UNIFIED TREATMENT OF ARTIN-TYPE PROBLEMS

OLLI JÄRVINIEMI AND ANTONELLA PERUCCA

Abstract. Since Hooley's seminal 1967 resolution of Artin's primitive root conjecture under the Generalized Riemann Hypothesis, numerous variations of the conjecture have been considered. We present a framework generalizing and unifying many previously considered variants, and prove results in this full generality (under GRH).

1 Introduction

Several problems related to Artin's primitive root conjecture may be viewed as instances of the following:

Index Map Problem. *Let K be a number field, and let $W_1, \dots, W_n$ be finitely generated subgroups of $K^\times$ of positive rank. For all but finitely many primes $\mathfrak{p}$ of K, their reduction modulo $\mathfrak{p}$ are subgroups of $k_\mathfrak{p}^\times$ of finite index ($k_\mathfrak{p}$ is the residue field), yielding the* index map

$$\Psi : \mathfrak{p} \mapsto (\mathrm{Ind}_\mathfrak{p}(W_1), \dots, \mathrm{Ind}_\mathfrak{p}(W_n)) .$$

Determine whether the preimage under Ψ of a subset of $\mathbb{Z}_{>0}^n$ is infinite (respectively, if it has a positive natural density). Possibly consider a finite Galois extension F/K, a union of conjugacy classes $C \subset \mathrm{Gal}(F/K)$, and restrict to the primes $\mathfrak{p}$ unramified in F such that $\left(\frac{F/K}{\mathfrak{p}}\right) \subset C$.

Consider the preimages of a tuple $(h_1, \dots, h_n) \in \mathbb{Z}_{>0}^n$. The original Artin's conjecture (possibly for higher rank) corresponds to the case $n = 1$ and $h_1 = 1$ because we look for a *primitive root*, and for a *near-primitive root* we can vary $h_1 \in \mathbb{Z}_{>0}$. For *simultaneous primitive roots* we may consider the preimage of the tuple $(1, \dots, 1)$, and more generally the *Schinzel-Wójcik problem* concerns the constant tuples. For the *two variable Artin conjecture* we consider $n = 2$ and all pairs (h_1, h_2) such that $h_1 \mid h_2$. For the *smallest primitive root problem* we let $W_1, \dots, W_n$ be generated by the first n primes and consider the tuples such that h_n is the only entry equal to 1. Notice that, over $\mathbb{Q}$, for all above-mentioned problems we could restrict to primes satisfying some congruence condition, which can be expressed by a suitable choice of F and C. Also notice that, in case we do not need the Frobenius condition, we may simply take $F = K$. The above list is surely non-exhaustive: we refer the reader to the survey by Moree on Artin's Conjecture [11] and, to name a few, to the following papers [3, 5, 10, 12–14, 19].

The main results of this work address the Index Map Problem in full generality.

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

Main Theorem. *Consider the Index Map Problem, assuming GRH.*

(1) [Theorem 4.1 and Remark 4.2] The preimage under the index map of any non-empty subset of $\mathbb{Z}_{>0}^n$ is either finite or it has a positive natural density.

(2) [Theorems 5.4 and 5.1] The image of the index map is uniquely determined by its intersection with the finite set $[1, C]^n$ for some suitable constant C. Moreover, the image of the index map is computable with an explicit finite procedure.

(3) [Theorem 6.2] If $F = K$, then the following two conditions are equivalent:

- *the image of the index map contains all positive multiples of some tuple $(H_1, \dots, H_n)$;*
- *for every $i = 1, \dots, n$ the rank of $\langle W_1, \dots, W_n \rangle$ is strictly larger than the rank of $\langle W_1, \dots, \cancel{W_i}, \dots, W_n \rangle$.*

Moreover, if the above conditions hold, then a tuple $(h_1, \dots, h_n) \in \mathbb{Z}_{>0}^n$ is in the image of the index map if and only if the same holds for the tuple

$$(\gcd(h_1, H_1), \dots, \gcd(h_n, H_n)) .$$

Let $F = K$. For $K = \mathbb{Q}$ the index map is never surjective onto $\mathbb{Z}_{>0}^n$ if $n \geqslant 2$, and in Section 6 we describe very explicitly its image if $n = 1$ and W_1 has rank 1. On the other hand, we prove that for any $K \neq \mathbb{Q}$ and for any n there are groups $W_1, \dots, W_n$ for which the index map is surjective onto $\mathbb{Z}_{>0}^n$, see Section 7. Notice that in the Index Map Problem the assumption that the groups have positive rank is justified by Remarks 4.4 and 6.6.

We make use of several results of Kummer theory, which we collect in Section 3 (some of our statements may be new). We also prove the following result of Kummer theory, that holds for every number field $K \neq \mathbb{Q}$: there are countably many elements of $K^\times$ such that any finite subset of them gives rise to Kummer extensions with maximal degree (in short, for the elements $\alpha_1, \dots, \alpha_r \in K^\times$, the degree of $K(\zeta_{mn}, \alpha_1^{1/n}, \dots, \alpha_r^{1/n})$ over $K(\zeta_{mn})$ equals n^r for all positive integers n and m), see Proposition 7.1.

Our main technical tool is Theorem 4.1, which is a generalization of a celebrated result by Lenstra [9], see also [7, Section 4] (notice that the essential analytic ideas stem from Hooley [5]). As in the proof of Theorem 4.1 we use an effective version of the Chebotarev Density Theorem which is conditional under GRH, most of our results on the Index Map Problem are conditional under GRH, as it is customary for problems related to Artin's primitive root conjecture.

2 Notation for the paper

General notation. In this paper K is a number field, F/K a finite Galois extension of K with Galois group $\mathrm{Gal}(F/K)$, and $C \subset \mathrm{Gal}(F/K)$ a union of conjugacy classes. The multiplicative group of K is denoted by $K^\times$, the ring of integers by O_K, and we fix some algebraic closure $\bar{K}$ containing F. We call τ_K the order of the torsion subgroup of $K^\times$. If n is a positive integer, then we write ζ_n for a root of unity of order n. We also use the notation $K(\zeta_\infty)$ and $K(\zeta_{\ell^\infty})$, in the obvious way, to define infinite cyclotomic extensions of K. We call Ω the smallest positive integer such that $K \cap \mathbb{Q}(\zeta_\infty) \subset \mathbb{Q}(\zeta_\Omega)$. The letters

p, q, ℓ are reserved for primes, and $\mathfrak{p}, \mathfrak{q}$ for primes of K i.e. non-zero prime ideals of O_K. The ideal norm of $\mathfrak{p}$ is $N\mathfrak{p}$, the residue field is $k_\mathfrak{p}$, and the Artin symbol is $\left(\frac{F/K}{\mathfrak{p}}\right)$.

Tuples. We write $I = \{1, \dots, n\}$ and hence we denote e.g. by h_I the tuple $(h_1, \dots, h_n)$. If h_I and H_I are in $\mathbb{Z}^n_{\geqslant 0}$, then h_I is smaller than or equal to H_I if $h_i \leq H_i$ holds for every $i \in I$, and we define $\min(h_I, H_I)$ as the tuple with entries $\min(h_i, H_i)$. Moreover, we call $\oplus h_I$ the set consisting of the tuples larger than or equal to h_I. If h_I and H_I are in $\mathbb{Z}^n_{>0}$, then h_I divides H_I if $h_i \mid H_i$ holds for every $i \in I$, and $\gcd(h_I, H_I)$ is the tuple with entries $\gcd(h_i, H_i)$. Moreover, we call $\otimes h_I$ the set consisting of the multiples of h_I, and the ℓ-adic valuation $v_\ell(h_I)$ is the tuple with entries $v_\ell(h_i)$.

Groups. The symbol W stands for a finitely generated subgroup of $K^\times$ of positive rank (by which we mean the rank of W modulo its torsion subgroup W_{tors}). We set $\tau := \#W_{\mathrm{tors}}$. For all but finitely many $\mathfrak{p}$ the reduction (W mod $\mathfrak{p}$) is a well-defined subgroup of $k_\mathfrak{p}^\times$ and we consider its index $\mathrm{Ind}_\mathfrak{p} W$, which we also write as $\mathrm{Ind}_\mathfrak{p}\alpha$ if $W = \langle\alpha\rangle$. If $n \in \mathbb{Z}_{>0}$, then $W^{1/n} \subset \bar{K}^\times$ consists of all n-th roots of all elements of W (we also consider $S^{1/n}$ for $S \subset K^\times$), and we similarly define $W^{1/\infty}$ and W^{1/ℓ^∞}.

Let $I = \{1, \dots, n\}$ and for $i \in I$ consider subgroups W_i of $K^\times$ of positive rank. Call $W := \langle W_i \mid i \in I\rangle$ and $W_{\neq i} := \langle W_j \mid j \in I, j \neq i\rangle$.

Separated groups. We call $W_1, \dots, W_n$ *separated* if for all $i \in I$ we have

$$\mathrm{rank}\ W > \mathrm{rank}\ W_{\neq i}\,.$$

The index map. For all but finitely many primes $\mathfrak{p}$ of K we can define the *index map*

$$\Psi : \mathfrak{p} \mapsto (\mathrm{Ind}_\mathfrak{p}(W_1), \dots, \mathrm{Ind}_\mathfrak{p}(W_n)) \in \mathbb{Z}^n_{>0}\,.$$

Its ℓ-adic valuation Ψ_ℓ is the composition of Ψ with the ℓ-adic valuation $\mathbb{Z}^n_{>0} \to \mathbb{Z}^n_{\geqslant 0}$. We similarly define its Q-adic valuation Ψ_Q for any positive squarefree integer Q, where the Q-adic valuation $v_Q(z)$ of $z \in \mathbb{Z}_{\neq 0}$ is the tuple consisting of the ℓ-adic valuation $v_\ell(z)$ for the primes $\ell \mid Q$.

