ON THE DISTRIBUTION OF THE ORDER AND INDEX FOR THE REDUCTIONS OF ALGEBRAIC NUMBERS

PIETRO SGOBBA

ABSTRACT. Let $\alpha_1, \dots, \alpha_r$ be algebraic numbers in a number field K generating a subgroup of rank r in $K^\times$. We investigate under GRH the number of primes $\mathfrak{p}$ of K such that each of the orders of $(\alpha_i \bmod \mathfrak{p})$ lies in a given arithmetic progression associated to α_i. We also study the primes $\mathfrak{p}$ for which the index of $(\alpha_i \bmod \mathfrak{p})$ is a fixed integer or lies in a given set of integers for each i. An additional condition on the Frobenius conjugacy class of $\mathfrak{p}$ may be considered. Such results are generalizations of a theorem of Ziegler from 2006, which concerns the case $r = 1$ of this problem.

1. INTRODUCTION

Consider a number field K and finitely many algebraic numbers $\alpha_1, \dots, \alpha_r \in K^\times$ which generate a multiplicative subgroup of $K^\times$ of positive rank r. Let $\mathfrak{p}$ be a prime of K such that for each i the reduction of α_i modulo $\mathfrak{p}$ is a well-defined element of $k_\mathfrak{p}^\times$ (where $k_\mathfrak{p}$ is the residue field at $\mathfrak{p}$). We study the set of primes such that for each i the multiplicative order of $(\alpha_i \bmod \mathfrak{p})$ lies in a given arithmetic progression.

More precisely, write $\operatorname{ord}_\mathfrak{p}(\alpha_i)$ for the order of $(\alpha_i \bmod \mathfrak{p})$. We will prove under GRH the existence of the density of primes $\mathfrak{p}$ satisfying $\operatorname{ord}_\mathfrak{p}(\alpha_i) \equiv a_i \bmod d_i$ for each i, where a_i, d_i are some fixed integers. In Theorem 1 we give an asymptotic formula for the number of such primes. We also study the density of primes satisfying conditions on the index. Write $\operatorname{ind}_\mathfrak{p}(\alpha_i)$ for the index of the subgroup generated by $(\alpha_i \bmod \mathfrak{p})$ in $k_\mathfrak{p}^\times$. Notice that $\operatorname{ind}_\mathfrak{p}(\alpha_i) = (\mathrm{N}\,\mathfrak{p} - 1)/\operatorname{ord}_\mathfrak{p}(\alpha_i)$. We prove the existence of the density of primes $\mathfrak{p}$ such that $\operatorname{ind}_\mathfrak{p}(\alpha_i) = t_i$ for each i, where the t_i's are positive integers, and more generally such that $\operatorname{ind}_\mathfrak{p}(\alpha_i)$ lies in a given sequence of integers. Given a finite Galois extension of K, a condition on the conjugacy class of Frobenius automorphisms of the primes lying above $\mathfrak{p}$ may also be introduced.

These results are generalizations of Ziegler's work [10] from 2006, which concerns the case of rank 1. Moreover, in [8] the author and Perucca have generalized Ziegler's results to study the set of primes for which the order of the reduction of a finitely generated group of algebraic numbers lies in a given arithmetic progression, and in [9] they have investigated properties of the density of this set. Notice that problems of this kind have been studied in various papers by Chinen and Murata, and by Moree, see for instance [1, 6], and that they are related to Artin's Conjecture on primitive roots, see the survey [5] by Moree.

2010 *Mathematics Subject Classification.* Primary: 11R44; Secondary: 11R45, 11R18, 11R21.
Key words and phrases. Number field, reduction, multiplicative order, density, Kummer theory.

1.1. **Notation.** We make use of the following standard notation: μ is the Möbius function; φ is Eluer's totient function; ζ_n is a primitive n-th root of unity; (x, y) is the greatest common divisor of x and y, while $[x_1, \dots, x_r]$ is the least common multiple of $x_1, \dots, x_r$; if S is a set of primes of K, then $S(x)$ is the number of elements of S having norm at most x. We write $N = (n_1, \dots, n_r)$ and $T = (t_1, \dots, t_r)$ for r-dimensional multi-indices, by which we mean r-tuples of positive integers. We thus write

$$\sum_N = \sum_{n_1 \geqslant 1} \cdots \sum_{n_r \geqslant 1}$$

for the multiple series on the indices n_i, and similarly for T, as well as for finite multiple sums. We denote by $K_{N,T}$ the compositum of the fields

$$K\big(\zeta_{n_i t_i}, \alpha_i^{1/n_i t_i}\big)$$

for $i \in \{1, \dots, r\}$, namely

$$K_{N,T} = K\big(\zeta_{[n_1 t_1, \dots, n_r t_r]}, \alpha_1^{1/n_1 t_1}, \dots, \alpha_r^{1/n_r t_r}\big)\,,$$

and we similarly define $F_{N,T}$, if F is a finite extension of K. Moreover, if F/K is Galois and $\mathfrak{p}$ is a prime of K which is unramified in F, then $(\mathfrak{p}, F/K)$ denotes the conjugacy class of $\mathrm{Gal}(F/K)$ consisting of Frobenius automorphisms associated to the primes of F lying above $\mathfrak{p}$.

1.2. **Main results.** The following results are conditional under (GRH), by which we mean the extended Riemann hypothesis for the Dedekind zeta function of a number field, which allows us to use the effective Chebotarev density theorem (see for instance [10, Theorem 2]).

In the following statements we tacitly exclude the finitely many primes $\mathfrak{p}$ of K that appear in the prime factorizations of the fractional ideals generated by the α_i's, and those that ramify in a given finite Galois extension F of K.

Theorem 1. *Let F/K be a finite Galois extension, and let C be a union of conjugacy classes of $\mathrm{Gal}(F/K)$. For $1 \leqslant i \leqslant r$, let a_i and $d_i \geqslant 2$ be integers. Define the following set of primes of K:*

$$\mathcal{P} := \left\{ \mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(\alpha_i) \equiv a_i \bmod d_i \ \forall i, \ \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\}\,.$$

Assuming (GRH), we have

$$\mathcal{P}(x) = \frac{x}{\log x} \sum_T \sum_N \frac{(\prod_i \mu(n_i)) c(N,T)}{[F_{w,N,T} : K]} + O\left(\frac{x}{(\log x)^{1+\frac{1}{r+1}}} \right)\,. \tag{1}$$

where $w = w(T) := [d_1 t_1, \dots, d_r t_r]$, and $F_{w,N,T}$ denotes the compositum of the fields $F(\zeta_w)$ and $F_{N,T}$, namely

$$F_{w,N,T} = F\big(\zeta_{[d_1 t_1, \dots, d_r t_r, n_1 t_1, \dots, n_r t_r]}, \alpha_1^{1/n_1 t_1}, \dots, \alpha_r^{1/n_r t_r}\big)\,,$$

and

$$c(N,T) = \left| \left\{ \sigma \in \mathrm{Gal}(F_{w,N,T}/K) : \ \forall i \ \sigma(\zeta_{d_i t_i}) = \zeta_{d_i t_i}^{1+a_i t_i},\ \sigma|_{K_{N,T}} = \mathrm{id},\ \sigma|_F \in C \right\} \right|\,.$$

In particular, $c(N,T)$ is nonzero only if $(1+a_it_i,d_i)=1$ and $(d_i,n_i)\mid a_i$ for all $i\in\{1,\dots,r\}$. The constant implied by the O-term depends only on K, F, the α_i's and the d_i's.

Remark 2. The multiple series involved in the asymptotic formula (1) converges. This statement is a consequence of the results of Section 2: more precisely, the convergence follows by Proposition 9 and Theorem 5, and we prove this property in Corollary 12. Notice that the same remark applies to the series in the formulas (3) and (5) below (see also Corollary 11).

