UNIFIED TREATMENT OF ARTIN-TYPE PROBLEMS II

OLLI JÄRVINIEMI, ANTONELLA PERUCCA AND PIETRO SGOBBA

ABSTRACT. This work concerns Artin's Conjecture on primitive roots and related problems for number fields. Let K be a number field and let W_1 to W_n be finitely generated subgroups of $K^\times$ of positive rank. We consider the index map, which maps a prime $\mathfrak{p}$ of K to the n-tuple of the indices of $(W_i \bmod \mathfrak{p})$. Conditionally under GRH, any preimage under the index map admits a density, and the aim of this work is describing it. For example, we express the density as a limit in various ways. We study in particular the preimages of sets of n-tuples that are defined by prescribing valuations for their entries. Under some mild assumptions we can express the density as a multiple of a (suitably defined) Artin-type constant.

1. INTRODUCTION

Let K be a number field, and let us work inside a fixed algebraic closure of K. Let $\alpha \in K^\times$ be not a root of unity, and consider the primes $\mathfrak{p}$ of K such that the reduction $(\alpha \bmod \mathfrak{p})$ is well-defined and non-zero, so that we may consider its index $\mathrm{Ind}_\mathfrak{p}(\alpha)$ in the multiplicative group of the residue field at $\mathfrak{p}$. This sets the ground for Artin's Conjecture on primitive roots and related problems: for an extensive account on the conjecture and its generalizations we refer to the survey by Moree [7].

Results on Artin's Conjecture on primitive roots by Hooley [3] and by Cooke and Weinberger [2] (that are conditional on GRH) ensure that the set of primes $\mathfrak{p}$ such that $\mathrm{Ind}_\mathfrak{p}(\alpha) = 1$ has a density, which can be expressed in terms of the degrees of cyclotomic-Kummer extensions:

$$\mathrm{dens}\,\big\{\mathfrak{p} : \mathrm{Ind}_\mathfrak{p}(\alpha) = 1\big\} = \sum_{n\geqslant 1} \frac{\mu(n)}{[K(\zeta_n, \alpha^{1/n}) : K]}\,. \tag{1}$$

More generally, we consider a sequence f_n of positive integers and the formal expression

$$\sum_{n\geqslant 1} \frac{\mu(n)}{[K(\zeta_{f_n}, \alpha^{1/f_n}) : K]}\,. \tag{2}$$

Fixing some positive integer t, Ziegler [11] proved (conditionally under GRH) that the set of primes $\mathfrak{p}$ such that $\mathrm{Ind}_\mathfrak{p}(\alpha) = t$ has a density given by (2) setting $f_n = nt$. Moreover, Lenstra [4] proved (conditionally under GRH) that the set of primes $\mathfrak{p}$ such that $\mathrm{Ind}_\mathfrak{p}(\alpha) \mid t$ has a density given by (2) setting $f_n = n \cdot \prod_{\ell \mid n} \ell^{v_\ell(t)}$.

For $k \geqslant 1$ we say that an integer is *k-free* if it is not divisible by a k-th power greater than 1: square-free is the same as 2-free, and the number 1 is the only 1-free positive integer. As a special case of the results in this paper we have (conditionally on GRH)

$$\mathrm{dens}\,\big\{\mathfrak{p} : \mathrm{Ind}_\mathfrak{p}(\alpha) \text{ is } k\text{-free}\big\} = \sum_{n\geqslant 1} \frac{\mu(n)}{[K(\zeta_{n^k}, \alpha^{1/n^k}) : K]}\,.$$

2020 *Mathematics Subject Classification.* Primary: 11R45; Secondary: 11R20, 12F10.

Key words and phrases. Artin's Conjecture on primitive roots, Kummer theory, multiplicative order, multiplicative index, Galois theory, Chebotarev density theorem.

More generally, we could fix a set $\mathcal{P}'$ of prime numbers and for every $\ell \in \mathcal{P}'$ some positive integer $k(\ell)$: we may then require that the ℓ-adic valuation of $\mathrm{Ind}_{\mathfrak{p}}(\alpha)$ is less than $k(\ell)$. Writing $\mathcal{P}'_\infty$ for the set of positive integers whose prime divisors all lie in $\mathcal{P}'$, under GRH we have

$$\mathrm{dens}\left\{\mathfrak{p} : \ \forall \ell \in \mathcal{P}' \ \ \ell^{k(\ell)} \nmid \mathrm{Ind}_{\mathfrak{p}}(\alpha)\right\} = \sum_{n \in \mathcal{P}'_\infty} \frac{\mu(n)}{[K(\zeta_{f_n}, \alpha^{1/f_n}) : K]}\,,$$

where $f_n = \prod_{\ell \mid n} \ell^{k(\ell)}$. This formula, including the special case of k-free index, is proven in Example 25, where we also express it as the rational multiple of an absolute constant.

As an application, we may derive the special case $K = \mathbb{Q}$, $a \in \mathbb{Q}^\times \setminus \{\pm 1\}$ and $\mathrm{Ind}_p(a)$ being square-free. We write b for the least common multiple of 2 and the primes ℓ such that $v_\ell(a) \neq 0$ or such that $\pm a$ is an ℓ-th power in $\mathbb{Q}^\times$, and we write C_b for the set of automorphisms in $\mathrm{Gal}(\mathbb{Q}(\zeta_{b^2}, a^{1/b^2})/\mathbb{Q})$ which, for all $\ell \mid b$, are not the identity on the field $\mathbb{Q}(\zeta_{\ell^2}, a^{1/\ell^2})$. We obtain the formula

$$\mathrm{dens}\{p : \mathrm{Ind}_p(a) \text{ square-free}\} = \prod_{\ell} \left(1 - \frac{1}{(\ell - 1)\ell^3}\right) \cdot \frac{\# C_b}{[\mathbb{Q}(\zeta_{b^2}, a^{1/b^2}) : \mathbb{Q}]} \prod_{\ell \mid b} \frac{\ell^4 - \ell^3}{\ell^4 - \ell^3 - 1}.$$

Notice that for some conditions on the index (for example, k-free for $k \geqslant 2$) one can get unconditional results because the involved cyclotomic-Kummer extensions contain a 'large' cyclotomic extension (see the method by Pappalardi [9]). Notice that the results stated above for α can be straight-forwardly generalized to the case of a finitely generated subgroup of $K^\times$ of positive rank.

This paper should be seen as the follow-up of [6] by the first two authors. Our results are again conditional under GRH, and we work in the same generality, namely we consider groups $W_1, \ldots, W_n$ that are finitely generated subgroups of $K^\times$ of positive rank. We consider any set $H \subset \mathbb{Z}^n_{>0}$ and the density

$$\mathrm{dens}\left\{\mathfrak{p} : (\mathrm{Ind}_{\mathfrak{p}}(W_1), \ldots, \mathrm{Ind}_{\mathfrak{p}}(W_n)) \in H\right\}, \tag{3}$$

which is known to exist by [6].

We say that H is *cut by valuations* if we have $H = \cap_\ell H_\ell$, where H_ℓ is the preimage under v_ℓ of $v_\ell(H)$: this means that H consists of the integers that have suitable ℓ-adic valuations for every ℓ, the conditions on the various ℓ being independent. Slightly more generally, we allow finitely many valuation conditions not to be independent (we say that the set is *almost cut by valuations*). More generally, we consider a set H which is *determined by valuations*, by which we mean that $H = \cap_Q H_Q$, where $Q > 1$ is square-free and H_Q is the preimage of the Q-adic valuation of H.

Concerning the groups $W_1, \ldots, W_n$, we occasionally require that they are *separated*, which means that for every i the rank of $\langle W_1, \ldots, \cancel{W_i}, \ldots, W_n \rangle$ is strictly smaller than the rank of $\langle W_1, \ldots, W_n \rangle$. This condition plays a role for the Kummer extensions and consequently for the *index map*

$$\mathfrak{p} \mapsto (\mathrm{Ind}_{\mathfrak{p}}(W_1), \ldots, \mathrm{Ind}_{\mathfrak{p}}(W_n))\,,$$

see [6]. Notice that auxiliary results of Kummer theory of independent interest are proven in Section 2.

General results about expressing (3) as a limit (in various ways) are contained in Section 3: Proposition 8 does not require additional assumptions, Theorem 9 only requires the groups to be separated, and Theorem 11 holds for all sets of tuples that are determined by valuations.

Section 4 is devoted to define Artin-type constants that represent heuristical densities. By Proposition 22 such constants are strictly positive if the groups are separated. Then for separated groups and sets which are almost cut by valuations, we can express the density in (3) as a multiple of an Artin-type constant, see Theorem 24 and Corollary 27. Finally, we can also handle correction factors, see Remark 28.

2. CYCLOTOMIC-KUMMER THEORY

Let K be a number field, and let W_1 to W_n be finitely generated subgroups of $K^\times$ of positive rank. We write $I = \{1, \dots, n\}$, and for every $J \subset I$ we write W_J for the smallest subgroup of $K^\times$ containing the groups W_i for all $i \in J$ (we set $W_\emptyset = \{1\}$).

