DENSITIES OF PRIMES AND REALIZATION OF LOCAL EXTENSIONS

A. B. IVANOV

Abstract. In this paper we introduce new densities on the set of primes of a number field. If K/K_0 is a Galois extension of number fields, we associate to any element $x \in \mathrm{G}_{K/K_0}$ a density $\delta_{K/K_0,x}$ on the primes of K. In particular, the density associated to $x = 1$ is the usual Dirichlet density on K. We also give two applications of these densities (for $x \neq 1$): the first is a realization results à la Grunwald-Wang theorem such that essentially, ramification is only allowed in a set of primes of density zero. The second concerns the so called saturated sets of primes, introduced by Wingberg.

1. Introduction

In this article we adress the question of generalizing the Dirichlet density on the set of primes of a number field. In particular, we provide sets of primes with Dirichlet density zero with an appropriate positive measure. We give two applications of these generalized densities to (i) a realization result of local extensions by global ones satisfying certain conditions and (ii) saturated sets of Wingberg.

To begin with, let K/K_0 be a finite Galois extension of number fields, i.e., of finite extensions of $\mathbb{Q}$. Let $x \in \mathrm{G}_{K/K_0}$ be of order d. Let P^x_{K/K_0} denote the set of all primes $\mathfrak{p}$ of K which are unramified in K/K_0 and satisfy $\mathrm{Frob}_{\mathfrak{p},K/K_0} = x$. We will introduce a density $\delta_{K/K_0,x}$ of a set S of primes of K, which measures how big the ratio of the sizes of $S \cap P^x_{K/K_0}$ and P^x_{K/K_0} is. This is done in the same way as for Dirichlet density, with the only difference that one has to take the limit over the ratio of terms of the kind $\sum_{\mathfrak{p}\in *} \mathrm{N}\,\mathfrak{p}^{-s}$ not over $s \rightarrow 1$ but over $s \rightarrow d^{-1}$ with s lying in the right half plane $\Re(s) > d^{-1}$. Further, $\delta_{K/K_0,x}$ is essentially independent of the base field K_0, so one also could replace K_0 once for all time by $\mathbb{Q}$, but it is easier to work with a *Galois* extension K/K_0.

Once introduced, the most interesting thing about such a density is its base change behavior. To explain it, let L/K be an extension such that L/K_0 is Galois. Write $H := \mathrm{G}_{L/K} \lhd \mathrm{G}_{L/K_0} =: G$ and $\pi\colon G \twoheadrightarrow G/H$ for the natural projection. For any $y \in \pi^{-1}(x)$ we have the map induced by restriction of primes $P^y_{L/K_0} \rightarrow P^x_{K/K_0}$. It is in general neither injective nor surjective. For $y, z \in \pi^{-1}(x)$ one easily sees that the images of the corresponding maps are either equal or disjoint and that the first is equivalent to y, z being H-conjugate (cf. Lemma 3.1). If C is an H-conjugacy

---

Key words and phrases. Number Field, Galois Cohomology, Restricted Ramification, Dirichlet Density.

The author was supported by the Technical University Munich.

class in $\pi^{-1}(x)$, let M_C denote the image of P^y_{L/K_0} for some (any) $y \in C$ in P^x_{K/K_0}. We will show the following generalization of Chebotarev's density theorem and then obtain a description of the base change behavior of $\delta_{K/K_0,x}$ as a direct corollary:

Proposition 3.2. *Let $L/K/K_0, \pi, x$ be as above. Let C be an H-conjugacy class in $\pi^{-1}(x)$. Then*

$$\delta_{K/K_0,x}(M_C) = \frac{\sharp C}{\sharp H}.$$

Corollary 3.4. *Let $y \in \pi^{-1}(x)$ and let C be its H-conjugacy class in $\pi^{-1}(x)$. Then*

$$\delta_{L/K_0,y}(S_L) = \frac{\sharp H}{\sharp C}\delta_{K/K_0,x}(S \cap M_C)$$

if both densities exist.

More general, for any function $\psi\colon \mathrm{G}_{K/K_0} \to \mathbb{C}$ one can define a weighted function by $\delta_{K/K_0,\psi}(S) := [K : K_0]^{-1}\sum_{x\in \mathrm{G}_{K/K_0}} \psi(x)\delta_{K/K_0,x}(S)$. Then for example the Dirichlet density is associated with the character of the regular representation of G.

Similarly as Serre extended the Dirichlet density to a density on the set of closed points of a scheme of finite type over $\operatorname{Spec}\mathbb{Z}$, also the densities associated to fixed Frobenius elements should generalize in this way. Furthermore, it would be intereting to know, whether in the case of varieties of dimension ≥ 2 over a perfect field, it is possible to define such fixed Frobenius densities for divisors (i.e, to non-closed points) as was done with the Dirichlet density by Holschbach [3].

Finally, we have an obsevation concerning L-functions: there is the following problem about extending L-functions in the same way as the densities above. Let $K/\mathbb{Q}$ be a finite Galois extension and $x \in \mathrm{G}_{K/\mathbb{Q}}$. Consider the following product associated to x and a Dirichlet character χ modulo $\mathfrak{m}$:

$$L_x(\mathfrak{m}, s, \chi) := \prod_{\mathfrak{p}\in P^x_{K/\mathbb{Q}}} \frac{1}{1-\chi(\mathfrak{p})\,\mathrm{N}\,\mathfrak{p}^{-s}}. \tag{1.1}$$

This product converges on the right half plane $\Re(s) > d^{-1}$, where d is the order of x. But in general this function has no analytic continuation to the whole complex plain (not even to the right half plane $\Re(s) > 0$). The reason is easy: let $\mathfrak{m} = 1, \chi = 1$. For $s \to d^{-1}$ this product behaves like $d^{-\frac{1}{d}}(\frac{1}{s-d^{-1}})^{\frac{1}{d}}$, i.e., their difference is bounded for $s \to d^{-1}$, and this last function clearly has no analytic continuation. A natural question is, whether this problem can be resolved, for example by taking the d-th power of the product above or by removing a half-line starting at d^{-1} from the complex plain. Luckily, one does not need any non-vanishing results on such L-functions to show Proposition 3.2, as it follows by simple counting arguments from Chebotarev's density theorem.

Applications. Now we turn to applications of the above densities. The one concerning stable sets of Wingberg and examples of Galois groups $\mathrm{G}_{K^R/K}$ containing torsion can be found in Section 6. We discuss here the other application to a realization result à la Grunwald-Wang.

Let us first fix some notations. Let $\mathfrak{c}$ be a full class of finite groups (in the sense of [5] 3.5.2). Let $R \subseteq S$ be two sets of primes of a number field K. Then $K_S^R(\mathfrak{c})$ denotes the maximal pro-$\mathfrak{c}$-extension of K which is unramified outside S and completely split in R. Moreover, for a prime $\mathfrak{p}$ of K we denote by $K_{\mathfrak{p}}(\mathfrak{c})$ the maximal pro-$\mathfrak{c}$-extension of $K_{\mathfrak{p}}$ and by $K_{\mathfrak{p}}^{\mathrm{nr}}$ the maximal unramified extension of $K_{\mathfrak{p}}$.

For ℓ a rational prime or ∞, let $\mathfrak{c}_{\leq \ell}$ denote the smallest full class of all finite groups, containing the groups $\mathbb{Z}/p\mathbb{Z}$ for all $p \leq \ell$. Our main result will be the following generalization of [5] 9.4.3, which handles the case of $\delta_K(S) = 1$.

Theorem 1.1. *Let K be a number field, $S \supseteq R$ sets of primes of K, such that R is finite and $S \overset{\supseteq}{\sim} P_{M/K}(\sigma)$ for some finite extension M/K and $\sigma \in \mathrm{G}_{M/K}$. For any $\ell \leq \infty$ and any prime $\mathfrak{p}$ of K we have:*

$$(K_S^R(\mathfrak{c}_{\leq \ell}))_{\mathfrak{p}} = \begin{cases} K_{\mathfrak{p}}(\mathfrak{c}_{\leq \ell}) & \text{if } \mathfrak{p} \in S \smallsetminus R \\ K_{\mathfrak{p}}(\mathfrak{c}_{\leq \ell}) \cap K_{\mathfrak{p}}^{\mathrm{nr}} & \text{if } \mathfrak{p} \notin S \\ K_{\mathfrak{p}} & \text{if } \mathfrak{p} \in R. \end{cases}$$

In particular, since absolute Galois groups of local fields are solvable, taking $\ell = \infty$ shows that the maximal solvable subextension of K_S^R/K lies dense in $\overline{K_{\mathfrak{p}}}$ resp. in $K_{\mathfrak{p}}^{\mathrm{nr}}$ for $\mathfrak{p} \in S \smallsetminus R$ resp. $\mathfrak{p} \notin S$.

One part of the proof of Theorem 1.1, namely to realize a p-extension with given local properties, when S is sharply p-stable (as introduced in [4]; see also Section 5.1 below) was already done in [4]. Essentially, sharp p-stability means that S contains many primes $\mathfrak{p}$, which are completely split in $K(\mu_p)/K$. The remaining and much more delicate case is when $\delta_{K(\mu_p)}(S_{K(\mu_p)}) = 0$ holds. Then the usual methods from [5] and [4] do not apply anymore. Moreover, in such a case the pro-p-version of the theorem easily can fail. For example, suppose that $\mu_p \not\subseteq K$ and $K(\mu_p)/K$ is totally ramified at each p-adic prime, let $1 \neq \sigma \in \mathrm{G}_{K(\mu_p)/K}$ and set $S := P_{K(\mu_p)/K}(\sigma)$. Then any prime $\mathfrak{p} \in S$ is unramified in $K_S(p)/K$, as $\mathfrak{p} \notin S_p$ and $\mu_p \not\subseteq K_{\mathfrak{p}}$. Hence $K_S(p) = K_{\emptyset}(p)$. In particular, let $K = \mathbb{Q}$ and p odd. Then $\mathbb{Q}_S(p) = \mathbb{Q}_{\emptyset}(p) = \mathbb{Q}$, i.e., the maximal possible local p-extension is realized nowhere.

However, in the pro-$\mathfrak{c}_{\leq \ell}$-case the theorem holds. For example take in the above example $\ell = 3$. The set $S := P_{\mathbb{Q}(\mu_3)/\mathbb{Q}}(\sigma)$ is sharply-p-stable for all $p \neq 3$, and in particular sharply 2-stable. Hence at any $\mathfrak{p} \in S$ the maximal pro-2-extension can be realized, and hence $\mu_3 \subseteq \mathbb{Q}_{S,\mathfrak{p}}$. After going up to an appropriate finite subextension $\mathbb{Q}_S(\mathfrak{c}_{\leq 2})/K/\mathbb{Q}$, the set $P_{\mathbb{Q}(\mu_3)/\mathbb{Q}}(\sigma)_K \cap \mathrm{cs}(K(\mu_3)/K)$ would at least be infinite and not more empty as for $K = \mathbb{Q}$. The main obstruction now is that this set has Dirichlet density 0, and no one of the usual arguments involving Dirichlet density will apply. To overcome this difficulty we will use the fixed Frobenius densities introduced above. Namely, it turns out that certain x-density of this set is positive and then one again can apply some density arguments. However, these arguments are in our situation much more subtle than in the situations where one can use Dirichlet density.

Finally, we remark that there are several other appraoches to realization results of similar spirit. As to the knowledge of the author, no one of them covers the abovementioned case, where one tries to realize p-extensions with ramification allowed only outside $\mathrm{cs}(K(\mu_p/K))$. We mention two recent approaches: a certain pro-p version of the theorem above is also known (only for primes in S) in the much harder situation of a finite set S by the work of A. Schmidt (cf. e.g. [6]) but only after enlarging S by an appropriate finite subset of a fixed set T of primes of density 1 (which, in particular, is sharply p-stable). A further, completely different and very powerful approach using automorphic forms, which deals with the whole pro-finite group and a finite set S, was introduced by Chenevier and Clozel [2], [1]. However, compared to results of this paper, the drawback is that one has to forget about solvability conditions and to assume $R = \emptyset$ (no control of the unramified extensions) and that at least one rational prime must lie in $\mathcal{O}_{K,S}^*$.

