DIVISIBILITY CONDITIONS ON THE ORDER OF THE REDUCTIONS OF ALGEBRAIC NUMBERS

PIETRO SGOBBA

ABSTRACT. Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. Without relying on (GRH) we prove an asymptotic formula for the number of primes $\mathfrak{p}$ of K such that the order of $(G \bmod \mathfrak{p})$ is divisible by a fixed integer. We also provide a rational expression for the natural density of this set. Furthermore, we study the primes $\mathfrak{p}$ for which the order is k-free, and those for which the order has a prescribed ℓ-adic valuation for finitely many primes ℓ. An additional condition on the Frobenius conjugacy class of $\mathfrak{p}$ may be considered. In order to establish these results, we prove an unconditional version of the Chebotarev density theorem for Kummer extensions of number fields.

1. INTRODUCTION

Consider a number field K and let G be a finitely generated subgroup of $K^\times$. If $\mathfrak{p}$ is a prime of K such that $v_\mathfrak{p}(g) = 0$ for all $g \in G$, then the reduction $(G \bmod \mathfrak{p})$ is a well-defined subgroup of $k_\mathfrak{p}^\times$, where $k_\mathfrak{p}$ is the residue field at $\mathfrak{p}$ and $v_\mathfrak{p}$ the $\mathfrak{p}$-adic valuation over K. In this paper we investigate the set consisting of the primes $\mathfrak{p}$ of K such that the order of $(G \bmod \mathfrak{p})$ is well-defined and it satisfies some divisibility conditions.

More precisely, denote by $\mathrm{ord}_\mathfrak{p}(G)$ the order of $(G \bmod \mathfrak{p})$. In Theorem 1 we prove an asymptotic formula for the number of primes $\mathfrak{p}$ such that $m \mid \mathrm{ord}_\mathfrak{p}(G)$, where m is any given positive integer. We also consider the primes $\mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p}(G)$ is k-free, i.e. it is not divisible by k-th powers (greater than 1), where $k \geqslant 2$. In Theorem 2, relying on the previous result, we prove an asymptotic formula for the number of primes satisfying this condition. Given a finite Galois extension of K, an additional condition on the conjugacy class of the Frobenius automorphisms of the primes lying above $\mathfrak{p}$ may also be considered. Notice that in this paper we do not rely on the Generalized Riemann Hypothesis (GRH). In fact, Theorem 10 gives an unconditional version of the Chebotarev density theorem for cyclotomic-Kummer extensions of number fields, allowing our proofs to be independent of (GRH).

The mathematical questions addressed in this paper are closely related to Artin's Conjecture on primitive roots, and hence are part of an active research area, see Moree's survey [4]. The density of rational primes p such that $m \mid \mathrm{ord}_p(g)$, where $g \in \mathbb{Q}^\times \setminus \{\pm 1\}$, has been recently studied by Pappalardi [6, 7] (also replacing g with a group of rational numbers), by Moree [3], and previously by Wiertelak [17]. Our paper provides generalizations of various results by Pappalardi and Moree, as described in the next sections. Over a number field, Debry and Perucca considered the density of the primes $\mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p}(G)$, where G is a group consisting of algebraic numbers, is not divisible by some fixed prime number (and described how this permits to treat general divisibility conditions), see [1, 9]. Under the assumption of (GRH), more general results over number fields hold, e.g. for $\mathrm{ord}_\mathfrak{p}(G)$ satisfying a given modular congruence,

2020 *Mathematics Subject Classification.* Primary: 11N37; Secondary: 11R44, 11R45.

Key words and phrases. Reductions, distribution of primes, multiplicative order, Chebotarev density theorem.

see [18] by Ziegler and [10] by Perucca and the author. For more references and historical background we refer to [4, Sect. 9.2 and 9.3].

1.1. **Notation.** If $m \geqslant 1$ is an integer, then we denote by ζ_m a primitive m-th root of unity, and by m^∞ the supernatural number $\prod_{p|m \text{ prime}} p^\infty$. As customary, μ is the Möbius function.

We fix an algebraic closure $\overline{K}$ of K. For $m, n \geqslant 1$ with $n \mid m$, we write $K_{m,n} := K(\zeta_m, G^{1/n})$ for the n-th Kummer extension related to G over $K(\zeta_m)$, i.e. the subextension of $\overline{K}/K(\zeta_m)$ obtained by adding the n-th roots of all elements in G. If F/K is a finite Galois extension, and $\mathfrak{p}$ is a prime of K which does not ramify in F, then we denote by $(\mathfrak{p}, F/K)$ the conjugacy class of the Frobenius elements at the primes of F above $\mathfrak{p}$. If $\mathcal{S}$ is a set of primes of K, then we let $\mathcal{S}(x)$ be the number of primes in $\mathcal{S}$ with norm up to x.

1.2. **Outline of the main results.** The main result is the following.

Theorem 1. *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r, and let m be a positive integer. Let F/K be a finite Galois extension, and let C be a conjugacy-stable subset of $\mathrm{Gal}(F/K)$. Consider the set of primes of K given by*

$$\mathcal{P}_m = \left\{ \mathfrak{p} : m \mid \mathrm{ord}_{\mathfrak{p}}(G),\ \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\}$$

(where we are tacitly excluding the finitely many primes $\mathfrak{p}$ that ramify in F or such that $v_{\mathfrak{p}}(g) \neq 0$ for some $g \in G$). Then, for $0 < \varepsilon < 1$ we have

$$\mathcal{P}_m(x) = \frac{x}{\log x} \varrho_{C,m} + O_\varepsilon\left(x \left(\frac{(\log\log x)^2}{\log x} \right)^{1+\frac{1-\varepsilon}{3(r+1)}} \right) \tag{1}$$

where

$$\varrho_{C,m} := \sum_{n \mid m^\infty} \sum_{d \mid m} \frac{\mu(d) c(mn, dn)}{[F_{mn,dn} : K]} \tag{2}$$

and where, for all positive integers a, b with $b \mid a$, we set

$$c(a,b) := |C \cap \mathrm{Gal}(F/F \cap K_{a,b})|. \tag{3}$$

The constant implied by the O-term depends only on ε, F, K, G.

The assumption that G is torsion-free allows some simplifications in the proofs, and in Remark 16 we explain how to deal with the general case. Also notice that the series in (2) is convergent by Proposition 15. The coefficient $c(a,b)$ in (3) is always at most $|C| \leqslant [F : K]$, and it is equal to 1 if the condition on the Frobenius is trivial.

The main challenge for the generalization of Pappalardi's method consists in proving a certain unconditional version of the Chebotarev density theorem for cyclotomic-Kummer extensions of number fields, as mentioned above. In Section 2 we will argue that this is not difficult if the base field K is normal over $\mathbb{Q}$. However, for the general case we need an improvement on the upper-bound of a possible zero of the Dedekind zeta function of $K_{m,n}$.

Section 3 is devoted to the proof of Theorem 1, whereas in Section 4 we justify that the natural density $\varrho_{C,m}$ is a positive rational number, and if $C = \mathrm{Gal}(F/K)$ (e.g. if $F = K$) then we express it in terms of finite sums and products, see Theorem 18.

Sections 5 and 6 are devoted to proving applications of Theorem 1. In Section 5 we apply Theorem 1 to prove the following result on the primes $\mathfrak{p}$ of K for which $\mathrm{ord}_{\mathfrak{p}}(G)$ is k-free.

Theorem 2. *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r, let F/K be a finite Galois extension, and let C be a conjugacy-stable subset of $\mathrm{Gal}(F/K)$. Let $k \geqslant 2$ be an integer and consider the following set of primes of K:*

$$\mathcal{N}_k := \left\{ \mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(G) \text{ is } k\text{-free}, \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\}$$

(where we are tacitly excluding the primes $\mathfrak{p}$ that ramify in F or such that $v_{\mathfrak{p}}(g) \neq 0$ for some $g \in G$). Then we have

$$\mathcal{N}_k(x) = \frac{x}{\log x} \sum_{m \geqslant 1} \mu(m) \varrho_{C,m^k} + O_k\left(\frac{x}{(\log x)^{1+\frac{k-1}{3(r+1)(k+1)}}} \right), \tag{4}$$

where ϱ_{C,m^k} is as in (2)*. The set $\mathcal{N}_k$ has natural density*

$$\beta_{C,k} := \sum_{m \geqslant 1} \sum_{n \mid m^\infty} \sum_{d \mid m} \frac{\mu(m)\mu(d) c(nm^k, dn)}{[F_{nm^k,dn} : K]},$$

where $c(a,b)$ is as in (3)*. The constant implied by the O-term depends only on k, F, K, G.*

Notice that the convergence of the series $\beta_{C,k}$ follows from Proposition 15. In Section 6, from Theorem 1 we also derive Theorem 21, which concerns the set of primes $\mathfrak{p}$ for which the ℓ-adic valuation of $\mathrm{ord}_{\mathfrak{p}}(G)$ has a prescribed value for finitely many prime numbers ℓ.

In Section 7, under (GRH), we derive some improvements on the error terms of formulas (1) and (4). Finally, in Section 8 we provide several numerical examples for the densities considered in this paper.

2. Chebotarev density theorem for cyclotomic-Kummer extensions

In this section we prove an effective version of the Chebotarev density theorem for cyclotomic-Kummer extensions of number fields which is "unconditional", i.e. it does not rely on (GRH). Let us first introduce some notation (in addition to the notation of Section 1.1).

2.1. Notation.

Given a finite Galois extension L/K of number fields and a conjugacy-stable subset C of $\mathrm{Gal}(L/K)$, we denote by $\pi(L/K, C)$ the set of primes $\mathfrak{p}$ of K which are unramified in L and such that $(\mathfrak{p}, L/K) \subseteq C$. Moreover, we say that $\mathfrak{p}$ is a prime of *degree* 1 in K if its ramification index and residue class degree over $\mathbb{Q}$ are equal to 1. We denote by $\pi^1(L/K, C)$ the set of primes in $\pi(L/K, C)$ which are of degree 1.

Also, d_K denotes the absolute discriminant of K, $\mathcal{O}_K$ the ring of integers of K, and ζ_K the Dedekind zeta function of K. For a finitely generated subgroup G of $K^\times$, $\mathcal{P}(G)$ is the set of primes $\mathfrak{p}$ in K such that $v_{\mathfrak{p}}(g) \neq 0$ for some $g \in G$ (recall that this set is finite).

