space is $\mathrm{K}(\pi, 1)$ if and only if an étale covering is (for a proof cf. [St] A.2.3):

Proposition 5.4. *Let X be a connected scheme and $Y \twoheadrightarrow X$ a connected pro-étale Galois cover. Then*

(i) X is algebraic $\mathrm{K}(\pi, 1) \Leftrightarrow Y$ is algebraic $\mathrm{K}(\pi, 1)$.

(ii) X is algebraic $\mathrm{K}(\pi, 1)$ for $p \Leftrightarrow Y$ is algebraic $\mathrm{K}(\pi, 1)$ for p.

(iii) If $Y \twoheadrightarrow X$ is a pro-p cover, then: X is pro-p $\mathrm{K}(\pi, 1) \Leftrightarrow Y$ is pro-p $\mathrm{K}(\pi, 1)$.

Lemma 5.5. *Let X be a connected scheme. The following are equivalent:*

(i) X is algebraic $\mathrm{K}(\pi, 1)$ for p.

(ii) the maps c_A^i are isomorphisms for all $i \geqslant 0$ and all finite simple π-modules A such that $pA = 0$.

Proof. Dévissage into simple π-modules. □

Lemma 5.6 (cf. [Sch] Proposition 2.1 (iv) $\Leftrightarrow$ (v))**.** *Let X be a connected scheme. The following are equivalent:*

(i) X is pro-p $\mathrm{K}(\pi, 1)$.

(ii) the maps $c^i_{p,\mathbb{Z}/p\mathbb{Z}}$ are isomorphisms for all $i \geqslant 0$.

Proof. Dévissage into simple $\pi^{(p)}$-modules and the fact that the only simple module under a pro-p group, which is killed by p, is trivial. □

5.3 Criterions for being $\mathrm{K}(\pi, 1)$

We repeat some well-known equivalent reformulations of $\mathrm{K}(\pi, 1)$ properties of rings of integers $\operatorname{Spec} \mathcal{O}_{K,S}$, where K is a number field and $S \supseteq S_\infty$ a set of primes.

5.3.1 Wild case

Let p be a rational prime, K a number field and S a set of primes of K. One says that one is in the *wild case*, if $S \supseteq S_p \cup S_\infty$. The wild case is well-understood:

Proposition 5.7 (cf. [Zi] Proposition 3.3.1, cf. also [Sch] Proposition 2.3)**.** *Let K be a number field and $S \supseteq S_p \cup S_\infty$ a set of primes of K. Assume that either p is odd, or K is totally imaginary. Then $\operatorname{Spec} \mathcal{O}_{K,S}$ is a pro-p $\mathrm{K}(\pi, 1)$ and an algebraic $\mathrm{K}(\pi, 1)$ for p.*

Proof. That $\operatorname{Spec} \mathcal{O}_{K,S}$ is algebraic $\mathrm{K}(\pi, 1)$ is shown by Zink in [Zi] Proposition 3.3.1. The pro-p case follows using [NSW] 10.4.8. □

5.3.2 A general criterion

For a scheme X let Fet_X denote the category of all finite étale coverings of X. For a number field K let

$$\delta_K = \begin{cases} 1 & \text{if } \mu_p \subseteq K, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 5.8. *Let K be a number field, $S \supseteq S_\infty$ a set of primes of K such that either $\delta_K = 0$ or $S_f \neq \varnothing$. Assume that either p is odd or K is totally imaginary. Let $X = \operatorname{Spec} \mathcal{O}_{K,S}$. The following are equivalent:*

(i) X is an algebraic $K(\pi, 1)$ for p.

(ii) One has

$$\varinjlim_{Y \in \mathrm{Fet}_X} \mathrm{H}^2(\mathrm{Y}_{\text{ét}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) = 0.$$

Proof. (i) $\Rightarrow$ (ii) holds for any connected scheme and follows from [St] A.3.1 and Proposition 5.4. Indeed, if X is $\mathrm{K}(\pi,1)$ for p, then any finite étale connected cover Y/X is and hence the map

$$\mathrm{H}^2(\mathrm{Y}_{\text{ét}},\mathbb{Z}/\mathrm{p}\mathbb{Z}) \to \varinjlim_{\mathrm{Z}\in\mathrm{Fet}_{\mathrm{Y}}} \mathrm{H}^2(\mathrm{Z}_{\text{ét}},\mathbb{Z}/\mathrm{p}\mathbb{Z})$$

is zero. This shows $\varinjlim_{Y\in\mathrm{Fet}_X} \mathrm{H}^2(\mathrm{Y}_{\text{ét}},\mathbb{Z}/\mathrm{p}\mathbb{Z}) = 0$.

(ii) $\Rightarrow$ (i). By [St] A.3.1 we have to show that for every $q > 0$ and every locally constant p-primary torsion sheaf A on $X_{\text{ét}}$, the map

$$\mathrm{H}^{\mathrm{q}}(\mathrm{X}_{\text{ét}},\mathrm{A}) \to \varinjlim_{\mathrm{Y}\in\mathrm{Fet}_{\mathrm{X}}} \mathrm{H}^{\mathrm{q}}(\mathrm{Y}_{\text{ét}},\mathrm{A}|_{\mathrm{Y}}) \tag{5.1}$$

is zero. This would follow from the even stronger statement that

$$\varinjlim_{Y\in\mathrm{Fet}_X} \mathrm{H}^{\mathrm{q}}(\mathrm{Y}_{\text{ét}},\mathrm{A}|_{\mathrm{Y}}) = 0$$

for each $q > 0$ and A as above. But since A is trivialized on some $Y \in \mathrm{Fet}_X$, we can assume that A is constant. By dévissage we are reduced to the case $A = \mathbb{Z}/p\mathbb{Z}$. The elements of $\mathrm{H}^1(\mathrm{Y}_{\text{ét}},\mathbb{Z}/\mathrm{p}\mathbb{Z})$ can be interpreted as torsors, which kill themselves. Thus we have $\varinjlim_{Y\in\mathrm{Fet}_X} \mathrm{H}^1(\mathrm{Y}_{\text{ét}},\mathbb{Z}/\mathrm{p}\mathbb{Z}) = 0$. Further by [SGA 4] Exposé X Proposition 6.1, $\mathrm{H}^{\mathrm{q}}(\mathrm{Y}_{\text{ét}},\mathbb{Z}/\mathrm{p}\mathbb{Z}) = 0$ for $q > 3$. Lemma 5.9 implies the case $q = 3$. Finally, the condition in (ii) gives the last piece of information, so that the map (5.1) is zero for any q, and thus X is a $K(\pi,1)$-space. □

Lemma 5.9. *Let K be a number field, S a set of primes primes of K. Assume p is odd or K is totally imaginary. Let $X = \operatorname{Spec}\mathcal{O}_{K,S}$. If $\delta_K = 0$ or $S_f \neq \varnothing$, then $\mathrm{H}^3(\mathrm{X}_{\text{ét}},\mathbb{Z}/\mathrm{p}\mathbb{Z}) = 0$.*