Notation. For any $a \in \mathbb{R}$ we denote by $\mathbb{H}_a$ the complex right half plane $\{s + it \colon \Re(s) > a\}$. Let G be a group and $\sigma \in G$ be any element. Then we denote by $C(\sigma, G)$ the conjugacy class of σ, by $\mathrm{ord}(\sigma)$ the order of σ and by $Z_G(\sigma)$ the centralizer of σ.

Let L/K be an extension of number fields. We write Σ_K for the set of all primes of K, $S_{\mathfrak{p}}(L)$ for the set of primes in L lying over a prime $\mathfrak{p}$ of K. If $S \subseteq \Sigma_K$, then we write S_L, $S(L)$ or sometimes simply S for the pull-back of S to L. If L/K is Galois and $x \in \mathrm{G}_{L/K}$, the Chebotarev set $P_{L/K}(x)$ is the set of primes in K which are unramified in L/K and whose Frobenius class is $C(x, \mathrm{G}_{L/K})$ and $P_{L/K}^x$ denotes the set of primes in L which are unramified in L/K and whose Frobenius is x. Moreover, we call a set which differs from a Chebotarev set only by a subset of Dirichlet density 0 an almost Chebotarev set. For $\mathfrak{p} \in \Sigma_K$, $\mathrm{N}\,\mathfrak{p}$ denotes the norm of $\mathfrak{p}$ over $\mathbb{Q}$, i.e., the cardinality of the residue field. If $S, T \subseteq \Sigma_K$, then $S \overset{\subseteq}{\sim} T$ means that S lies in T up to a (Dirichlet) density zero subset and $S \backsimeq T$ means $S \overset{\subseteq}{\sim} T$ and $T \overset{\subseteq}{\sim} S$.

Outline of the paper. In Section 2 we define the generalized densities. In Section 3 we establish some base-change formulas and an easy generalization of Chebotarev's density theorem for these densities. In Section 4 we generalize slightly the notion of these densities introduced in Section 2. In Section 5 we prove Theorem 1.1. In Section 6 we discuss the application to saturated sets.

2. Densities associated to Frobenius elements

Let K_0 be a fixed finite extension of $\mathbb{Q}$. Let K/K_0 be a finite Galois extension and $x \in G := \mathrm{G}_{K/K_0}$ an element of order d. Our starting point is the following easy but fundamental observation.

Lemma 2.1. *The series $\sum_{\mathfrak{p} \in P_{K/K_0}^x} \mathrm{N}\,\mathfrak{p}^{-s}$ converges for all s with $\Re(s) > d^{-1}$. It defines a holomorphic function on $\mathbb{H}_{d^{-1}}$ and*

$$\lim_{s \to d^{-1}+0} \sum_{\mathfrak{p} \in P^x_{K/K_0}} \mathrm{N}\,\mathfrak{p}^{-s} = \infty.$$

Proof. For $\mathfrak{p} \in P^x_{K/K_0}$ with $\mathfrak{p}_0 := \mathfrak{p}|_{K_0}$ we have $\mathrm{N}\,\mathfrak{p} = \mathrm{N}\,\mathfrak{p}_0^d$. The map $P^x_{K/K_0} \to P_{K/K_0}(x)$ is surjective and $\sharp\frac{Z_G(x)}{\langle x \rangle}$-to-1 (this is immediate; cf. also Lemma 3.3). Hence for all $s \in \mathbb{H}_{d^{-1}}$ and all $a > 0$ we get:

$$(2.1) \qquad \left(\sharp\frac{Z_G(x)}{\langle x \rangle}\right)^{-1} \sum_{\substack{\mathfrak{p} \in P^x_{K/K_0} \\ \mathrm{N}\,\mathfrak{p} < a^d}} |\,\mathrm{N}\,\mathfrak{p}^{-s}| = \sum_{\substack{\mathfrak{p}_0 \in P_{K/K_0}(x) \\ \mathrm{N}\,\mathfrak{p}_0 < a}} |\,\mathrm{N}\,\mathfrak{p}_0^{-ds}| \leq \sum_{\substack{\mathfrak{p}_0 \in \Sigma_{K_0} \\ \mathrm{N}\,\mathfrak{p}_0 < a}} |\,\mathrm{N}\,\mathfrak{p}_0^{-ds}|.$$

The last term converges for $a \to \infty$ and any fixed $s \in \mathbb{H}_{d^{-1}}$. One sees easily that the convergence is uniform on the half plane $\mathbb{H}_{d^{-1}+\epsilon}$ for any $\epsilon > 0$, hence the series in the lemma defines a holomorphic function on $\mathbb{H}_{d^{-1}}$. Finally, $\sum_{\mathfrak{p} \in \Sigma_{K_0}} \mathrm{N}\,\mathfrak{p}^{-s}$ goes to infinity if $s \to 1$ and $0 < \delta_{K_0}(P_{K/K_0}(x)) = \lim_{s \to 1} \frac{\sum_{\mathfrak{p} \in P_{K/K_0}(x)} \mathrm{N}\,\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \in \Sigma_{K_0}} \mathrm{N}\,\mathfrak{p}^{-s}}$, hence also $\sum_{\mathfrak{p} \in P_{K/K_0}(x)} \mathrm{N}\,\mathfrak{p}^{-s} \to \infty$ for $s \to 1$, and the last statement of the lemma follows from (2.1). □

Definition 2.2. Let K/K_0 be a finite Galois extension and $S \subseteq \Sigma_K$ a set of primes of K. For $x \in \mathrm{G}_{K/K_0}$ we call the real number

$$\delta_{K/K_0,x}(S) := \lim_{s \to \mathrm{ord}(x)^{-1}+0} \frac{\sum_{\mathfrak{p} \in S \cap P^x_{K/K_0}} \mathrm{N}\,\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \in P^x_{K/K_0}} \mathrm{N}\,\mathfrak{p}^{-s}},$$

if it exists, the density of S with respect to x (over K_0), or simply, the x-density of S.

Remarks 2.3.

(i) The x-density satisfies the usual properties: If exists, $\delta_{K/K_0,x}(S)$ is a real number lying in the interval $[0,1]$. If $\delta_{K/K_0,x}(S) = 0$, then for any $S' \subseteq S$, the x-density $\delta_{K/K_0,x}(S')$ also exists and is 0. By Lemma 2.1, finite sets of primes are irrelevant for the x-density: if S and T differ only by a finite set of primes, then $\delta_{K/K_0,x}(S)$ exists if and only $\delta_{K/K_0,x}(T)$ exists and if this is the case, then they are equal. Let S, T be two sets of primes of K having an x-density. If $S \cap T$ or $S \cup T$ has an x-density, then the second set does too and

$$\delta_{K/K_0,x}(S) + \delta_{K/K_0,x}(T) = \delta_{K/K_0,x}(S \cap T) + \delta_{K/K_0,x}(S \cup T).$$

(ii) More interesting, $\delta_{K/K_0,x}$ is essentially independent of K_0 as Lemma 2.4 below shows. Moreover, the density in K with respect to a fixed Frobenius element over a smaller subfield can be defined simply over $\mathbb{Q}$, but then (if

$K/\mathbb{Q}$ is not Galois and has Galois closure K^n) one has to deal with $\mathrm{G}_{K^n/K}$-cosets in $\mathrm{G}_{K^n/\mathbb{Q}}$, instead of elements in a Galois group, which is definitely less nice. Thus we decide to stay by our approach.

Lemma 2.4. *Assume $K/K_0'/K_0$ are finite Galois extensions of K_0. Let $x \in \mathrm{G}_{K/K_0'} \subseteq \mathrm{G}_{K/K_0}$ be of order d. Then for any set of primes S in K we have: $\delta_{K/K_0',x}(S)$ exists if and only $\delta_{K/K_0,x}(S)$ exists and if this is the case, then they are equal.*

Proof. Indeed, the sum $\sum_{P^x_{K/K_0'} \smallsetminus \mathrm{cs}(K_0'/K_0)(K)} \mathrm{N}\,\mathfrak{p}^{-s}$ is bounded for $s \to d^{-1}+0$ (since the inertia degree over K_0 and hence also over $\mathbb{Q}$ of primes in this set is bigger than d) and $P^x_{K/K_0'} \cap \mathrm{cs}(K_0'/K_0)(K) = P^x_{K/K_0}$ and hence by Lemma 2.1:

$$\delta_{K/K_0',x}(S) = \lim_{s \to d^{-1}+0} \frac{\sum_{\mathfrak{p} \in S \cap P^x_{K/K_0'}} \mathrm{N}\,\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \in P^x_{K/K_0'}} \mathrm{N}\,\mathfrak{p}^{-s}} = \lim_{s \to d^{-1}+0} \frac{\sum_{\mathfrak{p} \in S \cap P^x_{K/K_0}} \mathrm{N}\,\mathfrak{p}^{-s}}{\sum_{\mathfrak{p} \in P^x_{K/K_0}} \mathrm{N}\,\mathfrak{p}^{-s}} = \delta_{K/K_0,x}(S).$$

(when both exist). □

3. Pull-back properties of $\delta_{K/K_0,x}$

We fix the following setting in this section: $L/K/K_0$ are finite Galois extensions, $G := \mathrm{G}_{L/K_0}$, $H := \mathrm{G}_{L/K}$, $\pi\colon G \twoheadrightarrow G/H$ the natural projection, $x \in G/H$. For $y \in \pi^{-1}(x)$, let $\mathrm{pr} = \mathrm{pr}_{L/K}\colon P^y_{L/K_0} \to P^x_{K/K_0}$ denote the restriction of primes from L to K.

Lemma 3.1. *Let $y, z \in \pi^{-1}(x)$. Then $\mathrm{pr}(P^y_{L/K_0}), \mathrm{pr}(P^z_{L/K_0})$ are either disjoint or equal. They are equal if and only if y, z are H-conjugate.*

Proof. Assume that $\mathrm{pr}(P^y_{L/K_0}) \cap \mathrm{pr}(P^z_{L/K_0}) \neq \emptyset$. Then there are primes $\mathfrak{P} \in P^y_{L/K_0}, \mathfrak{Q} \in P^z_{L/K_0}$ with $\mathfrak{P}|_K = \mathfrak{Q}|_K =: \mathfrak{p}$. Let $\mathfrak{p}_0 := \mathfrak{p}|_{K_0}$. The primes in L lying over $\mathfrak{p}_0$ are in 1:1-correspondence with cosets of $\langle y \rangle = D_{\mathfrak{P},L/K_0} \subseteq G$:

$$G/\langle y \rangle \xrightarrow{\sim} S_{\mathfrak{p}_0}(L), \quad g\langle y \rangle \mapsto g\mathfrak{P}.$$

The Frobenius of $g\mathfrak{P}$ is gyg^{-1}; after reduction modulo H we obtain the same correspondence for K: $(G/H)/\langle x \rangle = G/H\langle y \rangle \xrightarrow{\sim} S_{\mathfrak{p}_0}(K)$ and $\mathfrak{P}, g\mathfrak{P}$ lie over the same prime of K if and only if $\pi(g) \in \langle x \rangle$, i.e., $g \in H\langle y \rangle$. So with our assumption we get $\mathfrak{Q} = g\mathfrak{P}$ for some $g \in H\langle y \rangle$ with $gyg^{-1} = z$. By multiplying with a power of y, we can modify g such that $g \in H$.