We make use of the letter ℓ only to denote a prime number. Consider an n-tuple $e_I \in \mathbb{Z}^n_{\geqslant 0}$, denoting by e_i its entries and by e its maximum. Calling $W_I^{1/\ell^{e_I}}$ the list $W_1^{1/\ell^{e_1}}, \dots, W_n^{1/\ell^{e_n}}$, we aim to describe the degree

$$[K(\zeta_{\ell^\infty}, W_I^{1/\ell^{e_I}}) : K(\zeta_{\ell^\infty})]\,. \tag{4}$$

Up to reordering the groups, we will suppose that the tuple e_I is *non-increasing*, namely that $e_1 \geqslant \ldots \geqslant e_n$. We also set $e_{n+1} = 0$. Let C be a constant and consider the set of indices I_C consisting of those $i \in I$ such that $e_i - e_{i+1} > C$. For $J \subseteq I$, we call $\delta_J \in \mathbb{Z}^n_{\geqslant 0}$ the n-tuple such that $\delta_i = 1$ for $i \in J$ and $\delta_i = 0$ for $i \notin J$.

Lemma 1. *For every sufficiently large C (larger than a constant depending only on K and $W_1, \dots, W_n$) the following holds: for all ℓ and for all intervals $J = [1, M]$ such that $M \in I_C$, we have*

$$v_\ell\big([K(\zeta_{\ell^\infty}, W_I^{1/\ell^{e_I+\delta_J}}) : K(\zeta_{\ell^\infty}, W_I^{1/\ell^{e_I}})]\big) = \operatorname{rank}(W_J)\,.$$

Proof. We assume w.l.o.g. that W_I is torsion-free because we are working over $K(\zeta_{\ell^\infty})$. We claim that the statement holds by fixing any single prime ℓ with a constant C_ℓ which may be taken 0 for all but finitely many ℓ. Then the statement holds by taking $C := \max_\ell C_\ell$. To prove the claim we fix ℓ, and we let C_ℓ be such that the following holds:

(i) for every $J \subseteq I$, the Kummer degree for W_J has maximal growth from C_ℓ onwards (see [10, Lemma 4.3]), namely we have

$$v_\ell\big([K(\zeta_{\ell^\infty}, W_J^{1/\ell^{C_\ell+x}}) : K(\zeta_{\ell^\infty}, W_J^{1/\ell^{C_\ell}})]\big) = x \operatorname{rank}(W_J)\,;$$

(ii) for every $J, J' \subseteq I$ such that $W_J \cap W_{J'}$ has positive rank,

$$v_\ell([W_J^{1/\infty} \cap W_{J'} : W_J \cap W_{J'}]) \leqslant C_\ell\,,$$

which means that the divisibility of the elements in W_J is bounded with respect to $W_{J'}$ (this is because only the finite torsion part of the quotient $W_{J'}/(W_J \cap W_{J'})$ matters for this divisibility).

Setting $\mathcal{W}_i = W_i^{\ell^{e_1-e_i}}$, we have to prove

$$v_\ell\big([K(\zeta_{\ell^\infty}, \mathcal{W}_J^{1/\ell^{e_1+1}}, \mathcal{W}_{I\setminus J}^{1/\ell^{e_1}}) : K(\zeta_{\ell^\infty}, \mathcal{W}_I^{1/\ell^{e_1}})]\big) = \operatorname{rank}(\mathcal{W}_J)\,.$$

Set $\Gamma = K(\zeta_{\ell^\infty})^{\times \ell^{e_1+1}}$. We have $[\mathcal{W}_J\Gamma : \mathcal{W}_J^\ell\Gamma] = \ell^{\operatorname{rank}(\mathcal{W}_J)}$ by (i) and $\mathcal{W}_J\Gamma \cap \mathcal{W}_{I\setminus J}\Gamma \subseteq \mathcal{W}_J^\ell\Gamma$ by (ii). So we get

$$[\mathcal{W}_J\mathcal{W}_{I\setminus J}^\ell\Gamma : \mathcal{W}_I^\ell\Gamma] = \ell^{\operatorname{rank}(\mathcal{W}_J)}\,.$$

We conclude because, by Kummer theory, we have

$$[K(\zeta_{\ell^\infty}, \mathcal{W}_I^{1/\ell^{e_1}}) : K(\zeta_{\ell^\infty})] = [\mathcal{W}_I^{\ell}\Gamma : \Gamma]$$
$$[K(\zeta_{\ell^\infty}, \mathcal{W}_J^{1/\ell^{e_1+1}}, \mathcal{W}_{I\setminus J}^{1/\ell^{e_1}}) : K(\zeta_{\ell^\infty})] = [\mathcal{W}_J \mathcal{W}_{I\setminus J}^{\ell}\Gamma : \Gamma]\,. \qquad \square$$

Notice that with several applications of the previous Lemma we may reduce the computation of the degree (4) for a general tuple e_I to the analogous degree corresponding to a tuple e_I satisfying $e_i - e_{i+1} \leqslant C$ for every $i = 1, \dots, n$.

We may now compute the degree (4) for any ℓ large enough. Recall that $W_{[1,0]} = \{1\}$.

Lemma 2. *There is a constant c (depending only on K and $W_1, \dots, W_n$) such that for every $\ell \nmid c$ and for every non-increasing $e_I \in \mathbb{Z}^n_{\geqslant 0}$ we have*

$$v_\ell([K(\zeta_{\ell^\infty}, W_I^{1/\ell^{e_I}}) : K(\zeta_{\ell^\infty})]) = \sum_{1\leqslant i\leqslant n} e_i(\operatorname{rank}(W_{[1,i]}) - \operatorname{rank}(W_{[1,i-1]}))\,.$$

Proof. We take c so that for every $\ell \nmid c$ we may take $C_\ell = 0$ in the proof of Lemma 1. It then suffices to apply $e_1 + \dots + e_n$ times Lemma 1. With $e_1 - e_2$ applications, we get the contribution $(e_1 - e_2)(\operatorname{rank}(W_{[1,1]}))$ and we may replace e_1 by e_2. Then with $e_2 - e_3$ applications we get the contribution $(e_2 - e_3)(\operatorname{rank}(W_{[1,2]}))$ and we may replace $e_1 = e_2$ by e_3. Continuing in this way, in n steps we obtain the zero n-tuple, the last contributions being $(e_{n-1} - e_n)(\operatorname{rank}(W_{[1,n-1]}))$ and $e_n(\operatorname{rank}(W_{[1,n]}))$. Collecting the various contributions gives the formula in the statement. $\square$

Fix ℓ and let C_ℓ be as in the proof of Lemma 1. If e_I is a non-increasing tuple and $i \in I_{C_\ell}$, then by Lemma 1 we can relate e_I with the tuple obtained by replacing e_j by $e_j - (e_i - e_{i+1} - C_\ell)$ for every $j \leqslant i$. We can do this procedure for every $i \in I_{C_\ell}$. In the end we obtain a tuple t_I such that $t_i - t_{i+1} = e_i - e_{i+1}$ holds for all $i \notin I_{C_\ell}$ and $t_i - t_{i+1} = C_\ell$ for all $i \in I_{C_\ell}$. By varying e_I, the tuple t_I varies in a finite set, which we call $\mathcal{T}_{C_\ell}$. We also define the function $\mathcal{T} : e_I \mapsto t_I$. The next result describes the degree (4) for all ℓ:

Theorem 3. *We keep the above notation. There exist polynomials $P_{\ell,T}(x_I) \in \mathbb{Z}[x_I]$, $T \in \mathcal{T}_{C_\ell}$ such that the following holds: for every non-increasing $e_I \in \mathbb{Z}^n_{\geqslant 0}$ with $\mathcal{T}(e_I) = T$ we have*

$$P_{\ell,T}(e_I) = v_\ell\big([K(\zeta_{\ell^\infty}, W_I^{1/\ell^{e_I}}) : K(\zeta_{\ell^\infty})]\big)\,.$$

There exist constants $c_{\ell,T}$ such that

$$P_{\ell,T}(x_I) + c_{\ell,T} = \sum_{1\leqslant i\leqslant n} x_i\big(\operatorname{rank}(W_{[1,i]}) - \operatorname{rank}(W_{[1,i-1]})\big)\,.$$

Moreover, for all but finitely many primes ℓ we have $c_{\ell,T} = 0$.