Proof. Let $\bar{X} = \operatorname{Spec}\mathcal{O}_K$. We consider X as an open subscheme of $\bar{X}$. The Artin-Verdier duality (cf. [Ma] 2.4 if K is totally imaginary, and [Zi] Theorem 3.2 and Corollary 2.4 if p is odd) implies a perfect pairing

$$\mathrm{H}^{\mathrm{r}}(\bar{\mathrm{X}},\mathrm{F}) \times \mathrm{Ext}^{3-\mathrm{r}}_{\bar{\mathrm{X}}}(\mathrm{F},\mathbb{G}_{\mathrm{m},\bar{\mathrm{X}}}) \to \mathrm{H}^3(\bar{\mathrm{X}},\mathrm{F}),$$

for any constructible sheaf F on $\bar{X}$ (we are only interested in the case $F = \mathbb{Z}/p\mathbb{Z}$). This can be used to compute (compare [Ma] 2.4):

$$\mathrm{H}^3(\bar{\mathrm{X}},\mathbb{Z}/\mathrm{p}\mathbb{Z}) = \mu_{\mathrm{p}}(\mathrm{K})^\vee,$$

where $(\cdot)^\vee$ denotes the Pontrjagin dual. Further, [Ma] 2.5 gives the exact sequence

$$\ldots \to \prod_{\mathfrak{p}\in S_f} \mu_p(K_\mathfrak{p})^\vee \to \mu_p(K)^\vee \to \mathrm{H}^3(\mathrm{X},\mathbb{Z}/\mathrm{p}\mathbb{Z}) \to 0. \tag{5.2}$$

Since $\delta_K = 0$ or $S_f \neq \varnothing$, the map $\mu_p(K) \to \prod_{\mathfrak{p}\in S_f} \mu_p(K_\mathfrak{p})$ is injective, hence the map on the left side in (5.2) is surjective. Hence $\mathrm{H}^3(\mathrm{X},\mathbb{Z}/\mathrm{p}\mathbb{Z}) = 0$. □

The same also holds in the pro-p case. Let $\mathrm{Fet}_X^{(p)}$ denote the category of finite étale pro-p coverings of X.

Proposition 5.10. *Let K be a number field, $S \supseteq S_\infty$ a set of primes of K such that either $\delta_K = 0$ or $S_f \neq \varnothing$. Let $X = \operatorname{Spec} \mathcal{O}_{K,S}$. Assume p is odd or K is totally imaginary. The following are equivalent:*

(i) X is a pro-p $K(\pi, 1)$.

(ii) One has

$$\varinjlim_{Y \in \mathrm{Fet}_X^{(p)}} \mathrm{H}^2(\mathrm{Y}_{\text{ét}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) = 0.$$

Remark 5.11 (A criterion of Wingberg in the pro-p case, cf. [Wi2] Proposition 2.1 (i) $\Leftrightarrow$ (iv))**.** For rational prime p and a prime $\mathfrak{p}$ of K, let $I_{\mathfrak{p}}(p) \subseteq \mathrm{G}_{K_{\mathfrak{p}}(p)/K_{\mathfrak{p}}}$ denote the inertia group of $K_{\mathfrak{p}}(p)/K_{\mathfrak{p}}$. Assume that either p is odd or K is totally imaginary. Let S be a set of primes of K. The following are equivalent:

(i) $\operatorname{Spec} \mathcal{O}_{K,S}$ is a pro-p $\mathrm{K}(\pi, 1)$.

(ii) The following assertions hold:

- $\operatorname{cd} \mathrm{G}_{K,S}(p) \leqslant 2$,
- $c^2_{p,\mathbb{Z}/p\mathbb{Z}}$ is bijective.

(iii) The following assertions hold:

- $\operatorname{cd} \mathrm{G}_{K,S}(p) \leqslant 2$,
- $\mathrm{H}^1(\mathrm{K}_{\mathrm{S}\cup\mathrm{S}_\mathrm{p}}(\mathrm{p})/\mathrm{K}_\mathrm{S}(\mathrm{p}), \mathbb{Z}/\mathrm{p}\mathbb{Z}) \xrightarrow{\sim} \bigoplus_{\mathfrak{p} \in (\mathrm{S}_\mathrm{p} \smallsetminus \mathrm{S})(\mathrm{K})} \mathrm{H}^1(\mathrm{I}_{\mathfrak{p}}(\mathrm{p}), \mathbb{Z}/\mathrm{p}\mathbb{Z})^{\mathrm{G}_{\mathrm{K}_{\mathfrak{p}}(\mathrm{p})/\mathrm{K}_{\mathfrak{p}}}}$,
- $\dim \operatorname{coker}^1(K_S(p)/K, S; \mathbb{Z}/p\mathbb{Z}) = \delta_K$.

Now (iii) is the most manageable list of conditions: there is "only" group cohomology of $\mathrm{G}_{K,S}(p)$ involved in it, and the second condition is a form of Riemann's existence theorem. In the case of the whole site Fet_X an analogous criterion would be more complicate, since in contrast to $\mathrm{G}_{K,S}(p)$, a simple $\mathrm{G}_{K,S}$-module, which is killed by p is not necessarily trivial.

5.4 Results

Theorem 5.12. *Let K be a number field, $S \supseteq S_\infty$ a set of primes of K and p a rational prime. Assume that either p is odd or K is totally imaginary.*

(i) Assume that S is p-stable for $K_{S\cup S_p}/K$ and has a p-stabilizing extension contained in $K_S(p)$. Then $\operatorname{Spec} \mathcal{O}_{K,S}$ is a pro-p $\mathrm{K}(\pi, 1)$.

(ii) Assume that S is stable and satisfies $(*)_p^{\mathrm{stab}}$. Then $\operatorname{Spec} \mathcal{O}_{K,S}$ is an algebraic $\mathrm{K}(\pi, 1)$ for p.

Remark 5.13. In the pro-p case, the assumption $S_\infty \subseteq S$ is superfluous as $\mathrm{G}_S(p) = \mathrm{G}_{S\cup S_\infty}(p)$: if $p > 2$, then this is true in general and if $p = 2$, then this is true since we have assumed that K is totally imaginary.

Corollary 5.14. *Let K be a number field, $S \supseteq S_\infty$ a stable set of primes of K, satisfying $(*)^{\mathrm{stab}}$ (in particular S can be any stable almost Chebotarev set with $S \supseteq S_\infty$). Then* $\operatorname{Spec} \mathcal{O}_{K,S}$ *is algebraic $K(\pi,1)$-space for almost all primes p. If $E^{\mathrm{stab}}(S) = \varnothing$ and K is totally imaginary, then* $\operatorname{Spec} \mathcal{O}_{K,S}$ *is algebraic $K(\pi,1)$-space.*

Sets S with arbitrary small density and $E^{\mathrm{pers}}(S) = \varnothing$ (and hence also $E^{\mathrm{stab}}(S) = \varnothing$) can be found in Examples 3.21 and 3.22. Thus the corollary shows that there are sets S of arbitrary small density, such that $\operatorname{Spec} \mathcal{O}_{K,S}$ is an algebraic $K(\pi,1)$.