Theorem 3. *Let F/K be a finite Galois extension, and let C be a union of conjugacy classes of $\operatorname{Gal}(F/K)$. Let $T=(t_1,\dots,t_r)$ be an r-tuple of positive integers. Define the following set of primes of K:*

$$\mathcal{R}:=\left\{\mathfrak{p}:\operatorname{ind}_{\mathfrak{p}}(\alpha_i)=t_i\ \forall i,\ \left(\frac{\mathfrak{p}}{F/K}\right)\subseteq C\right\}. \tag{2}$$

Assuming (GRH), and supposing that $x\geqslant t_i^3$ for all i, we have

$$\mathcal{R}(x)=\frac{x}{\log x}\sum_N\frac{(\prod_i\mu(n_i))c'(N,T)}{[F_{N,T}:K]}+O\left(\frac{x}{\log^2 x}+\sum_{i=1}^r\frac{x\log\log x}{\varphi(t_i)\log^2 x}\right), \tag{3}$$

where

$$c'(N,T)=\left|\left\{\sigma\in\operatorname{Gal}(F_{N,T}/K):\ \sigma|_{K_{N,T}}=\mathrm{id},\ \sigma|_F\in C\right\}\right|. \tag{4}$$

The constant implied by the O-term depends only on K,F and the α_i's.

Notice that applying Theorem 3 with $t_i=1$ for all i and $F=K$ (which gives $c'(N,T)=1$ for all N) yields a multidimensional variant of Artin's Conjecture on primitive roots over number fields.

Theorem 4. *Let F/K be a finite Galois extension, and let C be a union of conjugacy classes of $\operatorname{Gal}(F/K)$. For $1\leqslant i\leqslant r$, let S_i be some nonempty sets of positive integers. Define the following set of primes of K:*

$$\mathcal{S}:=\left\{\mathfrak{p}:\operatorname{ind}_{\mathfrak{p}}(\alpha_i)\in S_i\ \forall i,\ \left(\frac{\mathfrak{p}}{F/K}\right)\subseteq C\right\}.$$

Assuming (GRH), we have

$$\mathcal{S}(x)=\frac{x}{\log x}\sum_{\substack{T\\ t_i\in S_i}}\sum_N\frac{(\prod_i\mu(n_i))c'(N,T)}{[F_{N,T}:K]}+O\left(\frac{x}{(\log x)^{1+\frac{1}{r+1}}}\right), \tag{5}$$

where

$$c'(N,T)=\left|\left\{\sigma\in\operatorname{Gal}(F_{N,T}/K):\ \sigma|_{K_{N,T}}=\mathrm{id},\ \sigma|_F\in C\right\}\right|.$$

The constant implied by the O-term depends only on K, F and the α_i's.

In particular, we may choose S_i to be the set of positive integers lying in an arithmetic progression, say for instance $\{k\geqslant 1: k\equiv a_i \bmod d_i\}$, with a_i and $d_i\geqslant 2$ integers.

Notice that if we take $r=1$ in Theorems 1 and 3, then we obtain the same formulas as in [10, Theorem 1, Proposition 1], respectively.

1.3. **Overview.** In order to generalize Zielger's proofs [10] to obtain Theorems 1, 3 and 4, some crucial results are needed. The first one is Theorem 5 which is an estimate for a multiple series involving the Euler's totient function φ. Section 2 is devoted to the proof of this theorem. The other two results concern Kummer extensions of number fields and are proven in Section 3. More precisely, Proposition 9 states that the failure of maximality of their degree is bounded in a strong way, whereas Proposition 13 gives an estimate for their discriminant. All these results will be used to deal with the asymptotics of the sets of primes considered in Section 1.2.

In Section 4 we prove Theorem 3, and then we use this result in Section 5 to set more general conditions on the index and achieve Theorem 4. In Section 6 we prove Theorem 1 by transforming the conditions on the order into conditions on the index and on the Frobenius conjugacy class with respect to certain finite Galois extensions, thus allowing to apply the previous results.

2. On the Euler's totient function

In this section we estimate some expressions involving the Euler's totient function. We keep the notation introduced in Section 1.1. In particular, we write $N = (n_1, \dots, n_r)$ for a multi-index (whose components are positive integers). Also we denote by $\tau(n)$ the number of positive divisors of n.

Recall the following well-known estimates:

$$\tau(n) = O\left(n^{\varepsilon}\right) \quad \forall \varepsilon > 0\,, \tag{6}$$

(see [4, Formula (2.20)]);

$$\frac{n}{\varphi(n)} = O\left(n^{\varepsilon}\right) \quad \forall \varepsilon > 0\,, \tag{7}$$

which follows by noticing that for each prime p there is a constant $c_\varepsilon > 0$ such that $(1-1/p) \geqslant c_\varepsilon / p^\varepsilon$, and we may take $c_\varepsilon = 1$ for all p sufficiently large (with respect to ε);

$$\sum_{n \leqslant x} \frac{n}{\varphi(n)} = O\left(x\right)\ , \tag{8}$$

(see for instance [4, Formula (2.32)]).

Our goal is to prove a multidimensional variant of the estimate $\sum_{n>x} \frac{1}{\varphi(n)n} = O\big(\frac{1}{x}\big)$ (see for instance [10, Lemma 7]), namely

Theorem 5[1]**.** *We have*

$$\sum_{\substack{N \\ n_1 > x}} \frac{1}{\varphi([n_1, n_2, \dots, n_r]) n_1 n_2 \cdots n_r} = O\left(\frac{1}{x}\right)\ . \tag{9}$$

Lemma 6. *Let z be a positive integer, then for every $\varepsilon > 0$ we have*

$$\sum_{n \leqslant x} (n, z) \cdot \frac{n}{\varphi(n)} = O\left(x z^{\varepsilon}\right)\ .$$

[1] This result and its proof are due to Paul Pollack, see also the acknowledgments.

Proof. We have

$$\sum_{n\leqslant x}(n,z)\cdot\frac{n}{\varphi(n)}=\sum_{d|z}\sum_{\substack{n\leqslant x\\(n,z)=d}}d\cdot\frac{n}{\varphi(n)}$$

$$\leqslant\sum_{d|z}d\cdot\sum_{m\leqslant x/d}\frac{md}{\varphi(md)}\leqslant\sum_{d|z}\frac{d^2}{\varphi(d)}\sum_{m\leqslant x/d}\frac{m}{\varphi(m)}\,.$$

Then the formula (8) yields

$$\sum_{n\leqslant x}(n,z)\cdot\frac{n}{\varphi(n)}=O\left(x\sum_{d|z}\frac{d}{\varphi(d)}\right).$$

We may then conclude by using (6) and (7) with $\varepsilon/2$ to get

$$\sum_{d|z}\frac{d}{\varphi(d)}=O\left(\tau(z)\cdot\max_{d|z}\frac{d}{\varphi(d)}\right)=O\left(z^{\varepsilon}\right)\,. \qquad \square$$

Lemma 7. *We have*

$$\sum_{\substack{N\\n_1\leqslant x}}\frac{n_1}{\varphi([n_1,\ldots,n_r])n_2\cdots n_r}=O\left(x\right)\,.$$

Proof. We may assume $r\geqslant 2$, the case $r=1$ being just (8). We will make use of the formula $\varphi(n)=n\prod_{p|n}(1-1/p)$, where p denotes a prime number. The main term of the considered series can thus be written as

$$\frac{n_1}{[n_1,\ldots,n_r]n_2\cdots n_r}\prod_{p|[n_1,\ldots,n_r]}\left(1-\frac{1}{p}\right)^{-1}\,.$$