Assume conversely that for $y, z \in \pi^{-1}(x)$ there is some $g \in H$ with $gyg^{-1} = z$. Then we claim that $\mathrm{pr}(P^y_{L/K_0}) = \mathrm{pr}(P^z_{L/K_0})$. Indeed, let $\mathfrak{p} \in \mathrm{pr}(P^y_{L/K_0})$ with preimage $\mathfrak{P} \in P^y_{L/K_0}$. Using the above description of primes via cosets, it is immediate to see that $g\mathfrak{P} \in P^z_{L/K_0}$ also lies over $\mathfrak{p}$. □

For an H-conjugacy class C in $\pi^{-1}(x)$, let $M_C \subseteq P^x_{K/K_0}$ denote the image of P^y_{L/K_0} under *pr* for some (any) $y \in C$. Thus if $\mathrm{Ram}(L/K)$ denotes the set of primes of K, which ramify in L, then we have a disjoint decomposition

$$P^x_{K/K_0} = (\mathrm{Ram}(L/K) \cap P^x_{K/K_0}) \cup \bigcup_{C \subseteq \pi^{-1}(x)} M_C,$$

where the first set is finite and the union is taken over all H-conjugacy classes inside $\pi^{-1}(x)$. We have the following generalization of Chebotarev's density theorem (observe that $\sharp H = \sharp \pi^{-1}(x)$):

Proposition 3.2. *Let $L/K/K_0, \pi, x$ be as above. Let C be an H-conjugacy class in $\pi^{-1}(x)$. Then*

$$\delta_{K/K_0,x}(M_C) = \frac{\sharp C}{\sharp H}.$$

When setting $x = 1$, this reduces to the classical Chebotarev's density theorem for the Dirichlet density. Fortunately, the proof of this proposition does not need any new L-functions, it simply follows from the classical Chebotarev.

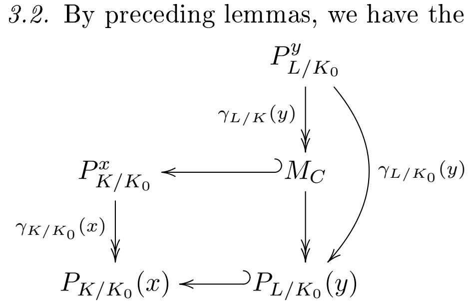
Lemma 3.3. *Let $L/K/K_0$, π, x be as above. Let d be the order of x in G/H. Let $y \in \pi^{-1}(x)$ and let $C \subseteq \pi^{-1}(x)$ denote the H-conjugacy class of y. Then the map $\mathrm{pr}\colon P^y_{L/K_0} \twoheadrightarrow M_C$ is surjective and $\gamma_{L/K}(y)$-to-1, where $\gamma_{L/K}(y) := \frac{\sharp Z_H(y)}{\sharp\langle y^d \rangle}$.*

Proof of Lemma 3.3. The surjectivity follows from definition. Using the description of primes via cosets modulo the decomposition group, one sees easily that for $\mathfrak{p} \in M_C$, the primes in $S_{\mathfrak{p}}(L) \cap P^y_{L/K_0}$ are in one-to-one correspondence with elements in the group $Z_G(y) \cap H\langle y \rangle / \langle y \rangle$. One sees then that the composition

$$Z_H(y) \hookrightarrow Z_G(y) \cap H\langle y \rangle \twoheadrightarrow Z_G(y) \cap H\langle y \rangle / \langle y \rangle$$

is surjective and its kernel is $\langle y^d \rangle$. □

Proof of Proposition 3.2. By preceding lemmas, we have the following diagram:



in which any vertical map is surjective and has fibers of equal cardinality, and the number on the arrow denotes the dergee (γ is as in Lemma 3.3). Thus the lower right map is $\beta(y) : 1$, with $\beta(y) = \frac{\sharp Z_G(y)}{\sharp\langle x \rangle \sharp Z_H(y)}$. It follows:

$$\delta_{K/K_0,x}(M_C) = \lim_{s \to d^{-1}+0} \frac{\sum_{M_C} \mathrm{N}\,\mathfrak{p}^{-s}}{\sum_{P^x_{K/K_0}} \mathrm{N}\,\mathfrak{p}^{-s}} = \lim_{t \to 1+0} \frac{\beta(y) \sum_{\mathfrak{p} \in P_{L/K_0}(y)} \mathrm{N}\,\mathfrak{p}^{-t}}{\gamma_{K/K_0}(x) \sum_{\mathfrak{p} \in P_{K/K_0}(x)} \mathrm{N}\,\mathfrak{p}^{-t}} = \frac{\beta(y)\delta_{K_0}(P_{L/K_0}(y))}{\gamma_{K/K_0}(x)\delta_{K_0}(P_{K/K_0}(x))}.$$

where δ_{K_0} denotes the usual Dirichlet density on Σ_{K_0}. By Chebotarev we have: $\delta_{K_0}(P_{L/K_0}(y)) = \frac{\sharp C(y,G)}{\sharp G} = \frac{1}{\sharp Z_G(y)}$ and $\delta_{K_0}(P_{K/K_0}(x)) = \frac{1}{\sharp Z_{G/H}(x)}$. Hence we obtain:

$$\delta_{K/K_0,x}(M_C) = \frac{\beta(y)\sharp Z_{G/H}(x)}{\gamma_{K/K_0}(x)\sharp Z_G(y)} = \frac{\sharp Z_G(y)}{\sharp\langle x\rangle \sharp Z_H(y)} \frac{\sharp\langle x\rangle}{\sharp Z_{G/H}(x)} \frac{\sharp Z_{G/H}(x)}{\sharp Z_G(y)} = \frac{1}{\sharp Z_H(y)} = \frac{\sharp C}{\sharp H}.$$

□

Now we can derive the pull-back behavior of $\delta_{K/K_0,x}$.

Corollary 3.4. *Let $y \in \pi^{-1}(x)$ and let C be its H-conjugacy class in $\pi^{-1}(x)$. Then*

$$\delta_{L/K_0,y}(S_L) = \delta_{K/K_0,x}(M_C)^{-1}\delta_{K/K_0,x}(S\cap M_C) = \frac{\sharp H}{\sharp C}\delta_{K/K_0,x}(S\cap M_C)$$

if all densities exist.

Proof. Let e denote the order of y in G and d the order of x in G/H. Then

$$\begin{aligned}\delta_{L/K_0,y}(S_L) &= \lim_{s\to e^{-1}+0} \frac{\sum_{\mathfrak{p}\in S_L\cap P^y_{L/K_0}} \mathrm{N}\,\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}\in P^y_{L/K_0}} \mathrm{N}\,\mathfrak{p}^{-s}} = \lim_{t\to d^{-1}+0} \frac{\sum_{\mathfrak{p}\in S\cap M_C} \mathrm{N}\,\mathfrak{p}^{-t}}{\sum_{\mathfrak{p}\in M_C} \mathrm{N}\,\mathfrak{p}^{-t}} \\ &= \delta_{K/K_0,x}(M_C)^{-1}\delta_{K/K_0,x}(S\cap M_C),\end{aligned}$$

where we made a change of variables by replacing s by $t := \frac{e}{d}s$ and used the fact that S_L is defined over K. Proposition 3.2 finishes the proof. □

The special case $x = y = 1$ in Corollary 3.4 gives the well-known formula

$$\delta_L(S_L) = [L:K]\delta_K(S\cap \mathrm{cs}(K/K_0)).$$

for the Dirichlet density. We compute the x-density of pull-backs of Chebotarev sets.

Corollary 3.5. *Let L, M be two finite Galois extensions of K. Let $\sigma \in \mathrm{G}_{M/K}$, $x \in \mathrm{G}_{L/K}$ with images $\bar\sigma, \bar x$ in $\mathrm{G}_{L\cap M/K}$ respectively. Let $S \simeq P_{M/K}(\sigma)$. Then*

$$\delta_{L/K,x}(S_L) = \begin{cases} \frac{\sharp C((x,\sigma),\mathrm{G}_{LM/K})}{[M:L\cap M]\sharp C(x,\mathrm{G}_{L/K})} & \text{if } \bar\sigma = \bar x, \\ 0 & \text{if } \bar\sigma \neq \bar x, \end{cases}$$

where we write (x,σ) for the unique element of $\mathrm{G}_{LM/K} \cong \mathrm{G}_{L/K}\times_{\mathrm{G}_{L\cap M/K}} \mathrm{G}_{M/K}$ mapping to x, σ under both projections.

Proof. Indeed, apply Corollary 3.4 to $\delta_{K/K,1}$ and $\delta_{L/K,x}$. Then $\delta_{K/K,1} = \delta_K$ is the Dirichlet density and we have $M_x = P_{L/K}(x)$ and

$$\delta_{L/K,x}(S_L) = \delta_K(P_{L/K}(x))^{-1}\delta_K(P_{L/K}(x)\cap S) = \delta_K(P_{L/K}(x))^{-1}\delta_K(P_{L/K}(x)\cap P_{M/K}(\sigma)).$$

The intersection $P_{L/K}(x)\cap P_{M/K}(\sigma)$ is empty unless $\bar\sigma = \bar x$, hence we can assume equality. Under this assumption, we have $P_{L/K}(x)\cap P_{M/K}(\sigma) = P_{LM/K}((\sigma,x))$ and the corollary follows immediately from Chebotarev. □

4. Densities associated to characters

Definition 4.1. Let K/K_0 be finite Galois and $S \subseteq \Sigma_K$ a subset.

(i) We call S *mesurable* (over K_0), if for all $x \in \mathrm{G}_{K/K_0}$ the density $\delta_{K/K_0,x}(S)$ exists (this is essentially independent of K_0).

(ii) Assume that S is mesurable. Then define the *characteristic function* of S as

$$\chi_{K/K_0,S}\colon \mathrm{G}_{K/K_0} \to [0,1], \quad x \mapsto \delta_{K/K_0,x}(S).$$

Remark 4.2. Notice that $\chi_{K/K_0,S}$ is only a real-valued function on G_{K/K_0}, which is not necessarily a class function. But, if S is defined over K_0, it is a class function (clearly, the converse is in general not true).

For a finite group G, let $G(\mathbb{C})$ be the set of complex valued functions on G. Then we have the inner product on $G(\mathbb{C})$ defined by

$$\langle \chi, \psi \rangle_G := \sharp G^{-1} \sum_{x \in G} f(x)\overline{g(x)}$$

for all $\chi, \psi \in G(\mathbb{C})$. If $G = \mathrm{G}_{L/K}$ we also write $\langle \cdot, \cdot \rangle_{L/K}$ (or even $\langle \cdot, \cdot \rangle_L$ if K is clear from the context) instead of $\langle \cdot, \cdot \rangle_{\mathrm{G}_{L/K}}$.

Definition 4.3. Let K/K_0 be finite Galois. For any $\psi \in \mathrm{G}_{K/K_0}(\mathbb{C})$ we define the $\mathbb{C}$-valued function $\delta_{K/K_0,\psi}$ on the set of all mesurable subsets of Σ_K by

$$\delta_{K/K_0,\psi}(S) := \langle \psi, \chi_{K/K_0,S} \rangle_K$$

for any mesurable set S. We say that $\delta_{K/K_0,\psi}$ is a *density*, if for all mesurable S it takes values in the real unit interval $[0,1]$ and $\delta_{K/K_0,\psi}(\Sigma_K) = 1$.

Lemma 4.4. *Let K/K_0 be finite Galois and $\psi \in G_{K/K_0}(\mathbb{C})$.*

(i) *Let S, T be mesurable. If one of the sets $S \cap T, S \cup T$ is mesurable, then the second set is too and*

$$\delta_{K/K_0,\psi}(S) + \delta_{K/K_0,\psi}(T) = \delta_{K/K_0,\psi}(S \cap T) + \delta_{K/K_0,\psi}(S \cup T).$$

(ii) *The function $\delta_{K/K_0,\psi}$ is a density if and only if ψ takes values only in the real interval $[0, [K : K_0]]$ and $\langle \psi, \mathbf{1} \rangle_{K/K_0} = 1$, where $\mathbf{1}$ denotes the trivial character of G_{K/K_0}.*

Proof. (i) follows from bilinearity of $\langle \cdot, \cdot \rangle_{K/K_0}$ and Remark 2.3 and (ii) is an immediate computation. □

Remark 4.5. In particular, the Dirichlet density δ_K corresponds to the character of the regular representation of G_{K/K_0} and $\delta_{K/K_0,x}$ for $x \in \mathrm{G}_{K/K_0}$ corresponds to the function defined by $\psi(y) = [K : K_0]\delta_{xy}$, where δ_{xy} is the Kronecker symbol.