Proof. By Lemma 1 we must have

$$P_{\ell,T}(e_I) - P_{\ell,T}(T) = \sum_{1\leqslant i\leqslant n} (e_i - T_i)\big(\operatorname{rank}(W_{[1,i]}) - \operatorname{rank}(W_{[1,i-1]})\big)\,.$$

So we may set

$$c_{\ell,T} = -v_\ell\big([K(\zeta_{\ell^\infty}, W_I^{1/\ell^{T}}) : K(\zeta_{\ell^\infty})]\big) + \sum_{1\leqslant i\leqslant n} T_i\big(\operatorname{rank}(W_{[1,i]}) - \operatorname{rank}(W_{[1,i-1]})\big)\,.$$

Since in the proof of Lemma 1 we may take $C_\ell = 0$ for all but finitely many ℓ, we deduce the last assertion by Lemma 2. $\square$

Remark 4. In Theorem 3 we have $c_{\ell,T} \geqslant 0$ whenever $\mathrm{rank}(W_I) = \sum_i \mathrm{rank}(W_i)$ because $\mathrm{rank}(W_i) = \mathrm{rank}(W_{[1,i]}) - \mathrm{rank}(W_{[1,i-1]})$ and

$$v_\ell\big([K(\zeta_{\ell^\infty}, W_I^{1/\ell^T}) : K(\zeta_{\ell^\infty})]\big) \leqslant \sum_{1\leqslant i\leqslant n} T_i\big(\mathrm{rank}(W_i)\big)\,.$$

3. LIMITS OF DENSITIES

3.1. **Valuation conditions.** Recall that we denote by ℓ only prime numbers. We consider the *ℓ-adic valuation* as a map $v_\ell : \mathbb{Z}^n_{>0} \to \mathbb{Z}^n_{\geqslant 0}$ and more generally for a square-free integer $Q > 1$ we define the *Q-adic valuation* $v_Q : \mathbb{Z}^n_{>0} \to \prod_{\ell\mid Q} \mathbb{Z}^n_{\geqslant 0}$ as the product of the maps v_ℓ for $\ell \mid Q$. Let $H \subset \mathbb{Z}^n_{>0}$, and write H_Q for the preimage under v_Q of $v_Q(H)$. For every ℓ large enough we have $0_I \in H_\ell$. For all square-free integers $Q, Q_0 > 1$ with $Q_0 \mid Q$ we have

$$H \subset H_Q \subset H_{Q_0} \cap \bigcap_{\ell\mid \frac{Q}{Q_0}} H_\ell \subset \bigcap_{\ell\mid Q} H_\ell\,. \tag{5}$$

Definition 5. We say that H is *cut by valuations* if $H = \cap_\ell H_\ell$. We say that H is *almost cut by valuations* if there is some square-free integer $Q_0 > 1$ such that

$$H = H_{Q_0} \cap \bigcap_{\ell\nmid Q_0} H_\ell\,.$$

We say that H is *determined by valuations* if $H = \cap_Q H_Q$ by varying $Q > 1$ square-free.

By (5) a set which is cut by valuations is almost cut by valuations, and a set which is almost cut by valuations is determined by valuations.

Example 6. The set of positive square-free integers is cut by valuations. The set of positive integers with an even number of prime divisors is not determined by valuations because we have $H_Q = \mathbb{Z}$ for every $Q > 1$. A finite set or, more generally, a set with finite support (the set of prime divisors of the entries is finite), is not necessarily cut by valuations, but it is almost cut by valuations. An example of set that is determined by valuations but is not almost cut by valuations is the set of prime numbers together with 1.

3.2. **Notation.** We keep the notation of [6]. In particular, ℓ is a prime number and $Q \geqslant 1$ is square-free. For $h_I \in \mathbb{Z}^n_{>0}$ we write $h := \mathrm{lcm}(h_1, \dots, h_n)$. Moreover, $h_{Q,I}$ is the n-tuple obtained by removing from the terms of h_I the prime factors coprime to Q, and we write $h_Q := \mathrm{lcm}(h_{Q,1}, \dots, h_{Q,n})$.

We fix some finite Galois extension F/K and a union of conjugacy classes $C \subset \mathrm{Gal}(F/K)$. We write

$$K_{Q^\infty, Q_I^\infty} = \bigcup_{e\geqslant 1} K(\zeta_{Q^e}, W_I^{1/Q^e})\,.$$

For $H \subset \mathbb{Z}^n_{>0}$ we define

$$C_{H,Q} := \bigcup_{h_I\in H} C_{h_{Q,I}} = \dot{\bigcup_{h_{Q,I}}} C_{h_{Q,I}} \subset \mathrm{Gal}(FK_{Q^\infty,Q_I^\infty}/K)\,, \tag{6}$$

where $\dot\cup$ denotes a disjoint union and $C_{h_{Q,I}}$ is the conjugacy-stable set of those automorphisms σ that satisfy all of the following conditions:

- the restriction of σ to F lies in C;

- the restriction of σ to $K(\zeta_{h_Q}, W_I^{1/h_{Q,I}})$ is the identity;
- for all $q \mid Q$ and for all $i \in I$ the restriction of σ to $K(\zeta_{qh_{Q,i}}, W_i^{1/qh_{Q,i}})$ is not the identity.

Consider the Haar measure μ_{Haar} on $\text{Gal}(FK_{Q^\infty,Q_I^\infty}/K)$. The set $C_{h_{Q,I}}$ (respectively, $C_{H,Q}$) is measurable and it has measure 0 if and only if it is empty. Moreover, we have

$$\mu_{\text{Haar}}(C_{H,Q}) = \sum_{h_{Q,I}} \mu_{\text{Haar}}(C_{h_{Q,I}})\,. \tag{7}$$

Finally, if $\mathfrak{p}$ is a prime of K unramified in F, then $\left(\frac{\mathfrak{p}}{F/K}\right)$ is the conjugacy class of the Frobenius elements at the primes of F above $\mathfrak{p}$.

3.3. **Results.** Consider the primes $\mathfrak{p}$ of K unramified in F for which the index map

$$\Psi : \mathfrak{p} \to (\text{Ind}_{\mathfrak{p}}(W_1), \ldots, \text{Ind}_{\mathfrak{p}}(W_n)) \tag{8}$$

is well-defined. Let the set $S_{C,H}$ consist of those $\mathfrak{p}$ such that $\left(\frac{\mathfrak{p}}{F/K}\right) \subset C$ and $\Psi(\mathfrak{p}) \in H$. Notice that we have

$$\mu_{\text{Haar}}(C_{H,Q}) = \text{dens}(S_{C,H_Q}). \tag{9}$$

Theorem 7 ([6, Remark 4.2])**.** *Assume GRH. The set $S_{C,H}$ admits a natural density, and we have*

$$\text{dens}(S_{C,H}) = \sum_{h_I \in H} \text{dens}(S_{C,\{h_I\}})\,. \tag{10}$$

Moreover, we have $\text{dens}(S_{C,H}) = 0$ *if and only if* $S_{C,H} = \emptyset$.

The sum in the above statement might have infinitely many terms. Formally, it is defined as a limit for $x \to \infty$ of sums over the n-tuples $h_I \in H$ with entries bounded from above by x. In the statements below the limit for $Q \to \infty$ is the limit $x \to \infty$ for $Q_x := \prod_{\ell \leqslant x} \ell$, while the limits $Q, B \to \infty$ and $Q, k \to \infty$ can be seen as double limits (where the order of the limits does not matter) but also as a single limit, for example $\min(Q, B) \to \infty$.

Proposition 8. *Assume GRH. We have*

$$\text{dens}(S_{C,H}) = \lim_{B \to \infty} \text{dens}(S_{C,H \cap [1,B]^n})\,. \tag{11}$$

If Q is a positive square-free number, calling Q^∞ the subset of $\mathbb{Z}^n_{>0}$ consisting of the n-tuples such that the prime divisors of each of the entries divide Q, we have

$$\text{dens}(S_{C,H}) = \lim_{Q \to \infty} \text{dens}(S_{C,H \cap Q^\infty}) \tag{12}$$

and

$$\text{dens}(S_{C,H}) = \lim_{Q,B \to \infty} \text{dens}(S_{C,H \cap Q^\infty \cap [1,B]^n})\,. \tag{13}$$

Calling $\mathbb{Z}^n_{k\text{-free}}$ the tuples consisting of k-free integers, we also have

$$\text{dens}(S_{C,H}) = \lim_{k \to \infty} \text{dens}(S_{C,H \cap \mathbb{Z}^n_{k\text{-free}}})\,, \tag{14}$$

and

$$\text{dens}(S_{C,H}) = \lim_{Q,k \to \infty} \text{dens}(S_{C,H \cap Q^\infty \cap \mathbb{Z}^n_{k\text{-free}}})\,. \tag{15}$$

Proof. By Theorem 7 all densities exist. Since $[1,B]^n \subset [1,B']^n$ for $B \leqslant B'$, the limit in (11) exists and the inequality $\geqslant$ holds. Thus to prove (11) it suffices to show that the density of the set $\{\mathfrak{p} : \Psi(\mathfrak{p}) \notin [1,B]^n\}$ goes to 0 for $B \to \infty$. This set is contained in the finite union of the sets $\{\mathfrak{p} : \mathrm{Ind}_{\mathfrak{p}}(W_i) > B\}$ for $i = 1, \dots, n$ and we conclude because

$$\sum_{t \geqslant 1} \mathrm{dens}\,\{\mathfrak{p} : \mathrm{Ind}_{\mathfrak{p}}(W_i) = t\} = 1 < \infty\,.$$