Corollary 5.15. *Let K be a number field, $S \supseteq S_\infty$ a set of primes of K and p a rational prime. Assume that either p is odd or K is totally imaginary.*

(i) Assume that S is p-stable for $K_{S\cup S_p}/K$ and has a p-stabilizing extension contained in $K_S(p)$. Then

$$\operatorname{cd} \mathrm{G}_{K,S}(p) = \operatorname{scd} \mathrm{G}_{K,S}(p) = 2.$$

(ii) Assume that S is stable and satisfies $(*)_p^{\mathrm{stab}}$. Then

$$\operatorname{cd}_p \mathrm{G}_{K,S} = \operatorname{scd}_p \mathrm{G}_{K,S} = 2.$$

Proof of Corollary 5.15. Since $S_f \neq \varnothing$, $\operatorname{Spec} \mathcal{O}_{K,S}$ has cohomological dimension 2. From Theorem 5.12 we obtain that $\operatorname{cd} \mathrm{G}_{K,S}(p) \leqslant 2$ (under (i)) resp. $\operatorname{cd}_p \mathrm{G}_{K,S} \leqslant 2$ (under (ii)). By Theorem 4.31 in the case (i) resp. by Corollary 4.33 in the case (ii), certain open subgroups of $\mathrm{G}_{K,S}(p)$ resp. $\mathrm{G}_{K,S}$ have cohomological dimension 2. This implies equality in both cases. The statements about the strict cohomological dimension follow from [NSW] 3.3.5(ii) using Theorem 4.31 resp. Corollary 4.33. □

Proof of Theorem 5.12. We begin with part (ii). Let $X := \operatorname{Spec} \mathcal{O}_{K,S}$. As L goes through finite subextensions of K_S/K, the normalization Y of X in L goes through all finite étale connected coverings of X. Let $V := S_p \setminus S$. For any such Y we have a decomposition

$$Y \setminus V \overset{j}{\hookrightarrow} Y \overset{i}{\hookleftarrow} V$$

in an open and a closed part. Now $Y \setminus V$ is a $\mathrm{K}(\pi,1)$ for p by Proposition 5.7 and since $\pi_1(Y \setminus V) = \mathrm{G}_{L,S\cup V}$, we obtain

$$c_A^i \colon \mathrm{H}^{\mathrm{i}}(\mathrm{G}_{\mathrm{L,S\cup V}}) \xrightarrow{\sim} \mathrm{H}^{\mathrm{i}}((\mathrm{Y} \setminus \mathrm{V})_{\text{ét}}, \mathrm{A}) \tag{5.3}$$

is an isomorphism for any $i \geqslant 0$ and any p-primary $\mathrm{G}_{L,S\cup V}$-module A. We have the Lerray spectral sequence for j:

$$E_2^{mn} = \mathrm{H}^{\mathrm{m}}(\mathrm{Y}, \mathrm{R}^{\mathrm{n}}\mathrm{j}_*\mathbb{Z}/\mathrm{p}\mathbb{Z}) \Rightarrow \mathrm{H}^{\mathrm{m+n}}(\mathrm{Y} \setminus \mathrm{V}, \mathbb{Z}/\mathrm{p}\mathbb{Z}).$$

Let us compute the terms in this spectral sequence. First of all we have

$$R^n j_* \mathbb{Z}/p\mathbb{Z} = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } n = 0, \\ \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^1(\mathscr{I}_{\mathfrak{p}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & \text{if } n = 1, \\ 0 & \text{if } n > 1, \end{cases}$$

where $\mathscr{I}_\mathfrak{p} \subseteq \mathscr{G}_\mathfrak{p}$ denotes the inertia subgroup of the full local Galois group at $\mathfrak{p}$. Thus

$$\begin{aligned} E_2^{01} &= \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^1(\mathscr{I}_\mathfrak{p}, \mathbb{Z}/\mathrm{p}\mathbb{Z})^{\mathscr{G}_\mathfrak{p}^{\mathrm{nr}}} \\ E_2^{11} &= \mathrm{H}^1(\mathrm{Y}_{\text{ét}}, \bigoplus_{\mathfrak{p}\in \mathrm{V}} \mathrm{H}^1(\mathscr{I}_\mathfrak{p}, \mathbb{Z}/\mathrm{p}\mathbb{Z})) = \bigoplus_{\mathfrak{p}\in \mathrm{V}} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \end{aligned}$$

and $E_2^{mn} = 0$ if $n > 1$ or if $n = 1$ and $m > 1$ (as $\mathrm{cd}_p(\mathscr{G}_\mathfrak{p}^{\mathrm{nr}}) = 1$). Further, $E_2^{m0} = 0$ for $m > 3$, as $\mathrm{cd}_p Y \leqslant 3$ and $E_2^{30} = \mathrm{H}^2(\mathrm{Y}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) = 0$ by Lemma 5.9. Further,

$$E_2^{10} = \mathrm{H}^1(\mathrm{Y}_{\text{ét}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) = \mathrm{H}^1(\mathrm{G}_{\mathrm{L,S}}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$$

Thus we have the following non-zero entries in the second tableau:

$$\begin{array}{cccc} \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^1(\mathscr{I}_\mathfrak{p}, \mathbb{Z}/\mathrm{p}\mathbb{Z})^{\mathscr{G}_\mathfrak{p}^{\mathrm{nr}}} & \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & 0 & 0 \\ & \searrow^{\delta_2^{01}} & & \\ \mathbb{Z}/p\mathbb{Z} & \mathrm{H}^1(\mathrm{G}_{\mathrm{L,S}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & \mathrm{H}^2(\mathrm{Y}_{\text{ét}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) & 0 \end{array}$$

From this and the isomorphism (5.3) we obtain the following exact sequence (from now on, we omit the $\mathbb{Z}/p\mathbb{Z}$-coefficients):

$$0 \longrightarrow \mathrm{H}^1(\mathrm{G}_{\mathrm{L,S}}) \longrightarrow \mathrm{H}^1(\mathrm{G}_{\mathrm{L,S\cup V}}) \longrightarrow \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^1(\mathscr{I}_\mathfrak{p})^{\mathscr{G}_\mathfrak{p}^{\mathrm{nr}}} \xrightarrow{\delta_2^{01}}$$

$$\longrightarrow \mathrm{H}^2(\mathrm{Y}_{\text{ét}}) \longrightarrow \mathrm{H}^2(\mathrm{G}_{\mathrm{L,S\cup V}}) \longrightarrow \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}) \longrightarrow 0$$

By Proposition 5.8 it is enough to show that $\varinjlim_{Y\in \mathrm{Fet}_X} \mathrm{H}^2(\mathrm{Y}_{\text{ét}}) = 0$. Therefore, we can go up in the tower and assume that L contains a p-stabilizing extension for S for $K_{S\cup S_p\cup S_\infty}$. For such L the map preceding δ_2^{01} is surjective by Grunwald-Wang Theorem 4.15, i.e., $\delta_2^{01} = 0$ and hence

$$\mathrm{H}^2(Y_{\text{ét}}) \cong Ш^2(K_{S\cup V}/L, V; \mathbb{Z}/p\mathbb{Z}).$$

To finish the proof consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{H}^2(\mathrm{G}_{\mathrm{L,S\cup V}}) & \longrightarrow & \bigoplus_{\mathfrak{p}\in S\cup V} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}) & \longrightarrow & \mu_p(L)^\vee & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}) & \xrightarrow{=} & \bigoplus_{\mathfrak{p}\in V} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}) & \longrightarrow & 0 & \longrightarrow & 0, \end{array}$$

in which the exactness of the upper row follows from $Ш^2(K_{S\cup V}/L, S\cup V; \mathbb{Z}/p\mathbb{Z}) = 0$ (cf. Corollary 4.11 or Proposition 4.34) and from the long exact Poitou-Tate sequence. Snake lemma shows that

$$\varinjlim_{Y\in \mathrm{Fet}_X} \mathrm{H}^2(Y_{\text{ét}}) \cong \varinjlim_{Y\in \mathrm{Fet}_X} Ш^2(K_{S\cup V}/L, V; \mathbb{Z}/p\mathbb{Z}) \subseteq \varinjlim_{Y\in \mathrm{Fet}_X} \bigoplus_{\mathfrak{p}\in S} \mathrm{H}^2(\mathscr{G}_\mathfrak{p}),$$

and the last limit vanishes as $p^\infty | [K_{S,\mathfrak{p}} : K_\mathfrak{p}]$ for all $\mathfrak{p} \in S$ by Proposition 4.21. This finishes the proof of (ii).