Then, in view of the identity $[n_1,\ldots,n_r]\cdot(n_1,[n_2,\ldots,n_r])=n_1[n_2,\ldots,n_r]$, we can bound our series from above by

$$\sum_{\substack{N\\n_1\leqslant x}}\frac{(n_1,[n_2,\ldots,n_r])}{[n_2,\ldots,n_r]n_2\cdots n_r}\prod_{i=1}^{r}\prod_{p|n_i}\left(1-\frac{1}{p}\right)^{-1}$$

$$=\sum_{n_2,\ldots,n_r\geqslant 1}\frac{1}{[n_2,\ldots,n_r]n_2\cdots n_r}\prod_{i=2}^{r}\frac{n_i}{\varphi(n_i)}\cdot\sum_{n_1\leqslant x}(n_1,[n_2,\ldots,n_r])\frac{n_1}{\varphi(n_1)}\,.$$

Taking $n=n_1$, $z=[n_2,\ldots,n_r]$ and $\varepsilon=1/2$, Lemma 6 says that the inner sum is estimated by $O\left(x[n_2,\ldots,n_r]^{1/2}\right)$. Applying the obvious inequalities

$$[n_2,\ldots,n_r]\geqslant(n_2\cdots n_r)^{1/(r-1)}\geqslant(n_2\cdots n_r)^{1/r}\,,$$

we can then estimate the series by

$$
\begin{aligned}
&O\left(x\sum_{n_2,\ldots,n_r\geqslant 1}\frac{1}{(n_2\cdots n_r)^{1+1/2r}}\cdot\prod_{i=2}^{r}\frac{n_i}{\varphi(n_i)}\right)\\
&=O\left(x\sum_{n_2,\ldots,n_r\geqslant 1}\frac{1}{(n_2\cdots n_r)^{1+1/4r}}\right)\\
&=O\left(x\left(\zeta\Big(1+\frac{1}{4r}\Big)\right)^{r-1}\right)=O\left(x\right)\ ,
\end{aligned}
$$

where in the first equality we used the estimates $\frac{n_i}{\varphi(n_i)}=O(n_i^{1/4r})$ in view of (7), and for the last equality we used the fact that the Riemann zeta function ζ is convergent at $(1+1/4r)$. □

We are now ready to prove Theorem 5.

Proof of Theorem 5. We may assume $r\geqslant 2$. We decompose the series considered in (9) into the sums over n_1 lying in dyadic intervals, i.e. we express it as

$$
\sum_{j\geqslant 0}\ \sum_{\substack{N\\ 2^jx<n_1\leqslant 2^{j+1}x}}\frac{1}{\varphi([n_1,\ldots,n_r])n_1\cdots n_r}\ . \tag{10}
$$

We now estimate each inner series on the multi-indices N in (10). For $j\geqslant 0$, each of them equals

$$
\begin{aligned}
&\sum_{2^jx<n_1\leqslant 2^{j+1}x}\frac{1}{n_1^2}\sum_{n_2,\ldots,n_r\geqslant 1}\frac{n_1}{\varphi([n_1,\ldots,n_r])n_2\cdots n_r}\\
&\leqslant\frac{1}{(2^jx)^2}\cdot\sum_{\substack{N\\ n_1\leqslant 2^{j+1}x}}\frac{n_1}{\varphi([n_1,\ldots,n_r])n_2\cdots n_r}\\
&=O\left(\frac{1}{(2^jx)^2}\cdot 2^{j+1}x\right)=O\left(\frac{1}{2^jx}\right)\ ,
\end{aligned}
$$

where the estimate is due to Lemma 7. Finally, we conclude by summing the obtained error terms over j, so that (10) equals $O\left(1/x\right)$. □

The following result is an immediate consequence of Theorem 5.

Corollary 8. *Let* $x_1,\ldots,x_r\geqslant 1$. *Then we have*

$$
\sum_{\substack{N\\ n_i>x_i}}\frac{1}{\varphi([n_1,n_2,\ldots,n_r])n_1n_2\cdots n_r}=O\left(\frac{1}{\max_i(x_i)}\right)\ .
$$

Proof. Up to swapping the variables, we may suppose that $x_1=\max_i(x_i)$ and apply Theorem 5. □

3. Kummer theory for number fields

Let K be a number field, and let $\alpha_1,\dots,\alpha_r$ be algebraic numbers which generate a multiplicative subgroup G of $K^\times$ of positive rank r. Notice that G is torsion-free. In this section we prove some results about cyclotomic-Kummer extensions of K of the type $K(\zeta_n,\alpha_1^{1/t_1},\dots,\alpha_r^{1/t_r})$ with $t_i\mid n$ for all i.

3.1. Bounded failure of maximality for Kummer degrees.

In [8, Theorem 3.1] Perucca and the author showed, with a direct proof, that the failure of maximality of Kummer degrees of the type $[K(\zeta_m,G^{1/n}):K(\zeta_m)]$, with $n\mid m$, is bounded in a strong way. The following result is a further generalization and a consequence of this fact.

Proposition 9. *There exists an integer $B\geqslant 1$, which depends only on K and the α_i's, such that for all positive integers $n,t_1,\dots,t_r$, where n is a common multiple of the t_i's, we have*

$$\frac{\prod_{i=1}^r t_i}{\big[K\big(\zeta_n,\alpha_1^{1/t_1},\dots,\alpha_r^{1/t_r}\big):K(\zeta_n)\big]}\mid B\,. \tag{11}$$

Proof. Let $n,t_1,\dots,t_r$ be arbitrary with $t:=[t_1,\dots,t_r]\mid n$. Then by [8, Theorem 3.1] there is $B\geqslant 1$ (depending only on K and the α_i's) such that

$$\frac{t^r}{\big[K\big(\zeta_n,\alpha_1^{1/t},\dots,\alpha_r^{1/t}\big):K(\zeta_n)\big]}\mid B\,. \tag{12}$$

We show that this bound B satisfies also (11). We have

$$K\big(\zeta_n,\alpha_1^{1/t_1},\dots,\alpha_r^{1/t_r}\big)\subseteq K\big(\zeta_n,\alpha_1^{1/t},\dots,\alpha_r^{1/t}\big)$$

and the degree of this extension divides $t^r/\prod_i t_i$ as $\alpha_i^{1/t}=(\alpha_i^{1/t_i})^{t_i/t}$ (up to a t-th root of unity) for every i. We deduce that the ratio in (11) is a divisor of the ratio in (12), and hence it divides B. □

Notice that the bound B considered in the proof is not optimal in general, but it is suitable for our purposes.

Corollary 10. *For all positive integers $n,t_1,\dots,t_r$, where n is a common multiple of the t_i's, we have*

$$\big[K\big(\zeta_n,\alpha_1^{1/t_1},\dots,\alpha_r^{1/t_r}\big):K\big]\geqslant\frac{\varphi(n)\prod_i t_i}{[K:\mathbb{Q}]B}\,,$$

where $B\geqslant 1$ is the integer from Proposition 9 associated to K and the α_i's.

Proof. By (11) the degree of the considered Kummer extension over $K(\zeta_n)$ is at least $\prod_i t_i/B$, whereas it is easy to see that $[K(\zeta_n):K]\geqslant\varphi(n)/[K:\mathbb{Q}]$. □

Recall the notation for the fields $K_{N,T}$ and $K_{w,N,T}$ from Section 1.1 and Theorem 1, where N,T are r-tuples of positive integers and $w=w(T):=[d_1t_1,\dots,d_rt_r]$ for some positive integers $d_1,\dots,d_r$.

Corollary 11. *Fix an r-tuple T. The series $\sum_N\frac{1}{[K_{N,T}:K]}$ converges.*

In particular, the series of this type, which we will consider in the later sections, converge absolutely and $\sum_N = \sum_{n_1\geqslant 1}\cdots\sum_{n_r\geqslant 1}$ can be interpreted as the series over the multi-indices N.