Convention. Starting from Theorem 4.1, up to excluding finitely many primes of K, we restrict Ψ to the primes that are not ramified over $\mathbb{Q}$, do not ramify in F, and do not lie over a prime divisor of τ_K.

3 Results from Kummer theory

Proposition 3.1. *The following holds:*

(1) There exists a positive integer z (depending on K and W, computable with an explicit finite procedure) such that for all positive integers t we have

$$[K(\zeta_\infty, W^{1/zt}) : K(\zeta_\infty, W^{1/z})] = t^{\mathrm{rank}\ W}\,.$$

(2) There exists a finite Galois extension K_W/K (depending on K and W, computable with an explicit finite procedure) such that for all coprime positive integers m, t we have

$$K\left(\zeta_m, W^{1/m}\right) \cap K\left(\zeta_t, W^{1/t}\right) \subset K_W\,.$$

(3) *There exists a positive integer c (depending on K and W, computable with an explicit finite procedure) such that for all positive integers m, t such that m is coprime to both t and c we have*

$$K\left(\zeta_m, W^{1/m}\right) \cap K\left(\zeta_t, W^{1/t}\right) = K$$

$$\text{and} \quad [K\left(\zeta_m, W^{1/m}\right) : K] = \varphi(m) m^{\operatorname{rank} W}.$$

We could additionally require that $K\left(\zeta_m, W^{1/m}\right) \cap F = K$ (in this case c also depends on F). We could additionally require that c is divisible by some given positive integer, or we may replace c by its square-free part.

Proof. For (1) we may suppose that W is torsion-free. By [16, Theorems 1.1 and 1.2] we can take z to be a positive integer maximizing the integer ratio

$$\frac{\varphi(z) z^{\operatorname{rank} W}}{[K\left(\zeta_z, W^{1/z}\right) : K]}.$$

We may also suppose that $K \cap \mathbb{Q}(\zeta_\infty) \subset K(\zeta_z)$, so that for (2) and (3) we may take $K_W = K\left(\zeta_z, W^{1/z}\right)$ and $c = z$. For the additional remarks in (3) notice that, since we may replace c by a multiple, we may suppose that $F \cap K\left(\zeta_\infty, W^{1/\infty}\right) \subset K\left(\zeta_c, W^{1/c}\right)$. □

Proposition 3.2. *Suppose that $W_1, \dots, W_n$ are separated.*

(1) *There exists $h_I \in \mathbb{Z}^n_{>0}$ such that the fields $K(\zeta_\infty, W_1^{1/H_1}, \dots, W_n^{1/H_n})$ for $H_I \in \otimes h_I$ are all distinct or, equivalently, the fields $K(\zeta_\infty, W_i^{1/H_i}, W_{\neq i}^{1/\infty})$ for $i \in I$ and $H_i \in h_i\mathbb{Z} \cap \mathbb{Z}_{>0}$ are all distinct: we say that the W_i's have* separated Kummer extensions *w.r.t. h_I. In particular, $\prod_{i\in I} H_i/h_i$ divides*

$$[K(\zeta_\infty, W_1^{1/H_1}, \dots, W_n^{1/H_n}) : K(\zeta_\infty, W_1^{1/h_1}, \dots, W_n^{1/h_n})].$$

(2) *For every ℓ there exists $e_I \in \mathbb{Z}^n_{\geqslant 0}$ such that the fields $K(\zeta_{\ell^\infty}, W_1^{1/\ell^{E_1}}, \dots, W_n^{1/\ell^{E_n}})$ for $E_I \in \oplus e_I$ are all distinct: we say that the W_i's have* ℓ-separated Kummer extensions *w.r.t. e_I.*

(3) *The set $Sep \subset \mathbb{Z}^n_{>0}$ and all sets $Sep_\ell \subseteq \mathbb{Z}^n_{\geqslant 0}$, consisting of the tuples with respect to which the W_i's have separated (respectively, ℓ-separated) Kummer extensions, are computable at once with an explicit finite procedure. There exist $h_I \in \mathbb{Z}^n_{>0}$ and $e_{\ell,I} \in \mathbb{Z}^n_{\geqslant 0}$ such that $Sep = \otimes h_I$, $Sep_\ell = \oplus e_{\ell,I}$, $0 \leqslant v_\ell(h_i) - e_{\ell,i} \leqslant v_\ell(\tau_K)$, and we have*

$$v_\ell(h_i) = \max\{z : K(\zeta_\infty, W_i^{1/\ell^z}) \subset K(\zeta_\infty, W_{\neq i}^{1/\ell^\infty}, W_i^{1/\ell^{z-1}})\} \tag{1}$$

$$e_{\ell,i} = \max\{z : K(\zeta_{\ell^\infty}, W_i^{1/\ell^z}) \subset K(\zeta_{\ell^\infty}, W_{\neq i}^{1/\ell^\infty}, W_i^{1/\ell^{z-1}})\}. \tag{2}$$

Proof. Comparing the eventual maximal growth of W and $W_{\neq i}$, see Proposition 3.1 (1), gives (2) and the first part of (1). In the second part of (1) we consider the degree of a tower of Kummer extensions of degree dividing a prime and that, being non-trivial, have maximal degree. We are left to prove (3).

Having $m_I \in Sep$ (respectively, $m_I \in Sep_\ell$) implies $\otimes m_I \subset Sep$ (respectively, $\oplus m_I \subset Sep_\ell$). Let $Z_{\ell,i}$ and $z_{\ell,i}$ be the right-hand-side in (1) and (2) respectively, and set $Z_i := \prod_\ell \ell^{Z_{\ell,i}}$, thus $Sep \subset \otimes Z_I$ and $Sep_\ell \subset \oplus z_{\ell,I}$. We may then take $h_I = Z_I$ and $e_{\ell,I} = z_{\ell,I}$ because by Kummer theory we have $Z_I \in Sep$ and $z_{\ell,I} \in Sep_\ell$. Clearly $v_\ell(h_i) - e_{\ell,i}$ is non-negative, and it is at most $v_\ell(\tau_K)$ by Schinzel's Theorem for abelian radical extensions (with the notation of [16], we have to consider the ℓ-adelic failure for W).

By the theory developed in [1, 15] we may compute $e_{\ell,I}$ for all ℓ, which is the zero tuple except for finitely many computable primes ℓ . We are left to compute $v_\ell(h_I)$ for $\ell \mid \tau_K$. Set $t_\ell := v_\ell(\tau_K) + \max_i(e_{\ell,i})$, and let T_ℓ be the product of $2\ell^{v_\ell(\tau_K)}$ and the primes $q \equiv 1 \bmod \ell$ such that $\ell \nmid v_{\mathfrak{q}}(w)$ holds for some $w \in W$ and for some prime $\mathfrak{q}$ of K lying over q. We conclude because by [4, Lemma C.1.7 and its proof] we have

$$v_\ell(h_i) - e_{\ell,i} = v_\ell\left(\frac{[K(\zeta_{T_\ell \ell^{t_\ell}}, W^{1/\ell^{t_\ell}}) : K(\zeta_{T_\ell \ell^{t_\ell}}, W_{\neq i}^{1/\ell^{t_\ell}})]}{[K(\zeta_{\ell^{t_\ell}}, W^{1/\ell^{t_\ell}}) : K(\zeta_{\ell^{t_\ell}}, W_{\neq i}^{1/\ell^{t_\ell}})]}\right).$$

□

With the notation of Proposition 3.2 we could have $e_{\ell,i} < v_\ell(h_i)$: indeed, for $K = \mathbb{Q}$ and $W = \langle 5 \rangle$ we have $Sep_2 = \mathbb{Z}_{\geqslant 0}$ and $Sep = 2\,\mathbb{Z}_{>0}$.

Lemma 3.3. *Let $\alpha_1, \dots, \alpha_r \in K^\times$ be multiplicatively independent. There exist a positive integer N and $S \subset (\mathbb{Z}/N\mathbb{Z})^{r+1}$ such that for $(z_0, \dots, z_r) \in \mathbb{Z}_{>0}^{r+1}$ with $\operatorname{lcm}(z_0, \dots, z_r) = z_0$ the following holds: given $(x_0, \dots, x_r) \in \mathbb{Z}_{>0}^{r+1}$, there is*

$$\sigma \in \operatorname{Gal}\left(F\left(\zeta_{z_0}, \alpha_1^{1/z_1}, \dots, \alpha_r^{1/z_r}\right)/K\right)$$

such that $\sigma|_F \in C$, $\sigma(\zeta_{z_0}) = \zeta_{z_0}^{x_0}$, and $\sigma\left(\alpha_i^{1/z_i}\right) = \zeta_{z_i}^{x_i}\alpha_i^{1/z_i}$ for $i = 1, \dots, r$ if and only if $\gcd(x_0, z_0) = 1$ and $(x_0 \pmod N, \dots, x_r \pmod N) \in S$. The integer N only depends on K, F and $\langle \alpha_1, \dots, \alpha_r \rangle$, and N, S are computable with an explicit finite procedure. Supposing that the prime divisors of $z_0, \dots, z_r$ belong to some set D, we may remove from N all prime factors not in D.