Also, we use the following standard notation: φ is the Euler's totient function; given $m \geqslant 1$, $\tau(m)$ is the number of positive divisors of m, and $\mathrm{rad}(m)$ is the radical of m, i.e. the largest squarefree integer dividing m; $\mathrm{Li}(x) = \int_2^x \frac{dx}{\log x}$ is the logarithmic integral function.

2.2. Chebotarev density theorem.

We start by stating the general result by Lagarias and Odlyzko, in the improved version by Serre.

Theorem 3 (Effective "unconditional" Chebotarev density theorem, [2, Theorem 1.2] and [15, Theorem 2])**.** *Let L/K be a finite Galois extension of number fields. Let C be a conjugacy-stable subset of $\mathrm{Gal}(L/K)$. There exist absolute constants c_1, c_2 such that, if*

$$\log x \geqslant c_1 [L:\mathbb{Q}] \log^2 |d_L|\,, \tag{5}$$

then

$$\pi(L/K, C)(x) = \frac{|C|}{[L:K]} \mathrm{Li}(x) + O\left(\frac{|C|}{[L:K]} \mathrm{Li}(x^\beta) + |\tilde{C}| x \exp\left(- c_2 \sqrt{\frac{\log x}{[L:\mathbb{Q}]}} \right) \right), \tag{6}$$

where β is a possible zero of $\zeta_L(s)$, and where $|\tilde{C}|$ denotes the number of conjugacy classes contained in C (if β does not exist, then the term $\frac{|C|}{[L:K]} \mathrm{Li}(x^\beta)$ is deleted).

Remark 4. Since the number of primes of K not of degree 1 with norm up to x can be estimated by $O\left(\sqrt{x}/\log x\right)$, see e.g. [18, Lemma 1], the same asymptotic formula (6) holds for $\pi^1(L/K, C)(x)$.

The difficulty in applying this result to cyclotomic-Kummer extensions consists in estimating the error term $O\left(\mathrm{Li}(x^\beta)\right)$, and hence bounding the value of β. As of today, the best known bound on β is provided by Stark in [16, Proof of Theorem 1', p.148]. In fact, if $K/\mathbb{Q}$ is normal, then that bound is good enough for our purpose, see Remark 8. However, for the general case we need to deduce from Stark's results some improvement which is suitable for our goal.

2.3. **On a possible zero of the Dedekind zeta function.**

Lemma 5 ([16, Lemma 3])**.** *Let $L \neq \mathbb{Q}$ be a number field. The Dedekind zeta function $\zeta_L(s)$ has at most one zero in the region*

$$\left\{ s \in \mathbb{C} : 1 - \frac{1}{4 \log |d_L|} \leqslant \mathrm{Re}(s) \leqslant 1 \text{ and } |\mathrm{Im}(s)| \leqslant \frac{1}{4 \log |d_L|} \right\}. \tag{7}$$

If such a zero exists, then it is real and simple.

Lemma 6. *Let L/K be a normal extension of number fields with $L \neq \mathbb{Q}$. If ζ_L has a real zero β such that*

$$1 - \frac{1}{4(2[K:\mathbb{Q}])! \cdot \log |d_L|} \leqslant \beta \leqslant 1, \tag{8}$$

then there is a quadratic number field M inside L such that $\zeta_M(\beta) = 0$.

The Lemma says, in particular, that if L has no quadratic subfields, then $\zeta_L(s)$ has no real zero in the range (8).

Proof. If $K = \mathbb{Q}$, then the statement holds by [16, Lemma 8], hence we suppose $K \neq \mathbb{Q}$. If $\zeta_L(s)$ has a zero with real part lying in the range (8), then by Lemma 5 it must be real, simple, and unique in that range. Since L/K is normal, by [16, Theorem 3] there is a subextension F of L/K, which is either trivial or quadratic over K, such that $\zeta_E(\beta) = 0$ for every field $F \subseteq E \subseteq L$. Therefore we have that either $\zeta_K(\beta) = 0$ or $\zeta_F(\beta) = 0$ for some quadratic extension F/K with $F \subseteq L$. We conclude by applying [16, Lemma 8] either to K or F, noticing that the range of the cited result contains the interval (8). □

Proposition 7. *Let L/K be a Galois extension of number fields with $L \neq \mathbb{Q}$. Then the possible unique zero β of the Dedekind zeta function $\zeta_L(s)$ in the region* (7) *is real and simple, and we have*

$$\frac{1}{2} \leqslant \beta \leqslant \max\left\{1 - \frac{1}{4(2[K:\mathbb{Q}])!\log|d_L|}, 1 - \frac{1}{c_3\,|d_L|^{1/[L:\mathbb{Q}]}}\right\}, \tag{9}$$

where $c_3 > 0$ is an effective absolute constant.

Proof. Clearly $\beta \geqslant 1/2$ as $4\log|d_L| \geqslant 2$. It suffices to show that if β is in the range (8), then β satisfies (9). We follow the same argument as in [16, Proof of Theorem 1', p.148]. If L has no quadratic subfields, then, as we mentioned above, $\zeta_L(s)$ has no real zero in the range (8) by Lemma 6 and hence (9) is satisfied. If L contains a quadratic field, suppose that $\zeta_L(\beta) = 0$ for some β in the range (8). By Lemma 6 there must be a quadratic subfield M of L such that $\zeta_M(\beta) = 0$. By [16, Lemma 11] we must have $\beta < 1 - (c_3\,|d_M|^{1/2})^{-1}$, for an effective absolute constant $c_3 > 0$. We may conclude because we have $|d_L| \geqslant |d_M|^{[L:\mathbb{Q}]/2}$. □

Remark 8. In fact, if in the proof of Lemma 6 we have $\zeta_K(\beta) = 0$, then the lower bound of (8) may be taken as $1 - (4[K:\mathbb{Q}]!\log|d_L|)^{-1}$. Moreover, if L is normal over $\mathbb{Q}$ or if there is a tower of normal extensions $\mathbb{Q} = k_0 \subset k_1 \subset \cdots \subset k_m = K$, then the lower bound of (8) may be taken to be $1 - (4\log|d_L|)^{-1}$ or $1 - (16\log|d_L|)^{-1}$, respectively (see [16, Lemmas 8 and 10]). Accordingly, the factor $4(2[K:\mathbb{Q}])!$ in (9) can be replaced by 4 or 16 in the respective cases, by following the same argument of the proof of Proposition 7.

2.4. **Chebotarev density theorem for cyclotomic-Kummer extensions.**

Proposition 9. *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. Then, for $m, n \geqslant 1$ with $n \mid m$, we have*

$$\frac{\log\left|d_{K_{m,n}}\right|}{[K_{m,n}:\mathbb{Q}]} \leqslant \log(\varphi(m)mn^r) + \sum_{p\in P(G)} \log p + \log|d_K|\,,$$

where $P(G)$ is the finite set of the rational primes lying below the primes in $\mathcal{P}(G)$.

Proof. Given a finite extension L/K we write $d_{L/K}$ for the relative discriminant. We have

$$d_{K_{m,n/\mathbb{Q}}} = \mathrm{N}_{K/\mathbb{Q}}(d_{K_{m,n}/K}) \cdot d_{K/\mathbb{Q}}^{[K_{m,n}:K]}\,, \tag{10}$$

see [5, Ch.III, Corollary 2.10]. By [15, Proposition 5], since $K_{m,n}/K$ is Galois, we have

$$\log\left|\mathrm{N}_{K/\mathbb{Q}}(d_{K_{m,n}/K})\right| \leqslant [K_{m,n}:\mathbb{Q}]\Big(\log[K_{m,n}:K] + \sum_{p\in P(K_{m,n}/K)} \log p\Big) \tag{11}$$

where $P(K_{m,n}/K)$ is the set of rational primes p lying below the primes of K that ramify in $K_{m,n}$. These prime numbers divide m or lie in $P(G)$, as they lie below the primes $\mathfrak{p}$ that divide $d_{K_{m,n}/K}$, and an estimate for this relative discriminant is [10, Formula (4.7)]:

$$d_{K_{m,n}/K} \mid \Big(mn^r \prod_{i=1}^{r} (\alpha_i\beta_i)^2\Big)^{n^r\varphi(m)} \mathcal{O}_K\,,$$

where $\alpha_i, \beta_i \in \mathcal{O}_K$ are such that the elements $\gamma_i := \alpha_i/\beta_i$ for $i \in \{1,\dots,r\}$ form a basis of G as a free $\mathbb{Z}$-module. Since $n \mid m$, we have

$$\sum_{p\in P(K_{m,n}/K)} \log p \leqslant \log m + \sum_{p\in P(G)} \log p\,. \tag{12}$$

We conclude by taking the logarithm of $\left|d_{K_{m,n}}\right|$, making use of (10), and by applying the bounds (11), (12) and $[K_{m,n} : K] \leqslant \varphi(m)n^r$. □

We are now ready to prove an effective unconditional Chebotarev density theorem for cyclotomic-Kummer extensions of number fields, extending [7, Lemma 4] to number fields.

Theorem 10. *Let F/K be a Galois extension of number fields, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. Let C be a conjugacy-stable subset of $\mathrm{Gal}(F/K)$, and for all integers $m, n \geqslant 1$ with $n \mid m$, define*

$$C_{m,n} := \{\sigma \in \mathrm{Gal}(F_{m,n}/K) : \sigma|_F \in C,\, \sigma|_{K_{m,n}} = \mathrm{id}\}\,, \tag{13}$$

which is a conjugacy-stable subset of $\mathrm{Gal}(F_{m,n}/K)$. Then there exist constants c_4 and c_5, which depend only on F and G, such that, uniformly for

$$m \leqslant c_4 \left(\frac{\log x}{(\log\log x)^2}\right)^{\frac{1}{3(r+1)}}\,, \tag{14}$$

we have

$$\pi(F_{m,n}/K, C_{m,n})(x) = \frac{|C_{m,n}|}{[F_{m,n} : K]}\,\mathrm{Li}(x) + O_{F,G}\left(\frac{x}{e^{c_5\sqrt[6]{\log x}\cdot\sqrt[3]{\log\log x}}}\right).$$

Proof. We apply Theorem 3 to $F_{m,n}/K$ and $C_{m,n}$. By Proposition 9 and since $[F_{m,n} : F] \leqslant m^{r+1}$ we have

$$\begin{aligned}[F_{m,n} : \mathbb{Q}]\log^2\left|d_{F_{m,n}}\right| &\leqslant [F : \mathbb{Q}]^3 m^{3(r+1)}\left(\log m^{r+2} + c_{F,G}\right)^2\\ &\ll_{F,G} m^{3(r+1)}\log^2 m\,,\end{aligned}$$

($c_{F,G}$ is a constant depending only on F and G). Thus, from (14) we deduce $m^{3(r+1)}\log^2 m \ll \log x$, hence (5) is satisfied.