(i) has the the same proof as (ii), with the only difference that one has to use the pro-p versions of corresponding results: one must use Proposition 4.35 instead of Proposition 4.34 and Proposition 5.10 instead of Proposition 5.8. □

Remark 5.16. Part (i) of Theorem 5.12 can also be shown using the criterion 5.11 of Wingberg, which itself follows from Lemma 5.6. The application of the analogous criterion to (ii) has the drawback that, in contrast to the pro-p case, there are non-trivial simple G_S-modules killed by p, i.e., only Lemma 5.5 is available, and the criterion gets accordingly more complicate.

6 Anabelian geometry of curves $\mathrm{Spec}(\mathcal{O}_{K,S})$ with S stable

In this section we generalize the birational anabelian result of Neukirch [Ne] to the case of "almost arithmetic curves", i.e., the curves $\mathrm{Spec}\,\mathcal{O}_{K,S}$ with S stable.

6.1 Overview

We will give two versions of the main theorem, with varying assumptions. Therefore, consider the following condition on a number field K and a set S of primes of K:

$Dec(K,S)$ For every $\bar{\mathfrak{p}} \in S_f$, the decomposition group $D_{\bar{\mathfrak{p}}} \subseteq \mathrm{G}_S$ is the full local group

It is for example satisfied, if there is a totally real subfield K_0 of K and a set S_0 of primes of K_0 with $S = S_{0,K}$ (with other words, S is defined over a totally real subfield) and such that $S \supseteq S_{p_1 p_2 \infty}$ for two different rational primes p_1, p_2 (cf. [CC] Theorem 5.1 and Remark 5.3(i)), or if S is stable and $E^{\mathrm{stab}}(S) = \varnothing$ (cf. Corollary 4.21).

Theorem 6.1 (Under Dec)**.** *For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i, such that $Dec(K_i, S_i)$ holds and*

- *K_1 is normal over $\mathbb{Q}$,*
- *for $i = 1, 2$, the set S_i is stable and satisfies $(*)^{\mathrm{stab}}_{\ell_i}$ for some odd prime ℓ_i,*
- *there are two odd rational primes under S_1 and $S_\infty \subseteq S_1$,*
- *there is a rational prime under S_2.*

If $\mathrm{G}_{K_1,S_1} \cong \mathrm{G}_{K_2,S_2}$, then $K_1 \cong K_2$.

Theorem 6.2 (Without Dec)**.** *For $i = 1, 2$, let K_i be a number field and S_i a set of primes of K_i, such that*

- *K_1 is normal over $\mathbb{Q}$,*
- *for $i = 1, 2$, the set S_i is stable and satisfies $(*)^{\mathrm{stab}}$,*
- *there are two different odd primes $\ell_1, \ell_2 \notin E^{\mathrm{stab}}(S_i)$ such that $\mu_{\ell_1 \ell_2} \subseteq K_{i,S_i}$ for $i \in \{1, 2\}$,*
- *there are two odd rational primes under S_1 and $S_\infty \subseteq S_1$,*
- *there is a rational p with $S_p \subseteq S_2$ and $p \notin E^{\mathrm{stab}}(S_i)$ for $i \in \{1, 2\}$.*

If $\mathrm{G}_{K_1,S_1} \cong \mathrm{G}_{K_2,S_2}$, then $K_1 \cong K_2$.

In Section 6.2 we deal with the local correspondence at the boundary which is needed in the proof of the above theorems. In sections 6.3 and 6.4 we prepare two further arguments, and finally in Section 6.5 we prove Theorems 6.1 and 6.2.

6.2 Local correspondence at the boundary

6.2.1 Definition

For $i = 1, 2$, let (K_i, S_i) be a number field and a set of primes of K_i and let

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

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, if the following conditions are satisfied:

(i) for any $\bar{\mathfrak{p}}_1 \in S_{1,f}(K_{1,S_1})$, there is a unique prime $\sigma_*(\bar{\mathfrak{p}}_1) \in S_{2,f}(K_{2,S_2})$, with $\sigma(D_{\bar{\mathfrak{p}}_1}) = D_{\sigma_*(\bar{\mathfrak{p}}_1)}$, such that σ induces a bijection

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

which is Galois-equivariant, i.e.

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

for each $g \in \mathrm{G}_{K_1,S_1}, \bar{\mathfrak{p}}_1 \in S_{1,f}(K_{1,S_1})$. In particular, for any finite subextension L_1 of $K_{1,S_1}/K_1$ with corresponding open subgroup $U_1 \subseteq \mathrm{G}_{K_1,S_1}$, 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

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

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

6.2.2 Under condition *Dec*

Theorem 6.3. *Let K be a number field and S a set of primes, such that* $\mathrm{Dec}(K, S)$ *is satisfied. Assume S is stable and satisfies $(*)_p^{\mathrm{stab}}$ for some $p > 2$. Then any subgroup of $\mathrm{G}_{K,S}$, which is isomorphic to an absolute Galois group of a local field with characteristic zero, is contained in a decomposition subgroup of a unique prime in S_f.*

In particular, the decomposition subgroups in $\mathrm{G}_{K,S}$ at primes in S_f are exactly the subgroups, which are isomorphic to local absolute Galois groups in characteristic zero and maximal with this property.

(Recall that local field means a non-archimedean local field).

Lemma 6.4. *Let K be a number field and S a set of primes. Assume S is stable and satisfies $(*)_p^{\mathrm{stab}}$ for some p. Then the following holds.*

(i) The intersection of two p-Sylow subgroups of two different decomposition groups inside $\mathrm{G}_{K,S}$ *is not open in each of them. The intersection of two different decomposition subgroups at primes in* S_f *inside* $\mathrm{G}_{K,S}$ *is not open in each of them.*

(ii) Let $H \subseteq \mathrm{G}_{K,S}$ *be a closed subgroup and* $H_0 \subseteq H$ *an open subgroup. If there is a prime* $\bar{\mathfrak{p}} \in S_f(K_S)$ *with* $H_0 \subseteq D_{\bar{\mathfrak{p}}}$*, then* $H \subseteq D_{\bar{\mathfrak{p}}}$*.*

Proof. (i) is Proposition 4.25. (ii) follows from (i) in the same way as in Corollary 1.7(i). □

Proof of the theorem. Uniqueness follows from Lemma 6.4(i) and Lemma 2.1. Start with a subgroup $H \subseteq \mathrm{G}_{K,S}$, which is isomorphic to a local absolute Galois group of a field κ of characteristic zero. Let $p > 2$ be a rational prime such that S satisfies $(*)_p^{\mathrm{stab}}$. By Lemma 6.4(ii), it is enough to show that an open subgroup of H is contained in a decomposition group. By replacing H by the intersection of kernels of all homomorphisms $H \to \mathbb{Z}/(p-1)\mathbb{Z}$, we can assume that $\mu_p \subset \kappa$. By Proposition 4.34, there is an open subgroup $U_0 \subseteq \mathrm{G}_{K,S}$, such that for any open $U \subseteq U_0$, we have $Ш^2(U; \mathbb{Z}/p\mathbb{Z}) = 0$. We can replace H by $H \cap U_0$. Let $M := K_S^H$. Taking the limit over all $U \subseteq U_0$, which contain H, we obtain by Lemma 2.13 an injection

$$\mathrm{H}^2(\mathrm{H}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \hookrightarrow \prod_{\mathfrak{p} \in \mathrm{S(M)}} \mathrm{H}^2(\mathscr{G}_{\mathfrak{p}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}).$$