Proof. The condition $\gcd(x_0, z_0) = 1$ is clearly necessary, so assume that it holds. Calling $W = \langle \alpha_1, \dots, \alpha_r \rangle$, by Proposition 3.1 there is some positive integer N such that $F \cap K(\zeta_\infty, W^{1/\infty}) \subset K(\zeta_N, W^{1/N})$ and such that for every positive multiple M of N we have

$$[K(\zeta_M, W^{1/M}) : K(\zeta_N, W^{1/N})] = (M/N)^r \cdot \varphi(M)/\varphi(N).$$

Thus we may replace z_i by $\gcd(z_i, N)$ and work in $\operatorname{Gal}(K(\zeta_N, W^{1/N})/K)$. □

Remark 3.4. By [1, Definitions 5 and 10] $\alpha_1, \dots, \alpha_r \in K^\times$ are strongly ℓ-independent if for $i = 1, \dots, r$ there is some prime $\mathfrak{q}_i$ of K such that $\ell \nmid v_{\mathfrak{q}_i}(\alpha_i)$ and $\ell \mid v_{\mathfrak{q}_i}(\alpha_j)$ for $j \neq i$. Indeed, if $\alpha := \prod \alpha_i^{z_i}$ for some integers z_i and w.l.o.g. $\ell \nmid z_1$, then $\ell \nmid v_{\mathfrak{q}_1}(\alpha)$ hence α is strongly ℓ-indivisible. Similarly, if the α_i's are not units and their norms $N_{K/\mathbb{Q}}(\alpha_i)$ are pairwise coprime and not of the form ± 1 times an ℓth power, then they are an ℓ-good basis (as in [1, Theorem 14]) for $\langle \alpha_1, \dots, \alpha_r \rangle$.

Kummer extensions contained in cyclotomic extensions

Consider a prime power $\ell^e \mid \tau_K$ and a cyclic Kummer extension L/K of degree ℓ^e with $L \subset K(\zeta_\infty)$. Calling K' the largest subfield of $K \cap \mathbb{Q}(\zeta_\infty)$ of degree a power of ℓ, we have $L = L'K$ for some unique $K' \subset L' \subset \mathbb{Q}(\zeta_\infty)$ such that $[L' : \mathbb{Q}]$ is a power of ℓ (and hence $[L' : K'] = \ell^e$). We have $L' \subset \mathbb{Q}(\zeta_n)$ for some positive integer n of the form

$$n = \ell^{T+e}Q \qquad \text{where} \qquad Q = \prod_{q \equiv 1 \pmod{\ell}} q \qquad \text{and} \qquad \zeta_{\ell^T} \in K(\zeta_Q)\,.$$

The extension L'/K' corresponds to a cyclic quotient of degree ℓ^e of $G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K')$.

Proposition 3.5. *Replace G by its largest quotient of exponent ℓ^e and suppose that $G \simeq \prod_{i\in I} \mathbb{Z}/\ell^{e_i}\mathbb{Z}$. The i-th factor corresponds to a cyclic Kummer extension $K'(\gamma_i)/K'$ of degree ℓ^{e_i} for some $\gamma_i \in \mathbb{Q}(\zeta_n)$ such that $\gamma_i^{\ell^{e_i}} \in K'$.*

(1) We have $L' = K'(\gamma)$ for some $\gamma := \prod_{i\in I} \gamma_i^{y_i}$, where $0 \leqslant y_i < \ell^{e_i}$ and for some $i \in I$ we have $e_i = e$ and $\ell \nmid y_i$.

(2) For every $q \mid n$ such that $q \nmid \ell\Omega$ fix an algebraic integer $g_q \in \mathbb{Q}(\zeta_{\ell^e q})$ such that $g_q^{\ell^e} \in \mathbb{Q}(\zeta_{\ell^e})$ and such that

$$v_\ell[\mathbb{Q}(\zeta_{\ell^e}, g_q) : \mathbb{Q}(\zeta_{\ell^e})] = e_q \qquad \text{where} \quad e_q := \min(e, v_\ell(q-1))\,.$$

For every $q \mid n$ we may fix one γ_i as follows: if $q \nmid \ell\Omega$, then $\gamma_i^{\ell^{e_i}} = g_q^{\ell^{e_q}}$, else γ_i is an algebraic integer in $\mathbb{Q}(\zeta_{\ell^e\Omega})$. Then $\ell \nmid v_\mathfrak{p}(\gamma_i^{\ell^{e_i}})$ holds for a prime $\mathfrak{p}$ of K only if $\mathfrak{p}$ lies over q or over a divisor of $\ell\Omega$ respectively, and in the former case there is such $\mathfrak{p}$.

Proof. Since the extensions $K'(\gamma_i)/K'$ are linearly disjoint, $\prod_i \gamma_i^{z_i} \in K$ implies $\ell^{e_i} \mid z_i$ for every i. Thus $\prod_i \gamma_i^{y_i}$ and $\prod_i \gamma_i^{Y_i}$ generate the same extension if and only if $Y_i \equiv ty_i \bmod \ell^{e_i}$ holds for every i and for some t coprime to ℓ, in other words if y_I and Y_I generate the same cyclic subgroup of G of order ℓ^e. By Pontryagin duality the number of those subgroups is the same as the number of cyclic quotients of G of order ℓ^e and hence (1) follows. For the first assertion of (2) it suffices to choose the isomorphism of G respecting the decomposition $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K') = \mathrm{Gal}(\mathbb{Q}(\zeta_{n_1})/K') \times \mathrm{Gal}(\mathbb{Q}(\zeta_{n_2})/\mathbb{Q})$, where $n = n_1n_2$ and n_2 consists of all prime factors $q \nmid \ell\Omega$. We then conclude by [4, Lemma C.1.7 and its proof]. □

Example 3.6. With the above notation, it may be that L is not contained in the compositum of K, $\mathbb{Q}(\zeta_{\ell^\infty})$, and subextensions of $\mathbb{Q}(\zeta_q)/K \cap \mathbb{Q}(\zeta_q)$ of degree dividing ℓ^e. Consider for example $\ell^e = 2$, $K = \mathbb{Q}(\sqrt{65})$, and the quartic cyclic field $L = \mathbb{Q}(\sqrt{65 + 8\sqrt{65}}) \subset \mathbb{Q}(\zeta_{65})$.

4 The Master Theorem on Artin type problems

For $h_I \in \mathbb{Z}^n_{>0}$, $h := \mathrm{lcm}(h_1, \dots, h_n)$, and a positive squarefree integer Q, we write

$$K_Q := K(\zeta_{Qh}, W_1^{1/Qh_1}, \dots, W_n^{1/Qh_n})$$

and we let $C_Q \subset \mathrm{Gal}\big(FK_Q/K_1\big)$ consist of the automorphisms whose restriction to F lies in C, and which, for $q \mid Q$ and $i \in I$, are not the identity on $K(\zeta_{qh_i}, W_i^{1/qh_i})$. For every

set $\mathcal{S}$ of primes of K we write $\mathcal{S}(x) := |\{\mathfrak{p} \in \mathcal{S} : N\mathfrak{p} \le x\}|$ and

$$\pi_K(x) := |\{\mathfrak{p} : N\mathfrak{p} \le x\}| = x/\log x + o(x/\log x)\,.$$

Theorem 4.1. *Assume GRH. Fix $h_I \in \mathbb{Z}^n_{>0}$, and let S be the set of primes $\mathfrak{p}$ of K for which Ψ is defined and we have*

$$\left(\frac{\mathfrak{p}}{F/K}\right) \subset C \quad \text{and} \quad \Psi(\mathfrak{p}) = h_I\,.$$

The natural density $d(S)$ of S exists, and it is 0 if and only if $S = \emptyset$ if and only if $C_Q = \emptyset$ for some positive squarefree integer Q. Writing $Q_x := \prod_{q \leqslant x} q$, we have

$$d(S) = \lim_{x\to\infty} d_{Q_x}\,, \quad \text{where} \quad d_{Q_x} := \frac{|C_{Q_x}|}{[FK_{Q_x} : K]}\,.$$

The property $\Psi(\mathfrak{p}) = h_I$ means that $\mathfrak{p}$ splits in $K(\zeta_{h_i}, W_i^{1/h_i})$ and it does not split in $K(\zeta_{qh_i}, W_i^{1/qh_i})$, for $i \in I$ and for all primes q. Requiring the above conditions only for $q \leqslant x$, we obtain a larger set with natural density d_{Q_x}. Theorem 4.1 states that these larger sets are good approximations for the set S for x large.

Proof. For Q a squarefree positive integer, we have $S \subset S_Q$, where

$$S_Q := \left\{\mathfrak{p} \ : \quad \left(\frac{\mathfrak{p}}{FK_Q/K}\right) \subset C_Q\right\}.$$

By the Chebotarev Density Theorem the natural density of S_Q is $d_Q := |C_Q|/[FK_Q : K]$. We have $d_Q = 0$ if and only if $C_Q = \emptyset$, and these conditions imply $S = \emptyset$.

We claim that for any positive integer t we have

$$S_{Q_t}(x) - S(x) \leqslant O(\pi_K(x)/t) + o(x/\log x)\,, \tag{3}$$

where the implied constants depend on n, K, F, W, h_I. We deduce that $d(S)$ exists and (as $x \mapsto d_{Q_x}$ is non-increasing) it equals $\inf\{d_{Q_x}\}$.