We now focus on the error terms of (6). Since $\beta \geqslant 1/2$ we have $\mathrm{Li}(x^\beta) = O(x^\beta/\log x)$. We make use of the two terms in the upper bound on β of Proposition 7 separately. On the one hand, by Proposition 9 we have

$$\left|d_{F_{m,n}}\right|^{1/[F_{m,n}:\mathbb{Q}]} \leqslant \exp\left(\log m^{r+2} + c_{F,G}\right) \ll_{F,G} m^{r+2},$$

which yields

$$\frac{x^\beta}{\log x} \leqslant \frac{x}{x^{1/(c_6 m^{r+2})}\log x} = \frac{x}{\exp\left(\frac{1}{c_6 m^{r+2}}\log x + \log\log x\right)} \leqslant \frac{x}{\exp\left(c_5\sqrt[6]{\log x}\sqrt[3]{\log\log x}\right)},$$

(c_5, c_6 are constants depending only on F and G).

On the other hand, the condition on m gives $\log\left|d_{F_{m,n}}\right| \leqslant \sqrt{\log x}$, so that

$$\frac{x^\beta}{\log x} \leqslant \frac{x}{x^{1/(4(2[K:\mathbb{Q}])!\log|d_{F_{m,n}}|)}\log x} \leqslant \frac{x}{\exp\left(c_5\sqrt[6]{\log x}\sqrt[3]{\log\log x}\right)},$$

where we used that $a^3 + b^3 \geqslant ab$ for all $a, b > 0$.

Finally, to bound the last error term in (6) it is enough to notice that

$$\sqrt{\frac{\log x}{[F_{m,n} : \mathbb{Q}]}} \geqslant \sqrt{\frac{\log x}{[F : \mathbb{Q}]m^{r+1}}} \gg_F \sqrt[3]{\log x}\sqrt[3]{\log\log x}\,.$$

Collecting all error terms gives the asymptotic formula. □

3. THE ORDER BEING DIVISIBLE BY A GIVEN INTEGER

In this section we prove Theorem 1. We first set some notation. Recall also the notation introduced in Sections 1.1 and 2.1.

3.1. **Notation.** Let F/K be a Galois extension of number fields, C a conjugacy-stable subset of $\mathrm{Gal}(F/K)$, and G a finitely generated and torsion-free subgroup of $K^\times$. For $m, n \geqslant 1$ with $n \mid m$ we define $\pi^1_{m,n}$ to be the set of primes $\mathfrak{p}$ of K which are of degree 1, split completely in $K_{m,n}$, do not ramify in F, and satisfy $(\mathfrak{p}, F/K) \subseteq C$. In other words, we set $\pi^1_{m,n} := \pi^1(F_{m,n}/K, C_{m,n})$, where $C_{m,n}$ is as in (13) (we are fixing K, F, G, and C).

For $\mathfrak{p} \notin \mathcal{P}(G)$, recall that $\mathrm{ord}_\mathfrak{p}(G)$ is the order of $(G \bmod \mathfrak{p})$, and we also denote by $\mathrm{ind}_\mathfrak{p}(G)$ the index of $(G \bmod \mathfrak{p})$, namely

$$\mathrm{ind}_\mathfrak{p}(G) = [k_\mathfrak{p}^\times : \langle G \bmod \mathfrak{p}\rangle] = (\mathrm{N}\,\mathfrak{p} - 1)/\,\mathrm{ord}_\mathfrak{p}(G).$$

Given integers $m, n \geqslant 1$, recalling the definition of the supernatural number m^∞, we have $(n, m^\infty) = \prod_{\ell \mid m \text{ prime}} \ell^{v_\ell(n)}$, where v_ℓ is the ℓ-adic valuation.

3.2. **Proof of Theorem 1.** The proof of Theorem 1 is based on [7, Theorem 1] and [3, Lemma 1]. Recall that if $\mathfrak{p}$ is a prime of K of degree 1 such that $\mathfrak{p} \notin \mathcal{P}(G)$, then $\mathrm{N}\,\mathfrak{p} \equiv 1 \bmod n$ if and only if $\mathfrak{p}$ splits completely in $K(\zeta_n)$, and $n \mid \mathrm{ind}_\mathfrak{p}(G)$ if and only if $\mathfrak{p}$ splits completely in $K_{n,n}$, where $n \geqslant 1$. Hence, we easily deduce that for $m, n \geqslant 1$ with $n \mid m$ we have

$$\pi^1_{m,n} = \left\{ \mathfrak{p} : \mathfrak{p} \text{ of degree } 1,\ \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m,\ n \mid \mathrm{ind}_\mathfrak{p}(G),\ \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\}, \tag{15}$$

see also [18, Lemma 2].

Lemma 11. *If $\mathcal{P}_m$ is as in Theorem 1, then we have*

$$\mathcal{P}_m(x) = \sum_{n \mid m^\infty} \sum_{d \mid m} \mu(d) \pi^1_{mn,dn}(x) + O\left(\frac{\sqrt{x}}{\log x}\right).$$

Proof. The proof is a variation of [3, Proof of Proposition 1]. The O-term estimates the primes of K which are not of degree 1. Let $\mathfrak{p} \in \mathcal{P}_m$ be a prime of degree 1, and let $\mathrm{N}\,\mathfrak{p} = p$. Then we have $m \mid (p-1)$ and there is a unique $n \mid m^\infty$ such that $p \equiv 1 \bmod mn$, $n \mid \mathrm{ind}_\mathfrak{p}(G)$ and $(\frac{\mathrm{ind}_\mathfrak{p}(G)}{n}, m) = 1$ (we must have $n = (\mathrm{ind}_\mathfrak{p}(G), m^\infty)$). Hence we can write

$$\mathcal{P}_m(x) = \sum_{n \mid m^\infty} \mathcal{B}_n(x) + O\left(\frac{\sqrt{x}}{\log x}\right),$$

where for $n \mid m^\infty$ we set

$$\mathcal{B}_n := \left\{ \mathfrak{p} : p \equiv 1 \bmod mn,\ n \mid \mathrm{ind}_\mathfrak{p}(G),\ \left(\frac{\mathrm{ind}_\mathfrak{p}(G)}{n}, m\right) = 1,\ \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\}$$

(we are tacitly assuming that the primes in $\mathcal{B}_n$ are of degree 1, do not lie in $\mathcal{P}(G)$ and do not ramify in F). Notice that, $\mathfrak{p} \in \mathcal{B}_n$ satisfies $m \mid \mathrm{ord}_\mathfrak{p}(G)$ because of the two conditions $p \equiv 1 \bmod mn$ and $(\mathrm{ind}_\mathfrak{p}(G)/n, m) = 1$ and the identity $\mathrm{ord}_\mathfrak{p}(G) \cdot \mathrm{ind}_\mathfrak{p}(G) = p - 1$.

Next we apply the inclusion-exclusion principle to the condition $(\mathrm{ind}_{\mathfrak{p}}(G)/n, m) = 1$, which amounts to $n \mid \mathrm{ind}_{\mathfrak{p}}(G)$ and $n\ell \nmid \mathrm{ind}_{\mathfrak{p}}(G)$ for all primes $\ell \mid m$, so that we obtain

$$\mathcal{B}_n(x) = \sum_{d|m} \mu(d) \left| \left\{ \mathfrak{p} : p \leqslant x,\, p \equiv 1 \bmod mn,\, dn \mid \mathrm{ind}_{\mathfrak{p}}(G),\, \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\} \right| .$$

We conclude by (15) that

$$\mathcal{B}_n(x) = \sum_{d|m} \mu(d) \pi^1_{mn,dn}(x)\,. \tag{16}$$ □

Remark 12. Notice that, in the proof of Lemma 11 we have

$$\mathcal{B}_n(x) \leqslant [K:\mathbb{Q}] \cdot |\{p \leqslant x : p \equiv 1 \bmod mn\}|\,,$$

and $\mathcal{B}_n(x) \leqslant \pi(F_{mn,n}/K, C_{mn,n})(x)$. From this last inequality, identity (16), and by the Chebotarev density theorem we deduce

$$0 \leqslant \sum_{d|m} \frac{\mu(d)\,|C_{mn,dn}|}{[F_{mn,dn}:K]} \leqslant \frac{|C_{mn,n}|}{[F_{mn,n}:K]} \leqslant \frac{1}{[K_{mn,n}:K]}.$$

We are now ready to prove Theorem 1.