Proof. By Corollary 10 we can bound

$$\frac{1}{[K_{N,T}:K]} \leqslant \frac{[K:\mathbb{Q}]B}{\varphi([n_1,\ldots,n_r])n_1\cdots n_r}\,.$$

Then the convergence follows by Theorem 5. □

Corollary 12. *The series* $\sum_T\sum_N \frac{1}{[K_{w,N,T}:K]}$ *converges.*

In particular, the series of this type, which we will consider in the later sections, converge absolutely and $\sum_T\sum_N = \sum_{t_1\geqslant 1}\cdots\sum_{t_r\geqslant 1}\sum_{n_1\geqslant 1}\cdots\sum_{n_r\geqslant 1}$ can be interpreted as the series over the multi-indices T and N.

Proof. Since the degree $[K_{N,T}:K]$ divides $[K_{w,N,T}:K]$ and $[n_1t_1,\ldots,n_rt_r]$ is divisible by $[n_1,t_1,\ldots,n_r,t_r]$, applying Corollary 10 we can bound

$$\frac{1}{[K_{w,N,T}:K]} \leqslant \frac{1}{[K_{N,T}:K]} \leqslant \frac{[K:\mathbb{Q}]B}{\varphi([n_1,t_1,\ldots,n_r,t_r])n_1t_1\cdots n_rt_r}\,.$$

The convergence follows again by Theorem 5. □

3.2. **Estimates for the discriminant.** We now prove an estimate for the discriminant of a cyclotomic-Kummer extension of the type $K(\zeta_n,\alpha_1^{1/t_1},\ldots,\alpha_r^{1/t_r})$. In fact, we give a variant of [8, Theorem 4.2].

We write $\mathcal{O}_K$ for the ring of integers of K. If L/K is a finite extension of number fields, we denote by $\mathrm{N}_{L/K}$ the relative norm for fractional ideals of L, by $d_{L/K}$ the relative discriminant, and by d_K the absolute discriminant of K. We will make use of the following relation for the relative discriminants of a tower of number fields $K''/K'/K$ (see for instance [7, Ch. III, Corollary 2.10]):

$$d_{K''/K} = \mathrm{N}_{K'/K}(d_{K''/K'})\cdot d_{K'/K}^{[K'':K']}\,. \tag{13}$$

Proposition 13. *Let K be a number field, and let $\gamma_1,\ldots,\gamma_r\in K^\times$ be algebraic numbers which are not roots of unity. Let $t_1,\ldots,t_r$ be positive integers and let n be a common multiple of the t_i's. Setting $F:=K(\zeta_n,\gamma_1^{1/t_1},\ldots,\gamma_r^{1/t_r})$, we have*

$$\frac{\log|d_F|}{\varphi(n)\prod_i t_i} \leqslant [K:\mathbb{Q}]\cdot\log\Big(n\prod_i t_i\Big)+O(1)\,.$$

For $1\leqslant i\leqslant r$, write $\gamma_i=\alpha_i/\beta_i$ with $\alpha_i,\beta_i\in\mathcal{O}_K$. Then the constant implied by the O-term can be taken to be

$$\log|d_K| + 2\sum_{i=1}^r \log\left|\mathrm{N}_{K/\mathbb{Q}}(\alpha_i\beta_i)\right|\,.$$

Proof. Set $t := \prod_{i=1}^{r} t_i$, and for $1 \leqslant i \leqslant r$, write L_i for the extension of K generated by some fixed root $\sqrt[t_i]{\gamma_i}$. We first estimate the relative discriminant $d_{F/K}$. The field F is the compositum of $K(\zeta_n)$ and the fields L_i, so that in view of [8, Lemma 4.1(3)] and the inequalities $[F : K(\zeta_n)] \leqslant t$ and $[F : L_i] \leqslant \varphi(n)t/t_i$ for all i, we have

$$d_{F/K} \mid (d_{K(\zeta_n)/K})^t \cdot \prod_{i=1}^{r} (d_{L_i/K})^{\varphi(n)t/t_i} . \tag{14}$$

As for the relative discriminants of the extensions $K(\zeta_n)/K$ and L_i/K we have the following estimates:

$$d_{K(\zeta_n)/K} \mid n^{\varphi(n)} \mathcal{O}_K \quad \text{and} \quad d_{L_i/K} \mid (\alpha_i\beta_i)^{2t_i} t_i^{t_i} \mathcal{O}_K ,$$

(see the proof of [8, Theorem 4.2], formulas (4.5) and (4.6), respectively). Combining these two divisibilities with (14) we obtain

$$d_{F/K} \mid \left(n^{\varphi(n)t} \cdot \prod_{i=1}^{r} \left((\alpha_i\beta_i)^{2t_i} t_i^{t_i} \right)^{\varphi(n)t/t_i} \right) \mathcal{O}_K = \left((nt)^{\varphi(n)t} \cdot A^{2\varphi(n)t} \right) \mathcal{O}_K , \tag{15}$$

where we set $A := \prod_{i=1}^{r} \alpha_i\beta_i$. In view of the identity (13), we have the following formula for the absolute discriminant of F:

$$|d_F| = \left| \mathrm{N}_{K/\mathbb{Q}}(d_{F/K}) \right| |d_K|^{[F:K]} ,$$

where $|I|$ denotes the nonnegative generator of the $\mathbb{Z}$-ideal I. Hence, using (15) we can bound $\log |d_F|$ from above with the sum of the following terms

$$\begin{aligned} \log \left| \mathrm{N}_{K/\mathbb{Q}}((nt)^{\varphi(n)t}\mathcal{O}_K) \right| &= \varphi(n)t \cdot [K : \mathbb{Q}] \cdot \log(nt) \\ \log \left| \mathrm{N}_{K/\mathbb{Q}}(A^{2\varphi(n)t}\mathcal{O}_K) \right| &= \varphi(n)t \cdot 2\log \left| \mathrm{N}_{K/\mathbb{Q}}(A) \right| \\ \log |d_K|^{[F:K]} &\leqslant \varphi(n)t \cdot \log |d_K| . \end{aligned}$$

We deduce

$$\frac{\log |d_F|}{\varphi(n)t} \leqslant [K : \mathbb{Q}] \log(nt) + \log |d_K| + 2\log \left| \mathrm{N}_{K/\mathbb{Q}}(A) \right| . \qquad \square$$

4. The asymptotic formula for the index

The aim of this section is proving Theorem 3 with the method of [10, Section 3]. We keep the notation of the introduction and, in particular, of Theorem 3. Recall that $N = (n_1, \ldots, n_r)$ and $T = (t_1, \ldots, t_r)$ are multi-indices (whose components are positive integers).

Notice that throughout Sections 4-6 we may assume $r \geqslant 2$, as the case $r = 1$ was proven in [10]. Yet all our arguments also work for $r = 1$. Moreover, from now on we say that a prime $\mathfrak{p}$ of K is of *degree* 1 if it has ramification index and residue class degree over $\mathbb{Q}$ equal to 1. When necessary, thanks to [10, Lemma 1] we will estimate the number of primes of K which are not of degree 1 by the error term $O\left(\sqrt{x}/\log x\right)$.