Let Q_0 be the squarefree part of the constant c from Proposition 3.1 (3), assuming $n!h \mid c$ and the additional condition involving F. We suppose $C_{Q_0} \neq \emptyset$ and prove $\inf\{d_{Q_x}\} > 0$. Let $L_q := K(\zeta_q, W^{1/q})$ and $L_{q,i} := K(\zeta_q, W_i^{1/q})$. Since $[L_{q,i} : K] \geqslant (q-1)q$ and by linear disjointness, for $x \geqslant Q_0$ we have

$$d_{Q_x} = d_{Q_0} \prod_{q\leqslant x, q\nmid Q_0} \frac{|\mathrm{Gal}(L_q/K) \setminus \bigcup_{i\in I} \mathrm{Gal}\,(L_q/L_{q,i}))\,|}{|\mathrm{Gal}(L_q/K)|} \geqslant d_{Q_0} \prod_{q>n} \left(1 - \frac{n}{q(q-1)}\right) > 0\,.$$

We are left to prove the claim. For t large enough, every $q > t$ satisfies $q \nmid h$ and $[L_{q,i} : K] \geqslant (q-1)q$. Setting $f_1(x) := \sqrt{x}/(\log x)^{100}$ and $f_2(x) := \sqrt{x}(\log x)^{100}$, consider the intervals

$$I_1 := (t, f_1(x)) \qquad I_2 := [f_1(x), f_2(x)] \qquad I_3 := (f_2(x), x]$$

and the corresponding sets

$$\Gamma_j := \{\mathfrak{p} : N\mathfrak{p} \leqslant x \text{ and } \mathfrak{p} \text{ splits in } L_{q,i} \text{ for some } i \in I \text{ and } q \in I_j\}\,.$$

Any $\mathfrak{p} \in S_{Q_t} \setminus S$ splits in some $L_{q,i}$ with $q > t$, and $N\mathfrak{p} \leqslant x$ implies $q \leqslant x$. Thus $S_{Q(t)}(x) - S(x) = O\left(|\Gamma_1| + |\Gamma_2| + |\Gamma_3|\right)$. We clearly have

$$|\Gamma_j| \leqslant \sum_{i\in I} \sum_{q\in I_j} |\{\mathfrak{p} : N\mathfrak{p} \leq x \text{ and } \mathfrak{p} \text{ splits in } L_{q,i}\}| \,.$$

By the effective Chebotarev Density Theorem under GRH [8, 17] we get

$$|\Gamma_1| \leqslant \sum_{i\in I} \sum_{q\in I_1} \left(\frac{\pi_K(x)}{q(q-1)} + O\left(\sqrt{x}(\log x)^{10}\right)\right) = O\left(\pi_K(x)/t\right) + o(x/\log x)\,.$$

Moreover, considering separately the primes of K of degree greater than 1 we have

$$|\Gamma_2| \leqslant n \sum_{q\in I_2} |\{\mathfrak{p} : N\mathfrak{p} \leqslant x \text{ is of degree 1 and } \mathfrak{p} \text{ splits in } K\left(\zeta_q\right)\}| + n[K:\mathbb{Q}]\sqrt{x}$$

and hence by the Brun-Titchmarsh inequality

$$\begin{aligned} |\Gamma_2| &\leqslant O\big(\sum_{q\in I_2} |\{p : p \leqslant x \text{ and } p \equiv 1 \bmod q\}| \big) + n[K:\mathbb{Q}]\sqrt{x} \\ &\leqslant O\left(\sum_{q\in I_2} \frac{2\pi(x)}{q-1} \right) + o(x/\log x) = o(x/\log x)\,. \end{aligned}$$

Fixing some $w_i \in W_i \setminus K^\times_{\mathrm{tors}}$ we have

$$\Gamma_3 \subset \bigcup_{i\in I} \{\mathfrak{p} : N\mathfrak{p} \leq x \text{ and } \mathfrak{p} \text{ splits in } K\left(\zeta_q, w_i^{1/q}\right) \text{ for some } q \in I_3\}.$$

Thus $\mathfrak{p} \in \Gamma_3$ implies $w_i^{(N\mathfrak{p}-1)/q} \equiv 1 \pmod{\mathfrak{p}}$ for some $i \in I$. Since $f_1(x)f_2(x) = x$, we have

$$\prod_{\mathfrak{p}\in\Gamma_3} N\mathfrak{p} \mid \prod_{i\in I} N_{K/\mathbb{Q}} \left(\prod_{k\leqslant f_1(x)} w_i^k - 1 \right) \leqslant 2^{O(f_1(x)^2)}$$

(the implied constant also depends on w_i), and hence $|\Gamma_3| = o(x/\log x)$. □

Remark 4.2. Assuming GRH, $d(S)$ also exists if we replace h_I by some $H \subset \mathbb{Z}^n_{>0}$. Indeed, calling $d^\pm$ the upper/lower density and $B(r) := \{1, \dots, r\}^n$, we have

$$\begin{aligned} d_-(\Psi^{-1}H) \geqslant \lim_{r\to\infty} \sum_{h\in H\cap B(r)} d_-(\Psi^{-1}\{h\}) = \lim_{r\to\infty} \sum_{h\in H\cap B(r)} d^+(\Psi^{-1}\{h\}) \geqslant \\ d^+(\Psi^{-1}H) - \lim_{r\to\infty} d^+(\Psi^{-1}(\mathbb{Z}^n_{>0} \setminus B(r)) = d^+(\Psi^{-1}H) \end{aligned}$$

by Theorem 4.1 and because $d^-(\Psi^{-1}B(r)) \to 1$: it is well-known that under GRH for $a \in \mathbb{Q} \setminus \{0, \pm 1\}$ the density of the primes p such that $\mathrm{ord}_p(a) := (p-1)/\mathrm{Ind}_p(a) \geqslant C$ exists and tends to 1 as $C \to \infty$, and the same holds for number fields following Hooley's proof [5, Theorem 4.1, especially (3)], see also [2, Theorem 4] or [18, Theorem 5.1].

Corollary 4.3. *Assume GRH. Let $h_I \in \mathbb{Z}^n_{>0}$ and $h := \mathrm{lcm}(h_1, \dots, h_n)$. We have $h_I \in \mathrm{Im}\,(\Psi)$ if and only if for every positive squarefree integer Q there is an automorphism in*

$$\mathrm{Gal}\big(K(\zeta_{Qh}, W_1^{1/Qh_1}, \dots, W_n^{1/Qh_n})/K(\zeta_h, W_1^{1/h_1}, \dots, W_n^{1/h_n})\big)$$

which for $i \in I$ and $q \mid Q$ is not the identity on $K(\zeta_{qh_i}, W_i^{1/qh_i})$.

Let $e_I \in \mathbb{Z}^n_{\geqslant 0}$ and $e := \max(e_1, \dots, e_n)$. We have $e_I \in \mathrm{Im}\,(\Psi_\ell)$ if and only if there is an automorphism in

$$\mathrm{Gal}\big(K(\zeta_{\ell^{e+1}}, W_1^{1/\ell^{e_1+1}}, \dots, W_n^{1/\ell^{e_n+1}})/K(\zeta_{\ell^e}, W_1^{1/\ell^{e_1}}, \dots, W_n^{1/\ell^{e_n}})\big)$$

which for $i \in I$ is not the identity on $K(\zeta_{\ell^{e_i+1}}, W_i^{1/\ell^{e_i+1}})$.

Proof. By Theorem 4.1 we may restrict to the primes $\mathfrak{p}$ of degree 1 hence for every positive integer t we have $t \mid \mathrm{Ind}_{\mathfrak{p}}(W_i)$ if and only if $\mathfrak{p}$ splits in $K(\zeta_t, W_i^{1/t})$. The second assertion is immediate, and we conclude by Theorem 4.1. □

Remark 4.4. In the Index Map Problem we assume that the groups have positive rank. If some of them is finite, then the preimage of any finite subset of $\mathbb{Z}^n_{>0}$ is finite, see Remark 6.6. However, the preimage of an infinite set could be an infinite set of density 0 or without a Dirichlet density. For example, consider $K = \mathbb{Q}$ and $W_1 = \langle 1 \rangle$, $W_2 = \langle 2 \rangle$: the preimage of $S \times \mathbb{Z}_{>0}$, where $S \subset \mathbb{Z}_{>0}$ is any infinite set such that $\{s + 1 \mid s \in S\}$ is a set of primes of density 0 (respectively, without a Dirichlet density), is as requested.

5 Computability of the image of the index map

For $J \subset I$ and $i \in I \setminus J$, we call $k_{J,i}$ the smallest positive integer z such that $W_i^z \subset \prod_{j \in J} W_j$ ($k_{J,i} = \infty$, if there is no z) and we call $k := \mathrm{lcm}(k_{J,i})$ (treating ∞ as 1).