Proof of Theorem 1. Notice that, for $a, b \geqslant 1$ with $b \mid a$, we have $c(a,b) = |C_{a,b}|$, because if $\sigma \in C$ is the identity on $F \cap K_{a,b}$, then σ can be lifted to a unique element of $C_{a,b}$. We are going to apply Lemma 11 and Theorem 10. For $n \mid m^\infty$ let $\mathcal{B}_n$ be as in the proof of Lemma 11, and recall (16). Set $y := c_4(\log x/(\log\log x)^2)^{1/3(r+1)}$, where c_4 is the constant of Theorem 10. Thus, we have

$$\begin{aligned}
\mathcal{P}_m(x) &= \sum_{\substack{n|m^\infty \\ nm\leqslant y}} \sum_{d|m} \mu(d)\pi^1_{mn,dn}(x) + O\left(\sum_{\substack{n|m^\infty \\ nm>y}} \mathcal{B}_n(x) \right) + O\left(\frac{\sqrt{x}}{\log x}\right) \\
&= \mathrm{Li}(x) \sum_{\substack{n|m^\infty \\ nm\leqslant y}} \sum_{d|m} \frac{\mu(d)c(mn,dn)}{[F_{mn,dn}:K]} + O_{F,G}\left(\frac{\tau(m)}{m} \frac{x\cdot y}{e^{c_5\sqrt[6]{\log x}\cdot\sqrt[3]{\log\log x}}} \right) \\
&\quad + O\left(\sum_{\substack{n|m^\infty \\ nm>y}} \mathcal{B}_n(x) \right) + O\left(\frac{\sqrt{x}}{\log x}\right).
\end{aligned}$$

In order to estimate the tail of the series in the main term we make use of Remark 12 and obtain

$$\mathcal{P}_m(x) = \mathrm{Li}(x) \sum_{n|m^\infty} \sum_{d|m} \frac{\mu(d)c(mn,dn)}{[F_{mn,dn}:K]} + O\left(\frac{x}{\log x} \sum_{\substack{n|m^\infty \\ mn>y}} \frac{1}{[K_{mn,n}:K]} \right) \tag{17}$$

$$+ O_{F,G}\left(\frac{x\cdot y}{e^{c_5\sqrt[6]{\log x}\cdot\sqrt[3]{\log\log x}}} \right) + O\left(\sum_{\substack{n|m^\infty \\ nm>y}} \mathcal{B}_n(x) \right). \tag{18}$$

The first error term in (18) is negligible with respect to the error term in the statement. Let us estimate the error term in (17). Since $[K(\zeta_{mn}):K] \gg_K \varphi(mn)$ and $mn/\varphi(mn) = m/\varphi(m)$

(as $\mathrm{rad}(n) \mid m$), applying [6, Lemma 3.3] for some $0 < \varepsilon < 1$, we can bound

$$\sum_{\substack{n \mid m^\infty \\ mn > y}} \frac{1}{[K_{mn,n} : K]} \ll_K \sum_{\substack{n \mid m^\infty \\ nm > y}} \frac{1}{\varphi(mn)} \ll_\varepsilon \frac{m}{\varphi(m)} \frac{1}{y^{1-\varepsilon}}. \tag{19}$$

Since $m/\varphi(m) = O(\log\log m)$, see e.g. [13, Theorem 15], and $m \leqslant x$ without loss of generality, we then have

$$\frac{x}{\log x} \sum_{\substack{n \mid m^\infty \\ mn > y}} \frac{1}{[K_{mn,n} : K]} \ll_{K,\varepsilon} \frac{x \log\log x}{y^{1-\varepsilon} \log x}. \tag{20}$$

Next we focus on the second error term in (18). In view of Remark 12, and by applying the Brun-Titchmarsh Theorem and the same estimates as above, for $z := (\log x)^{2/(1-\varepsilon)}$ we have

$$\begin{aligned} \sum_{\substack{n \mid m^\infty \\ nm \leqslant y}} \mathcal{B}_n(x) &\ll_K \sum_{\substack{n \mid m^\infty \\ y < nm \leqslant z}} |\{p \leqslant x : p \equiv 1 \bmod mn\}| + \sum_{\substack{n \mid m^\infty \\ nm > z}} |\{k \leqslant x : mn \mid k\}| \\ &\ll \sum_{\substack{n \mid m^\infty \\ y < nm \leqslant z}} \frac{x}{\varphi(mn)\log(x/mn)} + \sum_{\substack{n \mid m^\infty \\ nm > z}} \frac{x}{mn} \ll_\varepsilon \frac{x \log\log x}{\log(x/z)} \frac{1}{y^{1-\varepsilon}} + \frac{x}{\log^2 x}. \end{aligned} \tag{21}$$

Both expressions (20) and (21) are bounded by the error term in the statement. □

3.3. **Properties and remarks.**

Remark 13. One can see from [6, Proof of Lemma 3.3] that the constant depending on ε arising in (19) can be taken equal to

$$\prod_{\substack{p \leqslant 2^{1/\varepsilon} \\ \text{prime}}} \frac{1}{p^\varepsilon - 1}.$$

In fact, a slightly stronger error term could be obtained in Theorem 1.

Remark 14. Let $m \geqslant 1$, and $\omega(m)$ the number of prime factors of m. One can show that for $T \geqslant 1$ and $0 < c < 1$ we have

$$\sum_{\substack{k > T \\ m \mid k \mid m^\infty}} \frac{1}{k} \leqslant (1-c)^{-\omega(m)} \frac{1}{T^c}.$$

Indeed, by the Mean value theorem we obtain $1 - 1/p^b > bp^{-b}\log p$, with $0 < b < 1$ and p a prime number. Thus, from the proof of [6, Lemma 3.3] we have

$$\sum_{\substack{k > T \\ m \mid k \mid m^\infty}} \frac{1}{k} \leqslant \frac{1}{m^{1-c} T^c} \prod_{\substack{p \mid m \\ \text{prime}}} \left(1 - \frac{1}{p^{1-c}}\right)^{-1} \leqslant \frac{(1-c)^{-\omega(m)}}{T^c}.$$

Taking $c = 1 - 1/\log\log x$ and making use of this inequality in the proof of Theorem 1 reduces the final error term to

$$O_{F,K,G}\left(x (\log\log x)^{\omega(m)-1} \left(\frac{(\log\log x)^2}{\log x} \right)^{1 + \frac{1}{3(r+1)}} \right).$$

Notice that an extra factor $(\log\log x)^{\omega(m)}$ is also needed in the formula of [7, Theorem 1].

Proposition 15. *The series $\varrho_{C,m}$ from Theorem 1 is convergent, and for every $\varepsilon > 0$ we have*

$$\varrho_{C,m} = O_{K,\varepsilon}\left(\frac{1}{m^{1-\varepsilon}}\right).$$

Moreover, we also have $\varrho_{C,m^k} \ll_{K,\varepsilon} 1/m^{k-\varepsilon}$ for every $k \geqslant 1$.

Notice that the constant implied by the latter estimate is independent of k.

Proof. Applying Remark 12 and the estimate $[K_{mn} : K] \gg_K \varphi(mn) = \varphi(m)n$, we have

$$\varrho_{C,m} \leqslant \sum_{n|m^\infty} \frac{1}{[K_{mn,n} : K]} \ll_K \frac{1}{\varphi(m)} \sum_{n|m^\infty} \frac{1}{n} = \frac{1}{\varphi(m)} \prod_{p|m \text{ prime}} \frac{p}{p-1}.$$

We may bound the product by $c_\varepsilon m^{\varepsilon/2}$, where $c_\varepsilon > 0$ is a constant depending on ε, so we conclude by recalling that $m/\varphi(m) = O_\varepsilon(m^{\varepsilon/2})$. For the second assertion notice that $m^k/\varphi(m^k) = m/\varphi(m) = O_\varepsilon(m^{\varepsilon/2})$. □

Remark 16. The assumption that the group G is torsion-free allows some simplifications throughout the proof of Theorem 1. However, the general case can be treated easily. Let G' be a finitely generated subgroup of $K^\times$ with torsion, and write $G' = G \times \langle \zeta_t \rangle$, where $\zeta_t \in K^\times$, $t \geqslant 2$, and $G \subseteq K^\times$ is torsion-free. Then, for all primes $\mathfrak{p}$ of K of norm large enough, we have

$$m \mid \operatorname{ord}_\mathfrak{p}(G') \qquad \text{if and only if} \qquad \prod_{\substack{\ell|m \text{ prime} \\ v_\ell(m) > v_\ell(t)}} \ell^{v_\ell(m)} \mid \operatorname{ord}_\mathfrak{p}(G).$$

Remark 17. Let us consider the expression of the density $\varrho_{C,m}$ for some special cases of C. If $C = \mathrm{Gal}(F/K)$, then the condition on the Frobenius becomes trivial and $c(a,b) = [F : F \cap K_{a,b}]$. Therefore we obtain

$$\varrho_m := \varrho_{\mathrm{Gal}(F/K),m} = \sum_{n|m^\infty} \sum_{d|m} \frac{\mu(d)}{[K_{mn,dn} : K]}.$$

If $C = \{\mathrm{id}\}$, then the condition $(\mathfrak{p}, F/K) = \mathrm{id}$ is equivalent to $\mathfrak{p}$ splitting completely in F. In this case $c(a,b) = 1$, and hence $\varrho_{\{\mathrm{id}\},m}$ equals $1/[F : K]$ times the density of primes $\mathfrak{P}$ of F such that $m \mid \operatorname{ord}_\mathfrak{P}(G)$.

Finally, if F is linearly disjoint over K from $K_{a,b}$, then $c(a,b) = |C|$. Hence, if this holds for all a, b we obtain $\varrho_{C,m} = \varrho_m \cdot |C| / [F : K]$.

Clearly, analogous statements hold for the densities $\beta_{C,k}$ of Theorem 2 and $\gamma_{C,k,m}$ of Theorem 21.

4. A RATIONAL FORMULA FOR THE DENSITY

As a special case of [11, Corollary 7], the natural density $\varrho_{C,m}$ of the set $\mathcal{P}_m$ from Theorem 1 is a positive rational number. In this section we also provide an explicit closed formula for $\varrho_{C,m}$ when the condition on the Frobenius is trivial (in this case we write ϱ_m for $\varrho_{C,m}$, as in Remark 17). In the rest of the paper, ℓ will always represent a prime number (also when not mentioned explicitly).