Equalities (12) and (14) similarly follow from the identities $H = \bigcup_Q (H \cap Q^\infty)$ and $H = \bigcup_Q (H \cap \mathbb{Z}^n_{k\text{-free}})$, respectively. For (13) consider that $[1,B]^n \subset Q^\infty$ holds for some suitable Q (namely, the square-free part of $B!$). Finally, we can deduce (15) from (13) because $[1,B]^n \subset \mathbb{Z}^n_{k\text{-free}}$ holds for some suitable k (namely, 1 plus the largest valuation of the numbers in $[1,B]$). Notice that we could also deduce (14) from (15) by expressing the double limit as an iterated limit, as all limits are convergent. □

Theorem 9. *Assume GRH, and suppose that the groups W_i are separated. Then the following are equivalent:*

(i) $\mathrm{dens}(S_{C,H}) > 0$*;*
(ii) $C_{H,Q} \neq \emptyset$ *holds for every square-free integer* $Q > 1$*;*
(iii) $C_{H,Q_x} \neq \emptyset$ *holds for some sufficiently large integer x (which is computable and depends on K and $W_1, \dots, W_n$ but it does not depend on H).*

Proof. The implications (i)⇒(ii)⇒(iii) are clear. The implication (iii)⇒(i) holds for a singleton by [6, Theorem 4.1]. In general, since the groups are separated, it suffices to investigate the images of finitely many singletons by [6, Theorem 6.2 (iii)]. □

The conditions in the above theorem are clearly necessary to have $\mathrm{dens}(S_{C,H}) > 0$. They are also sufficient if H is a singleton by [6] but in general they are not: the following example can be generalized to any groups that are not separated, and it shows that we cannot have in general (ii)⇒(i).

Example 10. Consider $n = 2$, $K = F = \mathbb{Q}$, $W_1 = W_2 = \langle 2 \rangle$ and $H = \{(q, q^2) |\, q \text{ prime}\}$. Clearly $S_{C,H} = \emptyset$. However, for every Q the zero tuple is in $v_Q(H)$, hence $C_{H,Q} \neq \emptyset$ (by considering only v_Q we are not excluding those primes p such that $2 \bmod p$ is a primitive root).

Theorem 11. *Assume GRH and suppose that H is determined by valuations. Then we have*

$$\mathrm{dens}(S_{C,H}) = \lim_{Q \to \infty} \mu_{\mathrm{Haar}}(C_{H,Q}) \tag{16}$$

and

$$\mathrm{dens}(S_{C,H}) = \lim_{Q \to \infty} \mathrm{dens}\left\{\mathfrak{p} : \Psi(\mathfrak{p}) \in H_Q,\ \left(\frac{\mathfrak{p}}{F/K}\right) \subset C\right\}. \tag{17}$$

Proof. Formula (16) is a consequence of (17). To prove (17) it suffices to show that the density of the set $\{\mathfrak{p} : \Psi(\mathfrak{p}) \in H_Q \setminus H\}$ goes to 0 for $Q \to \infty$. Call $H' = \mathbb{Z}^n_{>0} \setminus H$. Then, since H is determined by valuations, we have $H' = \bigcup_Q (\mathbb{Z}^n_{>0} \setminus H_Q)$. Thus, to every $t_I \in H'$ we can associate the least positive integer z such that $t_I \notin H_{Q_x}$ whenever $x \geqslant z$. This function provides a partition of H' into sets H'_z. Moreover, by Theorem 7 we have

$$\mathrm{dens}(\Psi^{-1}(H')) = \sum_{z \geqslant 1} \mathrm{dens}(\Psi^{-1}(H'_z))\,.$$

As this series converges, we conclude because the complement of H_{Q_x} is contained in $\cup_{z\geqslant x} H'_z$. □

In the following statement we let Q_0 be as in Definition 5 (notice that in the limit we could restrict to those $\ell \mid Q$ such that $\ell \nmid Q_0$).

Corollary 12. *Assume GRH and suppose that H is almost cut by valuations. Then we have*

$$\operatorname{dens}(S_{C,H}) = \lim_{Q\to\infty} \operatorname{dens}\left\{\mathfrak{p} : \Psi(\mathfrak{p}) \in H_{Q_0} \cap \bigcap_{\ell \mid Q} H_\ell,\ \left(\frac{\mathfrak{p}}{F/K}\right) \subset C\right\}.$$

If H is cut by valuations, then we have

$$\operatorname{dens}(S_{C,H}) = \lim_{Q\to\infty} \operatorname{dens}\left\{\mathfrak{p} : \Psi(\mathfrak{p}) \in \bigcap_{\ell \mid Q} H_\ell,\ \left(\frac{\mathfrak{p}}{F/K}\right) \subset C\right\}.$$

Proof. This is a consequence of Theorem 11 by writing H_Q suitably. □

Example 13. We cannot expect Theorem 11 to hold for all sets H. For example, let $n = 1$, consider a trivial Frobenius condition, and let H be the set of prime numbers. Then $\cap_\ell H_\ell$ is the set of all positive square-free integers and we have $1 \in \cap_Q H_Q$. So by considering $\cap_\ell H_\ell$ or $\cap_Q H_Q$ we may obtain a strictly larger density (provided that there is a positive density of primes $\mathfrak{p}$ such that $\operatorname{Ind}_\mathfrak{p}(W_1) = 1$).

Remark 14. One may also consider the map $\mathfrak{p} \mapsto \operatorname{Ind}_\mathfrak{p}(W)$ where W is a torsion subgroup of $K^\times$. If the order of W is $t \geq 1$, then we consider those primes $\mathfrak{p}$ that do not divide t. We have $\operatorname{Ind}_\mathfrak{p}(W) = (\mathrm{N}\,\mathfrak{p} - 1)/t$, and in particular the index map has finite preimages. However, given a prime number ℓ, we may study for example the condition $v_\ell(\operatorname{Ind}_\mathfrak{p}(W)) = x$, which is equivalent to saying that $\mathfrak{p}$ splits completely in $K(\zeta_{t\ell^x})$ and not in $K(\zeta_{t\ell^{x+1}})$. Then the density of primes satisfying this condition can be obtained by applying the Chebotarev density theorem, and for all but finitely many ℓ it is given by $1/\varphi(\ell^x) - 1/\varphi(\ell^{x+1})$.

4. ARTIN-TYPE CONSTANTS

To study the density of the preimage of a set $H \subset \mathbb{Z}^n_{>0}$ under the index map (8), we define an Artin-type constant, whose value depends on H and on the ranks of the groups W_J, $J \subset I$.

For every $i \in I$, let $r_i := \operatorname{rank}(W_i)$. Also let $\mathcal{R}$ be the tuple of integers $R_J := \operatorname{rank}(W_J)$, $J \subset I$. By assuming that all W_i have positive rank, the following holds: $\mathcal{R}$ is a 2^n-tuple of integers satisfying $R_\emptyset = 0$ and $R_{J'} \geqslant R_J > 0$ whenever $J' \supset J \neq \emptyset$. If the groups are separated, then we have the strict inequality $R_{J'} > R_J$ if J' strictly contains J. If the groups are multiplicatively independent, then for every J we have $R_J = \sum_{j\in J} r_j$, and we write r_I instead of $\mathcal{R}$.

We define the *inclusion–exclusion function* on a tuple of real numbers x_I as follows (for the empty tuple we have $\mathcal{IE}(x_I) = 1$):

$$\mathcal{IE}(x_I) := \sum_{J\subset I} (-1)^{\#J} \prod_{j\in J} x_j = \prod_{i\in I} (1 - x_i).$$

Notice that, setting $x_i = \frac{1}{d_i}$, by the Chebotarev density theorem the function $\mathcal{IE}$ provides the density of the primes of a number field that do not split completely in any of finitely many linearly disjoint Galois extensions of the number field having degree d_i.

For any ℓ we let $V_\ell \subset \mathbb{Z}^n_{\geqslant 0}$, and we write $V := (V_\ell)_\ell$. Given H, we may set $V_\ell := v_\ell(H)$ and moreover, every V such that $0_I \in V_\ell$ holds for every $\ell \gg 1$ can be obtained in this way. We define an Artin-type constant

$$A_{V,\mathcal{R}} := \prod_\ell A_{V_\ell,\mathcal{R}}(\ell)$$

as an infinite product (which converges) of suitably defined real numbers in $[0,1]$. In turn, we define

$$A_{V_\ell,\mathcal{R}}(\ell) := \sum_{v_I \in V_\ell} F_{v_I,\mathcal{R}}(\ell)$$

as a series (which converges) of suitably defined real numbers in $[0,1]$. The numbers $F_{v_I,\mathcal{R}}(\ell)$ are the evaluation at ℓ of a rational function $F_{v_I,\mathcal{R}}(x)$ with integer coefficients, corresponding to a heuristical density of the primes $\mathfrak{p}$ satisfying $v_\ell(\mathrm{Ind}_\mathfrak{p}(W_i)) = v_i$ for all $i \in I$.