The next proposition shows that if L/K is a finite extension then χ_{L,S_L} is in a sense the induction of $\chi_{K,S}$ to L:

Proposition 4.6. *Let $L/K/K_0$ be finite Galois extensions. Denote by $\pi : \mathrm{G}_{L/K_0} \twoheadrightarrow \mathrm{G}_{K/K_0}$ the natural projection. Then for all $\psi \in \mathrm{G}_{K/K_0}(\mathbb{C})$ and all mesurable S we have*

$$\langle \inf_{\mathrm{G}_{K/K_0}}^{\mathrm{G}_{L/K_0}} \psi, \chi_{L,S_L} \rangle_L = \langle \psi, \chi_{K,S} \rangle_K$$

or equivalently,

$$\delta_{L/K_0,\psi\circ\pi}(S_L) = \delta_{K/K_0,\psi}(S).$$

Proof. Let $G := \mathrm{G}_{L/K_0}$, $H := \mathrm{G}_{L/K}$. For $y \in G$, let $C(y) \subseteq \pi^{-1}(\pi(y))$ denote its H-conjugacy class. Then (we write $\delta_{*,\psi}$ instead of $\delta_{*/K_0,\psi}$):

$$\begin{aligned}
\langle \psi \circ \pi, \chi_{L,S_L} \rangle_L &= \frac{1}{\sharp G} \sum_{y \in G} \psi(\pi(y)) \delta_{L,y}(S_L) \\
&= \frac{1}{\sharp G} \sum_{y \in G} \psi(\pi(y)) \frac{\sharp H}{\sharp C(y)} \delta_{K,x}(S \cap M_{C(y)}) \\
&= \frac{1}{\sharp (G/H)} \sum_{x \in G/H} \psi(x) \sum_{C \subseteq \pi^{-1}(x)} \sum_{y \in C} \frac{1}{\sharp C} \delta_{K,x}(S \cap M_C) \\
&= \frac{1}{\sharp (G/H)} \sum_{x \in G/H} \psi(x) \sum_{C \subseteq \pi^{-1}(x)} \delta_{K,x}(S \cap M_C) \\
&= \frac{1}{\sharp (G/H)} \sum_{x \in G/H} \psi(x) \delta_{K,x}(S) = \langle \psi, \chi_{K,S} \rangle_K.
\end{aligned}$$

where the second equality follows from Corollary 3.4. □

5. Realization of local extensions

5.1. **Complements on stable sets.** Before starting with the proof of Theorem 1.1, we recall for the convenience of the reader some definitions and results from [4].

Definition 5.1 (part of [4] Definitions 2.4, 2.7)**.** Let S be a set of primes of K and $\mathscr{L}/K$ any (algebraic) 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 $\lambda a > \delta_L(S_0) \geq a > 0$ for all finite subextensions $\mathscr{L}/L/L_0$. We say that S is **λ-stable** for $\mathscr{L}/K$, if it has a λ-stabilizing 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 $\lambda > 1$. We say that S is (λ-)**stable**, if it is (λ-)stable for K_S/K.

(ii) We say that S is **persistent** for $\mathscr{L}/K$ (with persisting field L_0, lying between $\mathscr{L}/K$) if the density of a subset $S_0 \subseteq S$ gets constant in the tower $\mathscr{L}/L_0$.

(iii) Let p be a rational prime. We say that S is **sharply p-stable** for $\mathscr{L}/K$, if $\mu_p \subseteq \mathscr{L}$ and S is p-stable for $\mathscr{L}/K$, or $\mu_p \not\subseteq \mathscr{L}$ and S is stable for $\mathscr{L}(\mu_p)/K$. We say that S is **sharply p-stable**, if S is sharply p-stable for K_S/K.

We will need the following crucial result about stable sets, which we take from [4].

Theorem 5.2 ([4] Theorem 5.9)**.** *Let K be a number field, S a set of primes of K and $\mathscr{L} \subseteq K_S$ a subextension normal over K, such that S is sharply p-stable for $\mathscr{L}/K$. Let T be a finite set of primes of K containing $(S_p \cup S_\infty) \smallsetminus S$. If $p^\infty | [\mathscr{L} : K]$, then*

$$\varinjlim_{\mathscr{L}/L/K, \mathrm{res}} \mathrm{coker}^1(K_{S \cup T}/L, T, \mathbb{Z}/p\mathbb{Z}) = 0.$$

Remark 5.3. Many results (e.g., such as the one quoted above, but also finite cohomological dimension, etc.) holding for sets with Dirichlet density one also hold (with respect to a prime p) for (sharply-p-)stable sets of primes. The proofs in the case of sets with density one rely heavily on the fact that various Tate-Shafarevich groups of $\mathrm{G}_{K,S}$ with finite resp. divisible coefficients vanish. This is in general not true for stable sets and the reason why many proofs (in particular, the proof of Theorem 5.2) still work, is that one can, using stability conditions, bound the size of Tate-Shafarevich groups, which in turn implies the vanishing of them in the limit taken over all finite subextensions of certain (infinite) subextensions $K_S/\mathscr{L}/K$.

By easy density computations we obtain:

Lemma 5.4 ([4] Proposition 3.3, Corollary 3.4)**.** *Let M/K be a finite Galois extension and $\sigma \in \mathrm{G}_{M/K}$.*

(i) *Let L/K be any finite extension. Let $L_0 := L \cap M$. Then:*

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

(ii) *Let $S \backsimeq P_{M/K}(\sigma)$. Let $\mathscr{L}/K$ be any extension. Then S is persistent for $\mathscr{L}/K$ with persisting field L_0 if and only if*

$$\mathrm{G}_{M/M\cap\mathscr{L}} \cap C(\sigma; \mathrm{G}_{M/K}) \neq \emptyset,$$

where $C(\sigma; \mathrm{G}_{M/K})$ denotes the conjugacy class of σ in $\mathrm{G}_{M/K}$.

From now on and until the end of the paper we prove Theorem 1.1. We let $M/K, \sigma, R \subseteq S$ and $\ell \leq \infty$ be as in the theorem.

5.2. **Some reduction steps.** Clearly, we can assume $\ell < \infty$. For any finite subextension $K_S^R/L/K$, any finite set T of primes of L and any rational prime p consider the cokernel

$$\mathrm{H}^1(K_{S\cup T}/L, \mathbb{Z}/p\mathbb{Z}) \to \prod_T \mathrm{H}^1(\overline{K_{\mathfrak{p}}}/L_{\mathfrak{p}}, \mathbb{Z}/p\mathbb{Z}) \twoheadrightarrow \mathrm{coker}^1(K_{S\cup T}/L, T; \mathbb{Z}/p\mathbb{Z})$$

of the restriction map. Theorem 1.1 for $K_S^R(\mathfrak{c}_{\leq \ell})/K$ follows easily from Claim 5.5 below for all $p \leq \ell$ (cf. [5] 9.2.7, 9.4.3).

Claim 5.5. *For all $T \supseteq R \cup S_p \cup S_\infty$, we have*

$$\varinjlim_L \mathrm{coker}^1(K_{S\cup T}/L, T; \mathbb{Z}/p\mathbb{Z}) = 0,$$

where the limit is taken over all finite subextensions L of $K_S^R(\mathfrak{c}_{\leq \ell})/K$.

Lemma 5.6. *There are two finite sets R_1, R_2 of primes of K with $R_1 \cap R_2 = R$ and such that $M \cap K_S^{R_j} = K$, i.e., $P_{M/K}(\sigma)$ (and hence also S) is persistent for $K_S^{R_j}/K$ with persisting field K for $i = 1, 2$.*

Proof. Indeed, choose a set of generators $g_1, \dots, g_r$ of $\mathrm{G}_{M/K}$ and for $j = 1, 2$ primes $\mathfrak{p}_{j,1}, \dots, \mathfrak{p}_{j,r}$ of K unramified in M/K such that the Frobenius conjugacy class corresponding to $\mathfrak{p}_{j,k}$ is the conjugacy class of g_k and such that the sets $\{\mathfrak{p}_{j,k} \colon k = 1, \dots, r\} \smallsetminus R$ are disjoint for $j = 1, 2$ (this is possible by Chebotarev). Let $R_j := \{\mathfrak{p}_{j,k} \colon k = 1, \dots, r\} \cup R$. Then any non-trivial (Galois) subextension of M/K is not completely split in at least one prime $\mathfrak{p} \in R_j$. Hence $M \cap K_S^{R_j} = K$ and hence by Lemma 5.4, $P_{M/K}(\sigma)$ is persistent for $K_S^{R_j}/K$ with persisting field K. $\square$

Step 1. By Lemma 5.6 we can enlarge R and hence assume that M satisfies $M \cap K_S^R = K$. In particular, $P_{M/K}(\sigma)$ is persistent for K_S^R/K with persisting field K by Lemma 5.4 (note also that the assumptions of the theorem are inherited if we replace K by a finite subextension $K_S^R(\mathfrak{c}_{\leq \ell})/L/K$ and S by S_L, as $P_{ML/L}(\sigma) \backsimeq P_{M/K}(\sigma)_L$ for any such L and since we also have $L_S^R(\mathfrak{c}_{\leq \ell}) = K_S^R(\mathfrak{c}_{\leq \ell})$ and $ML \cap L_S^R(\mathfrak{c}_{\leq \ell}) = L$ (as $K_S^R(\mathfrak{c}_{\leq \ell}) \cap M = K$)). Now Claim 5.5 for all $p \leq \ell$ such that S is sharply-p-stable for $K_R^S(\mathfrak{c}_{\leq \ell})/K$, follows by Theorem 5.2 (observe, in particular, that since $P_{M/K}(\sigma)$ is persistent for K_S^R/K and $\mu_2 \subseteq K$, S is always sharply-2-stable for K_S^R/K).

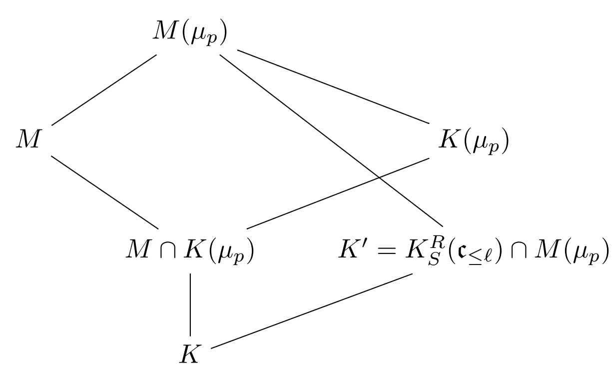
Step 2. Thus we can assume that $P_{M/K}(\sigma)$ is not sharply-p-stable for $K_R^S(\mathfrak{c}_{\leq \ell})/K$. By induction we assume that Claim 5.5 holds for all $p' < p$. As the assumptions are stable under enlarging K inside $K_S^R(\mathfrak{c}_{\leq \ell})$, it is enough to show that for each T as in the claim, there is a (not necessarily finite) subextension $K_S^R(\mathfrak{c}_{\leq \ell})/\mathscr{L}/K$, such that

$$\varinjlim_{\mathscr{L}/L/K} \operatorname{coker}^1(K_{S \cup T}/L, T; \mathbb{Z}/p\mathbb{Z}) = 0, \tag{5.1}$$

where the limit is taken over finite subextensions of $\mathscr{L}/K$. Further, since $P_{M/K}(\sigma)$ is persistent for $K_S^R(\mathfrak{c}_{\leq \ell})/K$, our assumption implies $\mu_p \not\subseteq K_S^R(\mathfrak{c}_{\leq \ell})$ and $\delta_{L(\mu_p)}(P_{M/K}(\sigma)) = 0$ for L a sufficently big finite subextension of $K_S^R(\mathfrak{c}_{\leq \ell})/K$. We replace K by such L, and so we can assume that $\delta_{K(\mu_p)}(P_{M/K}(\sigma)) = 0$.