Theorem 18. *Let K be a number field and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. Let $m \geqslant 1$ be an integer and let ϱ_m be the natural density of the set of primes $\mathfrak{p}$ of K such that $m \mid \mathrm{ord}_\mathfrak{p}(G)$ (where $\mathfrak{p} \notin \mathcal{P}(G)$). Then there is an integer z, which depends only on K and G, such that*

$$\varrho_m = \frac{1}{\varphi(m)} \prod_{\substack{\ell \mid m \\ \ell \nmid z}} \frac{\ell(\ell^r - 1)}{\ell^{r+1} - 1} \cdot \sum_{\substack{g \mid z \\ \mathrm{rad}(g) \mid (m,z) \mid g}} \sum_{h \mid g} \frac{p(g,h)}{[K_{g,h} : K]}, \tag{22}$$

where we set $p(g,h) = 0$ if and only if at least one of the following conditions holds:

- *there is $\ell \mid g$, $\ell \nmid h$ such that $v_\ell(g/(m,z)) > 0$,*
- *there is $\ell \mid h$ such that $v_\ell(z/g) > 0$ and $v_\ell(g/h) \notin \{v_\ell(m), v_\ell(m) - 1\}$,*
- *there is $\ell \mid h$ such that $v_\ell(z/g) = 0$ and $v_\ell(g/h) > v_\ell(m)$;*

else we define

$$p(g,h) = \frac{\varphi(g)}{h} \cdot \prod_{\substack{\ell \mid h,\ v_\ell(z/g) > 0 \\ v_\ell(g/h) = v_\ell(m) - 1}} -\ell \cdot \prod_{\substack{\ell \mid h,\ v_\ell(z/g) = 0 \\ 1 \leqslant v_\ell(g/h) < v_\ell(m)}} -(\ell - 1) \cdot \prod_{\substack{\ell \mid h \\ v_\ell(z/h) = 0}} \frac{-\ell^{r+1}(\ell - 1)}{\ell^{r+1} - 1}.$$

Notice that the formula for ϱ_m involves only finite sums and products. Moreover, for a general number field K and a finitely generated and torsion-free group $G \subseteq K^\times$, the integer z is explicitly described by the results of [12] (see e.g. [12, Theorem 1.2 and its proof]). Also, notice that for all m such that $(m,z) = 1$ we have

$$\varrho_m = \frac{\mathrm{rad}(m)}{\varphi(m)} \prod_{\ell \mid m} \frac{\ell^r - 1}{\ell^{r+1} - 1}.$$

Proof. By [12, Theorem 1.1] there is an integer z, which depends only on K and G, such that for $n \mid m$ we have

$$[K_{m,n} : K] = \frac{\varphi(m) n^r}{\varphi((m,z))(n,z)^r} \cdot [K_{(m,z),(n,z)} : K].$$

Therefore, we have

$$\varrho_m = \sum_{n \mid m^\infty} \sum_{d \mid m} \frac{\mu(d)}{[K_{mn,dn} : K]} = \frac{1}{\varphi(m)} \sum_{\substack{g \mid z \\ h \mid g}} \frac{\varphi(g) h^r}{[K_{g,h} : K]} \sum_{\substack{n \mid m^\infty \\ (mn,z) = g}} \sum_{\substack{d \mid m \\ (dn,z) = h}} \frac{\mu(d)}{n^{r+1} d^r}. \tag{23}$$

First of all, for all $n \mid m^\infty$ we have that $\mathrm{rad}(mn,z) = \mathrm{rad}(m,z)$, so that we may restrict the sum on $g \mid z$ to the divisors such that $(m,z) \mid g$ and $\mathrm{rad}(g) = \mathrm{rad}((m,z))$ both hold. To simplify the notation, let us denote $m_\ell = v_\ell(m)$, and similarly for z_ℓ, g_ℓ, h_ℓ. Then, by properties of the multiplicative functions, from (23) we obtain

$$\varrho_m = \frac{1}{\varphi(m)} \cdot \sum_{\substack{g \mid z \\ \mathrm{rad}(g) \mid (m,z) \mid g}} \sum_{h \mid g} \frac{\varphi(g) h^r}{[K_{g,h} : K]} \cdot \prod_{\ell \mid m} p_\ell(g,h)$$

where for $\ell \mid m$ we define

$$p_\ell(g,h) := \sum_{\substack{s \geqslant 0 \\ \min(m_\ell + s, z_\ell) = g_\ell}} \sum_{\substack{e \in \{0,1\} \\ \min(s+e, z_\ell) = h_\ell}} \frac{\mu(\ell^e)}{\ell^{s(r+1)} \ell^{er}}. \tag{24}$$

If $\ell \mid m$ and $\ell \nmid z$, then the two conditions on the indices are trivial and we have

$$p_\ell(g,h) = \frac{\ell(\ell^r-1)}{\ell^{r+1}-1}.$$

This computation already justifies the first product in (22). Next, we take

$$p(g,h) := \varphi(g)h^r \prod_{\ell \mid g} p_\ell(g,h),$$

and compute $p_\ell(g,h)$ depending on the prime factors ℓ of g (equivalently, of (m,z)).

Case 1: $\ell \mid g$ and $\ell \nmid h$. Since $\ell \nmid h$, the conditions on the indices in (24) hold only for $s = e = 0$, so that $p_\ell(g,h) = 1$ if $\min(m_\ell, z_\ell) = g_\ell$, and $p_\ell(g,h) = 0$ otherwise.

Case 2: $\ell \mid h$, and $g_\ell < z_\ell$. Since $1 \leqslant h_\ell < z_\ell$, the conditions on the indices hold only for $s + e = h_\ell$. Therefore, if $g_\ell = m_\ell + h_\ell$, then $p_\ell(g,h) = 1/\ell^{h_\ell(r+1)}$; if $g_\ell = m_\ell + h_\ell - 1$, then $p_\ell(g,h) = -\ell/\ell^{h_\ell(r+1)}$; otherwise $p_\ell(g,h) = 0$.

Case 3: $\ell \mid h$, and $h_\ell < g_\ell = z_\ell$. The conditions on the indices hold only for $s + e = h_\ell$ and $m_\ell + s \geqslant z_\ell = g_\ell$. Therefore, if $m_\ell + h_\ell - 1 \geqslant z_\ell$, then $p_\ell(g,h) = -(\ell-1)/\ell^{h_\ell(r+1)}$; if $m_\ell + h_\ell = z_\ell$, then $p_\ell(g,h) = 1/\ell^{h_\ell(r+1)}$; otherwise $p_\ell(g,h) = 0$.

Case 4: $\ell \mid h$ and $h_\ell = z_\ell$. Since $h_\ell = g_\ell = z_\ell \geqslant 1$, the conditions on the indices hold if and only if $s + e \geqslant h_\ell$. Therefore, we obtain

$$p_\ell(g,h) = -\frac{1}{\ell^{h_\ell(r+1)}} \frac{\ell^{r+1}(\ell-1)}{\ell^{r+1}-1}. \qquad \square$$

5. k-FREE ORDER

In this section we prove Theorem 2. The proof relies on ideas from [6, Theorem 1.2] (see also [7, Remark (8), p.388]).

Proof of Theorem 2. If $\mathfrak{p}$ is a prime of K with $\mathfrak{p} \notin \mathcal{P}(G)$, then $\mathrm{ord}_\mathfrak{p}(G)$ is k-free if and only if for every rational prime q we have $q^k \nmid \mathrm{ord}_\mathfrak{p}(G)$. Therefore, by the inclusion-exclusion principle we have

$$\mathcal{N}_k(x) = \sum_{m \geqslant 1} \mu(m) \mathcal{P}^1_{m^k}(x) + O\left(\frac{\sqrt{x}}{\log x}\right),$$

where $\mathcal{P}^1_m$ denotes the set of all primes in $\mathcal{P}_m$ which are of degree 1 (the O-term estimates the primes not of degree 1). Notice that for $\mathcal{P}^1_m(x)$ we may take the same asymptotic formula (1) as for $\mathcal{P}_m(x)$. Then, for $0 < a < 1$ and $z := \log^a x$ we have

$$\begin{aligned}
\mathcal{N}_k(x) &= \sum_{m \leqslant z} \mu(m) \mathcal{P}^1_{m^k}(x) + O\left(\sum_{m > z} \mathcal{P}^1_{m^k}(x)\right) + O\left(\frac{\sqrt{x}}{\log x}\right) \\
&= \frac{x}{\log x} \beta_{C,k} + O\left(\frac{x}{\log x} \sum_{m > z} \varrho_{C,m^k}\right) + O\left(\sum_{m > z} \mathcal{P}^1_{m^k}(x)\right) \qquad (25) \\
&\quad + O\left(\sum_{m \leqslant z} x \left(\frac{(\log\log x)^2}{\log x}\right)^{1 + \frac{1-\varepsilon}{3(r+1)}}\right) + O\left(\frac{\sqrt{x}}{\log x}\right). \qquad (26)
\end{aligned}$$

By Proposition 15 we have $\varrho_{C,m^k} \ll_\eta 1/m^{k-\eta}$ for every $0 < \eta < 1$. Hence we can bound the first O-term in (25) by

$$\frac{x}{\log x} \sum_{m>z} \frac{1}{m^{k-\eta}} = O_\eta\left(\frac{x}{(\log x)^{1+a(k-1-\eta)}}\right). \tag{27}$$

The primes $\mathfrak{p}$ in $\mathcal{P}^1_{m^k}$ are such that $p := \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m^k$. Hence the second error term in (25) is smaller than

$$[K:\mathbb{Q}]\left(\sum_{z<m\leqslant \log^2 x} \left|\left\{p \leqslant x : p \equiv 1 \bmod m^k\right\}\right| + \sum_{m>\log^2 x} \left|\left\{n \leqslant x : m^k \mid n\right\}\right|\right).$$

The second sum is bounded by

$$\sum_{m>\log^2 x} \frac{x}{m^k} = O\left(\frac{x}{(\log x)^{2(k-1)}}\right),$$

whereas applying the Brun-Titchmarsh Theorem we can bound the first sum with

$$\sum_{z<m\leqslant \log^2 x} \frac{x}{\varphi(m^k)\log(x/m^k)} \ll \frac{x}{\log x} \sum_{m>z} \frac{1}{\varphi(m^k)}.$$

In view of the estimate $m^k/\varphi(m^k) = O_\eta(m^\eta)$ (recall that $n/\varphi(n) \ll_\eta \mathrm{rad}(n)^\eta$), we deduce that both sums are bounded by the error term in (27).