Theorem 5.1. *Assume GRH. Let $h_I \in \mathbb{Z}^n_{>0}$, $h := \mathrm{lcm}(h_1, \dots, h_n)$, and let ω be the number of distinct prime divisors of h. Assuming that arithmetic operations and computing prime factors can be performed in negligible time, checking whether $h_I \in \mathrm{Im}\,(f)$ can be done in $O(\omega)$ steps (the implied constant depends on $K, F, n, W_1, \dots, W_n$).*

Proof. By Theorem 4.1 and by Proposition 3.1 (3), calling Q the square-free part of c, we have to check whether there is

$$\sigma \in \mathrm{Gal}\left(F\left(\zeta_{Qh\tau_K}, W^{1/Qh}\right)/K\right)$$

such that $\sigma\,|_F \in C$ and σ is the identity on $K(\zeta_{h_i}, W_i^{1/h_i})$ but not on $K(\zeta_{qh_i}, W_i^{1/qh_i})$ for $i \in I$ and $q \mid Qh$. Notice that, if F'/F is a finite Galois extension and $C' \subset \mathrm{Gal}(F'/K)$ consists of the automorphisms whose restriction to F is in C, then we do not change our problem by replacing F by F' and C by C'. Thus, up to extending F independently of h (and replacing C), by Proposition 3.1 (2) the cyclotomic-Kummer extensions for W made with coprime parameters are linearly disjoint over F. Hence we may consider the problem separately for different values of $q \mid Qh$.

Call $e_I := v_q(h_I)$ and suppose w.l.o.g. that e_I is non-increasing. The splitting conditions then become: for all $i \in I$, σ is the identity on $K(\zeta_{q^{e_i}}, W_i^{1/q^{e_i}})$ but not on $K(\zeta_{q^{e_i+1}}, W_i^{1/q^{e_i+1}})$.

We exclude the case $W_j^k \in \langle W_1, \dots, W_i \rangle$ and $e_j < e_i - v_q(k)$ for some $j > i$, as clearly $h_I \notin \mathrm{Im}\,\Psi$. We partition I into intervals T_j, their starting points being 1 and those $i \in I$ such that $e_i < e_{i-1} - v_q(k\tau_K)$. We call $\rho_i := v_q(\#W_{i,tors})$, $\mathcal{W}_j := \langle W_i : i \in T_j \rangle$, and for $i \in T_j$ we let $S_i \subset W_i$ be a minimal non-empty set of multiplicatively independent

elements such that $W_i \subset \langle K_{tors}^\times, S_i, \mathcal{W}_1, \dots, \mathcal{W}_{j-1}\rangle$. The splitting conditions then become: for all $i \in I$, σ is the identity on $K(\zeta_{q^{e_i+\rho_i}}, S_i^{1/q^{e_i}})$ but not on $K(\zeta_{q^{e_i+\rho_i+1}}, S_i^{1/q^{e_i+1}})$.

Fixing j, let $e := e_{\min T_j}$, and let $\alpha_1, \dots, \alpha_r \in \mathcal{W}_j$ be multiplicatively independent and such that $S_i \subset \langle K_{tors}^\times, \alpha_1, \dots, \alpha_r\rangle$ for $i \in T_j$. For any σ define $\mathbf{x} := (x_0, x_1, \dots, x_r)$ with the smallest positive integers such that

$$\sigma(\zeta_{Qh\tau_K}) = \zeta_{Qh\tau_K}^{x_0} \qquad \text{and} \quad \sigma\left(\alpha_i^{1/q^{e+1}}\right) = \zeta_{q^{e+1}}^{x_i}\alpha_i^{1/q^{e+1}} \quad \text{for } i = 1, \dots, r\,.$$

For $i \in T_j$ and $w_{i,i'} \in S_i$ define $\mathbf{f}_{i,i'} = (f_0, \dots, f_r)$ such that

$$w_{i,i'}^{1/q^e} = \zeta_{q^{v_q(\tau_K)+e+1}}^{f_0}\alpha_i^{f_1/q^e}\cdots\alpha_r^{f_r/q^e}.$$

The splitting conditions concerning some $i \in T_j$ amount to

$$\begin{array}{lllll} & x_0 \equiv 1 \pmod{q^{e_i+\rho_i}} & \text{and} & \langle \mathbf{x}, \mathbf{f}_{i,i'}\rangle \equiv 0 \pmod{q^{e_i}} & , \\ \text{and} & x_0 \not\equiv 1 \pmod{q^{e_i+\rho_i+1}} & \text{or} & \langle \mathbf{x}, \mathbf{f}_{i,i'}\rangle \not\equiv 0 \pmod{q^{e_i+1}} & \text{for some } i'\,. \end{array}$$

Considering all $i \in T_j$ we have various systems of linear incongruences and at least one system must have a solution in common with the linear congruences. Since there are only boundedly many system of incongruences, we may consider them separately and thus fix one of them.

Note that different sets T_j give different systems of (in)congruences. The only common variable between these systems is x_0. Any common solution to the systems necessarily has $v_q(x_0 - 1) \geq \max_i e_i + \rho_i$, and thus we cannot use the incongruence for x_0 if $e_i + \rho_i$ is smaller than its maximal value over $i \in I$. Hence we essentially have no common variables between the different systems, and thus we may now fix some T_j.

Let q^N and S be the integer and the set from Lemma 3.3, and consider separately each $\mathbf{s} := (s_0, \dots, s_r) \in S$. Setting $x_i := q^N y_i + s_i$ with $\mathbf{y} := (y_0, y_1, \dots, y_r)$, and rewriting $\langle \mathbf{x}, \mathbf{f}_{i,i'}\rangle \equiv 0$ as $\langle \mathbf{y}, q^N\mathbf{f}_{i,i'}\rangle \equiv -\langle \mathbf{s}, \mathbf{f}_{i,i'}\rangle$, we get a system of the form

$$\begin{cases} \langle \mathbf{y}, \mathbf{v}_i\rangle \equiv c(\mathbf{v}_i) \pmod{q^{e(\mathbf{v}_i)}} & \text{for all } i \in J \\ \langle \mathbf{y}, \mathbf{v}_i\rangle \not\equiv c(\mathbf{v}_i) \pmod{q^{e(\mathbf{v}_i)+1}} & \text{for all } i \in J' \end{cases} \tag{4}$$

for some $J' \subset J \subset T_j$, for some vectors $\mathbf{v}_i$, and for some integers $c(\mathbf{v}_i)$ and $e(\mathbf{v}_i) \in \{e_i, e_i + \rho_i\}$: the vectors $\mathbf{v}_i$ consist of the vectors $q^N\mathbf{f}_{i,i'}$ and of the vector $(q^N, 0, \dots, 0)$ to express the conditions for x_0. Notice that $|e(\mathbf{v}_i) - e(\mathbf{v}_{i'})| \leq nv_q(k\tau_K)$ for $i, i' \in J$.

Let $\mathcal{J} \subset J$ be a maximal subset such that $\mathbf{v}_i, i \in \mathcal{J}$ are $\mathbb{Q}$-linearly independent and $e(\mathbf{v}_i), i \in \mathcal{J}$ are as large as possible. For $i \in J$ let $\mathbf{u}_i$ be the vector of coefficients to express $\mathbf{v}_i$ as a $\mathbb{Q}$-linear combination of $\mathbf{v}_j, j \in \mathcal{J}$. As $\mathbf{y}$ varies over integer vectors, the values for $\mathbf{z} := (\langle \mathbf{y}, \mathbf{v}_i\rangle)_{i\in\mathcal{J}}$ are all preimages of the (non-empty) set $\mathcal{M}$ of their reductions modulo M, for some positive integer M. Since $\langle \mathbf{y}, \mathbf{v}_i\rangle = \langle \mathbf{z}, \mathbf{u}_i\rangle$ we may rewrite (4) as

$$\begin{cases} \langle \mathbf{z}, \mathbf{u}_i\rangle \equiv c(\mathbf{v}_i) \pmod{q^{e(\mathbf{v}_i)}} & \text{for all } i \in J \\ \langle \mathbf{z}, \mathbf{u}_i\rangle \not\equiv c(\mathbf{v}_i) \pmod{q^{e(\mathbf{v}_i)+1}} & \text{for all } i \in J' \\ (\mathbf{z} \bmod M) \in \mathcal{M}. \end{cases} \tag{5}$$

By the Chinese remainder theorem we replace the last condition by $\left(\mathbf{z} \bmod q^{v_q(M)}\right) \in \left(\mathcal{M} \bmod q^{v_q(M)}\right)$ without changing the solvability of the system. As $\mathbf{u}_i, i \in \mathcal{J}$ are the standard basis for $\mathbb{Q}^{|J|}$, $\mathbf{z}$ is determined modulo $q^{\min_{i\in J} e(\mathbf{v}_i)}$.

Suppose first that q is large enough (namely $q > |J'|$, $N = v_q(\tau_K) = v_q(M) = 0$, and the entries of $\mathbf{u}_i, i \in J$ are 0 or have q-adic valuation 0). Then (5) becomes

$$\begin{cases} \langle \mathbf{z}, \mathbf{u}_i \rangle \equiv 0 \pmod{q^{e(\mathbf{v}_i)}} & \text{for all } i \in J \\ \langle \mathbf{z}, \mathbf{u}_i \rangle \not\equiv 0 \pmod{q^{e(\mathbf{v}_i)+1}} & \text{for all } i \in J', \end{cases} \tag{6}$$

All congruences follow from the necessary conditions $z_i \equiv 0 \pmod{q^{e(\mathbf{v}_i)}}$ for $i \in \mathcal{J}$, and there are $q^{|\mathcal{J}|}$ values of $\mathbf{z}$ where $0 \leqslant z_i < q^{e(\mathbf{v}_i)+1}$ and $z_i \equiv 0 \pmod{q^{e(\mathbf{v}_i)}}$ for $i \in \mathcal{J}$. If for some $i \in J'$ we have $\min_{j:\mathbf{u}_{i,j}\neq 0} e(\mathbf{v}_j) \geqslant e(\mathbf{v}_i) + 1$, then the incongruence for i is not solvable, else the system is solvable, as each incongruence excludes at most $q^{|\mathcal{J}|-1}$ values. All large values of q may thus be solved at once (the $\mathbf{u}_i$'s depend on q only through the ordering of the e_i's).