Since $\mu_p \subset \kappa$, i.e., $\mathrm{H}^2(\mathrm{H}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \cong \mathbb{Z}/\mathrm{p}\mathbb{Z}$ we obtain $\mathrm{H}^2(\mathscr{G}_{\mathfrak{p}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \neq 0$ for at least one $\mathfrak{p} \in S(M)$, which must be non-archimedean, since $p > 2$. The same surjectivity argument as in [NSW] 12.1.9 or in the proof of Proposition 2.12 finishes the proof. We repeat the argument here for the convenience of the reader. We have to show that the prime $\mathfrak{p} = \bar{\mathfrak{p}}|_M$ is indecomposed in K_S/M, i.e., that $H = D_{\bar{\mathfrak{p}}, K_S/M} \subseteq D_{\bar{\mathfrak{p}}}$. Therefore, consider an open subgroup $H' \subseteq H$ with corresponding 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

$$\mathrm{H}^2(\mathrm{U}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \to \bigoplus_{\mathfrak{q} \in \mathrm{T}_{\mathfrak{p},\mathrm{H}'}(\mathrm{U})} \mathrm{H}^2(\mathrm{D}_{\mathfrak{q},\mathrm{K_S/L}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \to 0,$$

This sequence is exact by [NSW] 9.2.1, 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:

$$\mathrm{H}^2(\mathrm{H}', \mathbb{Z}/\mathrm{p}\mathbb{Z}) \to \bigoplus_{\mathfrak{p}' \in \mathrm{S}_{\mathfrak{p}}(\mathrm{M}')} \mathrm{H}^2(\mathrm{D}_{\mathfrak{p}',\mathrm{K_S/M}'}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \to 0. \tag{6.1}$$

Let κ'/κ denote the finite extension of κ corresponding to H'. We have $\mu_p \subset \kappa \subseteq \kappa'$. Hence $\mathrm{H}^2(\mathrm{H}', \mathbb{Z}/\mathrm{p}\mathbb{Z}) \cong \mathbb{Z}/\mathrm{p}\mathbb{Z}$. Further, $\mathrm{H}^2(\mathrm{D}_{\mathfrak{p}',\mathrm{K_S/M}'}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \neq 0$. In fact, $D_{\mathfrak{p}',K_S/M'}$ is conjugate to an open subgroup of $D_{\mathfrak{p},K_S/M}$. But since $\mathrm{H}^2(\mathrm{D}_{\bar{\mathfrak{p}},\mathrm{K_S/M}}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \neq 0$, also $\mathrm{H}^2(\mathrm{V}, \mathbb{Z}/\mathrm{p}\mathbb{Z}) \neq 0$ for any open subgroup $V \subseteq D_{\bar{\mathfrak{p}},K_S/M}$ (this follows from [NSW] 7.1.8 (i),(ii)). Finally, since (6.1) is exact, there is only one prime lying over $\mathfrak{p}$ in any finite extension M'/M. Hence $\bar{\mathfrak{p}}|_M$ is indecomposed. □

From this group-theoretic description we obtain the local correspondence at the boundary.

Corollary 6.5 (Local correspondence at the boundary)**.** *For $i = 1, 2$ let K_i be a number field and S_i a set of primes, such that $Dec(K_i, S_i)$ holds. Assume S_i is stable and satisfies $(*)_{p_i}^{\mathrm{stab}}$ for some $p_i > 2$. Let*

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

be an isomorphism. Then the local correspondence at the boundary holds and moreover, for any open $U_1 \subseteq \mathrm{G}_{K_1,S_1}$ with corresponding field L_1, σ preserves inertia subgroups and σ_{*,U_1} preserves the residue characteristic and the absolute degree of all primes in $S_{1,f}(L_1)$ (and not only of all but finitely many).

Proof. Theorem 6.3 allows to define σ_* in an obvious way. We show the Galois-equivariance: let $g \in \mathrm{G}_{K_1,S_1}$ and $\bar{\mathfrak{p}} \in S_{1,f}(K_{1,S_1})$. Then

$$D_{\sigma_*(g\bar{\mathfrak{p}})} = \sigma(D_{g\bar{\mathfrak{p}}}) = \sigma(gD_{\bar{\mathfrak{p}}}g^{-1}) = \sigma(g)\sigma(D_{\bar{\mathfrak{p}}})\sigma(g)^{-1} = \sigma(g)D_{\sigma_*(\bar{\mathfrak{p}})}\sigma(g)^{-1} = D_{\sigma(g)\sigma_*(\bar{\mathfrak{p}})},$$

which by Lemma 6.4(i) implies that $\sigma_*(g\bar{\mathfrak{p}}) = \sigma(g)\sigma_*(\bar{\mathfrak{p}})$. That σ preserves inertia subgroups and σ_{*,U_1} preserves the residue characteristics and the absolute degree of all primes in $S_{1,f}(L_1)$ follows from $Dec(K_i, S_i)$ and anabelian properties of local fields (cf. Section 2.2).

□

6.2.3 General case

We refer to Section 1.2 for the definition of a group of p-decomposition type.

Theorem 6.6. *Let K be a number field and S a set of primes. Assume S is stable and satisfies $(*)_p^{\mathrm{stab}}$ for some $p > 2$. Assume further that $\mu_p \subset K_S$. Then any subgroup of $\mathrm{G}_{K,S}$ which is isomorphic to a group of p-decomposition type, is contained in a decomposition subgroup of a unique prime in $(S_f \setminus S_p)(K_S)$.*

Remark 6.7. The assumption $\mu_p \subset K_S$ is needed for technical reasons: we can not show that for any $\mathfrak{p} \in S_f$, we have $\mu_p \subseteq K_{S,\mathfrak{p}}$. But only in this case the decomposition group $D_{\mathfrak{p}} \subseteq \mathrm{G}_S$ with $\mathfrak{p} \in S$ is of p-cohomological dimension 2, which is a crucial point in the proof.