Step 3. We have $\mu_p \not\subseteq K_S^R(\mathfrak{c}_{\leq \ell})$ and after replacing K by a finite subextension of $K_S^R(\mathfrak{c}_{\leq \ell})/K$ if necessary, we can assume that for any finite subextension $K_S^R(\mathfrak{c}_{\leq \ell})/L/K$, the natural map $\mathrm{G}_{L(\mu_p)/L} \to \mathrm{G}_{K(\mu_p)/K}$ is an isomorphism. We write $\Delta := \mathrm{G}_{K(\mu_p)/K}$ and $d := \operatorname{ord}(\Delta)$. The group Δ can canonically be identified with a subgroup of $\mathbb{F}_p^*$, an element $x \in \mathbb{F}_p^*$ acting on $\zeta \in \mu_p$ by $\zeta \mapsto \zeta^x$. Note that by assumption we have $1 < d < p$.

Step 4. We replace M by $M(\mu_p)$. Therefore consider the following diagram of extensions of K:



We have $\mathrm{G}_{M(\mu_p)/K} = \mathrm{G}_{M/K} \times_{\mathrm{G}_{M\cap K(\mu_p)/K}} \mathrm{G}_{K(\mu_p)/K}$. Let $K' := K_S^R \cap M(\mu_p)$. Then $K' \cap M \subseteq K_S^R(\mathfrak{c}_{\leq \ell}) \cap M = K$, hence $\mathrm{G}_{M(\mu_p)/K'}$ and $\mathrm{G}_{M(\mu_p)/M}$ together generate $\mathrm{G}_{M(\mu_p)/K}$ and hence the composition $\mathrm{G}_{M(\mu_p)/K'} \hookrightarrow \mathrm{G}_{M(\mu_p)/K} \twoheadrightarrow \mathrm{G}_{M/K}$ is surjective. Let σ' be a preimage of σ inside $\mathrm{G}_{M(\mu_p)/K'} \subseteq \mathrm{G}_{M(\mu_p)/K}$. Then $P_{M(\mu_p)/K}(\sigma') \subseteq P_{M/K}(\sigma) \overset{\subsetneq}{\sim} S$ and $P_{M(\mu_p)/K'}(\sigma') \simeq P_{M(\mu_p)/K'}(\sigma') \cap \mathrm{cs}(K'/K)_{K'} = P_{M(\mu_p)/K}(\sigma')_{K'}$. Hence $P_{M(\mu_p)/K'}(\sigma') \overset{\subsetneq}{\sim} S_{K'}$. Thus we can replace $(K, P_{M/K}(\sigma))$ by $(K', P_{M(\mu_p)/K'}(\sigma'))$ and, in particular, we can assume that μ_p *subseteqM*. We have now the following easy situation:

$$
\begin{array}{ccccc}
MK_S^R(\mathfrak{c}_{\leq \ell}) & \text{———} & K_S^R(\mathfrak{c}_{\leq \ell})(\mu_p) & \text{———} & K_S^R(\mathfrak{c}_{\leq \ell}) \\
| & & | & & | \\
M & \text{———} & K(\mu_p) & \text{———} & K
\end{array}
\tag{5.2}
$$

and the right and the outer squares are cartesian, i.e., $M \cap K_S^R(\mathfrak{c}_{\leq \ell}) = K$ and $K(\mu_p) \cap K_S^R(\mathfrak{c}_{\leq \ell}) = K$. By Lemma 5.7 also the left square is cartesian, i.e., $M \cap K_S^R(\mathfrak{c}_{\leq \ell})(\mu_p) = K(\mu_p)$. Observe also that the situation is now stable under replacing $K, K(\mu_p), M$ by $L, L(\mu_p), ML$ for a finite subextension $K_S^R(\mathfrak{c}_{\leq \ell})/L/K$ and the Galois groups $\mathrm{G}_{M/K}, \mathrm{G}_{M/K(\mu_p)}, \mathrm{G}_{K(\mu_p)/K} = \Delta$ will stay unchanged under such a replacement.

Lemma 5.7. *In the above situation we have $M \cap K_S^R(\mathfrak{c}_{\leq \ell})(\mu_p) = K(\mu_p)$.*

Proof. We have natural homomorphisms $\mathrm{G}_{MK_S^R(\mathfrak{c}_{\leq \ell})/M} \to \mathrm{G}_{K_S^R(\mathfrak{c}_{\leq \ell})(\mu_p)/K(\mu_p)} \to \mathrm{G}_{K_S^R(\mathfrak{c}_{\leq \ell})/K}$. The right one and the composition of both are isomorphisms. Hence also the left one is an isomorphism. □

Observe that $C(\sigma, \mathrm{G}_{M/K}) \cap \mathrm{G}_{M/K(\mu_p)} = \emptyset$ since $\delta_{K(\mu_p)}(P_{M/K}(\sigma)) = 0$ (cf. Lemma 5.4), and hence the image $\bar{\sigma}$ of σ in $\Delta = \mathrm{G}_{K(\mu_p)/K}$ is unequal 1.

Step 5. Let $\mathfrak{p} \notin R$ be a prime of K. Recall the number $1 < d < p$ from step 3. By the induction assumption in step 2, we can realize a cyclic extension of order d at $\mathfrak{p}$ by a finite subextension of $K_S^R(\mathfrak{c}_{\leq \ell})/K$. More precisely, there is a finite subextension $K_S^R(\mathfrak{c}_{\leq \ell})/K_0/K$ such that the decomposition group $D_{\mathfrak{p}_1, K_0/K}$ at a prime $\mathfrak{p}_1$ of K_0 lying over $\mathfrak{p}$ contains a cyclic subgroup H_0 of order d. We replace K by $K_0^{H_0}$ (and $P_{M/K}(\sigma)$ by $P_{MK_0^{H_0}/K_0^{H_0}}(\sigma)$) and hence can assume that K has a cyclic extension K_0 of degree d inside $K_S^R(\mathfrak{c}_{\leq \ell})$.

We summarize the special situation obtained by all reduction steps: we have a number field K, two sets of primes $S \supseteq R$ of K with R finite. We have further a finite extension $M/K(\mu_p)/K$ such that all squares in the diagram (5.2) in step 4 are cartesian, an element $\sigma \in \mathrm{G}_{M/K}$ with $P_{M/K}(\sigma) \overset{\subsetneq}{\sim} S$ and image $1 \neq \bar{\sigma} \in \Delta = \mathrm{G}_{K(\mu_p)/K}$. We have $d := \sharp\Delta$ with $1 < d < p$, and there is a finite cyclic subextension $K_S^R(\mathfrak{c}_{\leq \ell})/K_0/K$ of degree d with Galois group $H_0 := \mathrm{G}_{K_0/K}$. In this very special situation we want to show Claim 5.5 for p. As remarked in step 2, it is enough to show that for each finite set $T \supseteq R \cup S_p \cup S_\infty$, there is a subextension

$K_S^R(\mathfrak{c}_{\leq \ell})/\mathscr{L}/K$, such that (5.1) holds. Recall that Poitou-Tate duality implies a surjection:

$$Ш^1(K_{S\cup T}/K, S \smallsetminus T, \mu_p)^\vee \twoheadrightarrow \mathrm{coker}^1(K_{S\cup T}/K, T; \mathbb{Z}/p\mathbb{Z})$$

(cf. [5] 9.2.2), where the transition maps res on the right correspond to $\mathrm{cor}^\vee$ on the left. By exactness of $\varinjlim$, it is enough to find a subextension $K_S^R/\mathscr{L}/K$ with

$$\varinjlim_{\mathscr{L}/L/K, \mathrm{cor}^\vee} Ш^1(K_{S\cup T}/L, S \smallsetminus T; \mu_p)^\vee = 0. \tag{5.3}$$

Finally remark that for any subfields $K_S^R(\mathfrak{c}_{\leq \ell})/L'/L/K$ the restriction maps

$$\mathrm{res}_L^{L'} \colon \mathrm{H}^1(K_{S\cup T}/L, \mu_p) \hookrightarrow \mathrm{H}^1(K_{S\cup T}/L', \mu_p),$$

are injective, as one sees from the Hochschild-Serre spectral sequence using the fact that μ_p is not trivialized by L'. We can and will see these restriction maps as embeddings and identify the first group with a subgroup of the second via $\mathrm{res}_L^{L'}$.

5.3. **Construction of the tower $\mathscr{L}/K$.** Recall that $\bar{\sigma} \neq 1$ denotes the image of $\sigma \in \mathrm{G}_{M/K}$ in $\mathrm{G}_{K(\mu_p)/K} = \Delta$ and $H_0 = \mathrm{G}_{K_0/K}$ is cyclic of order d. By the order of a character of a group we mean the cardinality of its image.

Lemma 5.8. *There is a character $\chi \colon H_0 \to \mathbb{F}_p^*$ of order $\geq \mathrm{ord}(\bar{\sigma})$ and a tower of Galois extensions*

$$K \subset K_0 \subset K_1 \subset \cdots \subset K_i \subset \cdots \subset \bigcup_{i=0}^{\infty} K_i =: \mathscr{L} \subseteq K_S^R$$

such that for all $i \geq 1$ we have:

$$H_i := \mathrm{G}_{K_i/K} \cong H_0 \ltimes (\prod_{j=1}^{i} \mathbb{Z}/p\mathbb{Z}),$$

where H_0 acts diagonally on $\prod_{j=1}^{i} \mathbb{Z}/p\mathbb{Z}$ and the action on each component is given by χ.

Proof. K_0 and H_0 were constructed in step 5 of Section 5.2. We have $M \cap K_S^R = K$ and hence

$$P_{M/K}(\sigma) = \bigcup_{x \in H_0} P_{MK_0/K}(\sigma, x).$$

up to finitely many ramified primes (cf. [7] Proposition 2.1). By looking at the Dirichlet density, $S \cap P_{MK_0/K}(\sigma, x)$ is infinite for any $x \in H_0$, hence also $S_{K_0} \cap P_{MK_0/K}(\sigma, x)_{K_0}$ is infinite. Choose such an x with $\mathrm{ord}(x) = \mathrm{ord}(\bar{\sigma})$ and write $S' := S \cap P_{MK_0/K}(\sigma, x)$. Then for almost all $\mathfrak{p} \in S'_{K_0}$, the local extensions $K_{0,\mathfrak{p}}/K_{\mathfrak{p}}$ and $K(\mu_p)_{\mathfrak{p}}/K_{\mathfrak{p}}$ are unramified of degree $\mathrm{ord}(\bar{\sigma})$, hence $K_0(\mu_p)_{\mathfrak{p}}/K_{0,\mathfrak{p}}$ is completely split in $\mathfrak{p}$, i.e., $\mu_p \subseteq K_{0,\mathfrak{p}}$. In particular, by [5] 10.7.3, $X := \mathrm{H}^1(K_{0,S'}/K_0, \mathbb{Z}/p\mathbb{Z})$ is infinite. X is a (semisimple) $\mathbb{F}_p[H_0]$-module, hence it decomposes into isotypical components $X(\phi)$ where ϕ goes through all $\mathbb{F}_p^*$-valued characters of H_0. From the Hochschild-Serre spectral sequence for the Galois groups of the extensions $K_{0,S'}/K_0/K_0^{\ker(\phi)}$ and $(\ abs\ker(\phi), p) = 1$ it follows that

$$X(\phi) \subseteq \mathrm{H}^1((K_0^{\ker(\phi)})_{S'}/K_0^{\ker(\phi)}, \mathbb{Z}/p\mathbb{Z}) \subseteq \mathrm{H}^1(K_{0,S'}/K_0, \mathbb{Z}/p\mathbb{Z}) \tag{5.4}$$