Next, we can bound the first error term in (26) by

$$(\log x)^a \cdot x\left(\frac{(\log\log x)^2}{\log x}\right)^{1+\frac{1-\varepsilon}{3(r+1)}} \leqslant \frac{x(\log\log x)^3}{(\log x)^{1+\frac{1-\varepsilon}{3(r+1)}-a}}, \tag{28}$$

and we may choose $a = \frac{1-\varepsilon}{3(r+1)(k-\eta)}$, so that (28) can be bounded by (27). With a suitable choice of ε and η (depending on k), the exponent in the denominator of (27) can be reduced to $1 + \frac{k-1}{3(r+1)(k+1)}$. Collecting the errors yields the result. □

Remark 19. In the context of Theorem 2, the case of groups with torsion is straightforward: if G' is a finitely generated subgroup of $K^\times$ with torsion of order t, and $G = G'/\langle\zeta_t\rangle$, then the density of the set $\mathcal{N}_{k,G'}$ (i.e. $\mathcal{N}_k$ defined for the group G') is equal to the density of $\mathcal{N}_{k,G}$ if t is k-free, and it is 0 otherwise.

Next we prove an explicit formula for the density $\beta_{C,k}$ of Theorem 2 if the condition on the Frobenius is trivial, and in this case we simply write β_k. The formula consists of a rational factor times a constant expressed by an infinite product.

Corollary 20. *Let K be a number field and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. Let $k \geqslant 2$ and let β_k be the natural density of the set of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_\mathfrak{p}(G)$ is k-free (where $\mathfrak{p} \notin \mathcal{P}(G)$). Then there is an integer z, which depends only on K and G, such that*

$$\beta_k = \prod_{\ell\nmid z}\left(1 - \frac{\ell^r - 1}{(\ell-1)(\ell^{r+1}-1)\ell^{k-2}}\right) \cdot \sum_{\substack{g\mid z\\ (\mathrm{rad}(g)^k, z)\mid g}} \sum_{h\mid g} \frac{p(g,h)}{[K_{g,h}:K]}, \tag{29}$$

where we set $p(g,h) = 0$ if and only if at least one of the following conditions is satisfied:

- *there is $\ell \mid g$, $\ell \nmid h$ and $v_\ell(g) \neq v_\ell((\ell^k, z))$,*
- *there is $\ell \mid h$ such that $v_\ell(g/h) > k$, or $v_\ell(z/g) > 0$ and $v_\ell(g/h) < k-1$;*

else we define $p(g,h)$ *to be*

$$\frac{g}{h\,\mathrm{rad}(g)^k}\cdot\prod_{\substack{\ell\mid g,\ell\nmid h,\ v_\ell(g/(\ell^k,z))=0\\ or\ \ell\mid h, v_\ell(g/h)=k}}(-1)\cdot\prod_{\substack{\ell\mid h,\ v_\ell(z/g)>0\\ v_\ell(g/h)=k-1}}\ell\cdot\prod_{\substack{\ell\mid h,\ v_\ell(z/g)=0\\ 0<v_\ell(g/h)<k}}(\ell-1)\cdot\prod_{\substack{\ell\mid h\\ v_\ell(z/h)=0}}\frac{\ell^{r+1}(\ell-1)}{\ell^{r+1}-1}$$

Notice that, setting

$$A_{k,r}:=\prod_{\ell\text{ prime}}\Big(1-\frac{\ell^r-1}{(\ell-1)(\ell^{r+1}-1)\ell^{k-2}}\Big), \tag{30}$$

a constant which only depends on the integer k and on the rank r of G, the infinite product in (29) is equal to

$$A_{k,r}\cdot\prod_{\ell\mid z}\Big(1-\frac{\ell^r-1}{(\ell-1)(\ell^{r+1}-1)\ell^{k-2}}\Big)^{-1}.$$

Proof. Applying [12, Theorem 1.1] as in the proof of Theorem 18 we obtain

$$\begin{aligned}\beta_k=\sum_{m\geqslant1}\sum_{\substack{n\mid m^\infty\\ d\mid m}}\frac{\mu(m)\mu(d)}{[K_{nm^k,dn}:K]}&=\sum_{\substack{g\mid z\\ h\mid g}}\frac{\varphi(g)h^r}{[K_{g,h}:K]}\sum_{m\geqslant1}\sum_{\substack{n\mid m^\infty\\ (nm^k,z)=g}}\sum_{\substack{d\mid m\\ (dn,z)=h}}\frac{\mu(m)\mu(d)}{n^{r+1}d^r\varphi(m^k)}\\ &=\sum_{\substack{g\mid z\\ h\mid g}}\frac{\varphi(g)h^r}{[K_{g,h}:K]}\prod_{\ell\text{ prime}}p_\ell(g,h)\end{aligned} \tag{31}$$

where for $\ell\nmid z$ (and hence $\ell\nmid g$) we have

$$p_\ell(g,h)=1-\frac{1}{\varphi(\ell^k)}\sum_{s\geqslant0}\sum_{e\in\{0,1\}}\frac{\mu(\ell^e)}{\ell^{s(r+1)+er}}=1-\frac{1}{\varphi(\ell^k)}\frac{\ell(\ell^r-1)}{\ell^{r+1}-1},$$

and for $\ell\mid z$, $\ell\nmid g$ we have $p_\ell(g,h)=1$, whereas for $\ell\mid g$, setting $z_\ell:=v_\ell(z)$ and similarly for g_ℓ,h_ℓ, we have

$$p_\ell(g,h)=-\frac{1}{\varphi(\ell^k)}\sum_{\substack{s\geqslant0\\ \min(k+s,z_\ell)=g_\ell}}\sum_{\substack{e\in\{0,1\}\\ \min(s+e,z_\ell)=h_\ell}}\frac{\mu(\ell^e)}{\ell^{s(r+1)+er}}.$$

We take $p(g,h):=\varphi(g)h^r\prod_{\ell\mid g}p_\ell(g,h)$ (and make use of the identity $\varphi(g)/\varphi(\mathrm{rad}(g)^k)=g/\mathrm{rad}(g)^k$). Let us compute $p_\ell(g,h)$ depending on the prime $\ell\mid g$. If $g_\ell<\min(k,z_\ell)$, then $p_\ell(g,h)=0$, so that we may restrict the sum in (31) to the divisors g such that $(\mathrm{rad}(g)^k,z)\mid g$.

Case 1: $\ell\nmid h$. The conditions on the indices hold only for $s=e=0$. Thus, if $g_\ell=\min(k,z_\ell)$, then $p_\ell(g,h)=-1/\varphi(\ell^k)$, otherwise $p_\ell(g,h)=0$.

Case 2: $\ell\mid h$ *and* $h_\ell=g_\ell=z_\ell$. The sums reduce to the indices s,e such that $s+e\geqslant h_\ell$ (recall that $k\geqslant2$). Hence, we have

$$p_\ell(g,h)=\frac{1}{\varphi(\ell^k)\ell^{(r+1)h_\ell}}\frac{\ell^{r+1}(\ell-1)}{\ell^{r+1}-1}.$$

Case 3: $\ell\mid h$ *and* $h_\ell<g_\ell=z_\ell$. The conditions on the indices become $s+e=h_\ell$ and $k+s\geqslant g_\ell$. Hence, we have: $p_\ell(g,h)=0$ if $g_\ell-h_\ell>k$; $p_\ell(g,h)=-1/(\varphi(\ell^k)\ell^{(r+1)h_\ell})$ if $g_\ell-h_\ell=k$; $p_\ell(g,h)=(\ell-1)/(\varphi(\ell^k)\ell^{(r+1)h_\ell})$ if $g_\ell-h_\ell<k$.

Case 4: $\ell \mid h$ *and* $g_\ell < z_\ell$. The conditions on the indices become $s + e = h_\ell$ and $k + s = g_\ell$. Thus, we have: if $g_\ell - h_\ell = k$, then $p_\ell(g, h) = -1/(\varphi(\ell^k)\ell^{(r+1)h_\ell})$; if $g_\ell - h_\ell = k - 1$, then $p_\ell(g, h) = \ell/(\varphi(\ell^k)\ell^{(r+1)h_\ell})$; otherwise, $p_\ell(g, h) = 0$. □

6. Prescribing valuations for the order

In this section we apply Theorem 1 to prove an asymptotic formula for the number of primes $\mathfrak{p}$ of K for which the order of $(G \bmod \mathfrak{p})$ has some prescribed ℓ-adic valuations for finitely many given primes ℓ.

Theorem 21. *Let K be a number field and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. Let F/K be a finite Galois extension, and let C be a conjugacy-stable subset of* $\mathrm{Gal}(F/K)$. *Consider finitely many prime numbers ℓ, and for each of them fix a nonnegative integer a_ℓ. Set $k = \prod \ell$ and $m = \prod \ell^{a_\ell}$, where ℓ runs through the considered primes. Consider the set of primes of K given by*

$$\mathcal{V} = \left\{ \mathfrak{p} : v_\ell(\mathrm{ord}_\mathfrak{p}(G)) = a_\ell \ \forall \ell \mid k, \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\},$$

where we are assuming that $\mathfrak{p} \notin \mathcal{P}(G)$ and $\mathfrak{p}$ does not ramify in F. Then, for $0 < \varepsilon < 1$ we have

$$\mathcal{V}(x) = \frac{x}{\log x} \sum_{f \mid k} \mu(f) \varrho_{C,mf} + O_\varepsilon \left(\tau(k) x \left(\frac{(\log\log x)^2}{\log x} \right)^{1 + \frac{1-\varepsilon}{3(r+1)}} \right),$$

where, for $t \geqslant 1$, $\varrho_{C,t}$ is as in (2)*, so that the set $\mathcal{V}$ has natural density*

$$\gamma_{C,k,m} := \sum_{f \mid k} \sum_{n \mid (fm)^\infty} \sum_{d \mid fm} \frac{\mu(f)\mu(d) c(fmn, dn)}{[F_{fmn,dn} : K]}$$

(with $c(a, b)$ as in (3)*). The constant implied by the O-term depends only on ε, F, K, G.*

It follows from Proposition 15 that the series $\gamma_{C,k,m}$ is convergent.

Proof. We must have that $\mathrm{ord}_\mathfrak{p}(G)$ is divisible by m and not by $m\ell$ for any prime factor ℓ of k. Hence applying the inclusion-exclusion principle and Theorem 1 we obtain the desired formula. □

Notice that $\gamma_{C,k,m}$ is given by a finite sum of terms of the form $\pm\varrho_{C,t}$.

Remark 22. Let k be a positive integer. The density of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_\mathfrak{p}(G)$ is coprime with k and $(\mathfrak{p}, F/K) \subseteq C$ is given by

$$\sum_{f \mid k} \mu(f) \varrho_{C,f}.$$

This follows directly from Theorem 1 and it is a special case of Theorem 21.