Let us define these heuristical densities $F_{v_I,\mathcal{R}}$. We first note that the event $v_\ell(\mathrm{Ind}_\mathfrak{p}(W)) \geqslant 1$ ought to happen with probability $\ell^{-\mathrm{rank}(W)}$ assuming that $\mathfrak{p}$ splits completely in $K(\zeta_\ell)$. This leads to the following formula in the simple case of the zero n-tuple 0_I.

Definition 15. For the zero n-tuple, we define

$$F_{0_I,\mathcal{R}}(\ell) := \frac{\ell-2}{\ell-1} + \frac{1}{\ell-1}\sum_{J\subset I}\frac{(-1)^{\#J}}{\ell^{R_J}} = 1 + \frac{1}{\ell-1}\sum_{\emptyset\neq J\subset I}\frac{(-1)^{\#J}}{\ell^{R_J}}\,.$$

Now consider an n-tuple $v_I \neq 0_I$. There is a permutation σ such that the tuple $(v_{\sigma_1}, \dots, v_{\sigma_n})$ is non-increasing, that is we have $v_{\sigma_1} \geqslant \cdots \geqslant v_{\sigma_n}$. Then we define a function $f : \mathbb{Z}^n_{\geqslant 0} \to \mathbb{Z}$ by setting

$$f(v_I) = \sum_{i=1}^n v_{\sigma_i}\left(R_{\{\sigma_1,\dots,\sigma_i\}} - R_{\{\sigma_1,\dots,\sigma_{i-1}\}}\right).$$

Notice that the choice of σ does not affect the value of f at v_I (to see this it suffices to make swaps of neighboring indices σ_i, σ_{i+1} such that $v_{\sigma_i} = v_{\sigma_{i+1}}$). Setting $v = \max(v_I)$, by Theorem 3 the value $f(v_I)$ represents the theoretical value of the degree $[K(\zeta_{\ell^v}, W_I^{1/\ell^{v_I}}) : K(\zeta_{\ell^v})]$. Indeed, in the theoretical case, in Theorem 3 we may take $C = 0$ and $c_{\ell,T} = 0$, and we may work over $K(\zeta_{\ell^v})$.

Definition 16. Given $v_I \neq 0_I$, we set $I' := \{i \in I : v_i = v\}$. We define

$$F_{v_I,\mathcal{R}}(\ell) := \frac{1}{\varphi(\ell^v)\ell^{f(v_I)}}\left(\frac{\ell-1}{\ell}\sum_{\substack{J\subset I\\ J\cap I'=\emptyset}}\frac{(-1)^{\#J}}{\ell^{f(v_I+\delta_J)-f(v_I)}} + \frac{1}{\ell}\sum_{J\subset I}\frac{(-1)^{\#J}}{\ell^{f(v_I+\delta_J)-f(v_I)}}\right). \tag{18}$$

Let us motivate this definition. First, the factor $1/\varphi(\ell^v)$ expresses the theoretical density of the primes $\mathfrak{p}$ of K splitting completely in $K(\zeta_{\ell^v})$. The factor $1/\ell^{f(v_I)}$ is obtained by requiring additionally that $\mathfrak{p}$ splits completely in $K(\zeta_{\ell^v}, W_I^{1/\ell^{v_I}})$. Conditionally on $\mathfrak{p}$ splitting completely in

$$K(\zeta_{\ell^v}, W_{\sigma_1}^{1/\ell^{v_{\sigma_1}}}, \dots, W_{\sigma_{i-1}}^{1/\ell^{v_{\sigma_{i-1}}}}),$$

there is a density of

$$\ell^{-v_{\sigma_i}(R_{\{\sigma_1,\dots,\sigma_i\}} - R_{\{\sigma_1,\dots,\sigma_{i-1}\}})}$$

that $\mathfrak{p}$ splits completely in

$$K(\zeta_{\ell^v}, W_{\sigma_1}^{1/\ell^{v_{\sigma_1}}}, \dots, W_{\sigma_i}^{1/\ell^{v_{\sigma_i}}})$$

as well. We then consider the density of the primes $\mathfrak{p}$ that do not split completely in any of the extensions $K(\zeta_{\ell^{v_i+1}}, W_i^{1/\ell^{v_i+1}})$, considering separately two cases depending on whether $\mathfrak{p}$ splits completely in $K(\zeta_{\ell^{v+1}})$. The first sum in (18) corresponds to the case where it does not, while the second sum corresponds to the case where it does, the formulas being obtained by inclusion–exclusion and reasoning as above.

While it is not obvious from (18), the values $F_{v_I,\mathcal{R}}(\ell)$ are non-negative and under a separatedness condition strictly positive, see Proposition 22. Formula (18) may also be rewritten as

$$F_{v_I,\mathcal{R}}(\ell) = \frac{1}{\ell^v}\Bigg(\sum_{\substack{J\subset I\\ J\cap I'=\emptyset}} \frac{(-1)^{\#J}}{\ell^{f(v_I+\delta_J)}} + \frac{1}{\ell-1}\sum_{J\subset I} \frac{(-1)^{\#J}}{\ell^{f(v_I+\delta_J)}}\Bigg). \tag{19}$$

Example 17. For $n = 1$ (setting $r = r_1$) we have

$$F_{v,r}(\ell) = \begin{cases} 1 - \frac{1}{\ell^r(\ell-1)} & \text{for } v = 0\\ \frac{1}{\ell^{v(r+1)}} \cdot \frac{\ell}{(\ell-1)}(1 - \frac{1}{\ell^{r+1}}) & \text{for } v > 0\,. \end{cases}$$

Example 18. For a constant n-tuple $v_I \neq 0_I$ we have

$$F_{v_I,\mathcal{R}}(\ell) = \frac{1}{\ell^{v(1+R_I)}} \cdot \Big(1 + \frac{1}{\ell-1}\sum_{J\subset I}\frac{(-1)^{\#J}}{\ell^{R_J}}\Big)$$

because we can write $f(v_I + \delta_J) = vR_I + R_J$.

Example 19. For $n = 2$, supposing that $R_I = r_1 + r_2$, we have

$$F_{v_I,r_I}(\ell) = \begin{cases} 1 + \frac{1}{\ell-1}(\mathcal{IE}(\ell^{-r_1},\ell^{-r_2}) - 1) & \text{for } v_1 = v_2 = 0\\ \frac{1}{\ell^{v(1+r_1+r_2)}} \cdot \frac{\ell}{\ell-1} \cdot \big(1 + \frac{1}{\ell} \cdot (\mathcal{IE}(\ell^{-r_1},\ell^{-r_2}) - 1)\big) & \text{for } v_1 = v_2 > 0\\ \frac{1}{\ell^{v+v_1r_1+v_2r_2}} \cdot \frac{\ell}{\ell-1} \cdot \mathcal{IE}(\ell^{-r_m},\ell^{-(r_M+1)}) & \text{for } v_1 \neq v_2 \end{cases}$$

where $I = \{m, M\}$ is such that $v_M = v$.

Example 20. Suppose that for every J we have $R_J = \sum_{j\in J} r_j$. Then we have

$$F_{0_I,r_I}(\ell) = \frac{\ell-2}{\ell-1} + \frac{1}{\ell-1}\mathcal{IE}(\ell^{-r_I})\,.$$

For $v_I \neq 0$ we have

$$\begin{aligned} F_{v_I,r_I}(\ell) &= \frac{1}{\ell^{v+\sum_i v_ir_i}} \cdot \Big(\mathcal{IE}(\ell^{-r_{I\setminus I'}}) + \frac{1}{\ell-1}\mathcal{IE}(\ell^{-r_I})\Big)\\ &= \frac{1}{\ell^{v+\sum_i v_ir_i}} \cdot \frac{\ell}{\ell-1} \cdot \mathcal{IE}(\ell^{-r_{I\setminus I'}}) \cdot \Big(1 + \frac{1}{\ell} \cdot (\mathcal{IE}(\ell^{-r_{I'}}) - 1)\Big) \end{aligned}$$

because we can write $f(v_I + \delta_J) - \sum_{i\in I} v_ir_i = \sum_{i\in J} r_i$.

Next, we prove that the heuristics for (18) to be the density of the preimage is rigorous for all but finitely many primes ℓ. Moreover, for all ℓ such that $\zeta_\ell \notin K$ we may suppose that the involved subgroups of $K^\times$ are torsion-free.