Proof of Theorem 6.6. Uniqueness follows from Lemma 6.4(i) and Lemma 1.4(ii). By Lemma 6.4(ii) we can assume $\mu_p \subset K$. Since now $\mu_p \subset K_{\mathfrak{p}}$ for any $\mathfrak{p} \in S$, it follows from Corollary 4.21 that for any $\bar{\mathfrak{p}} \in S_f \setminus S_p(K_S)$, the composition

$$\mathscr{G}_{\mathfrak{p},p} \hookrightarrow \mathscr{G}_{\mathfrak{p}} \twoheadrightarrow D_{\bar{\mathfrak{p}}} \hookrightarrow \mathrm{G}_{K,S}$$

is injective, or with other words, the p-Sylow subgroup of $D_{\bar{\mathfrak{p}}}$ is of p-decomposition type (cf. Section 1.3.1). Let H be a closed subgroup of $\mathrm{G}_{K,S}$ of p-decomposition type. By exactly the same argument as in the proof of Theorem 6.3, H is contained in a decomposition group $D_{\bar{\mathfrak{p}}}$ of a prime $\bar{\mathfrak{p}} \in S_f(K_S)$. Now, Lemma 2.11 shows that $\bar{\mathfrak{p}}$ does not lie over p, which finishes the proof. □

Using the theorem one can reconstruct the decomposition subgroups at $S_f \setminus S_p$ from the group $\mathrm{G}_{K,S}$ exactly as in Section 2.8. For the convenience of the reader, we repeat here the construction. For any open $U \subseteq \mathrm{G}_{K,S}$ with fixed field L, such that $\mu_p \subseteq L$, let

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

We claim that $\mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ is exactly the set of all maximal subgroups of p-decomposition type of U. Indeed, any $H \in \mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ with $H \subseteq D_{\bar{\mathfrak{p}}}$ is clearly of p-decomposition type and if there is some $H' \supseteq H$, which is also of p-decomposition type, then this inclusion is open by Lemma 1.4(ii), and by Lemma 6.4(ii) we get $H' \subseteq D_{\mathfrak{p}}$, i.e., $H = H'$. With other words, H is maximal. Conversely, let H be a maximal subgroup of p-decomposition type. By Theorem 6.6, $H \subseteq D_{\bar{\mathfrak{p}}}$ for some prime $\bar{\mathfrak{p}} \in S_f \smallsetminus S_p$. But then H is contained in a p-Sylow subgroup of $D_{\bar{\mathfrak{p}}}$, which is again of p-decomposition type, and since H is maximal, H is equal to this p-Sylow subgroup. This proves our claim and shows that $\mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ is determined by the group-theoretic structure of $\mathrm{G}_{K,S}$. Further, U acts on this set by conjugation, and we have an U-equivariant surjection, where U acts trivially on the right:

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

which sends H to the (unique by Lemma 6.4(i)) prime $\bar{\mathfrak{p}}|_L$, 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

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

It defines an equivalence relation on $\mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ by $H \sim H' :\Leftrightarrow \ker(\mathrm{res}^U_H) = \ker(\mathrm{res}^U_{H'})$, which is again determined by group structure of $\mathrm{G}_{K,S}$. By Lemma 2.18, we have

$$H \sim H' \Leftrightarrow \psi(H) = \psi(H')$$

and 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 additionally U is normal in $\mathrm{G}_{K,S}$, then $\mathrm{G}_{K,S}$ acts on $\mathrm{Syl}_p(U, S_f \smallsetminus S_p)$ by conjugation, and via ψ this induces an action on $(S_f \smallsetminus S_p)(U)$, which coincides with the natural action of $\mathrm{G}_{K,S}$ on this set. Thus the group-theoretic structure of $\mathrm{G}_{K,S}$ encodes the projective system of $\mathrm{G}_{K,S}$-sets

$$\{(S_f \smallsetminus S_p)(U) \colon U \subseteq U_0, U \trianglelefteq \mathrm{G}_{K,S}\},$$

where $U_0 \subseteq \mathrm{G}_{K,S}$ is certain open subgroup. Now the decomposition subgroups inside $\mathrm{G}_{K,S}$ of primes in $S_f \smallsetminus S_p$ are exactly the stabilizers in $\mathrm{G}_{K,S}$ of elements in the $\mathrm{G}_{K,S}$-set

$$\varprojlim_{U \subseteq U_0, U \trianglelefteq \mathrm{G}_{K,S}} (S_f \smallsetminus S_p)(U).$$

Remark 6.8. It is not possible to treat the primes in $S_p \cap S$ by the same method as above, as we do not have a very good control over the p-Sylow subgroups $\mathrm{G}_{\kappa,p}$ of G_κ with κ local p-adic: they still have $\mathrm{cd}_p(\mathrm{G}_{\kappa,p}) = 2$, but must not be isomorphic to the (well-understood) maximal pro-p quotient $\mathrm{G}_\kappa(p)$ (and moreover the kernel of $\mathscr{G}_{\mathfrak{p},p} \twoheadrightarrow \mathscr{G}_{\mathfrak{p}}(p)$ is infinitely generated).

From this intrinsic description of the decomposition subgroups, we obtain the local correspondence at the boundary.

Corollary 6.9 (Local correspondence at the boundary)**.** *For $i = 1, 2$ let K_i be a number field and S_i a stable set of primes satisfying $(*)^{\mathrm{stab}}$. Assume there are two different odd rational primes $p_1, p_2 \notin E^{\mathrm{stab}}(S_i)$ such that $\mu_{p_1 p_2} \subset K_{i,S_i}$ for $i = 1, 2$. Let*

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

be an isomorphism. Then the local correspondence at the boundary holds. Moreover, for any open $U_1 \subseteq \mathrm{G}_{K_1,S_1}$ with corresponding field L_1, σ_{*,U_1} preserves the residue characteristics and absolute degrees of all primes $\mathfrak{p} \in S_{1,f}(L_1)$, which do not lie over rational primes contained in the (finite) set $E^{\mathrm{stab}}(S_1) \cup E^{\mathrm{stab}}(S_2)$.

Proof. For $p \in \{p_1, p_2\}$, the above considerations allow to define a bijection

$$\sigma_{p,*}\colon (S_{1,f} \smallsetminus S_p)(K_{1,S_1}) \xrightarrow{\sim} (S_{2,f} \smallsetminus S_p)(K_{2,S_2})$$

in an obvious way. Let $\bar{\mathfrak{p}}_1 \in (S_{1,f} \smallsetminus S_{p_1 p_2})(K_{1,S_1})$. Then we have

$$D_{\sigma_{p_1,*}(\bar{\mathfrak{p}}_1)} = \sigma(D_{\bar{\mathfrak{p}}_1}) = D_{\sigma_{p_2,*}(\bar{\mathfrak{p}}_1)},$$

which by Lemma 6.4(i) implies that $\sigma_{p_1,*}(\bar{\mathfrak{p}}_1) = \sigma_{p_2,*}(\bar{\mathfrak{p}}_1)$, i.e., $\sigma_{p_1,*}$ and $\sigma_{p_2,*}$ coincide on $(S_{1,f} \smallsetminus S_{p_1 p_2})(K_{1,S_1})$. By patching them together, we obtain the desired bijection

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

The Galois-equivariance of σ_* follows in the same way as in Corollary 6.5. Observe that the set $E^{\mathrm{stab}}(S_1) \cup E^{\mathrm{stab}}(S_2)$ is finite since S_1, S_2 satisfy $(*)^{\mathrm{stab}}$. It remains to show that for any finite $K_{1,S_1}/L_1/K_1$ with corresponding open subgroup U_1 and for all primes in $S_{1,f}(L_1)$ not lying over $p \in E^{\mathrm{stab}}(S_1) \cup E^{\mathrm{stab}}(S_2)$, the map σ_{*,U_1} preserves the residue characteristic and the local absolute degree. We can assume $L_1 = K_1$. Since $(*)^{\mathrm{stab}}$ holds for S_i $(i = 1, 2)$, there is a finite exceptional set $T = E^{\mathrm{stab}}(S_1) \cup E^{\mathrm{stab}}(S_2)$, such that for any rational prime $\ell \notin T$, the set S_i satisfies $(*)_\ell^{\mathrm{stab}}$, and by Corollary 4.21 the maximal local ℓ-extension of $K_{i,\mathfrak{p}}$ for any prime $\mathfrak{p} \in S_i$ is attained by K_{i,S_i}. This means, in particular, that for all primes $\mathfrak{p} \in S_i$ with residue characteristic $\ell = \ell(\mathfrak{p}) \notin T$, the maximal ℓ-extension of $K_{i,\mathfrak{p}}$ is attained by K_{i,S_i}. Let $\mathfrak{p} \in S_i$ be such a prime and $\bar{\mathfrak{p}}$ an extension to K_{i,S_i}. Lemma 6.10 shows that $D_{\bar{\mathfrak{p}}}$ encodes the information about the residue characteristic and the absolute degree of $\mathfrak{p}$. Thus σ_{*,K_1} preserves residue characteristic and local degree of all primes in $S_1 \smallsetminus T(K)$. □