In the following we provide an explicit formula for the special case of trivial condition on the Frobenius.

Corollary 23. *Let K be a number field and let G be a torsion-free subgroup of $K^\times$ of positive rank r. Let $k, m \geqslant 1$ be integers with k squarefree and* $\mathrm{rad}(m) \mid k$. *Let $\gamma_{k,m}$ be the natural*

density of the set of primes $\mathfrak{p}$ of K such that $v_\ell(\mathrm{ord}_\mathfrak{p}(G)) = v_\ell(m)$ for all $\ell \mid k$ (where $\mathfrak{p} \notin \mathcal{P}(G)$). Then there is an integer z, which depends only on K and G, such that

$$\gamma_{k,m} = \frac{1}{\varphi(m)} \prod_{\substack{\ell \mid m \\ \ell \nmid z}} \frac{(\ell-1)(\ell^r-1)}{\ell^{r+1}-1} \prod_{\substack{\ell \mid k \\ \ell \nmid mz}} \left(1 - \frac{\ell(\ell^r-1)}{(\ell^{r+1}-1)(\ell-1)}\right) \cdot \sum_{\substack{g \mid z \\ (m,z) \mid g \\ \mathrm{rad}(g) \mid k}} \sum_{h \mid g} \frac{p(g,h)}{[K_{g,h} : K]},$$

where, for $h \mid g$, we set $p(g,h) = 0$ if and only if at least one of the following conditions holds:

- *there is $\ell \mid (k,g)$, $\ell \nmid m$, such that $v_\ell(g/h) > 1$,*
- *there is $\ell \mid (g,m)$, $\ell \nmid h$, such that we have $v_\ell(g) \notin \{v_\ell(z), v_\ell(m), v_\ell(m)+1\}$, or $v_\ell(g) = v_\ell(z) > v_\ell(m)+1$,*
- *there is $\ell \mid (h,m)$, such that we have $v_\ell(g/h) > v_\ell(m)+1$, or we have $v_\ell(z/g) > 0$ and $v_\ell(g/h) < v_\ell(m) - 1$;*

else we define $p(g,h) = \frac{\varphi(g)}{h} \cdot q_1(g,h) q_2(g,h)$, with

$$q_1(g,h) = \prod_{\substack{\ell \mid g, \ell \nmid m \\ v_\ell(g/h)=1}} \frac{-1}{\ell-1} \cdot \prod_{\substack{\ell \mid h, \ell \nmid m \\ v_\ell(z/h)=0}} \frac{\ell^{r+1}}{\ell^{r+1}-1} \cdot \prod_{\substack{\ell \mid h, \ell \nmid m \\ v_\ell(h)=v_\ell(g)<v_\ell(z)}} \frac{\ell}{\ell-1}$$

(the primes involved in these products are coprime with m), and

$$q_2(g,h) = \prod_{\substack{\ell \mid (h,m) \\ v_\ell(z/h)=0}} \frac{-\ell^r(\ell-1)^2}{\ell^{r+1}-1} \cdot \prod_{\substack{\ell \mid (g,m) \\ v_\ell(g/h)=v_\ell(m)+1}} \frac{-1}{\ell} \cdot \prod_{\substack{\ell \mid g, \ell \nmid h \\ v_\ell(g)=v_\ell(z)\leqslant v_\ell(m)}} \frac{\ell-1}{\ell} \cdot \prod_{\substack{\ell \mid (h,m), v_\ell(z/g)>0 \\ v_\ell(g/h)=v_\ell(m)}} 2 \cdot$$
$$\prod_{\substack{\ell \mid h, v_\ell(z/g)=0 \\ 0<v_\ell(g/h)<v_\ell(m)}} \frac{-(\ell-1)^2}{\ell} \cdot \prod_{\substack{\ell \mid h, v_\ell(z/g)=0 \\ v_\ell(g/h)=v_\ell(m)>0}} \frac{2\ell-1}{\ell} \cdot \prod_{\substack{\ell \mid h, v_\ell(z/g)>0 \\ v_\ell(g/h)=v_\ell(m)-1}} -\ell$$

(the primes involved in these products are prime factors of m).

Proof. The proof is similar to that of Theorem 18 and does not contain new ingredients: one needs to first apply [12, Theorem 1.1], then transform the obtained inner sums into a product on the prime factors ℓ of k, and compute these through a certain case distinction. □

7. Conditional results assuming GRH

In this section we show how Theorems 1 and 2 can be improved if we assume (GRH) for the Dedekind zeta functions of number fields of the type $K_{m,n}$. In fact, in this case we can apply the stronger version of the Chebotarev density theorem, namely [15, Théorème 4] or [18, Theorem 2], and we obtain smaller error terms. Let us first apply this theorem to cyclotomic-Kummer extensions of K.

Lemma 24. *Let F/K be a Galois extension of number fields, C a conjugacy-stable subset of $\mathrm{Gal}(F/K)$, and let G be a finitely generated and torsion-free subgroup of $K^\times$. Assuming (GRH), the number of primes $\mathfrak{p}$ of K with $\mathrm{N}\,\mathfrak{p} \leqslant x$ which split completely in $K_{m,n}$, where $n \mid m$, and such that the Frobenius conjugacy class $(\mathfrak{p}, F/K)$ is in C (in other words, $(\mathfrak{p}, F/K) \subseteq C_{m,n}$, where $C_{m,n}$ is as in* (13)*) is given by*

$$\pi(F_{m,n}/K, C_{m,n})(x) = \frac{|C_{m,n}|}{[F_{m,n} : K]} \mathrm{Li}(x) + O_{F,G}\left(\sqrt{x}\log(mx)\right). \tag{32}$$

Proof. Applying [15, Théorème 4] we have

$$\frac{|C_{m,n}|}{[F_{m,n}:K]}\operatorname{Li}(x)+O\left(\frac{|C_{m,n}|}{[F_{m,n}:K]}\sqrt{x}\log\left(\left|d_{F_{m,n}}\right|x^{[F_{m,n}:\mathbb{Q}]}\right)\right).$$

Recalling that $|C_{m,n}|\leqslant[F:K]$ and applying Lemma 9, we can reduce the error term to

$$O_F\left(\sqrt{x}\cdot\frac{\log\left|d_{F_{m,n}}\right|}{[F_{m,n}:\mathbb{Q}]}+\sqrt{x}\log x\right)=O_{F,G}\left(\sqrt{x}\log m+\sqrt{x}\log x\right). \qquad \square$$

Theorem 25. *With the setup of Theorem 1, assuming (GRH), for all $0<\varepsilon<1/4$ we have*

$$\mathcal{P}_m(x)=\operatorname{Li}(x)\varrho_{C,m}+O_{F,K,G,\varepsilon}(x^{3/4+\varepsilon}).$$

Proof. We follow the proof of Theorem 1. Recall (16), where $\mathcal{B}_n$ was defined in the proof of Lemma 11. Applying first Lemma 11, and then Lemma 24 to the functions $\pi^1_{mn,dn}(x)$ (notice that (32) also holds if we restrict to the primes of K of degree 1), setting $y:=x^{1/4}$ we obtain:

$$\mathcal{P}_m(x)=\operatorname{Li}(x)\varrho_{C,m}+O\left(\sum_{n\leqslant y/m}\sum_{d\mid m}\sqrt{x}\log(mnx)\right)+O\left(\frac{\sqrt{x}}{\log x}\right) \tag{33}$$

$$+O\left(\operatorname{Li}(x)\sum_{\substack{n\mid m^\infty\\ nm>y}}\sum_{d\mid m}\frac{\mu(d)c(mn,dn)}{[F_{mn,dn}:K]}\right)+O\left(\sum_{\substack{n\mid m^\infty\\ nm>y}}\mathcal{B}_n(x)\right). \tag{34}$$

The first O-term in (33) is bounded by

$$\tau(m)\sqrt{x}\left(\sum_{n\leqslant y/m}\log n+\sum_{n\leqslant y/m}2\log x\right)\ll x^{3/4}\log x.$$

For $0<\varepsilon<1/4$ and $z>y$, the two O-terms in (34) are bounded by

$$\frac{x\log\log x}{x^{1/4-\varepsilon}\log x}\qquad\text{and}\qquad x\Big(\frac{\log\log x}{\log(x/z)x^{1/4-\varepsilon}}+\frac{1}{z^{1-4\varepsilon}}\Big),$$

respectively. Taking $z=\sqrt{x}$ and collecting all error terms yields the formula in the statement. $\square$

Corollary 26. *Assume (GRH). With the setup of Theorem 2, we have*

$$\mathcal{N}_k(x)=\operatorname{Li}(x)\beta_{C,k}+O_{F,K,G}\left(\frac{x}{\log^2 x}\right).$$

Moreover, with the setup of Theorem 21, for all $0<\varepsilon<1/4$ we have

$$\mathcal{V}(x)=\operatorname{Li}(x)\gamma_{C,k,m}+O_{F,K,G,\varepsilon}\big(\tau(k)x^{3/4+\varepsilon}\big).$$

Proof. As for the first assertion, it is sufficient to follow the proof of Theorem 2, making use of Theorem 25 instead of Theorem 1. This yields

$$\mathcal{N}_k(x)=\operatorname{Li}(x)\beta_{C,k}+O\left(\frac{x}{(\log x)^{1+a(k-1-\eta)}}\right)+O\big(x^{3/4+\varepsilon}(\log x)^a\big).$$

We may conclude by taking $a=1/(k-1-\eta)$ (with η,ε sufficiently small). The second assertion is a direct consequence of Theorem 25. $\square$

8. NUMERICAL DATA

In this section we provide several examples of densities computed with the formulas of Theorem 18 and Corollaries 20 and 23. All values have been verified with SageMath [14] by computing the approximated density that considers only primes up to a certain bound. In particular, we have tested these formulas for K and G as in the several numerical examples from [1, 6–9] (notice that in [1, Table 3, left side] the density for the fifth and seventh entries should both read $121/960$).

Let K be a number field and G a finitely generated subgroup of $K^\times$. Recall the notation ϱ_m introduced in Theorem 18. In Tables 1-4 we provide several examples of densities ϱ_m.