Remark 14. The defining conditions of the set $\mathcal{R}$ (see (2)), namely $\mathrm{ind}_{\mathfrak{p}}(\alpha_i) = t_i$, are equivalent to: $t_i \mid \mathrm{ind}_{\mathfrak{p}}(\alpha_i)$ and $qt_i \nmid \mathrm{ind}_{\mathfrak{p}}(\alpha_i)$ for every prime q. With finitely many applications of the inclusion-exclusion principle, we get:

$$\mathcal{R}(x)=\sum_N\left(\prod_{i=1}^r\mu(n_i)\right)\cdot\left|\left\{\mathfrak{p}:\mathrm{N}\,\mathfrak{p}\leqslant x,\,\forall i\ n_it_i\mid \mathrm{ind}_{\mathfrak{p}}(\alpha_i),\,\left(\frac{\mathfrak{p}}{F/K}\right)\subseteq C\right\}\right|\,.$$

If $\mathfrak{p}$ is of degree 1, then by [10, Lemma 2] the condition $n_it_i\mid\mathrm{ind}_{\mathfrak{p}}(\alpha_i)$ holds if and only if $\mathfrak{p}$ splits completely in $K(\zeta_{n_it_i},\alpha_i^{1/n_it_i})$. Moreover, $\mathfrak{p}$ splits completely in each of these fields, for $1\leqslant i\leqslant r$, if and only if it splits completely in their compositum. Hence we can write $\mathcal{R}(x)$ as

$$\sum_N\left(\prod_{i=1}^r\mu(n_i)\right)\cdot\left|\left\{\mathfrak{p}:\mathrm{N}\,\mathfrak{p}\leqslant x,\,\left(\frac{\mathfrak{p}}{K_{N,T}/K}\right)=\mathrm{id},\,\left(\frac{\mathfrak{p}}{F/K}\right)\subseteq C\right\}\right|+O\left(\frac{\sqrt{x}}{\log x}\right).$$

For real numbers $\xi,\eta\geqslant 1$, fix an r-tuple T and define the sets

$$\mathcal{M}_\xi:=\left\{\mathfrak{p}:\forall i\ t_i\mid\mathrm{ind}_{\mathfrak{p}}(\alpha_i)\ \text{ and }\ t_iq\nmid\mathrm{ind}_{\mathfrak{p}}(\alpha_i)\,\forall q<\xi\text{ prime},\,\left(\frac{\mathfrak{p}}{F/K}\right)\subseteq C\right\},$$

$$\mathcal{M}_{\xi,\eta}:=\left\{\mathfrak{p}:t_iq\mid\mathrm{ind}_{\mathfrak{p}}(\alpha_i)\text{ for some }i\text{ and some }\xi\leqslant q<\eta\text{ prime},\,\left(\frac{\mathfrak{p}}{F/K}\right)\subseteq C\right\}$$

(where we tacitly exclude the finitely many primes $\mathfrak{p}$ of K appearing in the factorization of the α_i's or ramifying in F).

Since for $\mathfrak{p}$ with $\mathrm{N}\,\mathfrak{p}\leqslant x$ we have $\mathrm{ind}_{\mathfrak{p}}(\alpha_i)\mid\mathrm{N}\,\mathfrak{p}-1<\lfloor x\rfloor$, it is clear that we have

$$\mathcal{R}(x)=\mathcal{M}_{\lfloor x\rfloor}(x)\,.$$

Setting $\xi:=\frac{1}{6r}\log x$ and $\eta:=\lfloor x\rfloor$, we have $\mathcal{M}_\eta(x)\leqslant\mathcal{M}_\xi(x)$. On the other hand, $\mathcal{M}_\eta(x)$ can be obtained by subtracting from $\mathcal{M}_\xi(x)$ the number of those primes $\mathfrak{p}$ satisfying $t_iq\nmid\mathrm{ind}_{\mathfrak{p}}(\alpha_i)$ for all i and for all prime numbers $q<\xi$ but with $t_iq\mid\mathrm{ind}_{\mathfrak{p}}(\alpha_i)$ for some i and some prime $\xi\leqslant q<\eta$, so that

$$\mathcal{M}_\eta(x)\geqslant\mathcal{M}_\xi(x)-\mathcal{M}_{\xi,\eta}(x)\,.$$

Therefore we get

$$\mathcal{R}(x)=\mathcal{M}_\xi(x)+O\big(\mathcal{M}_{\xi,\eta}(x)\big)\,. \tag{16}$$

First we estimate the main term $\mathcal{M}_\xi(x)$.

Lemma 15. *Assume (GRH). Let $x\geqslant t_i^3$ for all i. Then we have*

$$\mathcal{M}_\xi(x)=\frac{x}{\log x}\sum_N\frac{(\prod_i\mu(n_i))c'(N,T)}{[F_{N,T}:K]}+O\left(\frac{x}{\log^2 x}\right),$$

where $c'(N,T)$ is defined in (4).

Notice that by definition, the coefficients $c'(N,T)$ are bounded by the size of C and hence by $[F:K]$, independently of N,T.

Proof. Denote by E the set of the positive squarefree integers which can be written as a product of primes q with $q < \xi$. Applying the inclusion-exclusion principle as in Remark 14 yields

$$\mathcal{M}_\xi(x) = \sum_{\substack{N \\ n_i \in E}} \left(\prod_{i=1}^{r} \mu(n_i) \right) \cdot \left| \left\{ \mathfrak{p} : \mathrm{N}\,\mathfrak{p} \leqslant x, \left(\frac{\mathfrak{p}}{F_{N,T}/K} \right) \subseteq C_{N,T} \right\} \right| + O\left(\frac{\sqrt{x}}{\log x} \right),$$

where $C_{N,T}$ is defined by

$$C_{N,T} = \left\{ \sigma \in \mathrm{Gal}(F_{N,T}/K) : \sigma|_{K_{N,T}} = \mathrm{id}, \sigma|_F \in C \right\}$$

and has size $c'(N,T)$ (see (4)).

Since we are assuming (GRH), by the effective Chebotarev Density Theorem (see for instance [10, Theorem 2]) the number of primes $\mathfrak{p}$ of K which are unramified in $F_{N,T}$ and such that $\mathrm{N}\,\mathfrak{p} \leqslant x$ and the Frobenius conjugacy class of $\mathfrak{p}$ is contained in $C_{N,T}$ is given by (recalling that $c'(N,T) \leqslant [F : K]$)

$$\mathrm{Li}(x) \frac{c'(N,T)}{[F_{N,T} : K]} + O\left(\frac{\sqrt{x} \log\left(x^{[F_{N,T}:\mathbb{Q}]} \cdot \left| d_{F_{N,T}} \right| \right)}{[F_{N,T} : K]} \right),$$

where $d_{F_{N,T}}$ is the absolute discriminant of $F_{N,T}$. Then we write $\mathcal{M}_\xi(x)$ as the multiple sum

$$\mathrm{Li}(x) \sum_{\substack{N \\ n_i \in E}} \frac{(\prod_i \mu(n_i)) c'(N,T)}{[F_{N,T} : K]} + O\left(\sum_{\substack{N \\ n_i \in E}} \frac{\sqrt{x} \log\left(x^{[F_{N,T}:\mathbb{Q}]} \cdot \left| d_{F_{N,T}} \right| \right)}{[F_{N,T} : K]} \right). \tag{17}$$

We can decompose the O-term in two parts, the first one being

$$O\left(\sqrt{x} \log x \cdot \sum_{\substack{N \\ n_i \in E}} 1 \right) = O\left(\sqrt{x} \log x \, |E|^r \right) = O\left(x^{2/3} \log x \right),$$

as we have $|E| \leqslant 2^{\pi(\xi)} \leqslant e^\xi = x^{1/6r}$, where π is the prime counting function. In particular, this shows that the error term in (17) includes $O\left(\sqrt{x} / \log x \right)$.