Corollary 21. *There exists a constant c such that for every $\ell \nmid c$ the preimage of v_I under $v_\ell \circ \Psi$ has density $F_{v_I,\mathcal{R}}(\ell)$.*

Proof. Let c be the integer of Lemma 2, and we also suppose that c is a multiple of the primes ℓ such that $K \cap \mathbb{Q}(\zeta_\ell) \neq \mathbb{Q}$. Fix $\ell \nmid c$. The condition $v_\ell(\mathrm{Ind}_{\mathfrak{p}}(W_i)) = v_i$ for all i is equivalent to $\mathfrak{p}$ splitting completely in $K(\zeta_{\ell^v}, W_I^{1/\ell^{v_I}})$ and not in $K(\zeta_{\ell^{v_i+1}}, W_i^{1/\ell^{v_i+1}})$ for all i. Hence, setting $m_J := \max(v_I + \delta_J)$, by inclusion–exclusion the density of these primes equals

$$\sum_{J \subseteq I} \frac{(-1)^{\#J}}{[K(\zeta_{\ell^{m_J}}, W_I^{1/\ell^{v_I+\delta_J}}) : K]}. \tag{20}$$

For $v_I = 0_I$, the involved degrees have maximal value by the proof of Lemma 1, because for $\ell \nmid c$ we may take $C_\ell = 0$ and for $J \neq \emptyset$ we may work over $K(\zeta_\ell)$. Hence, we obtain

$$1 + \frac{1}{\ell - 1} \sum_{\emptyset \neq J \subset I} \frac{(-1)^{\#J}}{\ell^{R_J}},$$

which equals $F_{0_I,\mathcal{R}}(\ell)$, as defined in Definition 16. Let $v_I \neq 0_I$. By Theorem 3, since for $\ell \nmid c$ we may work over $K(\zeta_{\ell^{m_J}})$ and $c_{\ell,T} = 0$, we have

$$\left[K(\zeta_{\ell^{m_J}}, W_I^{1/\ell^{v_I+\delta_J}}) : K\right] = \varphi(\ell^{m_J}) \ell^{f(v_I+\delta_J)}.$$

Replacing the value of the degree in (20) and distinguishing the cases for $J \cap I'$ being empty or not yields the value $F_{v_I,\mathcal{R}}(\ell)$ as expressed in (19). □

Corollary 21 holds unconditionally (without GRH) because we work inside the finite extension $K(\zeta_{\ell^{v+1}}, W_I^{1/\ell^{v_I+\delta_I}})/K$, so that one needs to apply the Chebotarev density theorem only finitely many times. Finally, we note that if the groups $W_1, \dots, W_n$ are separated, then $F_{v_I,\mathcal{R}}(\ell)$ is indeed strictly positive, as is the resulting Artin-type constant $A_{V,\mathcal{R}}$.

Proposition 22. *Suppose that $W_1, \dots, W_n$ are separated. Then for every ℓ and for every $v_I \in \mathbb{Z}_{\geqslant 0}^n$ we have $F_{v_I,\mathcal{R}}(\ell) > 0$. Moreover, if $0_I \in V_\ell$ holds for $\ell \gg 1$, then the Artin-type constant $A_{V,\mathcal{R}}$ is strictly positive.*

Proof. The second claim follows from the first because for $\ell \gg 1$, supposing w.l.o.g. that $V_\ell = \{0_I\}$ holds, we have

$$F_{0_I,\mathcal{R}}(\ell) \geqslant 1 - \frac{1}{\ell - 1} \sum_{\emptyset \neq J \subset I} \frac{1}{\ell} > 1 - \frac{2^n}{\ell^2 - \ell} > 1 - \frac{1}{\ell^{3/2}}\,.$$

The product over ℓ of the terms $1 - 1/\ell^{3/2}$ is shown to be strictly positive by first taking logarithms and then proving that the obtained series is finite by means of Taylor approximation.

The claim on the positivity of $F_{v_I,\mathcal{R}}(\ell)$ is proven via a probabilistic interpretation. Note that the value of $F_{v_I,\mathcal{R}}(\ell)$ only depends on W_I through the tuple $\mathcal{R}$ of ranks. Hence we may reduce to the torsion-free case: if G is the torsion group of W_I, we may replace W_i by $W_i \cdot G/G$ without affecting the ranks of the product groups.

For $1 \leqslant i \leqslant n$, let $b_{i,1}, \dots, b_{i,r_i}$ be a basis for W_i and let B denote the multiset $\{b_{i,j} | 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant r_i\}$. Associate to each $b_{i,j}$ a random variable $X_{i,j}$, for which

$$P(X_{i,j} = k) = \frac{1}{\ell^k} - \frac{1}{\ell^{k+1}} \text{ for } 0 \leqslant k < v+1, \quad P(X_{i,j} = v+1) = \frac{1}{\ell^{v+1}},$$

with the random variables $X_{i,j}$ independent of each other. Introduce a further random variable X_ζ with

$$P(X_\zeta = k) = \frac{1}{\varphi(\ell^k)} - \frac{1}{\varphi(\ell^{k+1})} \text{ for } 0 \leqslant k < v+1, \quad P(X_\zeta = v+1) = \frac{1}{\varphi(\ell^{v+1})},$$

with $X_{i,j}$ and X_ζ all independent of each other. (Intuitively, X_ζ and $X_{i,j}$ correspond to the largest k such that a random prime $\mathfrak{p}$ splits completely in $K(\zeta_{\ell^k})$ or $K(\zeta_{\ell^k}, b_{i,j}^{1/\ell^k})$.)

For each subset $B' \subset B$ and $b_{i,j} \in B \setminus B'$ for which we have $b_{i,j} \in \langle B' \rangle^{1/\infty}$, we consider the condition

$$X_{i,j} \geq \min_{b_{i',j'} \in B'} X_{i',j'} \tag{21}$$

on our random variables. Let E denote the event corresponding to all of such conditions holding. Note that $P(E) \geqslant P(X_{i,j} = v+1 \text{ for all } i,j) > 0$ hence, we may condition on E. (The event E accounts for the fact that the groups W_i and fields $K(\zeta_{\ell^k}, W_i^{1/\ell^k})$ may interact with each other.)

Consider then the conditional probability

$$P(\text{for all } i \in [1,n], \min(X_{i,1}, \ldots, X_{i,r_i}, X_\zeta) = v_i | E).$$

The probabilistic motivation given for (18) shows that this probability equals $F_{v_I,\mathcal{R}}(\ell)$. This already proves that $F_{v_I,\mathcal{R}}(\ell)$ is non-negative. For strict positivity, note that by the assumption on the separatedness of $W_1, \ldots, W_n$, there are $t_1, \ldots, t_n$ such that the basis elements b_{i,t_i} are multiplicatively independent with $B \setminus \{b_{i,t_i}\}$. It follows that for any condition of the type (21), X_{i,t_i} only arises on the right hand side, and furthermore for any such condition there exists a corresponding condition with b_{i,t_i} removed from B'. Hence there are effectively no conditions on the variables X_{i,t_i}, and thus

$$\begin{aligned}&P(\text{for all } i \in [1,n], \min(X_{i,1}, \ldots, X_{i,r_i}, X_\zeta) = v_i | E) \geqslant \\ &P(X_\zeta = v+1 \text{ and for all } i \in [1,n], X_{i,t_i} = v_i \text{ and for all } j \neq t_i, X_{i,j} = v+1 | E) > 0.\end{aligned}$$

□

5. EULER PRODUCTS AND MULTIPLICATIVE CORRECTION FACTORS

In this section we show how the densities $\operatorname{dens}(S_{C,H})$ can be expressed as multiples of an Artin-type constant. Correction factors arising in generalizations of Artin's Conjecture were studied by Lenstra, Moree and Stevenhagen in [5], where they have been expressed in terms of character sums describing the nature of the entanglement. Moreover, this method was applied in a recent paper [1] to compute constants in other Artin-type problems. Over number fields, the correction factors arising in (1) and in the density for $\operatorname{Ind}_\mathfrak{p}(\alpha) \mid t$ have been considered by Palenstijn [8, Theorems 1.5 and 5.2].

For a positive integer Q, we write H_Q for the preimage under v_Q of $v_Q(H)$, and the conjugacy-stable set $C_{H,Q}$ of K-automorphisms is defined in (6).

Proposition 23. *Assume GRH. Suppose that H is almost cut by valuations, and let $Q_0 > 1$ be a square-free integer such that $H = H_{Q_0} \cap \bigcap_{\ell \nmid Q_0} H_\ell$. There is a square-free integer $B \geqslant 1$, which depends only on K, $W_1, \ldots, W_n$ and F, such that*

$$\operatorname{dens}(S_{C,H}) = \mu_{\mathrm{Haar}}(C_{H,\operatorname{lcm}(B,Q_0)}) \cdot \prod_{\ell \nmid \operatorname{lcm}(B,Q_0)} \mu_{\mathrm{Haar}}(C_{H,\ell}).$$