For each of the finitely many remaining values of q we may check the solvability of (5) by brute force: if $v_q(M) > \max_{i\in J} e(\mathbf{v}_i)$, this is because the moduli are bounded in terms of $K, F, n, W_1, \ldots, W_n$; else, the congruences determine $(z_i \bmod q^{e(\mathbf{v}_i)})$ hence the condition on $(\mathbf{z} \bmod q^{v_q(M)})$ is either trivially satisfied or impossible, moreover the number of possible values for $(z_i \bmod q^{\max e(\mathbf{v}_i)+1})$ to be checked is at most $q^{\max e(\mathbf{v}_i)+1-\min e(\mathbf{v}_i)}$. □

Remark 5.2. Let $e_I \in \mathbb{Z}^n_{\geqslant 0}$ and consider the question whether $\mathrm{Gal}(\bar{K}/K)$ contains an automorphism whose restriction to F is in C and that for $i \in I$ it is the identity on $K(\zeta_{q^{e_i}}, W_i^{1/q^{e_i}})$ but not on $K(\zeta_{q^{e_i}}, W_i^{1/q^{e_i+1}})$.

(1) By the proof of Theorem 5.1, the answer does not depend on q for all q larger than a constant (depending on $K, F, n, W_1, \ldots, W_n$ and computable with an explicit finite procedure).

(2) By the proof of Theorem 5.1, there is a constant c (depending on $K, F, n, W_1, \ldots, W_n$ and computable with an explicit finite procedure) such that for any q the answer is not affected by changing e_I as follows: for some non-empty $J \subset I$ such that

$$d_J := \min_{j\in J} e_j - (c + \max_{i\in I\setminus J} e_i) > 0$$

we replace e_i by $e_i - d_J$ for $i \in J$.

(3) If $F = K$, then we can answer by applying the Chebotarev Density Theorem (and the inclusion-exclusion principle), computing the degrees of the given cyclotomic-Kummer extensions and of their various compositum fields.

Example 5.3. Consider $K = F = \mathbb{Q}(i)$, $C = \{\mathrm{id}_K\}$, $\alpha = 2 + i$, $\beta = 3 + 2i$, and

$$W_1 = \langle \alpha \rangle, \quad W_2 = \langle \beta \rangle, \quad W_3 = \langle \alpha\beta \rangle, \quad W_4 = \langle \alpha^2\beta \rangle .$$

By Example 7.3 for every $m \geqslant 1$ we have $[K(\zeta_\infty, \alpha^{1/m}, \beta^{1/m}) : K(\zeta_\infty)] = m^2$ hence for $h_I \in \mathbb{Z}^4_{>0}$ we have $h_I \in \mathrm{Im}\ (\Psi)$ if and only if $v_q(h_I) \in \mathrm{Im}\ (\Psi_q)$ for every q. For $q \neq 2$, $\mathrm{Im}\ (\Psi_q)$ consists of those $e_I \in \mathbb{Z}^4_{\geqslant 0}$ such that $e_1 = e_2 = e_3 = e_4$ or there is a permutation f such that $e_{f(1)} > e_{f(2)} = e_{f(3)} = e_{f(4)}$. We sketch the proof of this fact, supposing for

simplicity that e_I is non-decreasing. For any $\mathbf{x} = (x_0, x_1, x_2)$ such that $q \nmid x_0$ there exists an automorphism σ such that

$$\sigma(\zeta_{q^{e_1+1}}) = \zeta_{q^{e_1+1}}^{x_0}, \quad \sigma\left(\alpha^{1/q^{e_1+1}}\right) = \zeta_{q^{e_1+1}}^{x_1}\alpha^{1/q^{e_1+1}}, \quad \sigma\left(\beta^{1/q^{e_1+1}}\right) = \zeta_{q^{e_1+1}}^{x_2}\beta^{1/q^{e_1+1}}.$$

We now look for $\mathbf{x}$ satisfying the congruences

$$\begin{cases} x_0 \equiv 1 & \pmod{q^{e_1}} \\ x_1 \equiv 0 & \pmod{q^{e_1}} \\ x_2 \equiv 0 & \pmod{q^{e_2}} \\ x_1 + x_2 \equiv 0 & \pmod{q^{e_3}} \\ 2x_1 + x_2 \equiv 0 & \pmod{q^{e_4}} \end{cases}$$

and some incongruences, e.g. for W_4 we can have $x_0 \not\equiv 1 \pmod{q^{e_4+1}}$ or $2x_1 + x_1 \not\equiv 0 \pmod{q^{e_4+1}}$. Partitioning I into intervals regrouping the indices i with the same e_i, we get either $\{1\}, \{2,3,4\}$ or $\{1,2,3,4\}$, else there is no $\mathbf{x}$ as requested. In the former case there are solutions, as we require $x_0 \equiv 1 \pmod{q^{e_1}}, x_1 \equiv 0 \pmod{q^{e_1}}, x_2 \equiv 0 \pmod{q^{e_2}}$ and $x_2 \not\equiv 0 \pmod{q^{e_2+1}}$, and either $x_0 \not\equiv 1 \pmod{q^{e_1+1}}$ or $x_1 \not\equiv 0 \pmod{q^{e_1+1}}$. In the latter case there are solutions, as we require $x_0 \equiv 1 \pmod{q^{e_1}}, x_1 \equiv x_2 \equiv 0 \pmod{q^{e_1}}$, and either $x_0 \not\equiv 1 \pmod{q^{e_1+1}}$ (which can be satisfied for any $q \geq 3$) or $x_1, x_2, x_1 + x_2, 2x_1 + x_2 \not\equiv 0 \pmod{q^{e+1}}$ (which can be satisfied for $q > 3$).

Theorem 5.4. *There exist a positive squarefree integer Q and a positive integer Z (computable with an explicit finite procedure) such that the following holds:*

(1) For $h_I \in \mathbb{Z}_{>0}^n$, we have $h_I \in \operatorname{Im}\Psi$ if and only if $v_Q(h_I) \in \operatorname{Im}\Psi_Q$ and $v_\ell(h_I) \in \operatorname{Im}\Psi_\ell$ for all $\ell \nmid Q$.

(2) For $\ell \nmid Q$, the image of Ψ_ℓ does not depend on ℓ and it is determined by its intersection with $\{0, 1, \dots, v_\ell(Z)\}^n$. The image of Ψ_Q is determined by its intersection with $\prod_{\ell \mid Q}\{0, 1, \dots, v_\ell(Z)\}^n$.

(3) The image of Ψ is determined by its intersection with $\{1, \dots, Z\}^n$.

Proof. Let Q be the squarefree part of the constant from Proposition 3.1 (3), where we require the additional condition with F (enlarging F as in the proof of Theorem 5.1 and replacing C accordingly). Then (1) is clear, (2) is a consequence of Remark 5.2, and (3) follows. □

6 The index map for separated groups

Remark 6.1. Assume GRH, and recall Corollary 4.3. If the W_i's have separated Kummer extensions w.r.t. $x_I \in \mathbb{Z}_{>0}^n$, then for all $y_I \in \mathbb{Z}_{>0}^n$ such that $x_I \in \otimes y_I$ we have $y_I \in \operatorname{Im}(\Psi)$ if and only if there is an automorphism in

$$\operatorname{Gal}\big(K(\zeta_{\operatorname{lcm}(x_i)}, W_1^{1/x_1}, \dots, W_n^{1/x_n})/K(\zeta_{\operatorname{lcm}(y_i)}, W_1^{1/y_1}, \dots, W_n^{1/y_n})\big)$$

which, for every prime q and $i \in I$ such that $qy_i \mid x_i$, is not the identity on $K(\zeta_{qy_i}, W_i^{1/qy_i})$. If the W_i's have ℓ-separated Kummer extensions w.r.t. $x_I \in \mathbb{Z}_{\geqslant 0}^n$ and $y_I \in \mathbb{Z}_{\geqslant 0}^n$ is such that $x_I \in \oplus y_I$, then we have $y_I \in \operatorname{Im}(\Psi_\ell)$ if and only if there is an automorphism in

$$\operatorname{Gal}\big(K(\zeta_{\ell^{\max(x_i)}}, W_1^{1/\ell^{x_1}}, \dots, W_n^{1/\ell^{x_n}})/K(\zeta_{\ell^{\max(y_i)}}, W_1^{1/\ell^{y_1}}, \dots, W_n^{1/\ell^{y_n}})\big)$$

which, for every $i \in I$ such that $y_i < x_i$, is not the identity on $K(\zeta_{\ell^{y_i+1}}, W_i^{1/\ell^{y_i+1}})$.

Theorem 6.2. *Assume GRH. The following are equivalent for x_I in $\mathbb{Z}_{>0}^n$ (resp., $\mathbb{Z}_{\geqslant 0}^n$):*

(1) The W_i's have separated (resp., ℓ-separated) Kummer extensions w.r.t. x_I.