Lemma 6.10. *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 D encodes the information about ℓ and $[\kappa : \mathbb{Q}_\ell]$.*

Proof. Let $\mathscr{G}_\kappa$ be the absolute Galois group of κ. We have the surjection $\pi\colon \mathscr{G}_\kappa \twoheadrightarrow D$, and for any open $U \subseteq \mathscr{G}_\kappa$, a surjection $U \twoheadrightarrow \pi(U)$, which for any rational prime p induces an injection $\mathrm{H}^1(\pi(\mathrm{U}), \mathbb{Z}/\mathrm{p}\mathbb{Z}) \hookrightarrow \mathrm{H}^1(\mathrm{U}, \mathbb{Z}/\mathrm{p}\mathbb{Z})$. For all primes $p \neq \ell$, the dimensions of the spaces on the right (and hence also on the left) is bounded by 2, and for $p = \ell$, the dimension of the space on the

left gets arbitrary big, if U gets arbitrary small. Thus D determines the residue characteristic ℓ. Further,

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

6.3 Uniform bound

Besides the local correspondence established before, the following argument plays a central role in the proof of Theorems 6.1 and 6.2:

Proposition 6.11 (Uniform bound)**.** *For $i = 1, 2$ let K_i be a number field and S_i a set of primes of K_i, and let*

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

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 6.12. *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 6.12. Indeed, for any n vectors of 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 6.11. Since S_1 is stable, by Proposition 3.11, 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 6.12 and since M_1 is a union of finite extensions of K_1, which are normal over $\mathbb{Q}$, we can assume M_1/K_1 finite. Let

$$S_1' := S_1(M_1) \cap \mathrm{cs}(M_1/\mathbb{Q})(M_1).$$

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

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

Lemma 6.13. *Let $S_2' := \sigma_*(S_1')$. Then*

(i) $\delta_{M_2}(S_2') = \delta_{M_1}(S_1')$.

(ii) $S_2' \overset{\subset}{\sim} \mathrm{cs}(M_1M_2/M_2)$.

Proof of Lemma 6.13. (i): follows from the local correspondence at the boundary by explicitly computing the density and using formula (3.1), since σ_* preserves the residue characteristic and the absolute degree of almost all primes in S_1' (and in particular, almost all primes in S_2' are completely split over $\mathbb{Q}$).

(ii): Let $\mathfrak{p}_1 \in S_1'$ be such that σ_* preserves the residue characteristic and the absolute degree of $\mathfrak{p}_1$. Let $\mathfrak{p}_2 := \sigma_*(\mathfrak{p}_1) \in S_2'$ and $\mathfrak{p} := \mathfrak{p}_2|_{M_1\cap M_2}$. The fibre $\mathcal{O}_{M_1M_2} \otimes_{\mathcal{O}_{M_2}} \kappa(\mathfrak{p}_2)$ over $\mathfrak{p}_2$ in $\operatorname{Spec}\mathcal{O}_{M_1M_2}$ 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

$\mathfrak{p}_2|_{\mathbb{Q}} = \mathfrak{p}_1|_{\mathbb{Q}} \in \mathrm{cs}(K_1/\mathbb{Q})$ and hence $\mathfrak{p} \in \mathrm{cs}(M_1/\mathbb{Q})(M_1 \cap M_2) \subseteq \mathrm{cs}(M_1/M_1 \cap M_2)$. This implies that $\mathcal{O}_{M_1} \otimes_{\mathcal{O}_{M_1 \cap M_2}} \kappa(\mathfrak{p})$ is isomorphic to 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 $M_1 M_2$. □

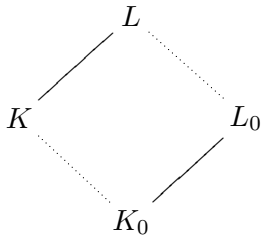
Using Lemma 6.13, and since $M_1 M_2/M_2$ is normal, we obtain:

$$\begin{aligned} [M_1 : M_1 \cap M_2]^{-1} &= [M_1 M_2 : M_2]^{-1} \\ &= \delta_{M_2}(\mathrm{cs}(M_1 M_2/M_2)) \\ &\geqslant \delta_{M_2}(S_2') \\ &= \delta_{M_1}(S_1') \\ &> N^{-1}. \end{aligned}$$

This proves Proposition 6.11. □

6.4 Non-existence of lifts

Last but not least, Proposition 6.14 proven in this section provides the last argument which we need in the proof of Theorems 6.1 and 6.2. 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 $L = KL_0$:



In this case the group $\mathrm{G}_{L/K}$ sits in the sequence

$$1 \to \mathrm{G}_{L/K} \to \mathrm{G}_{L/K_0} \to \mathrm{G}_{K/K_0} \to 1,$$

in which the right map splits, and the image G_{L/L_0} of this splitting is normal, i.e., one has $\mathrm{G}_{L/K_0} \cong \mathrm{G}_{L/K} \times \mathrm{G}_{L/L_0}$. Thus we want to know, under which conditions $\mathrm{G}_{L/K}$ does not fit into such a diagram with K/K_0 non-trivial.

Proposition 6.14. *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 hold:*

(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 $\mathrm{G}_{K,S_p}(p)$. By [NSW] 10.3.20, the number of independent $\mathbb{Z}_p$-extensions of K satisfies

$$\mathrm{rk}_{\mathbb{Z}_p}\, \mathrm{G}^{\mathrm{ab}}_{\mathrm{K},\mathrm{S_p}}(\mathrm{p}) \geqslant \mathrm{r}_2(\mathrm{K}) + 1$$

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

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

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

Assume (b) holds. Let $\psi\colon \mathrm{G}_{L/K} \xrightarrow{\sim} \mathrm{G}_{L_0/K_0}$ denote the canonical isomorphism obtained by restriction. 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 chose 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 $[K:K_0] = 1$. □

6.5 Proof of Theorems 6.1 and 6.2

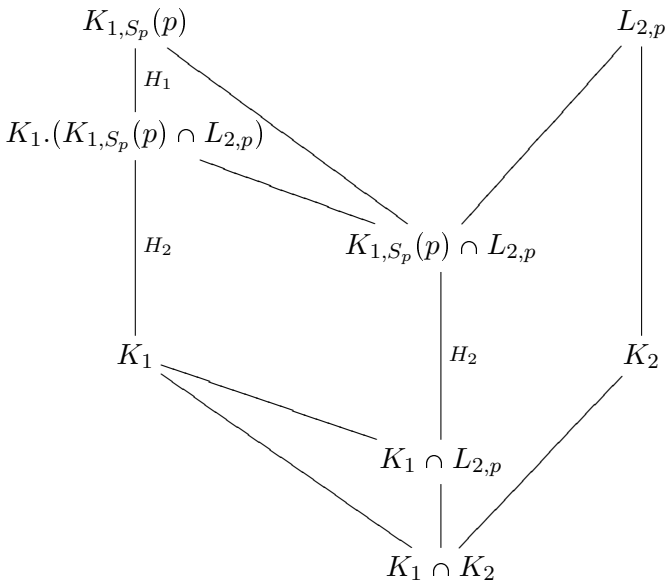
We consider all occurring fields to be subfields of a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