In particular, if $\mathrm{ord}(\phi) < \mathrm{ord}(\bar{\sigma})$, then the order of the image of x in $H_0/\ker(\phi) = \mathrm{G}_{K_0^{\ker(\phi)}/K}$ is $< \mathrm{ord}(\bar{\sigma})$ and for all primes $\mathfrak{p} \in S'(K_0^{\ker(\phi)})$ one has $\mu_p \not\subseteq (K_0^{\ker(\phi)})_{\mathfrak{p}}$. By [5] 10.7.3, the group in the middle of (5.4) is finite and hence there must be a chracter χ of H_0 of order $\geq \mathrm{ord}(\bar{\sigma})$ such that $X(\chi)$ is infinite. For a family $(\alpha_i)_{i=1}^{\infty}$ of linearly independent elements of $X(\chi)$, let $K_0(\alpha_i)$ be the cyclic $\mathbb{Z}/p\mathbb{Z}$-extension of K_0 corresponding to α_i and define K_i to be the compositum of the fields $\{K_0(\alpha_j)\}_{j=0}^{i}$. □

5.4. **Action of $\Delta \times H_i$ on $Ш^1(K_{S\cup T}/K_i, S \smallsetminus T, \mu_p)$.** Let $\mathscr{L}/K_i/K$ be one of the fields defined above. We write

$$Ш^1_i := Ш^1(K_{S\cup T}/K_i, S \smallsetminus T; \mu_p).$$

We have the following embeddings:

$$\begin{array}{ccccccc} Ш^1_i & \hookrightarrow & \mathrm{H}^1(K_{S\cup T}/K_i,\mu_p) & \hookrightarrow & \mathrm{H}^1(\overline{K}/K_i,\mu_p) & = & K_i^*/p \\ & & \big\downarrow{\scriptstyle\Delta} & & \big\downarrow{\scriptstyle\Delta} & & \big\downarrow{\scriptstyle\Delta} \\ & & \mathrm{H}^1(K_{S\cup T}/K_i(\mu_p),\mu_p) & \hookrightarrow & \mathrm{H}^1(\overline{K}/K_i(\mu_p),\mu_p) & = & K_i(\mu_p)^*/p \end{array}$$

where the Δ on the arrows means that the upper entry is obtained from the lower one by taking Δ-invariants. The horizontal isomorphisms on the right are canonical and given by Kummer theory. The vertical maps come from the Hochschild-Serre spectral sequence. As a subset of the lower right entry $Ш^1_i$ defines by Kummer theory a p-primary Galois extension of $K_i(\mu_p)$. Further, the subgroup $Ш^1_i$ is invariant under the $\Delta \times H_i$-action on the lower entries. Indeed, the H_i-invariance results simply from the definition of $Ш^1_i$ and the fact that $S \smallsetminus T$ is defined over K, and the Δ-invariance is obvious from the diagram. Let L_i denote the abelian p-primary extension of $K_i(\mu_p)$, which is associated to $Ш^1_i \subseteq K_i(\mu_p)^*/p$ via Kummer theory. The invariance discussed above implies that the composite extension $L_i/K_i(\mu_p)/K$ is Galois. Fix a trivialization of μ_p; this gives an isomorphism of the Galois group of $L_i/K_i(\mu_p)$ with $Ш^{1,\vee}_i := \mathrm{Hom}(Ш^1_i, \mathbb{Z}/p\mathbb{Z})$ and Δ acts on it via the embedding $\Delta \hookrightarrow \mathbb{F}_p^*$. Here is a diagram of the involved extensions:

$$\begin{array}{ccc} & & L_i \\ & & \big|{\scriptstyle Ш^{1,\vee}_i} \\ K_i & \text{---} & K_i(\mu_p) \\ {\scriptstyle H_i}\big| & & \big| \\ K & \underset{\Delta}{\text{---}} & K(\mu_p) \end{array}$$

We have shown the following lemma:

Lemma 5.9. *The composite extension $L_i/K_i(\mu_p)/K$ is Galois. In particular, we have the extension of Galois groups:*

$$1 \to Ш^{1,\vee}_i \to \mathrm{G}_{L_i/K} \to \Delta \times H_i \to 1.$$

The group $\Delta \times H_i$ acts on $Ш_i^{1,\vee}$ as follows: Δ acts by scalars via the canonical embedding $\Delta \hookrightarrow \mathbb{F}_p^*$, and the action of H_i on $Ш_i^{1,\vee}$ is dual to the natural action of H_i on $Ш_i^1$.

Observe that by construction, $L_i/K_i(\mu_p)$ is completely split in $S \smallsetminus T$. Now we investigate the action of H_i more precise. For all $i > 0$, choose compatible sections $\lambda_i \colon H_0 \hookrightarrow H_i$ of the projections $H_i \twoheadrightarrow H_0$ (they exist as $\sharp H_0 = d$ is prime to $[K_i : K_0] = p^i$). Via $\lambda_i \colon H_0 \xrightarrow{\sim} \lambda_i(H_0)$ we identify the character group $H_0^\vee$ of H_0 with that of $\lambda_i(H_0)$. We have a decomposition

$$Ш_i^1 = \bigoplus_{\psi \in H_0^\vee} Ш_i^1(\psi),$$

such that $\lambda_i(H_0)$ acts on $Ш_i^1(\psi)$ by ψ. Observe that the subspace $Ш^i(\psi)$ is again $\Delta \times H_i$-stable, hence the corresponding Kummer subextension $L_i(\psi)/K_i(\mu_p)$ of $L_i/K_i(\mu_p)$ is Galois over K. We denote the Galois group of $L_i(\psi)/K_i$ by $Ш_i^1(\psi)^\vee$. We have $Ш_i^1(\psi)^\vee = \mathrm{Hom}(Ш_i^1(\psi), \mu_p)$ and $\lambda_i(H_0)$ acts on it by ψ^{-1}.

5.5. **Reduction to uniform boundedness.** We reduce equation (5.3) for the tower $\mathscr{L}/K$ defined in Section 5.3 which we have to show, to the following two propositions (which we will prove in Subsections 5.6 and 5.7), both of them bounding $Ш_i^1(\psi)$ in two different cases:

Proposition 5.10. *Let $i \geq 1$ and let $\psi \in H_0^\vee$ be of order $< \mathrm{ord}(\bar{\sigma})$. Then*

$$Ш_i^1(\psi) \subseteq \mathrm{H}^1(K_{S \cup T}/K_0, \mu_p)$$

(both regarded as subgroups of $\mathrm{H}^1(K_{S\cup T}/K_i, \mu_p)$).

Proposition 5.11. *There is a constant $C > 0$ depending only on $M/K, p, \sigma$ (but not on i) such that for all $\psi \in H_0^\vee$ of order $\geq \mathrm{ord}(\bar{\sigma})$ one has*

$$\sharp Ш_i^1(\psi) < C$$

for each $i \geq 1$.

Indeed, to deduce equation (5.3), it is enough to show that for $j \gg i \gg 0$, the map

$$\mathrm{cor}_{ji} \colon Ш_j^1 \to Ш_i^1$$

is the zero map (we denote by cor_{ji} resp. res_{ij} the corestriction resp. the restriction maps between the levels K_i and K_j for $i \leq j$). By compatibility of the chosen sections $\lambda_i \colon H_0 \hookrightarrow H_i$, we have $\mathrm{res}_{ij}(Ш_i^1(\psi)) \subseteq Ш_j^1(\psi)$ for $i \leq j$. Since the restriction maps are injective, we can choose by Proposition 5.11 an $i_0 \geq 0$ such that the inclusion

$$\mathrm{res}_{ij} \colon Ш_i^1(\psi) \hookrightarrow Ш_j^1(\psi)$$

is an isomorphism for all $j \geq i \geq i_0$ and all $\psi \in H_0^\vee$ of order $\geq \mathrm{ord}(\bar{\sigma})$. Then for $j > i \geq i_0$ we have:

$$Ш_j^1 = \bigoplus_{\substack{\psi \in H_0^\vee \\ \mathrm{ord}(\psi) \geq \mathrm{ord}(\bar{\sigma})}} Ш_j^1(\psi) \oplus \bigoplus_{\substack{\psi \in H_0^\vee \\ \mathrm{ord}(\psi) < \mathrm{ord}(\bar{\sigma})}} Ш_j^1(\psi),$$

where the first summand is contained in $\mathrm{res}_{i_0 j}(Ш^1_{i_0})$ and the second summand is contained in $\mathrm{H}^1(K_{S\cup T}/K_0, \mu_p)$ by Proposition 5.10. Thus we conclude that

$$Ш^1_j \subseteq \mathrm{res}_{ij}(\mathrm{H}^1(K_{S\cup T}/K_i, \mu_p)).$$

where both groups are seen as subgroups of $\mathrm{H}^1(K_{S\cup T}/K_j, \mu_p)$. Finally, recall that for L'/L Galois, the composition $\mathrm{cor}_L^{L'} \circ \mathrm{res}^L_{L'}$ is equal to the multiplication by the degree $[L' : L]$, that further p divides $[K_j : K_i]$ for $j > i \geq 0$ and that the group $\mathrm{H}^1(K_{S\cup T}/K_i, \mu_p)$ is killed by p. So, for all i, j with $j > i \geq i_0$ and for any $a \in Ш^1_j$ with preimage $b \in \mathrm{H}^1(K_{S\cup T}/K_i, \mu_p)$ we have

$$\mathrm{cor}_{ji}(a) = \mathrm{cor}_{ji}\,\mathrm{res}_{ij}(b) = 0,$$

i.e., $\mathrm{cor}_{ji} \colon Ш^1_j \to Ш^1_i$ is the zero map. Hence also $\mathrm{cor}^\vee_{ji}$ is the zero map, which shows equation (5.3).

5.6. **Dealing with characters of small order.** Here is the proof of Proposition 5.10: let $K_0^\psi := (K_0)^{\ker(\psi)}$, which is a proper subfield of K_0. Let $H_i^\psi := \mathrm{G}_{K_i/K_0^\psi} = \pi_i^{-1}(\ker(\psi))$, where π_i denotes the projection $H_i \twoheadrightarrow H_0$. Further, $\lambda_i(\ker(\psi))$ acts trivially on $Ш^1_i(\psi)$. With $\lambda_i(\ker(\psi))$ also the normal subgroup $\langle\langle \lambda_i(\ker(\psi))\rangle\rangle$ generated by it in H_i acts trivially on $Ш^1_i(\psi)$. By Lemma 5.12, $\langle\langle \lambda_i(\ker(\psi))\rangle\rangle = H_i^\psi$. Hence:

$$Ш^1_i(\psi) \subseteq \mathrm{H}^1(K_{S\cup T}/K_i, \mu_p)^{H_i^\psi} = \mathrm{H}^1(K_{S\cup T}/K_0^\psi, \mu_p),$$

where the last equality (inside $\mathrm{H}^1(K_{S\cup T}/K_i, \mu_p)$) results from the Hochschild-Serre spectral sequence and the fact that $\mu_p(K_i) = \{1\}$. Finally, Proposition 5.10 follows as $\mathrm{H}^1(K_{S\cup T}/K_0^\psi, \mu_p) \subseteq \mathrm{H}^1(K_{S\cup T}/K_0, \mu_p)$ via restriction.

Lemma 5.12. *We have* $\langle\langle \lambda_i(\ker(\psi))\rangle\rangle = H_i^\psi$.