(2) We have $\otimes x_I \subset \mathrm{Im}\ (\Psi)$ (resp., $\oplus x_I \subset \mathrm{Im}\ (\Psi_\ell)$).

(3) For y_I in $\mathbb{Z}_{>0}^n$ (resp., $\mathbb{Z}_{\geqslant 0}^n$) we have y_I in $\mathrm{Im}\ (\Psi)$ (resp., in $\mathrm{Im}\ (\Psi_\ell)$) if and only if $\gcd(y_I, x_I) \in \mathrm{Im}\ (\Psi)$ (resp., $\min(y_I, x_I) \in \mathrm{Im}\ (\Psi_\ell)$).

Proof. We make use of Corollary 4.3. For $x_I \in \mathbb{Z}_{>0}^n$, it is straight-forward that (1) implies (2) and (3). Moreover, (3) implies (2) because $\mathrm{Im}\ (\Psi) \cap \otimes x_I \neq \emptyset$ (consider primes of K that split completely in $K(\zeta_{\mathrm{lcm}}(x_i), W^{1/\mathrm{lcm}(x_i)})$). If (1) does not hold, then (2) does not hold because w.l.o.g. there are positive integers N_1, N and a prime q such that $x_1 \mid N_1$, $\mathrm{lcm}(x_1, \ldots, x_n, qN_1) \mid N$ and

$$K(\zeta_N, W_1^{1/qN_1}, W_{\neq 1}^{1/N}) = K(\zeta_N, W_1^{1/N_1}, W_{\neq 1}^{1/N})$$

hence $(N_1, N, \ldots, N) \notin \mathrm{Im}\ (\Psi)$. The equivalence of the respective assertions is similar. □

Remark 6.3. To determine the image of Ψ (respectively, Ψ_ℓ) for separated groups, it suffices to compute the image of $\mathfrak{p}$ for the finitely many excluded primes (see Section 2) and, by Proposition 3.2 (3) and Theorem 6.2, apply finitely many times Remark 6.1. Moreover, $\mathrm{Im}\ (\Psi)$ is the preimage of its reduction modulo M for some positive integer M if and only if the groups are separated, see (3) and (2) for $\ell \nmid M$ of Theorem 6.2.

Now consider the index map $p \mapsto \mathrm{Ind}_p(a)$, where $a \in \mathbb{Q}^\times \setminus \{\pm 1\}$ and p varies in the rational primes such that $v_p(a) = 0$.

Proposition 6.4. *Assume GRH. Let $a \in \mathbb{Q}^\times \setminus \{\pm 1\}$, and write*

$$a = (-1)^\epsilon \left(b^2 \cdot 2^\delta \cdot T\right)^{2^d} \quad \textit{where} \quad T = \prod_{p_i \equiv 1 \pmod 4} p_i \prod_{q_j \equiv 3 \pmod 4} (-q_j)$$

where $b \in \mathbb{Q}^\times$, $d \geqslant 0$ ($d > 0$ if $\pm a$ is a square in $\mathbb{Q}^\times$), $\epsilon, \delta \in \{0, 1\}$, and p_i, q_j are distinct primes. Considering a set of primes p of density 1 such that $p \neq 2$ and $v_p(a) = 0$, the values for $\mathrm{Ind}_p(a)$ are $\mathbb{Z}_{>0}$ with the following exceptions:
- if a equals T times a square in $\mathbb{Q}^\times$, the odd multiples of T;
- if a is minus a square in $\mathbb{Q}^\times$ and $v_2(a) \equiv 2 \bmod 4$, the multiples of T congruent to 2 modulo 4;
- if $3 \mid T$ and a is a cube in $\mathbb{Q}^\times$, the multiples of $2^{\max(3\delta, d+1)}T/3$ not divisible by 3.

Proof. Call $E := \max(3\delta, d+1)$, D the largest odd integer such that a is a D-th power in $\mathbb{Q}^\times$, and $Z := 2^E \mathrm{lcm}(T, D)$. By Theorem 6.2 we only have to determine which positive divisors z of Z are values for the index map, namely whether $\mathrm{Gal}(\mathbb{Q}(\zeta_Z, a^{1/Z})/\mathbb{Q}(\zeta_z, a^{1/z}))$ contains an automorphism which for every prime q such that $qz \mid Z$ is not the identity on $\mathbb{Q}(\zeta_{qz}, a^{1/qz})$. Fixing z, and calling Q the product of such primes q, we may replace here Z by zQ. As we have $\zeta_{zq} \notin \mathbb{Q}(\zeta_{Z/q}, a^{q/Z})$ for $q > 3$, we are left to check

whether $\mathrm{Gal}(\mathbb{Q}(\zeta_{6z}, a^{1/6z})/\mathbb{Q}(\zeta_z, a^{1/z}))$ contains an automorphism which is not the identity on $\mathbb{Q}(\zeta_{2z}, a^{1/2z})$ if $2^E \nmid z$ and it is not the identity on $\mathbb{Q}(\zeta_{3z}, a^{1/3z})$ if $v_3(z) < \max(v_3(T), v_3(D))$.

Calling $v := v_2(z)$ and $V := v_3(z)$, the automorphism exists unless $v < E$ and $\mathbb{Q}(\zeta_{2z}, a^{1/2z}) = \mathbb{Q}(\zeta_z, a^{1/z})$, or $V < \max(v_3(T), v_3(D))$ and $\mathbb{Q}(\zeta_{3z}, a^{1/3z}) = \mathbb{Q}(\zeta_z, a^{1/z})$.

We determine those z such that $v < E$ and $\zeta_{2^{v+1}}, a^{1/2^{v+1}} \in \mathbb{Q}(\zeta_z, a^{1/2^v})$. If $v = 0$, then $\sqrt{a} \in \mathbb{Q}(\zeta_z)$ holds when $\epsilon = 0$ and either $d > 0$ or $d = \delta = 0$ and $T \mid z$. There is no such z with $v \geqslant 3$ because $\zeta_{16} \notin \mathbb{Q}(\zeta_{8w})$ for w odd, and neither with $v = 2$: for $\epsilon = 0$ we must have $d \leqslant 1$ to get $\sqrt{2}$ and $d \geqslant 2$ to get $\sqrt[8]{a}$; for $\epsilon = 1$ we must have $d \geqslant 2$ and we conclude because $\zeta_{16} \notin \mathbb{Q}(\zeta_{8w})$ for w odd. If $v = 1$, then we need $\epsilon = 1$ and $d \geqslant 1$ to get ζ_4; as $\zeta_8 \notin \mathbb{Q}(\zeta_{4w})$ for w odd, we also need $d = \delta = 1$ and $T \mid z$.

We determine those z such that $V < \max(v_3(T), v_3(D))$ and $\zeta_{3^{V+1}}, a^{1/3^{V+1}} \in \mathbb{Q}(\zeta_z, a^{1/z})$. We get $\zeta_{3^{V+1}}$ only if $V = 0$, and we get $a^{1/3^{V+1}}$ only if a is a cube. Finally, $\zeta_3 \in \mathbb{Q}(\zeta_z, a^{1/2^v})$ holds if and only if $v \geqslant d + 1$, $3 \mid T$, $(T/3) \mid z$, and $8 \mid z$ or $\delta = 0$. □

The strategy of the above proof should extend to a number field K known very explicitly (e.g. a quadratic field), and we could replace a by a finitely generated subgroup of $K^\times$.

Example 6.5. The index map $p \mapsto \mathrm{Ind}_p(2)$ is surjective by Proposition 6.4, and also by Theorem 6.2, as its image contains all positive divisors of 8 (consider $p = 3, 7, 113, 73$).

The image of the index map $p \mapsto \mathrm{Ind}_p(-100)$ consists of the positive integers not congruent to 10 (mod 20): these values must be excluded, as $-100 = (\sqrt{5}(1 + \zeta_4))^4$, so $10 \mid \mathrm{Ind}_p(-100)$ implies $4 \mid \mathrm{Ind}_p(-100)$.

For $a = -3$ (resp., $a = (-3)^3$) and $p \geqslant 5$ we have $3 \mid \mathrm{Ind}_p(a)$ only if (resp., if and only if) $2 \mid \mathrm{Ind}_p(a)$ because $\mathbb{Q}(\zeta_2, a^{1/2})$ is contained in (resp., equals) $\mathbb{Q}(\zeta_3, a^{1/3})$.

Remark 6.6. Over K, fix some positive integer $m \mid \tau_K$ and consider the index map $\mathfrak{p} \mapsto \mathrm{Ind}_\mathfrak{p}(\zeta_m)$ for $\mathfrak{p} \nmid mO_K$. Its image has density 0 inside $\mathbb{Z}_{>0}$ because $\mathrm{Ind}_\mathfrak{p}(\zeta_m) = (N\mathfrak{p} - 1)/m$. For $K = \mathbb{Q}$ we have $\mathrm{Ind}_2(-1) = 1$ and $\mathrm{Ind}_p(-1) = (p-1)/2$ for p odd, while for $K = \mathbb{Q}(\zeta_4)$ we have $\mathrm{Ind}_{1+\zeta_4}(\zeta_4) = 1$ and $\mathrm{Ind}_\mathfrak{p}(\zeta_4)$ is $(p-1)/2$ (resp., $(p^2-1)/2$) if $\mathfrak{p}$ lies over a prime $p \equiv 1 \bmod 4$ (resp., $p \equiv 3 \bmod 4$). These examples show that the image of the index map for one or several finite groups is easy to describe, however the description is not explicit. Thus, if we remove from the Index Map Problem the assumption that the groups have positive rank, then we may not be able to compute the image of the index map with a finite procedure, nor characterize it by its intersection with a finite subset of $\mathbb{Z}^n_{>0}$.