Proof. By [6, Proposition 3.1 (iii)] (see also [10, Theorem 1.1]) there is a square-free integer B, which depends only on K, W_I and F, such that for any prime number ℓ and any integer t

with ℓ coprime to both B and t we have:

$$K(\zeta_\ell, W_I^{1/\ell}) \cap F(\zeta_t, W_I^{1/t}) = K\,.$$

This implies, in particular, that by varying $\ell \nmid B$, the conditions on the K-automorphisms being the identity on $K(\zeta_\ell, W_I^{1/\ell})$ are pairwise independent, and they are also independent from the Frobenius condition related to F. Notice that B is divisible by the primes ℓ such that $\zeta_\ell \in K$. Hence, setting $B' := \operatorname{lcm}(B, Q_0)$, for all square-free integers $Q > 1$ with $B' \mid Q$, we have

$$C_{H,Q} = C_{H,B'} \times \bigoplus_{\ell \nmid B', \ell \mid Q} C_{H,\ell}.$$

We then conclude by Theorem 11. □

Theorem 24. *Assume GRH. There is an integer $B \geqslant 1$, which depends only on K, $W_1, \ldots, W_n$ and F, such that the following assertions hold. If H is almost cut by valuations, with Q_0 as in Proposition 23, then we have*

$$\operatorname{dens}(S_{C,H}) = \mu_{\mathrm{Haar}}(C_{H,\operatorname{lcm}(B,Q_0)}) \cdot \prod_{\ell \nmid \operatorname{lcm}(B,Q_0)} A_{V_\ell,\mathcal{R}}(\ell). \tag{22}$$

If additionally we assume that $W_1, \ldots, W_n$ are separated, then we have

$$\operatorname{dens}(S_{C,H}) = A_{V,\mathcal{R}} \cdot \left(\mu_{\mathrm{Haar}}(C_{H,\operatorname{lcm}(B,Q_0)}) \cdot \prod_{\ell \mid \operatorname{lcm}(B,Q_0)} A_{V_\ell,\mathcal{R}}(\ell)^{-1} \right), \tag{23}$$

and $\operatorname{dens}(S_{C,H})$ *is strictly positive if* $\mu_{\mathrm{Haar}}(C_{H,\operatorname{lcm}(B,Q_0)}) > 0$.

Notice that, in case $C_{H,B}$ is the preimage of its projection to a finite Galois group, $\operatorname{dens}(S_{C,H})$ is a rational multiple of the Artin-type constant $A_{V,\mathcal{R}}$ by (23).

Proof. Let B be as in Proposition 23, and we may suppose that B is also a multiple of the integer c of Corollary 21. For $\ell \nmid B$, observing by (9) that

$$\mu_{\mathrm{Haar}}(C_{h_{\ell,I}}) = \operatorname{dens}(S_{C,v_\ell^{-1}(v_\ell(h_{\ell,I}))}) = \operatorname{dens}\left((v_\ell \circ \Psi)^{-1}(v_\ell(h_{\ell,I})) \right)$$

for every $h_{\ell,I}$ with $h_I \in H$, by Corollary 21 and (7) we have $\mu_{\mathrm{Haar}}(C_{H,\ell}) = A_{V_\ell,\mathcal{R}}(\ell)$. Therefore, since H is almost cut by valuations, by Proposition 23 we obtain (22). For the second assertion it suffices to apply Proposition 22. □

The following example illustrates how from our results we can obtain an expression for the natural density both in the form of a series and of an Euler product.

Example 25. Fix a set $\mathcal{P}'$ of prime numbers and for every $\ell \in \mathcal{P}'$ some positive integer $k(\ell)$. Then let H be the set of positive integers z such that $v_\ell(z) < k(\ell)$ holds for every $\ell \in \mathcal{P}'$. Let $n = 1$, set $W := W_1 \subseteq K^\times$, and call S the set of primes $\mathfrak{p}$ of K such that $\operatorname{Ind}_\mathfrak{p}(W) \in H$. Recall the notation $\mathcal{P}'_\infty$ for the set of positive integers whose prime divisors all lie in $\mathcal{P}'$, and Q^∞ for the set of positive integers whose square-free kernel divides Q. For $Q \geqslant 1$ square-free, setting $f_n := \prod_{\ell \mid n} \ell^{k(\ell)}$, using the inclusion–exclusion principle (on the conditions $v_\ell(\operatorname{Ind}_\mathfrak{p}(W)) < k(\ell)$ for $\ell \mid Q$) and Chebotarev's density theorem we have

$$\operatorname{dens}\left(\Psi^{-1}\Big(\bigcap_{\ell \mid Q} H_\ell \Big) \right) = \sum_{n \in \mathcal{P}'_\infty \cap Q^\infty} \frac{\mu(n)}{[K(\zeta_{f_n}, W^{1/f_n}) : K]},$$

and hence, since H is cut by valuations, by Corollary 12 we have

$$\mathrm{dens}(S) = \sum_{n\in\mathcal{P}'_\infty} \frac{\mu(n)}{[K(\zeta_{f_n}, W^{1/f_n}) : K]}. \tag{24}$$

A side note: as a special case, if $\mathcal{P}'$ is the set of all prime numbers and $k(\ell) = k$ for all ℓ, then we are requiring $\mathrm{Ind}_\mathfrak{p}(W)$ to be k-free (square-free, if $k = 2$); another special case is requiring $\mathrm{Ind}_\mathfrak{p}(W) \mid t$ which amounts to take for $n \geq 1$ square-free $f_n := n \cdot \prod_{\ell\mid n} \ell^{v_\ell(t)}$; with a similar reasoning involving the exclusion–inclusion principle we can deal with the condition $\mathrm{Ind}_\mathfrak{p}(W) = t$, taking $f_n := nt$.

Next we evaluate $\mathrm{dens}(S)$ as an Euler product (the appropriate Artin-type constant) multiplied by a correction factor. By Example 17, for $\ell \in \mathcal{P}'$ we have

$$A_{V_\ell,r}(\ell) = \sum_{v=0}^{k(\ell)-1} F_{v,r}(\ell) = 1 - \frac{1}{(\ell-1)\ell^{k(\ell)(r+1)-1}}$$

and $A_{V,r} = \prod_{\ell\in\mathcal{P}'} A_{V_\ell,r}(\ell)$ (notice that for $\ell \notin \mathcal{P}'$ we have $A_{V_\ell,r}(\ell) = 1$). By Theorem 24 there is a square-free integer B (which depends only on K and W) such that

$$\mathrm{dens}(S) = A_{V,r} \cdot \frac{\#C_B}{[K(\zeta_{B'}, W^{1/B'}) : K]} \cdot \prod_{\ell\in\mathcal{P}',\ell\mid B} A_{V_\ell,r}(\ell)^{-1}$$

where $B' := \prod_{\ell\in\mathcal{P}',\ell\mid B} \ell^{k(\ell)}$ and C_B is the subset of $\mathrm{Gal}(K(\zeta_{B'}, W^{1/B'})/K)$ consisting of those automorphisms that, for every $\ell \in \mathcal{P}'$ with $\ell \mid B$, are not the identity on $K(\zeta_{\ell^{k(\ell)}}, W^{1/\ell^{k(\ell)}})$. In particular, the density vanishes if and only if $C_B = \emptyset$. Recall that, if W is torsion-free, one may take for B any positive integer maximizing the ratio $\varphi(z)z^r/[K(\zeta_z, W^{1/z}) : K]$ by varying $z \geqslant 1$; see [10] for an explicit description.

Example 26. With the same setup of Example 25, and fixing $k \geqslant 2$, we consider the primes $\mathfrak{p}$ such that the index $\mathrm{Ind}_\mathfrak{p}(W)$ is a k-th power. If H is the set of k-th powers, then $V_\ell = k\mathbb{Z}_{\geqslant 0}$, H_ℓ is the set of positive integers with ℓ-adic valuation divisible by k, hence $H = \bigcap_\ell H_\ell$ and H is cut by valuations.

For B as in Theorem 24 for K and W, let K_{B^∞,B^∞} be the union of all fields $K(\zeta_{B^e}, W^{1/B^e})$ for $e \geqslant 1$, and let C_B be the subset of $\mathrm{Gal}(K_{B^\infty,B^\infty}/K)$ consisting of the automorphisms σ satisfying the following: for every $\ell \mid B$ there is an integer $m \geqslant 0$ such that σ is the identity on $K(\zeta_{\ell^{km}}, W^{1/\ell^{km}})$, and it is not the identity on $K(\zeta_{\ell^{km+1}}, W^{1/\ell^{km+1}})$. By Theorem 24, we obtain

$$\mathrm{dens}\{\mathfrak{p} : \mathrm{Ind}_\mathfrak{p}(W) \text{ is a } k\text{-th power}\} = A_{V,r} \cdot \mu_{\mathrm{Haar}}(C_B) \cdot \prod_{\ell\mid B} A_{V_\ell,r}(\ell)^{-1}$$

where $A_{V,r} = \prod_\ell A_{V_\ell,r}(\ell)$ and by Example 17 we have

$$A_{V_\ell,r}(\ell) = \sum_{v=0}^{\infty} F_{kv,r}(\ell) = 1 - \frac{\ell^{k(r+1)} - \ell^{r+1}}{\ell^r(\ell-1)(\ell^{k(r+1)}-1)}.$$

Corollary 27. *Assume GRH. There is a square-free integer $B \geqslant 1$, depending only on K, W_I, F, such that for every $h_I \in \mathbb{Z}^n_{>0}$ we have*

$$\mathrm{dens}(S_{C,\{h_I\}}) = \mu_{\mathrm{Haar}}(C_{h_{B,I}}) \cdot \prod_{\ell\nmid B} F_{v_\ell(h_I),\mathcal{R}}(\ell)\,.$$

Moreover, if $W_1, \dots, W_n$ *are separated, then* $\operatorname{dens}(S_{C,\{h_I\}})$ *is strictly positive if we have* $\mu_{\text{Haar}}(C_{h_{B,I}}) > 0$.