As for the second part of the O-term, applying Corollary 10 first and then Proposition 13, we obtain

$$\begin{aligned}
&O\left(\sqrt{x}\sum_{\substack{N\\ n_i\in E}}\frac{\log\left|d_{F_{N,T}}\right|}{\varphi([n_1t_1,\dots,n_rt_r])n_1t_1\cdots n_rt_r}\right)\\
&=O\left(\sqrt{x}\sum_{\substack{N\\ n_i\in E}}\Big(\log([n_1t_1,\dots,n_rt_r]n_1t_1\cdots n_rt_r)+O\left(1\right)\Big)\right)\\
&=O\left(\sqrt{x}\cdot 2\sum_{\substack{N\\ n_i\in E}}\left(\sum_{j=1}^{r}\log n_j\right)+\sqrt{x}\cdot 2\sum_{\substack{N\\ n_i\in E}}\left(\sum_{j=1}^{r}\log t_j\right)\right)\\
&=O\left(\sqrt{x}\left|E\right|^{r-1}\cdot\sum_{k\in E}\log k\right)+O\left(\sqrt{x}\left|E\right|^{r}\cdot\log\left(\max_i(t_i)\right)\right).
\end{aligned}$$

By assumption we have $\log t_i=O\left(\log x\right)$ for all i, whereas since the largest integer in E is $\prod_{q<\xi}q$, where q runs through rational primes, we have

$$\sum_{k\in E}\log k\leqslant|E|\cdot\sum_{q<\xi}\log q\leqslant|E|\cdot\xi\leqslant x^{1/6r}\log x,$$

where the second inequality follows by [3, Theorem 415], and the last one by recalling that $|E|\leqslant x^{1/6r}$ and $\xi\leqslant\log x$. Thus, making use of these estimates, also these error terms are reduced to $O\left(x^{2/3}\log x\right)$.

We now focus on the main term of (17) and we will estimate the tail of the series as

$$\left|\sum_{\substack{N\\ n_i\notin E\text{ for some }i}}\frac{\prod_i\mu(n_i)c'(N,T)}{[F_{N,T}:K]}\right|\leqslant\sum_{\substack{N\\ n_i\notin E'\text{ for some }i}}\frac{c'(N,T)}{[F_{N,T}:K]},$$

where E' is the set of all positive integers whose prime factors q satisfy $q<\xi$. Then we bound the latter series of nonnegative terms by

$$\left(\sum_{\substack{N\\ n_1\notin E'}}+\dots+\sum_{\substack{N\\ n_r\notin E'}}\right)\frac{c'(N,T)}{[F_{N,T}:K]}\leqslant\left(\sum_{\substack{N\\ n_1\geqslant\xi}}+\dots+\sum_{\substack{N\\ n_r\geqslant\xi}}\right)\frac{c'(N,T)}{[F_{N,T}:K]}.$$

Since $c'(N,T)\leqslant[F:K]$, applying Corollary 10 and Theorem 5, we can estimate each series by $O\left(1/\xi\right)=O\left(1/\log x\right)$. Using that $\mathrm{Li}(x)=O\left(x/\log x\right)$ and summing up all the errors, we obtain $O(x/\log^2 x)$. Finally, because of the formula $\mathrm{Li}(x)=x/\log x+O(x/\log^2 x)$, we can replace $\mathrm{Li}(x)$ with $x/\log x$ in the the main term of $\mathcal{M}_\xi(x)$ as the multiple series converges by Corollary 11. □

Let us now focus on the error term of (16).

Lemma 16. *Assume (GRH). Let $x \geqslant t_i^3$ for all i. Then we have*

$$\mathcal{M}_{\xi,\eta}(x) = O\left(\frac{x}{\log^2 x}\right) + O\left(\frac{x \log\log x}{\log^2 x} \sum_{i=1}^{r} \frac{1}{\varphi(t_i)}\right) .$$

Proof. We can bound $\mathcal{M}_{\xi,\eta}(x)$ by

$$\sum_{i=1}^{r} \left| \left\{ \mathfrak{p} : \mathrm{N}\,\mathfrak{p} \leqslant x,\, t_i q \mid \mathrm{ind}_{\mathfrak{p}}(\alpha_i) \text{ for some prime } \xi \leqslant q < \eta,\, \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\} \right| ,$$

and we can conclude directly because each of these terms can be bounded by the sum of three errors (see [10, page 73]) which are estimated in [10, Lemmas 9, 10, 11]. Notice that our different value for ξ does not change the proof of [10, Lemma 11], whereas [10, Lemmas 9, 10] do not depend on ξ.

Moreover, it is straightforward to see that these Lemmas hold also for algebraic numbers (see also [8, Proof of Proposition 5.1]). In fact, in [10, Proof of Lemma 9], if $\alpha = \beta/\gamma$ with $\beta, \gamma \in \mathcal{O}_K$, then the congruence $\alpha^{(\mathrm{N}\,\mathfrak{p}-1)/tq} \equiv 1 \bmod \mathfrak{p}$ yields the inclusion of integral ideals $\mathfrak{p} \supseteq (\beta^{(\mathrm{N}\,\mathfrak{p}-1)/tq} - \gamma^{(\mathrm{N}\,\mathfrak{p}-1)/tq})$, and then proceeding with the original proof we set A to be the maximum of $\{1\} \cup \{|\sigma(\beta)|, |\sigma(\gamma)| : \sigma \in \mathrm{Gal}(K/\mathbb{Q})\}$. □

Proof of Theorem 3. The statement follows by invoking formula (16) and applying Lemmas 15 and 16. □

5. Setting conditions on the index

In this section we prove Theorem 4, keeping the notation of the introduction. The following result is a variant of [10, Lemma 13].

Lemma 17. *Assume (GRH). Let γ be a nonzero algebraic number of K which is not a root of unity. Let $0 < \rho < 1$. We have that*

$$|\{\mathfrak{p} : \mathrm{N}\,\mathfrak{p} \leqslant x,\, \mathrm{ind}_{\mathfrak{p}}(\gamma) > (\log x)^{\rho}\}| = O\left(\frac{x}{(\log x)^{1+\rho}}\right) + O\left(\frac{x}{(\log x)^{2-\rho}}\right) .$$

Notice that we are discarding the finitely many primes $\mathfrak{p}$ of K appearing in the factorization of γ.

Proof. We only point out the modification with respect to the proof of [10, Lemma 13] (where $\rho = 1/2$). Let $y := \lfloor (\log x)^{\rho} \rfloor$. Following the original proof, the error terms that we obtain are:

$$O\left(\frac{xy}{\log^2 x}\right) = O\left(\frac{x}{(\log x)^{2-\rho}}\right)$$

$$O\left(\frac{x}{y \log x}\right) = O\left(\frac{x}{(\log x)^{1+\rho}}\right) .$$

Notice that $O\left(\sqrt{x}/\log x\right)$ is included in these error terms. □

Proof of Theorem 4. We take $0 < \rho \leqslant 1/2$, so that the set considered in the previous Lemma has size $O(x/(\log x)^{1+\rho})$. Write $y := (\log x)^\rho$, and write $\mathcal{R}_T$ for the set $\mathcal{R}$ in (2) to make the dependence on the r-tuple T explicit. Then we can partition the set $\mathcal{S}$ as the disjoint union of all sets $\mathcal{R}_T$ with $t_i \in S_i$ for all i. We have

$$\sum_{\substack{T \\ t_i \in S_i}} \mathcal{R}_T(x) - \sum_{\substack{T \\ t_i \leqslant y,\, t_i \in S_i}} \mathcal{R}_T(x) \leqslant \sum_{\substack{T \\ t_1 > y}} \mathcal{R}_T(x) + \ldots + \sum_{\substack{T \\ t_r > y}} \mathcal{R}_T(x)\,. \tag{18}$$

Applying Lemma 17, each multiple series on the right-hand side can be bounded by

$$|\{\mathfrak{p} : \mathrm{N}\,\mathfrak{p} \leqslant x,\ \mathrm{ind}_\mathfrak{p}(\alpha_i) > y\}| = O\left(\frac{x}{(\log x)^{1+\rho}}\right)\,,$$

respectively. This yields the formula

$$\mathcal{S}(x) = \sum_{\substack{T \\ t_i \leqslant y,\, t_i \in S_i}} \mathcal{R}_T(x) + O\left(\frac{x}{(\log x)^{1+\rho}}\right)\,. \tag{19}$$

We now replace the asymptotic (3) for the functions $\mathcal{R}_T(x)$ in (19), as $x > y^3$. Let us first focus on the main term that we obtain, namely

$$\frac{x}{\log x} \sum_{\substack{T \\ t_i \leqslant y,\, t_i \in S_i}} \sum_N \frac{(\prod_i \mu(n_i))c'(N,T)}{[F_{N,T} : K]}\,. \tag{20}$$