7 Examples of groups with surjective index map

Proposition 7.1. *If $K \neq \mathbb{Q}$, then there exist countably many multiplicatively independent $\alpha_i \in K^\times$ (for $i \in \mathbb{Z}_{>0}$) which are algebraic integers and not units, whose norms $N(\alpha_i)$ are pairwise coprime, and such that for all positive integers r, n we have*

$$[K(\zeta_\infty, \alpha_1^{1/n}, \ldots, \alpha_r^{1/n}) : K(\zeta_\infty)] = n^r \,. \tag{7}$$

Assuming GRH, for any distinct $i_1, \ldots, i_r$ the index map $\mathfrak{p} \to (\mathrm{Ind}_\mathfrak{p}(\alpha_{i_1}), \ldots, \mathrm{Ind}_\mathfrak{p}(\alpha_{i_r}))$ is surjective onto $\mathbb{Z}^r_{>0}$.

Proof. Theorem 6.2 implies the second assertion follows from (7), and it suffices to show (7) when $n = \ell$ is prime. Call z the squarefree part of 2Ω. For all $\ell \mid z$ at once we construct by induction $\alpha_{\ell,i}$ as in Lemma 7.2 and with pairwise coprime norms. The algebraic integers $\alpha_i := \prod_{\ell \mid z} \alpha_{\ell,i}^{z/\ell}$ are not units and have coprime norms. Then (7) holds for $\ell \mid z$ because any finite product $\prod_j \alpha_j^{z_j/\ell}$ is not in $K(\zeta_\infty)$ unless we have $\ell \mid z_j$ for all j. It also holds for $\ell \nmid z$ by Proposition 3.5, Remark 3.4, and [1, Theorem 18], as for every i there is some prime $\mathfrak{p}$ of K such that $\ell \nmid v_\mathfrak{p}(\alpha_i)$ and $\ell \mid v_\mathfrak{p}(\alpha_j)$ for $i \neq j$. □

Lemma 7.2. *Let $K \neq \mathbb{Q}$, fix some prime ℓ and $x > 0$, and for each $q \equiv 1 \pmod{\ell}$ let $1 \leqslant e_q \leqslant v_\ell(q-1)$ be arbitrary and let g_q be as in Proposition 3.5. There exists an algebraic integer $\alpha \in K^\times$ which is not a unit such that the following holds: $\alpha^{1/\ell} \notin K(\zeta_\infty)$; for all primes $\mathfrak{p}$ of K we have $v_\mathfrak{p}(\alpha) < \ell$; the norm $N(\alpha)$ is only divisible by primes $q > x$ not inert in K such that $q \nmid \ell\Omega$, $q \equiv 1 \bmod \ell$; for some of these q there is no $t \in \mathbb{Z}$ such that $v_\mathfrak{q}(\alpha) \equiv t v_\mathfrak{q}(g_q^{\ell^{e_q}}) \bmod \ell$ holds for all primes $\mathfrak{q}$ of K over q.*

Proof. There are infinitely many $q > x$ not inert in K such that $q \nmid \ell\Omega$, $q \equiv 1 \bmod \ell$. Considering the primes $\mathfrak{q}_j$ over q, by a counting argument there is an ideal $I_q := \prod_j \mathfrak{q}_j^{z_j}$ such that $0 \leqslant z_j < \ell$ and for no $t \in \mathbb{Z}$ we have $z_j \equiv v_{\mathfrak{q}_j}(g_q^{t\ell^{e_q}}) \bmod \ell$ for all j. Calling (α) the generator of a principal ideal of the form $\prod_{q \in S} I_q$, for $q \in S$ we have $v_{\mathfrak{q}_j}(\alpha) = z_j$ hence $\alpha^{1/\ell} \notin K(\zeta_\infty)$ by Proposition 3.5. □

Example 7.3. If $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_r)$ and α_i^2 are distinct primes greater than 3, or if $K = \mathbb{Q}(i)$ and α_i are Gaussian primes whose norms are distinct primes (see Remark 3.4), then (7) holds for every n.

Remark 7.4. We expect (7) to hold for generic elements $\alpha_1, \ldots, \alpha_r \in K^\times$. Firstly, we expect that the α_i's are strongly ℓ-independent for every prime ℓ and strongly 2-independent over $K(\zeta_4)$ (see [1]) hence $[K(\zeta_{\ell^\infty}, \alpha_1^{1/\ell^n}, \ldots, \alpha_r^{1/\ell^n}) : K(\zeta_{\ell^\infty})] = \ell^{nr}$. We are left to check that for $\ell \mid \tau_K$ and $\alpha := \prod_i \alpha_i^{z_i}$ (where $0 \leqslant z_i < \ell$ and the z_i's are not all zero) we have $\alpha^{1/\ell} \notin K(\zeta_\infty)$. If we had $\alpha^{1/\ell} \in K(\zeta_\infty)$, then $\ell \mid v_\mathfrak{p}(\alpha)$ for all primes $\mathfrak{p}$ of K over $p \nmid \tau_K$ and over $p \not\equiv 1 \bmod \ell$ (see Proposition 3.5), and there are few admissible values for the tuple $(v_\mathfrak{q}(\alpha))$, where $\mathfrak{q}$ varies over the primes of K over any fixed $q \equiv 1 \bmod \ell$ not inert in K such that $q \neq \ell\Omega$ (see the proof of Lemma 7.2). Generically, the non-zero valuations of the α_i's are (with few exceptions) 1 and concern primes of K of degree 1 lying over distinct primes q. For such q, if $z_i \neq 0$, then the tuple $(v_\mathfrak{q}(\alpha))$ for the primes $\mathfrak{q}$ over q has one non-zero entry hence $\alpha^{1/\ell} \notin K(\zeta_\infty)$ by [6, Theorem 12].

Example 7.5. If $a, b \in \mathbb{Q}^\times$, then the index map $p \mapsto (\mathrm{Ind}_p(a), \mathrm{Ind}_p(b))$ is not surjective because, considering the fraction $a = \frac{n}{d}$, the condition $4nd \mid \mathrm{Ind}_p(b)$ implies $p \equiv 1 \pmod{4|nd|}$ hence $2 \mid \mathrm{Ind}_p(a)$. Similarly, if $W_1 = \langle \frac{n_1}{d_1}, \ldots, \frac{n_r}{d_r} \rangle$, then we cannot have $2 \nmid \mathrm{Ind}_p(W_1)$ and $4n_1d_1 \cdots n_rd_r \mid \mathrm{Ind}_p(W_2)$.

Acknowledgements

We would like to thank Fritz Hörmann, Flavio Perissinotto, and Pietro Sgobba for helpful discussions. The first author was supported by the Emil Aaltonen foundation.

REFERENCES

[1] C. Debry and A. Perucca. Reductions of algebraic integers. *J. Number Theory*, 167(1):259–283, 2016.
[2] P. Erdös and M. R. Murty. On the order of a (mod p). In *CRM Proceedings and Lecture Notes*, volume 19, pages 87–97, 1999.
[3] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Q. J. Math.*, 37(1):27–38, 1986.
[4] M. Hindry and J. H. Silverman. *Diophantine Geometry*. Number 201 in Graduate Texts in Mathematics. Springer-Verlag, New York, 2000.
[5] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
[6] F. Hörmann, A. Perucca, P. Sgobba, and S. Tronto. Explicit Kummer generators for cyclotomic extensions. *JP J. Algebra, Number Theory Appl.*, 53(1):69–84, 2022.
[7] O. Järviniemi. Equality of orders of a set of integers modulo a prime. *Proc. Amer. Math. Soc.*, 149(09):3651–3668, 2021.
[8] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, 1977.
[9] H. W. Lenstra. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.*, 42:201–224, 1977.
[10] K. Matthews. A generalisation of Artin's conjecture for primitive roots. *Acta Arith.*, 29(2):113–146, 1976.
[11] P. Moree. Artin's primitive conjecture – a survey. *Integers*, 12(6):1305–1416, 2012.
[12] P. Moree and P. Stevenhagen. A two-variable Artin conjecture. *J. Number Theory*, 85(2):291–304, 2000.
[13] M. R. Murty, F. Séguin, and C. L. Stewart. A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences. *J. Number Theory*, 194:8–29, 2019.
[14] F. Pappalardi. On the r-rank Artin conjecture. *Math. Comp.*, 66(218):853–868, 1997.
[15] A. Perucca and P. Sgobba. Kummer theory for number fields and the reductions of algebraic numbers. *Int. J. Number Theory*, 15(8):1617–1633, 2019.
[16] A. Perucca, P. Sgobba, and S. Tronto. The degree of Kummer extensions of number fields. *Int. J. Number Theory*, 17(5):1091–1110, 2021.
[17] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, 54:323–401, 1981.
[18] S. Wagstaff. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.*, 2(41):141–150, 1982.
[19] J. Wójcik. On a problem in algebraic number theory. *Math. Proc. Cambridge Philos. Soc.*, 119(2):191–200, 1996.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TURKU, FI-20014 TURUN YLIOPISTO, FINLAND

Email address: olli.a.jarviniemi@utu.fi

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

Email address: antonella.perucca@uni.lu