In particular, for separated groups, altering h_I with prime factors $\ell \gg 1$ does not affect the positivity of the density.

Proof. Recall the notation of Section 3.2. This is a special case of Theorem 24 as the set $\{h_I\}$ is trivially cut by valuations with $H_\ell = \{(m_1\ell^{v_\ell(h_1)}, \dots, m_n\ell^{v_\ell(h_n)}) : \ell \nmid \operatorname{lcm}(m_1, \dots, m_n)\}$ and $V_\ell = \{v_\ell(h_I)\}$ for every ℓ. Therefore, it suffices to notice that $C_{\{h_I\},B} = C_{h_{B,I}}$ and

$$A_{\{v_\ell(h_I)\},\mathcal{R}}(\ell) = F_{v_\ell(h_I),\mathcal{R}}(\ell).$$

Alternatively, we may prove the statement with a more direct approach. By Proposition 23 we have

$$\operatorname{dens}(S_{C,\{h_I\}}) = \mu_{\text{Haar}}(C_{h_{B,I}}) \cdot \prod_{\ell \nmid B} \mu_{\text{Haar}}(C_{h_{\ell},I}),$$

where $\mu_{\text{Haar}}(C_{h_\ell,I})$ is the proportion of automorphisms of

$$F(\zeta_{\ell h_\ell}, W_I^{1/(\ell h_{\ell,I})})/K(\zeta_{h_\ell}, W_I^{1/h_{\ell,I}}),$$

whose restriction to $K(\zeta_{\ell h_{\ell,i}}, W_i^{1/\ell h_{\ell,i}})$ is not the identity for any i, and whose restriction to F lies in C. In other words, this factor is the density of primes splitting completely in $K(\zeta_{h_\ell}, W_I^{1/h_{\ell,I}})$, but not in any of the fields $K(\zeta_{\ell h_{\ell,i}}, W_i^{1/\ell h_{\ell,i}})$, and with Frobenius in C. By Corollary 21, assuming also that $\ell \nmid c$, this density is equal to $F_{v_\ell(h_I),\mathcal{R}}(\ell)$. The last assertion is a consequence of Proposition 22. □

The formula of Corollary 27 can be further manipulated. Since $v_\ell(h_I) \neq 0_I$ only for finitely many primes ℓ, we may take a positive integer D which is divisible by these finitely many primes and by B. Then we have

$$\operatorname{dens}(S_{C,\{h_I\}}) = \mu_{\text{Haar}}(C_{h_{D,I}}) \cdot \prod_{\ell \nmid D} F_{0_I,\mathcal{R}}(\ell)\,.$$

If we know that $F_{0_I,\mathcal{R}}(\ell) > 0$ for all primes ℓ (e.g. if the groups W_i are separated), then we can write

$$\operatorname{dens}(S_{C,\{h_I\}}) = A_{V,\mathcal{R}} \cdot \mu_{\text{Haar}}(C_{h_{D,I}}) \cdot \prod_{\ell \mid D} F_{0_I,\mathcal{R}}(\ell)^{-1}\,, \tag{25}$$

where $A_{V,\mathcal{R}}$ is the Artin-type constant with $V_\ell = \{0_I\}$ for every ℓ. This constant is the heuristical density for the primes $\mathfrak{p}$ satisfying $\Psi(\mathfrak{p}) = \delta_I$, i.e. the indices $\operatorname{Ind}_{\mathfrak{p}}(W_i)$ being all 1. Thus the factor multiplying $A_{V,\mathcal{R}}$ in (25) is the correction factor, and we denote it by $m(h_I)$.

Remark 28. Suppose that the groups W_i are separated. For general sets H, one method for computing $\operatorname{dens}(S_{C,H})$ is provided by (10). Indeed, for every $h_I \in \mathbb{Z}^n_{>0}$, by the above (see also [6, proof of Theorem 4.1]) we know that $\operatorname{dens}(S_{C,\{h_I\}})$ is a rational multiple of the strictly positive Artin-type constant $A_{V,\mathcal{R}}$ with $V_\ell = \{0_I\}$ for every ℓ. Hence, with $m(h_I)$ the multiplicative correction factor defined above, we obtain the formula

$$\operatorname{dens}(S_{C,H}) = A_{V,\mathcal{R}} \cdot \sum_{h_I \in H} m(h_I)\,.$$

Notice that the integer D involved in each $m(h_I)$ depends in particular on h_I. For some 'easy' sets H the sum over correction factors may be simplified via other means.

Example 29. Let $n = 1$, $W = W_1$, $\mathrm{rank}(W) = 1$, $K = F = \mathbb{Q}$, and let H be the set of prime numbers. Call A_t the density of the primes p for which $\mathrm{Ind}_p(W) = t$. Suppose that $A_1 > 0$, which implies that the generator of W is not a perfect square. Then for all but finitely many primes q we have by Corollary 27 and Example 17

$$\frac{A_q}{A_1} = \frac{F_{1,1}(q)}{F_{0,1}(q)} = \left(\frac{1}{q(q-1)}\Big(1 - \frac{1}{q^2}\Big)\right) \cdot \left(1 - \frac{1}{q(q-1)}\right)^{-1} = \frac{q^2-1}{q^2(q^2-q-1)}\,.$$

If the above formula holds for all q and we have $A_1 = A$, where $A = \prod_\ell \big(1 - \frac{1}{\ell(\ell-1)}\big)$ is the Artin constant, then the requested density is

$$A \cdot \sum_q \frac{q^2-1}{q^2(q^2-q-1)}\,.$$

In general, the density is of the form

$$cA + A_1 \sum_q \frac{q^2-1}{q^2(q^2-q-1)},$$

where c is a rational number and here A_1 is also a rational multiple of A. For example, the density of the primes p such that the index of $(2 \bmod p)$ is prime is given by

$$A + A \sum_q \frac{q^2-1}{q^2(q^2-q-1)}.$$

Notice that if $A_1 = 0$ (in this case the generator of W is a perfect square), then the index $\mathrm{Ind}_p(W)$ cannot be an odd prime, so it is prime if and only if it equals 2.

Acknowledgments. We would like to thank the anonymous referees for their valuable feedback and insights, which led to a general improvement of the paper. The first author was supported by the Emil Aaltonen foundation and worked in the Finnish Centre of Excellence in Randomness and Structures (Academy of Finland grant no. 346307).

REFERENCES

[1] A. AKBARY, M. FAKHARI, *Constants for Artin-like problems in Kummer and division fields*, Res. Number Theory **10**, 22 (2024). doi.org/10.1007/s40993-024-00509-6

[2] G. COOKE, P. J.WEINBERGER, *On the construction of division chains in algebraic number rings, with applications to SL_2*, Comm. Algebra **3** (1975), 481–524.

[3] C. HOOLEY, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[4] H. W. LENSTRA, *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224.

[5] H. W. LENSTRA, P. STEVENHAGEN, P. MOREE, *Character sums for primitive root densities*, Math. Proc. Cambridge Philos. Soc. **157** (2014), no. 3, 489–511.

[6] O. JÄRVINIEMI, A. PERUCCA, *Unified treatment of Artin-type problems*, Res. Number Theory **9**, 10 (2023). doi.org/10.1007/s40993-022-00418-6.

[7] P. MOREE, *Artin's primitive root conjecture – a survey*, Integers **12** (2012), no. 6, 1305–1416.

[8] W. J. PALENSTIJN, *Radicals in arithmetic*, PhD thesis, University of Leiden (2014), hdl.handle.net/1887/25833.

[9] F. PAPPALARDI, *On Hooley's theorem with weights*, Rend. Sem. Mat. Univ. Pol. Torino **53** (1995), no. 4, 375–388.

[10] A. PERUCCA, P. SGOBBA, S. TRONTO, *The degree of Kummer extensions of number fields*, Int. J. Number Theory, **17** (2021), no. 5, 1091–1110.

[11] V. ZIEGLER, *On the distribution of the order of number field elements modulo prime ideals*, Unif. Distrib. Theory **1** (2006), no. 1, 65–85.

Conflict of Interest

The authors have no conflicts of interest to disclose.

Data Availability

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF TURKU, 20014 TURKU, FINLAND

Email address: `olli.jarviniemi@gmail.com`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LUXEMBOURG, 6 AV. DE LA FONTE, 4364 ESCH-SUR-ALZETTE, LUXEMBOURG

Email address: `antonella.perucca@uni.lu`

DEPARTMENT OF PURE MATHEMATICS, XI'AN JIAOTONG–LIVERPOOL UNIVERSITY, 111 REN'AI ROAD, SUZHOU 215123, CHINA

Email address: `pietro.sgobba@xjtlu.edu.cn`