Proof. We can represent H_i as the follows (recall that $\chi\colon H_0 \to \mathbb{F}_p^*$ is the character defining the action of H_0 on $\ker(H_i \twoheadrightarrow H_0)$; it has order $\geq \mathrm{ord}(\bar\sigma)$):

$$H_i \cong \left\{(a, v) \colon a \in H_0, v \in \mathbb{F}_p^i\right\}, \quad (a, v).(b, w) = (ab, v + \chi(a)w).$$

As $\mathrm{ord}(\chi) \geq \mathrm{ord}(\bar\sigma) > \mathrm{ord}(\psi)$, we have $\ker(\psi) \supsetneq \ker(\chi)$. Let $h \in \ker(\psi) \smallsetminus \ker(\chi)$. Write $\lambda_i(h) = (h, v)$. Then for any $w \in \mathbb{F}_p^i$, the commutator

$$(h, v)^{-1}.(1, w).(h, v).(1, -w) = (1, \chi(h)^{-1}w - w)$$

lies in $\langle\langle \lambda_i(\ker(\psi))\rangle\rangle$. As $1 \neq \chi(h) \in \mathbb{F}_p^*$, we easily see that $\langle\langle \lambda_i(\ker(\psi))\rangle\rangle = H_i^\psi$. □

5.7. **Uniform bounds and generalized densities.** It remains to prove Proposition 5.11. We use the fixed Frobenius densities introduced in preceding sections. All densities are taken over K, so we omit K from the notation and write $\delta_{L,x}$ instead of $\delta_{L/K,x}$ if L/K is finite Galois and $x \in \mathrm{G}_{L/K}$. Let $S_0 := P_{M/K}(\sigma) \cap S$. Then $S_0 \backsimeq P_{M/K}(\sigma)$. For any $i > 0$ and any $x \in H_i$, we consider the element $(\bar\sigma, x) \in \Delta \times H_i = \mathrm{G}_{K_i(\mu_p)/K}$. We apply Corollary 3.5 to $\sigma \in \mathrm{G}_{M/K}$ and $(\bar\sigma, x) \in \Delta \times H_i$: σ and $(\bar\sigma, x)$ lie over the same element $\bar\sigma \in \Delta$ and $M \cap K_i(\mu_p) = K(\mu_p)$. Hence

$$
\begin{aligned}
\delta_{K_i(\mu_p),(\bar\sigma,x)}(S_0) &= \frac{\sharp C((\sigma,x),\mathrm{G}_{MK_i/K})}{[M:K(\mu_p)]\sharp C((\bar\sigma,x),\Delta\times H_i)} \\
&= \frac{\sharp C(\sigma,\mathrm{G}_{M/K})\sharp C(x,H_i)}{[M:K(\mu_p)]\sharp C(\bar\sigma,\Delta)\sharp C(x,H_i)} \qquad (5.5)\\
&= \frac{\sharp C(\sigma,\mathrm{G}_{M/K})}{[M:K(\mu_p)]\sharp C(\bar\sigma,\Delta)}
\end{aligned}
$$

(this computation uses that all involved Galois groups which are a priori fibered products, decompose into simple direct products). Thus we see that for any x, the $(\bar\sigma,x)$-density of S_0 in $K_i(\mu_p)$ remains constant >0 and independent of i and of x. Let $C>0$ be some fixed constant such that

$$\delta_{K_i(\mu_p),(\bar\sigma,x)}(S_0) > C^{-1}. \tag{5.6}$$

Let now $x\in H_0$ be an element such that $\psi(x)=\bar\sigma\in\Delta\subseteq\mathbb{F}_p^*$. This choice is possible since $\mathrm{ord}(\psi)\geq\mathrm{ord}(\bar\sigma)$ and hence $\langle\bar\sigma\rangle\subseteq\psi(H_0)\subseteq\Delta\subseteq\mathbb{F}_p^*$ (being cyclic, $\mathbb{F}_p^*$ has at most one subgroup of each order). Thus the element $y:=(\bar\sigma,\lambda_i(x))\in\Delta\times H_i$ operates on $\text{Ш}_i^1(\psi)^\vee$ trivially. Consider the Galois extensions:

$$
\begin{array}{c}
L_i(\psi)\\
\Big| \, {\scriptstyle \text{Ш}_i^1(\psi)^\vee}\\
K_i(\mu_p)\\
\Big| \, {\scriptstyle \Delta\times H_i}\\
K
\end{array}
$$

We have the following commutative diagram with exact rows:

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & \text{Ш}_i^1(\psi)^\vee & \longrightarrow & \mathrm{G}_{L_i(\psi)/K} & \xrightarrow{\pi} & \Delta\times H_i & \longrightarrow & 1\\
 & & \| & & \uparrow & & \uparrow & & \\
1 & \longrightarrow & \text{Ш}_i^1(\psi)^\vee & \longrightarrow & G_y & \longrightarrow & \langle y\rangle & \longrightarrow & 1,
\end{array}
$$

where G_y is defined to be the pull-back of $\langle y\rangle$ and $\mathrm{G}_{L_i(\psi)/K}$ over $\Delta\times H_i$. Now $\mathrm{ord}(\bar\sigma)|\,\mathrm{ord}(x)=\mathrm{ord}(\lambda_i(x))$. Hence $\mathrm{ord}(y)=\mathrm{lcm}(\mathrm{ord}(\bar\sigma),\mathrm{ord}(x))=\mathrm{ord}(x)$ is coprime to p. The group $\text{Ш}_i^1(\psi)^\vee$ is abelian p-primary, hence the lower sequence in the above diagram splits. Since by construction the action of y on $\text{Ш}_i^1(\psi)^\vee$ is trivial, we have: $G_y\cong\text{Ш}_i^1(\psi)^\vee\times\langle y\rangle$. This shows explicitely that there is precisely one element $\tilde y$ in the preimage of y in G_y (resp. in $\mathrm{G}_{L_i(\psi)/K}$, which is the same) such that $\mathrm{ord}(\tilde y)=\mathrm{ord}(y)$.

As in Section 3, for $z\in\pi^{-1}(y)$, let M_z be the image of $P^z_{L_i(\psi)/K}$ in $P^y_{K_i(\mu_p)/K}$ under the natural projection map. In particular, Proposition 3.2 gives

$$\delta_{K_i(\mu_p),y}(M_{\tilde y}) = \frac{1}{\sharp\text{Ш}_i^1(\psi)^\vee} = \frac{1}{\sharp\text{Ш}_i^1(\psi)} \tag{5.7}$$

as by the above order computations, the $Ш^1_i(\psi)^\vee$-conjugacy class of $\tilde{y}$ in $\pi^{-1}(y)$ contains the only element $\tilde{y}$. The fundamental observation is now the following lemma.

Lemma 5.13. *We have* $P^y_{K_i(\mu_p)/K} \cap \mathrm{cs}(L_i(\psi)/K_i(\mu_p)) \subseteq M_{\tilde{y}}$.

Proof. Let $\mathfrak{p} \in P^y_{K_i(\mu_p)/K} \cap \mathrm{cs}(L_i(\psi)/K_i(\mu_p))$. Then $\mathfrak{p}$ is unramified in $L_i(\psi)/K_i(\mu_p)$ and hence lies in one of the sets M_z for some $z \in \pi^{-1}(y)$. Thus the Frobenius of a lift of $\mathfrak{p}$ to $L_i(\psi)$ is $Ш^1_i(\psi)^\vee$-conjugate to z inside $\pi^{-1}(y)$. But since $\mathfrak{p}$ is completely split in $L_i(\psi)$, we must have $\mathrm{ord}(z) = \mathrm{ord}(y)$, and this can only be satisfied for $z = \tilde{y}$. □

Finally, $S_0 \smallsetminus T \subseteq \mathrm{cs}(L_i(\psi)/K_i(\mu_p))$ by construction and Lemma 5.13 implies

$$(S_0 \smallsetminus T) \cap P^y_{K_i(\mu_p)/K} = (S_0 \smallsetminus T) \cap M_{\tilde{y}}.$$

Together with (5.7) and Corollary 3.4, this gives (since T is finite, we can ignore it in density computations):

$$\begin{aligned} 1 &\geq \delta_{L_i(\psi),\tilde{y}}(S_0) \\ &= \delta_{K_i(\mu_p),y}(M_{\tilde{y}})^{-1}\delta_{K_i(\mu_p),y}(S_0 \cap M_{\tilde{y}}) \\ &= \sharp Ш^1_i(\psi)\delta_{K_i(\mu_p),y}(S_0 \cap P^y_{K_i(\mu_p)/K}) \\ &= \sharp Ш^1_i(\psi)\delta_{K_i(\mu_p),y}(S_0). \end{aligned}$$

Hence by (5.6):

$$\sharp Ш^1_i(\psi) \leq \delta_{K_i(\mu_p),y}(S_0)^{-1} < C.$$

This finishes the proof of Proposition 5.11 and hence of Theorem 1.1.

6. Densities and saturated sets

In this section we discuss an application of "infinitesimal" densties to saturated sets introduced by Wingberg in [7].

6.1. **Saturated sets.** Let us first recall the necessary notions concerning saturated sets and generalized densities. In [8], Wingberg defines a set R of primes of K to be

- *saturated* if $R = \mathrm{cs}(K^R/K)$,
- *stably saturated* if R_L is saturated for any finite subextension $K^R/L/K$, or equivalently, if R is saturated and $(K^R)_\mathfrak{p}/K_\mathfrak{p}$ has infinite degree for any $\mathfrak{p} \notin R$,
- *strongly saturated* if R is saturated and $(K^R)_\mathfrak{p} = \overline{K_\mathfrak{p}}$ for all $\mathfrak{p} \notin R$.

A *saturation* $\hat{R}$ of R is the set $\mathrm{cs}(K^R/K)$. The same definitions can also be made with respect to a rational prime p, e.g., R is saturated with respect to p if $R = \mathrm{cs}(K^R(p)/K)$, etc. In [8], Wingberg discuss properties and give examples of saturated sets. Let us point out some of these properties:

(i) A set R with positive Dirichlet density is saturated if and only if $R = \mathrm{cs}(L/K)$ for some finite extension L of K.

(ii) If $R \neq \Sigma_K$ is stably saturated, then $\delta_K(R) = 0$.
(iii) For any $n > 0$, there is a set R with $\delta_K(R) = 0$ and $\delta_K(\hat{R}) = \frac{1}{n}$ ([8] Remark 3).
(iv) There are sets R such that $\delta_K(\hat{R}) = \delta_K(R) = 0$. Indeed, Wingberg showed that if p is an odd prime, K is a CM-field containg p-roots of unity, with maximal totally real subfield K^+, and $x \in \mathrm{G}_{K/K^+}$ is the non-trivial element, then $P^x_{K/K^+} \cup S_p$ is strongly saturated (for p). This set has Dirichlet density zero but $\delta_{K/K^+,x}(R) = 1$.
(v) Stably saturated sets are arithmetically interesting, because they behave like finite sets with respect to Riemann's existence theorem (cf. [8] Theorem 2).

Below we show the following property of stably saturated sets (Proposition 6.3): if R is stably saturated (resp. stably saturated for p) set of primes in K defined over K_0, and $\delta_{K/K_0,x}(R) = 1$, then $R \supseteq P_{K/K_0}(x)_K \smallsetminus S_p(K)$.

6.2. **The case of x-density one.** In this section we let $L/K/K_0$ be finite Galois extensions of a number field K_0. All x-densities are taken over K_0, so we write $\delta_{K,x}$ instead of $\delta_{K/K_0,x}$.