Call D_T the (inner) multiple series on the multi-indices N appearing in (20) and notice that $D_T \geqslant 0$. Similarly to (18), we have

$$\sum_{\substack{T \\ t_i \in S_i}} D_T - \sum_{\substack{T \\ t_i \leqslant y,\, t_i \in S_i}} D_T \leqslant \sum_{\substack{T \\ t_1 > y}} D_T + \ldots + \sum_{\substack{T \\ t_r > y}} D_T\,. \tag{21}$$

Since $[n_1 t_1, \ldots, t_r n_r]$ is a multiple of $[t_1, n_1, \ldots, t_r, n_r]$, applying Corollary 10 we have

$$\frac{1}{[F_{N,T} : F]} \leqslant \frac{B[F : \mathbb{Q}]}{\varphi([t_1, n_1, \ldots, t_r, n_r]) t_1 n_1 \cdots t_r n_r}\,,$$

and hence by Theorem 5 each series on the right-hand side of (21), multiplied by $x/\log x$, has size (recalling $c'(N,T) \leqslant [F : K]$)

$$O\left(\frac{x}{y \log x}\right) = O\left(\frac{x}{(\log x)^{1+\rho}}\right)\,.$$

Next we study the error terms that we obtain when replacing $\mathcal{R}_T(x)$ in (19). The first part of the O-term of (3) gives

$$O\left(\frac{xy^r}{\log^2 x}\right) = O\left(\frac{x}{(\log x)^{2-\rho r}}\right)\,,$$

where we suppose that ρ satisfies $2 - \rho r > 0$. Recall the formula $\sum_{k<y} 1/\varphi(k) = O(\log y)$ (see for instance [10, Lemma 8]). Then, for each $j \in \{1, \ldots, r\}$, the second part of the O-term

of (3) yields the sum of errors

$$O\left(\frac{x\log\log x}{\log^2 x}\sum_{\substack{T\\ t_i\leqslant y}}\frac{1}{\varphi(t_j)}\right)=O\left(\frac{x\log\log x}{\log^2 x}\cdot y^{r-1}\log y\right)$$

$$=O\left(\frac{x(\log\log x)^2}{(\log x)^{2-\rho(r-1)}}\right)=O\left(\frac{x}{(\log x)^a}\frac{(\log\log x)^2}{(\log x)^b}\right)$$

where we take $a,b>0$ such that $a+b=2-\rho(r-1)$. Note that b can be chosen arbitrarily small, because $(\log\log x)^2/(\log x)^b$ tends to zero as $x\to\infty$ for any $b>0$. Therefore, for $j\in\{1,\dots,r\}$, this error term becomes $O(x/(\log x)^a)$ for some $0<a<2-\rho(r-1)$ and thus can be included in $O(x/(\log x)^{2-\rho r})$.

It remains to choose a suitable value for ρ. In the O-terms we have the exponents $1+\rho$ and $2-\rho r$. A possible choice is $\rho=1/(r+1)$, yielding the error term

$$O\left(\frac{x}{(\log x)^{1+\frac{1}{r+1}}}\right).$$

This concludes the proof. □

6. The asymptotic formula for the order

In this section we obtain an asymptotic formula for the function $\mathcal{P}(x)$ of Theorem 1 by expressing it as a sum of functions of the type $\mathcal{R}(x)$. Let us keep the notation of the introduction.

Let $\mathfrak{p}\in\mathcal{P}$ be of degree 1, and call p the rational prime below $\mathfrak{p}$. Because of the identity $\operatorname{ord}_{\mathfrak{p}}(\alpha_i)\cdot\operatorname{ind}_{\mathfrak{p}}(\alpha_i)=\mathrm{N}\,\mathfrak{p}-1$, the condition $\operatorname{ord}_{\mathfrak{p}}(\alpha_i)\equiv a_i \bmod d_i$ is equivalent to $\operatorname{ind}_{\mathfrak{p}}(\alpha_i)=t_i$ and $p\equiv 1+a_it_i \bmod d_it_i$. We define the sets of primes of K satisfying these conditions by setting

$$\mathcal{V}_T:=\left\{\mathfrak{p}:\forall i\ \operatorname{ind}_{\mathfrak{p}}(\alpha_i)=t_i,\ p\equiv 1+a_it_i \bmod d_it_i,\ \left(\frac{\mathfrak{p}}{F/K}\right)\subseteq C\right\}.$$

Notice that the sets $\mathcal{V}_T$ give a partition of $\mathcal{P}$ as the multi-index T varies, up to discarding the primes which are not of degree 1. Thus we have

$$\mathcal{P}(x)=\sum_T\mathcal{V}_T(x)+O\left(\frac{\sqrt{x}}{\log x}\right). \tag{22}$$

Given T such that $1+a_it_i$ and d_i are not coprime for some i, the set $\mathcal{V}_T$ contains at most $[K:\mathbb{Q}]$ primes, as in this case a prime $\mathfrak{p}\in\mathcal{V}_T$ must lie above a fixed prime divisor of d_i. There are finitely many primes $\mathfrak{p}$ lying in some $\mathcal{V}_T$ with $1+a_it_i$ and d_i not coprime for some i (at most $[K:\mathbb{Q}]$ primes $\mathfrak{p}$ for each rational prime p dividing one of the integers d_i), and since the sets $\mathcal{V}_T$ are disjoint, they are counted only once. Therefore, we may restrict the multiple series in (22) to the multi-indices T with $(1+a_it_i,d_i)=1$ for every i.

Recall the notation $w=w(T):=[d_1t_1,\dots,d_rt_r]$.

Lemma 18. *Fix T such that $(1+a_it_i,d_i)=1$ for all i. Then the set $\mathcal{V}_T$ can be written as*

$$\mathcal{V}_T=\left\{\mathfrak{p}:\operatorname{ind}_\mathfrak{p}(\alpha_i)=t_i\,\forall i,\ \left(\frac{\mathfrak{p}}{F(\zeta_w)/K}\right)\subseteq C_w\right\}\,,$$

where

$$C_w:=\left\{\sigma\in\operatorname{Gal}(F(\zeta_w)/K):\forall i\ \sigma(\zeta_{d_it_i})=\zeta_{d_it_i}^{1+a_it_i},\ \sigma|_F\in C\right\}\,.$$

Moreover, assuming (GRH) and letting $x\geqslant t_i^3$ for all i, the function $\mathcal{V}_T(x)$ satisfies

$$\mathcal{V}_T(x)=\frac{x}{\log x}\sum_N\frac{(\prod_i\mu(n_i))c(N,T)}{[F_{w,N,T}:K]}+O\left(\frac{x}{\log^2 x}+\sum_{i=1}^r\frac{x\log\log x}{\varphi(t_i)\log^2 x}\right)\,, \tag{23}$$

where $F_{w,N,T}$ and $c(N,T)$ are as in Theorem 1. Moreover, $c(N,T)>0$ holds only if we have $(d_i,n_i)\mid a_i$ for all i. The constant implied by the O-term depends only on K, F, the α_i's and the d_i's.

Proof. We keep the notation and the assumptions described above. Since $1+a_it_i$ and d_i are coprime for all i, if $\mathfrak{p}\in\mathcal{V}_T$ and $\mathrm{N}\,\mathfrak{p}=p$, then $p\nmid d_it_i$ for all i and we have the equivalence

$$p\equiv 1+a_it_i \bmod d_it_i \quad\Longleftrightarrow\quad \left(\frac{p}{\mathbb{Q}(\zeta_{d_it_i})/\mathbb{Q}}\right)\text{ satisfies }\zeta_{d_it_i}\mapsto\zeta_{d_it_i}^{1+a_it_i}\,. \tag{24}$$

The first part of the statement is now clear, because the condition on the right of (24) holds for all i if and only if $(\mathfrak{p},K(\zeta_w)/K)$ acts as the exponentiation by $1+a_it_i$ on $\zeta_{d_it_i}$ for all i.