Step 1 - Local correspondence. The assumptions in both versions of the theorem imply by Corollary 6.5 resp. Corollary 6.9, that for σ the local correspondence at the boundary holds: for any open subgroup $U_1 \subseteq \mathrm{G}_{K_1,S_1}$ with fixed field L_1, σ induces a bijection

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

which preserves the residue characteristic and the absolute degree of all primes in Theorem 6.1 and almost all primes in Theorem 6.2. We obtain $[K_2:\mathbb{Q}] \leqslant [K_1:\mathbb{Q}]$ from this. Indeed, under the assumptions of Theorem 6.1, it follows from the existence of some p with $S_p \subseteq S_2$; in the case of Theorem 6.2, there is a prime p with $S_p \subseteq S_2$ and $p \notin T = E^{\mathrm{stab}}(S_1) \cup E^{\mathrm{stab}}(S_2)$, and hence σ_* preserves the residue characteristic and the absolute degree of primes in $S_p(K_1)$ by Corollary 6.9.

Step 2 - Totally imaginary case. We assume that K_1 is totally imaginary. We have two rational primes p_1, p_2, such that $S_{p_j} \subseteq S_1$, $p_j > 2$, whose existence was required in the statement of the theorems. So let $p \in \{p_1, p_2\}$. The quotient $\mathrm{G}_{K_1,S_p}(p)$ of G_{K_1,S_1} is torsion-free (cf. [NSW] 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 $\mathrm{G}_{K_{1,S_p}(p)/K_{1,S_p}(p)\cap L_{2,p}}$ and of $\mathrm{G}_{K_1,S_p}(p)$. But the first of these two groups is finite by Proposition 6.11, and the second is torsion-free. Hence $H_1 = 1$, i.e., $H_2 = \mathrm{G}_{K_1,S_p}(p)$. By Proposition 6.14(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 $j = 1, 2$. Since by step 1 we have $[K_2 : \mathbb{Q}] \leqslant [K_1 : \mathbb{Q}]$, we conclude that $K_1 = K_2$.

Step 3 - General case. Now assume K_1 is arbitrary. Let p_1, p_2 be as in step 2. For $j = 1, 2$ let $K_{2,j}$ be the extension of K_2 corresponding under σ to the extension $K_1(\mu_{p_j})/K_1$. By the preceding two steps, we see that $K_1(\mu_{p_j}) = K_{2,j}$, since the assumptions carry over from K_1, K_2 to $K_1(\mu_{p_j}), K_{2,j}$. Now $K_1(\mu_{p_1}) \cap K_1(\mu_{p_2}) = K_1$ and this is equivalent to the fact that the subgroups of G_{K_1,S_1} corresponding to these fields, generate G_{K_1,S_1}, hence the same is true after applying σ, i.e., $K_{2,1} \cap K_{2,2} = K_2$. Thus we get:

$$K_1 = K_1(\mu_{p_1}) \cap K_1(\mu_{p_2}) = K_{2,1} \cap K_{2,2} = K_2.$$

This finishes the proof. □

Remark 6.15. The technical assumptions in both versions of the theorem are chosen such that one can show

- the local correspondence at the boundary,
- $[K_2 : \mathbb{Q}] \leqslant [K_1 : \mathbb{Q}]$,
- the existence of two linearly disjoint extensions M_j/K_1 (j = 1,2), such that
  - (i) $M_j/\mathbb{Q}$ is normal,
  - (ii) G_{M_j/K_1} is torsion-free.

Bibiliography

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

[CC] 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.

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

[Ik] Ikeda M.: *Completeness of the absolute Galois group of the rational number field*, J. Reine Angew. Math. **291** (1977) 1-22.

[Ja] Jannsen U.: *Galoismoduln mit Hasse-Prinzip*. J. Reine Angew. Math. **337** (1982), 154-158.

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

[La] Landau E.: *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Teubner, 1918.

[Ma] Mazur B.: Notes on étale cohomology of number fields, Ann. Scient. Ecole Norm. Sup., 4.sér., **6** (1973), 521-553.

[Na] Narkiewicz W.: *Elementary and analytic theory of algebraic numbers*, Springer, 2004, third edition.

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

[Ne2] Neukirch J.: *Kennzeichnung der endlich-algebraischen Zahlkörper durch die Galoisgruppe der maximal auflösbaren Erweiterungen*, J. Reine Angew. Math. **238** (1969), 135âĂŞ147.

[Ne3] Neukirch J.: *Algebraische Zahlentheorie*, Springer, 2007.

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

[Po1] Pop F.: *On Grothendieck's conjecture of birational anabelian geometry*, Ann. of Math. **138** (1994) 145-182.

[Po2] Pop F.: *On Grothendieck's conjecture of birational anabelian geometry II*, preprint 1994.

[Po3] Pop F.: *Alterations and birational anabelian geometry*, Resolution of singularities (Obergurgl, 1997), Progr. Math. 181, Birkhäuser Basel 2000, 519-532.

[Sch] Schmidt A.: *Rings of integers of type $K(\pi, 1)$*, 2007, Doc. Math. **12** (2007), 441-471.

[Sch2] Schmidt A.: *On the $K(\pi, 1)$-property of rings of integers in the mixed case*, RIMS Kokyuroku Bessatsu **B12** (2009), 91-100.

[Sch3] Schmidt A.: *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. reine u. angew. Math. **640** (2010) 203-235.

[SchS] Schmidt S.: *Galoistheoretische Invarianten globaler Körper*, Diplomarbeit, Bonn 2004.

[SGA 4] Artin M., Grothendieck A., Verdier J. L.: *Théorie de Topos et Cohomologie étale de schémas*, LNM **269**, **270**, **305**, Springer, 1972-1973.

[St] Stix J.: *Projective anabelian curves in positive characteristic and descent theory for log-étale covers*, Dissertation, Univ. of Bonn, 2002.

[Sz] Szamuely T.: *Groupes de Galois de corps de type fini (d'après Pop)*. Astérisque No. **294** (2004), ix, 403-431.

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

[Uc] Uchida K.: *Isomorphisms of Galois groups*, J. Math. Soc. Japan **28** (1976), 617-620.

[Uc2] Uchida K.: *Isomorphisms of Galois groups of algebraic function fields*, Ann. of Math. **106** (1977), 589-598.

[Uc3] Uchida K.: *Isomorphisms of Galois groups of solvably closed Galois extensions*, Tohoku Math. Journ. **31** (1979), 359-362.

[Wi] Wingberg K.: *On Chebotarev sets*, Math. Res. Lett. **13** (2006), no. 2, 179-197.

[Wi2] Wingberg K.: *Riemann's Existence theorem and the $K(\pi,1)$-property of rings of integers*, Preprint Heidelberg 2007.

[Zi] Zink T.: *Étale cohomology and duality in number fields*, Haberland, Galois cohomology, Berlin, 1978, Appendix 2.