Proposition 6.1. *Let $x \in \mathrm{G}_{K/K_0}$ and $\pi\colon \mathrm{G}_{L/K_0} \twoheadrightarrow \mathrm{G}_{K/K_0}$ be the natural projection. Then the following holds:*

$$\delta_{K/K_0,x}(\mathrm{cs}(L/K)) = 1 \Rightarrow \forall y \in \pi^{-1}(x)\colon \operatorname{ord}(y) = \operatorname{ord}(x).$$

Proof. Write $R = \mathrm{cs}(L/K)$. Assume $\delta_{K/K_0,x}(R) = 1$ holds and let $y \in \pi^{-1}(x)$ have order $> \operatorname{ord}(x)$. Let M_y denote the image of P^y_{L/K_0} in P^x_{K/K_0} under the natural restriction map. Let $\mathfrak{p} \in M_y$ with some extension $\mathfrak{P} \in P^y_{L/K_0}$ to L. As $\mathrm{Frob}_{\mathfrak{P},L/K_0} = y$ and $\mathrm{Frob}_{\mathfrak{p},K/K_0} = x$, $\mathfrak{P}|\mathfrak{p}$ has nontrivial inertia degree. Hence $\mathfrak{p} \notin R$. Thus we have shown: if $\operatorname{ord}(y) > \operatorname{ord}(x)$, then $M_y \cap R = \emptyset$, i.e., $R \cap P^x_{K/K_0} \subseteq R \cap (P^x_{K/K_0} \smallsetminus M_y)$. This last would imply $\delta_{K,x}(P^x_{K/K_0} \smallsetminus M_y) \geq \delta_{K,x}(R \cap P^x_{K/K_0}) = \delta_{K,x}(R) = 1$. But this would contradict Proposition 3.2, which shows $\delta_{K/K_0,x}(M_y) > 0$. □

Corollary 6.2. *Let $x \in \mathrm{G}_{K/K_0}$ and let R be a set of primes of K, defined over K_0 with $\delta_{K/K_0,x}(R) = 1$. Then any prime $\mathfrak{p} \in P^x_{K/K_0}$ has trivial inertia degree in K^R/K, i.e., $D^{\mathrm{nr}}_{\mathfrak{p},K^R/K} = 1$.*

Proof. Assume $D^{\mathrm{nr}}_{\mathfrak{p},K^R/K} \neq 1$ for some $\mathfrak{p} \in P^x_{K/K_0}$. Since R is defined over K_0, K^R/K_0 is Galois and hence by our assumption there must be a finite subextension $K^R/L/K$ such that L/K_0 is Galois and $D^{\mathrm{nr}}_{\mathfrak{p},L/K} \neq 1$. Choose an extension $\mathfrak{P}$ of $\mathfrak{p}$ to L. We have the commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & D_{\mathfrak{P},L/K} & \longrightarrow & D_{\mathfrak{P},L/K_0} & \longrightarrow & D_{\mathfrak{p},K/K_0} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & D^{\mathrm{nr}}_{\mathfrak{P},L/K} & \longrightarrow & D^{\mathrm{nr}}_{\mathfrak{P},L/K_0} & \longrightarrow & D^{\mathrm{nr}}_{\mathfrak{p},K/K_0} & \longrightarrow & 1
\end{array}$$

The right vertical arrow is an isomorphism, since $\mathfrak{p}$ is unramified in K/K_0. Now, $D^{\mathrm{nr}}_{\mathfrak{p},K/K_0}$ is cyclic, generated by x, and $D^{\mathrm{nr}}_{\mathfrak{P},L/K_0}$ is also cyclic, generated by a preimage y of x and as the left lower entry is non-zero, we have $\mathrm{ord}(y) > \mathrm{ord}(x)$. This contradicts Proposition 6.1. □

Proposition 6.3. *Let p be a prime, K/K_0 a finite Galois extension of nubmer fields and $x \in \mathrm{G}_{K/K_0}$. Let R be a set of primes of K and $R_0 \subseteq R$ the subset defined over K_0. If $\delta_{K/K_0,x}(R_0) = 1$ and R is stably p-saturated, then $R \supseteq P^x_{K/K_0} \smallsetminus S_p$. In particular, if $R = R_0$, then $R \supseteq P_{K/K_0}(x)_K \smallsetminus S_p(K)$.*

Proof. By Corollary 6.2 and the first assumption, for any $\mathfrak{p} \in P^x_{K/K_0} \smallsetminus (R \cup S_p)$, the extension $K^R(p)_{\mathfrak{p}}/K_{\mathfrak{p}}$ is totally ramified. Such extensions, being Galois, must be finite, which contradicts the second assumption. Hence $P^x_{K/K_0} \smallsetminus (R \cup S_p) = \emptyset$ finishing the proof. □

Example 6.4. We give examples of Galois groups $\mathrm{G}_{K^R/K}$ which contain many torsion elements.

(i) *A set R, such that R differs by a finite subset from a set of the form P^x_{k/k_0} and $\mathbb{Z}/p\mathbb{Z} \subseteq \mathrm{G}_{k^R(p)/k}$.* Indeed, let k_0 be a number field, p a rational prime and let k, l_0 be two disjoint $\mathbb{Z}/p\mathbb{Z}$-extensions of k_0, such that there is a prime $\mathfrak{p}_0$ of k_0 which is not p-adic, (totally) ramified in l_0/k_0 and inert in k/k_0. Let $\mathfrak{p}$ be the (unique) lift of $\mathfrak{p}_0$ to k and denote by $1 \neq x \in \mathrm{G}_{k/k_0}$ the Frobenius of $\mathfrak{p}$. We have then $\mathrm{G}_{k/k_0} = \langle x \rangle$, $\mathrm{G}_{kl_0/k_0} = \mathrm{G}_{k/k_0} \times \mathrm{G}_{l_0/k_0}$ and:

$$P_{k/k_0}(x) = \{\mathfrak{q} \in \Sigma_{k_0} \colon \mathrm{Frob}_{\mathfrak{q},k/k_0} = x, \mathfrak{q} \in \mathrm{Ram}(l_0/k_0)\} \cup \bigcup_{g \in \mathrm{G}_{l_0/k_0}} P_{kl_0/k_0}(x, g).$$

In particular, $\mathfrak{p}_0$ lies in the first set on the right side. Observe that since both $k/k_0, l_0/k_0$ are $\mathbb{Z}/p\mathbb{Z}$-extensions, all primes in $P_{kl_0/k_0}(x, g)_k$ for any $g \in \mathrm{G}_{l_0/k_0}$ are completely decomposed in kl_0/k. This means $(P_{kl_0/k_0}(x) \smallsetminus \mathrm{Ram}(l_0/k_0))_k \subseteq \mathrm{cs}(kl_0/k)$. Let $R := (P_{k/k_0}(x) \smallsetminus \mathrm{Ram}(l_0/k_0))_k$. Then $kl_0 \subseteq k^R(p)$ and $D_{\mathfrak{p},k^R(p)/k} \twoheadrightarrow D_{\mathfrak{p},kl_0/k} \cong D_{\mathfrak{p}_0,l_0/k_0} = I_{\mathfrak{p}_0,l_0/k_0} \cong \mathbb{Z}/p\mathbb{Z}$. In particular, $D_{\mathfrak{q},k^R(p)/k}$ is non-trivial. On the other side, we have $\delta_{k/k_0,x}(R) = 1$, hence by Corollary 6.2, $D^{\mathrm{nr}}_{\mathfrak{q},k^R(p)/k} = 1$ and as in the proof of Proposition 6.3, $D_{\mathfrak{p},k^R(p)/k}$ must be finite. This gives us a non-trivial torsion subgroup $\mathbb{Z}/p\mathbb{Z} \subseteq \mathrm{G}_{k^R(p)/k}$.

(ii) Now we make this example even worse and construct *a set R, up to an x-density zero subset equal to P^x_{k/k_0}, such that it contains infinite torsion.* Therefore, let p be a rational prime and k/k_0 a fixed $\mathbb{Z}/p\mathbb{Z}$-extension. Assume that $\mu_p \subseteq k_0$ and $(p, \sharp\mathrm{Cl}(k_0)) = 1$. Let $1 \neq x \in \mathrm{G}_{k/k_0}$ be an element. In the set $P_{k/k_0}(x) \smallsetminus S_p$ choose an infinite subset $T := \{\mathfrak{p}_i\}_{i=0}^{\infty}$ such that $\delta_{k_0}(T) = 0$. As $(p, \sharp\,\mathrm{Cl}(k_0)) = 1$, for each $\mathfrak{p}_i$, there is an element $a_i \in k_0^*$ such that $\mathrm{val}_{\mathfrak{p}_i}(a_i) \equiv 1 \mod p$ for all i and $\mathrm{val}_{\mathfrak{q}}(a_i) \equiv 0 \mod p$ for all $\mathfrak{q} \neq \mathfrak{p}_i$. As $\mu_p \subseteq k_0$, the extension

$$l_i := k_0(a_i^{1/p})/k_0$$

is Galois with Galois group $\mathbb{Z}/p\mathbb{Z}$ and with

$$\{\mathfrak{p}_i\} \subseteq \mathrm{Ram}(l_i/k_0) \subseteq \{\mathfrak{p}_i\} \cup S_p(k_0).$$

Oberve that for any finite $J \subseteq \mathbb{Z}_{>0}$ and $i \in \mathbb{Z}_{>0} \smallsetminus J$, the field extensions $k.\prod_{j\in J} \ell_j$ and ℓ_i are linearly disjoint over k_0 (indeed, ℓ_i/k_0 is totally ramified in $\mathfrak{p}_i$ and $k.\prod_{j\in J}\ell_j/k_0$ is unramified in $\mathfrak{p}_i$). Now make the construction from (i) for each of the l_i and consider $R := P^x_{k/k_0} \smallsetminus (T_k \cup S_p) = (P_{k/k_0}(x) \smallsetminus (T \cup S_p))_k$. Then $R \subseteq \mathrm{cs}(k.\prod_{i=0}^{\infty} l_i/k)$,hence $k.\prod_{i=0}^{\infty}\ell_i \subseteq k^R$. In particular, we have

$$\delta_k(\hat{R}) = \delta_k(R) = 0$$

where $\hat{R}$ is the saturation of R. On the other side, by Corollary 3.4, $\delta_{k,x}(T_k) = 0$, i.e., $\delta_{k,x}(R) = 1$. Hence $\mathrm{G}_{k^R(p)/k} \twoheadrightarrow \prod_{i=0}^{\infty} \mathrm{G}_{l_i/k_0} \cong \prod_{i=0}^{\infty} \mathbb{Z}/p\mathbb{Z}$ and (as in (i)), $D_{\mathfrak{p}_i,k^R(p)/k} \cong \mathbb{Z}/p\mathbb{Z}$ is finite.

Remark 6.5. Observe that the examples of Wingberg (cf. [8] Example 2 after Remark 4) do not show how big $k^R(p)/k$ in the above examples really is, as in our case p divides the order of k/k_0. It would be interesting to know the saturation of R in either of these examples.

Acknowledgements. I want to thank Jakob Stix, Kay Wingberg, Jochen Gärtner and Daniel Harrer for fruitful discussions on this subject, from which I learned a lot. Also I want to thank the hospitality of the HIM center at the University of Bonn, where parts of this work were done and the Technical Univeristy Munich, where the rest was done.

References

[1] Chenevier G., Clozel L.: *Corps de nombres peu ramifiés et formes automorphes autoduales*, J. of the AMS, vol. 22, no. 2, 2009, p. 467-519.

[2] Chenervier G.: *On number fields with given ramification*, Comp. Math. 143 (2007), no. 6, 1359-1373.

[3] Holschbach A., *A Chebotarev-type density theorem for divisors on algebraic varieties*, preprint, arXiv:1006.2340, 2010.

[4] Ivanov A.: *Stable sets of primes in number fields*, 2013, to appear in Algebra & Number Theory J., arXiv:1309.2800.

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

[6] Schmidt A.: *Über Pro-p-Fundamentalgruppen markierter arithmetischer Kurven*, J. reine u. angew. Math. **640** (2010) 203-235.

[7] Wingberg K.: *On Chebotarev sets*, Math. Res. Lett. **13** (2006), no. 2, 179-197.

[8] Wingberg K.: *Sets of completely decomposed primes in extensions of number fields*, preprint, Heidelberg 2013.

E-mail address: ivanov@ma.tum.de

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