In order to get an asymptotic formula for $\mathcal{V}_T(x)$, it is sufficient to apply Theorem 3 to the field extension $F(\zeta_w)/K$ and C_w. Notice that in this application of Theorem 3 the number $c'(N,T)$ coincides with the number $c(N,T)$ of Theorem 1. Moreover, the coefficient $c(N,T)$ is zero if $(d_i,n_i)\nmid a_i$ for some i because if an automorphism σ is counted, then it must act on $\zeta_{(d_i,n_i)t_i}$ as the identity and as the exponentiation by $1+a_it_i$.

As for the constant implied by the O-term, one can check easily that applying Theorem 3 to $F(\zeta_w)/K$ and C_w preserves its independence from the parameters t_i (except for the factors $\varphi(t_i)$, which are already explicit). Indeed, in the proof of Lemma 15 it is sufficient to take into account the bound $c(N,T)\leqslant[F:K]$, and to see $F_{w,N,T}$ as a cyclotomic-Kummer extension of F when applying Proposition 13. □

We are now ready to prove Theorem 1.

Proof of Theorem 1. Let $\mathcal{V}_T$ be as above. We follow the proof of Theorem 4 closely. Take $0<\rho\leqslant 1/2$ and set $y:=(\log x)^\rho$. Consider formula (22). We estimate the tail of the function $\mathcal{P}(x)$ in the same way as we did for the function $\mathcal{S}(x)$, i.e. similarly as in (18) and then applying Lemma 17 (we may take S_i to be the set of all positive integers for all i). We obtain

$$\mathcal{P}(x)=\sum_{\substack{T\\ t_i\leqslant y}}\mathcal{V}_T(x)+O\left(\frac{x}{(\log x)^{1+\rho}}\right)\,, \tag{25}$$

where we may restrict the indices t_i to those satisfying $(1+a_it_i,d_i)=1$ for all i. Notice that $O\left(\sqrt{x}/\log x\right)$ is also included in the error term.

We choose $\rho = 1/(r+1)$. As $x > y^3$, by Lemma 18 we may replace in (25) $\mathcal{V}_T(x)$ by the asymptotic (23). Let us first focus on the main term, namely

$$\frac{x}{\log x} \sum_{\substack{T \\ t_i \leqslant y}} \sum_{N} \frac{(\prod_i \mu(n_i))c(N,T)}{[F_{w,N,T} : K]}\,,$$

where we may restrict the indices n_i to those with $(d_i, n_i) \mid a_i$. We deal with the multiple sum on the multi-indices T as we did in (21) (where the condition $t_i \in S_i$ trivially holds). Since the degree $[F_{w,N,T} : K]$ is a multiple of $[F_{N,T} : K]$, we can then proceed as in the proof of Theorem 4, i.e. by applying Theorem 5 (recalling that $c(N,T) \leqslant [F : K]$). Finally, we control the error terms directly as we did for $\mathcal{S}(x)$. □

Notice that in the case $r = 1$, our choice for ρ yields the same error obtained by Ziegler in [10, Theorem 1].

Remark 19. For N, T fixed, we could say more about the necessary conditions for the coefficient $c(N,T)$ to be nonzero. Suppose it counts at least one element $\sigma \in \mathrm{Gal}(F_{w,N,T}/K)$. Then for each i, σ must act as the exponentiation by $1 + a_i t_i$ on the root of unity $\zeta_{d_i t_i}$, so that the system of congruences $y \equiv a_i t_i \bmod d_i t_i$ must be solvable. This is the case if and only if we have $a_i t_i \equiv a_j t_j \bmod (d_i t_i, d_j t_j)$ for every i, j, and the solution y will be unique modulo w. This integer $y = y(T)$ would be such that $[t_1, \dots, t_r] \mid y$ and $\sigma(\zeta_w) = \zeta_w^{1+y}$.

Suppose that the above-mentioned system has a solution y. Then the element $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_w)/\mathbb{Q})$ such that $\tau(\zeta_w) = \zeta_w^{1+y}$ must be the identity on $\mathbb{Q}(\zeta_w) \cap K_{N,T}$. This implies that τ fixes $\zeta_{(w,v)}$ where $v = v(N,T) := [n_1 t_1, \dots, n_r t_r]$, so that we must have $(w, v) \mid y$. This condition implies for instance that $(d_i t_i, n_j t_j) \mid a_i t_i$ for every $i, j \in \{1, \dots, r\}$ (because $y \equiv a_i t_i \bmod d_i t_i$).

Remark 20. Let K be a number field, and let $G_1, \dots, G_r$ be finitely generated subgroups of $K^\times$ of finite positive rank $s_1, \dots, s_r$, respectively, which generate a torsion-free subgroup of $K^\times$ of rank $\sum_i s_i$. For a prime $\mathfrak{p}$ of K, let $\mathrm{ord}_\mathfrak{p}(G_i)$ be the order of the reduction of G_i modulo $\mathfrak{p}$, when this is well-defined. In Theorem 1, one could instead study the set of primes $\mathfrak{p}$ of K satisfying $\mathrm{ord}_\mathfrak{p}(G_i) \equiv a_i \bmod d_i$ for all i (and possibly an additional condition on the Frobenius). The result would be analogous, simply replacing α_i with G_i in the definitions of $F_{w,N,T}$ and $c(N,T)$. The error term would be the same, i.e. with the exponent $(1 + 1/(r+1))$ in the denominator.

Indeed, the author and Perucca generalized Ziegler's results [10] to finite rank in [8], so that one could use the latter work to achieve directly all the steps of the present paper for the problem introduced in this remark.

Write $\mathrm{ind}_\mathfrak{p}(G_i)$ for the index of the reduction of G_i modulo $\mathfrak{p}$. One could also study the sets analogous to those of Theorems 3 and 4 with the conditions $\mathrm{ind}_\mathfrak{p}(G_i) = t_i$ and $\mathrm{ind}_\mathfrak{p}(G_i) \in S_i$, respectively. The analogous results can be obtained also in this case.

Acknowledgments

The author would like to thank Antonella Perucca for suggesting the problem and for her valuable feedback. A special thank to Paul Pollack for his considerable help with the results of Section 2.

References

[1] Chinen, K. - Murata, L., *On a distribution property of the residual order of* $a \pmod{p}$ *IV*. Number theory, 11–22, Dev. Math., **15**, Springer, New York, 2006.

[2] Debry, C. - Perucca, A., *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283.

[3] Hardy, G. - Wright, E.: *An Introduction to the Theory of Numbers*, 5th ed., Oxford at the Clarendon Press, Oxford, 1979.

[4] Montgomery, H. - Vaughan, R.: *Multiplicative Number Theory I: Classical Theory*, (Cambridge Studies in Advanced Mathematics), Cambridge University Press, Cambridge, 2006.

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

[6] Moree, P., *On the distribution of the order and index of* $g \pmod{p}$ *over residue classes III*. J. Number Theory **120** (2006), no. 1, 132–160.

[7] Neukirch, J., *Algebraic Number Theory*. Springer, Berlin Heidelberg, 1999.

[8] Perucca, A. - Sgobba, P., *Kummer theory for number fields and the reductions of algebraic numbers*, Int. J. Number Theory, **15** , No. 8 (2019), 1617–1633.

[9] Perucca, A. - Sgobba, P., *Kummer theory for number fields and the reductions of algebraic numbers II*, Unif. Distrib. Theory **15** (2020), no. 1, 75–92.

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

Department of Mathematics, University of Luxembourg, 6 Avenue de la Fonte, 4364 Esch-sur-Alzette, Luxembourg

Email address: pietro.sgobba@uni.lu