G	ϱ_2	ϱ_3	ϱ_4	ϱ_6	ϱ_9	ϱ_{12}	ϱ_{16}	ϱ_{27}
$\langle 2\rangle$	$17/24$	$3/8$	$5/12$	$17/64$	$1/8$	$5/32$	$1/24$	$1/24$
$\langle 16\rangle$	$1/12$	$3/8$	$1/24$	$1/32$	$1/8$	$1/64$	$1/96$	$1/24$
$\langle 3\rangle$	$2/3$	$3/8$	$1/3$	$5/16$	$1/8$	$1/16$	$1/12$	$1/24$
$\langle 27\rangle$	$2/3$	$1/8$	$1/3$	$5/48$	$1/24$	$1/48$	$1/12$	$1/72$
$\langle 2, 3\rangle$	$195/224$	$6/13$	$27/56$	$333/728$	$2/13$	$3/14$	$5/56$	$2/39$
$\langle 16, 27\rangle$	$75/112$	$5/13$	$75/224$	$235/728$	$5/39$	$95/1456$	$75/896$	$5/117$
$\langle 2, 27, 25\rangle$	$839/960$	$37/80$	$59/120$	$17723/38400$	$37/240$	$1073/4800$	$11/120$	$37/720$

TABLE 1. Examples of densities ϱ_m with $K = \mathbb{Q}$

G	ϱ_2	ϱ_3	ϱ_4	ϱ_6	ϱ_9	ϱ_{12}	ϱ_{16}	ϱ_{27}
$\langle 2\rangle$	$17/24$	$3/4$	$5/12$	$17/32$	$1/4$	$5/16$	$1/24$	$1/12$
$\langle 16\rangle$	$1/12$	$3/4$	$1/24$	$1/16$	$1/4$	$1/32$	$1/96$	$1/12$
$\langle 3\rangle$	$5/6$	$3/4$	$1/6$	$5/8$	$1/4$	$1/8$	$1/24$	$1/12$
$\langle 27\rangle$	$5/6$	$1/4$	$1/6$	$5/24$	$1/12$	$1/24$	$1/24$	$1/36$
$\langle 2, 3\rangle$	$111/112$	$12/13$	$13/28$	$333/364$	$4/13$	$3/7$	$3/56$	$4/39$
$\langle 16, 27\rangle$	$47/56$	$10/13$	$19/112$	$235/364$	$10/39$	$95/728$	$19/448$	$10/117$
$\langle 2, 27, 25\rangle$	$479/480$	$37/40$	$29/60$	$17723/19200$	$37/120$	$1073/2400$	$7/120$	$37/360$

TABLE 2. Examples of densities ϱ_m with $K = \mathbb{Q}(\zeta_3)$

G	ϱ_2	ϱ_3	ϱ_4	ϱ_6	ϱ_9	ϱ_{12}	ϱ_{16}	ϱ_{27}
$\langle 2\rangle$	$11/12$	$3/4$	$5/6$	$11/16$	$1/4$	$5/8$	$1/12$	$1/12$
$\langle 16\rangle$	$1/6$	$3/4$	$1/12$	$1/8$	$1/4$	$1/16$	$1/48$	$1/12$
$\langle 3\rangle$	$2/3$	$3/4$	$1/3$	$1/2$	$1/4$	$1/4$	$1/12$	$1/12$
$\langle 27\rangle$	$2/3$	$1/4$	$1/3$	$1/6$	$1/12$	$1/12$	$1/12$	$1/36$
$\langle 2, 3\rangle$	$55/56$	$12/13$	$13/14$	$165/182$	$4/13$	$6/7$	$3/28$	$4/39$
$\langle 16, 27\rangle$	$19/28$	$10/13$	$19/56$	$95/182$	$10/39$	$95/364$	$19/224$	$10/117$
$\langle 2, 27, 25\rangle$	$239/240$	$37/40$	$29/30$	$8843/9600$	$37/120$	$1073/1200$	$7/60$	$37/360$

TABLE 3. Examples of densities ϱ_m with $K = \mathbb{Q}(\zeta_4, \sqrt{3})$

G	ϱ_2	ϱ_3	ϱ_4	ϱ_6	ϱ_9	ϱ_{12}	ϱ_{16}	ϱ_{27}
$\langle 2\zeta_4\rangle$	$2/3$	$3/8$	$1/3$	$1/4$	$1/8$	$1/8$	$1/12$	$1/24$
$\langle 16\zeta_4\rangle$	$47/48$	$3/8$	$23/24$	$47/128$	$1/8$	$23/64$	$1/48$	$1/24$
$\langle 3\zeta_4\rangle$	$5/6$	$3/8$	$2/3$	$11/32$	$1/8$	$5/16$	$1/6$	$1/24$
$\langle 27\zeta_4\rangle$	$5/6$	$1/8$	$2/3$	$11/96$	$1/24$	$5/48$	$1/6$	$1/72$
$\langle 2\zeta_4, 3\zeta_4\rangle$	$13/14$	$6/13$	$5/7$	$165/364$	$2/13$	$3/7$	$5/28$	$2/39$
$\langle 16\zeta_4, 27\rangle$	$1791/1792$	$5/13$	$447/448$	$4475/11648$	$5/39$	$1115/2912$	$75/448$	$5/117$
$\langle 2\zeta_4, 27, 25\rangle$	$29/30$	$37/80$	$11/15$	$259/600$	$37/240$	$259/1200$	$11/60$	$37/720$

TABLE 4. Examples of densities ϱ_m with $K = \mathbb{Q}(\zeta_4)$

Recall the notation β_k from Corollary 20 (which is the density of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_{\mathfrak{p}}(G)$ is k-free), and the constants $A_{k,r}$ defined in (30). In Table 5 we show some values for these constants $A_{k,r}$, approximated by considering only the primes ℓ up to 10^5. In Tables 6 and 7 we provide some examples of densities β_k, expressed both as rational multiples of the constants $A_{k,r}$ and as approximated value.

$A_{k,r}$	$k=2$	$k=3$	$k=4$	$k=5$	$k=6$	$k=7$	$k=8$
$r=1$	0.530712	0.788163	0.901926	0.953511	0.977581	0.989060	0.994618
$r=2$	0.434934	0.734313	0.875354	0.940597	0.971280	0.985966	0.993091
$r=3$	0.401045	0.714103	0.865118	0.935552	0.968798	0.984741	0.992484
$r=4$	0.386687	0.705354	0.860624	0.933316	0.967691	0.984192	0.992211
$r=5$	0.380106	0.701307	0.858528	0.932267	0.967169	0.983932	0.992082

TABLE 5. Examples of constants $A_{k,r}$ approximated ($\ell < 10^5$)

G	β_2	β_3	β_4	β_5
$\langle 2\rangle$	$\frac{3}{4}A_{2,1} \approx 0.398$	$\frac{121}{115}A_{3,1} \approx 0.829$	$\frac{805}{781}A_{4,1} \approx 0.930$	$\frac{5029}{4945}A_{5,1} \approx 0.970$
$\langle 16\rangle$	$\frac{69}{56}A_{2,1} \approx 0.654$	$\frac{517}{460}A_{3,1} \approx 0.886$	$\frac{3325}{3124}A_{4,1} \approx 0.960$	$\frac{20437}{19780}A_{5,1} \approx 0.985$
$\langle 3\rangle$	$\frac{15}{14}A_{2,1} \approx 0.569$	$\frac{121}{115}A_{3,1} \approx 0.829$	$\frac{805}{781}A_{4,1} \approx 0.930$	$\frac{5029}{4945}A_{5,1} \approx 0.970$
$\langle 27\rangle$	$\frac{55}{42}A_{2,1} \approx 0.695$	$\frac{77}{69}A_{3,1} \approx 0.880$	$\frac{2461}{2343}A_{4,1} \approx 0.947$	$\frac{15181}{14835}A_{5,1} \approx 0.976$
$\langle 2, 3\rangle$	$\frac{135}{176}A_{2,2} \approx 0.334$	$\frac{875}{814}A_{3,2} \approx 0.789$	$\frac{5989}{5750}A_{4,2} \approx 0.912$	$\frac{37823}{36994}A_{5,2} \approx 0.962$
$\langle 16, 27\rangle$	$\frac{899}{704}A_{2,2} \approx 0.555$	$\frac{21935}{19536}A_{3,2} \approx 0.824$	$\frac{48763}{46000}A_{4,2} \approx 0.928$	$\frac{914711}{887856}A_{5,2} \approx 0.969$
$\langle 2, 27, 25\rangle$	$\frac{95201}{119193}A_{2,3}$ ≈ 0.320	$\frac{105751169}{96766014}A_{3,3}$ ≈ 0.780	$\frac{524265887}{500045142}A_{4,3}$ ≈ 0.907	$\frac{116376274169}{113496822354}A_{5,3}$ ≈ 0.959

TABLE 6. Examples of densities β_k over $K = \mathbb{Q}(\zeta_3)$

G	β_2	β_3	β_4	β_5
$\langle 2\rangle$	$\frac{1}{4}A_{2,1} \approx 0.133$	$A_{3,1} \approx 0.788$	$A_{4,1} \approx 0.902$	$A_{5,1} \approx 0.953$
$\langle 16\rangle$	$\frac{11}{8}A_{2,1} \approx 0.730$	$\frac{23}{20}A_{3,1} \approx 0.906$	$\frac{47}{44}A_{4,1} \approx 0.963$	$\frac{95}{92}A_{5,1} \approx 0.985$
$\langle 3\rangle$	$\frac{3}{7}A_{2,1} \approx 0.227$	$\frac{91}{115}A_{3,1} \approx 0.624$	$\frac{709}{781}A_{4,1} \approx 0.819$	$\frac{4729}{4945}A_{5,1} \approx 0.912$
$\langle 27\rangle$	$\frac{11}{21}A_{2,1} \approx 0.278$	$\frac{283}{345}A_{3,1} \approx 0.647$	$\frac{2149}{2343}A_{4,1} \approx 0.827$	$\frac{331}{345}A_{5,1} \approx 0.915$
$\langle 2,3\rangle$	$\frac{9}{176}A_{2,2} \approx 0.0222$	$\frac{329}{407}A_{3,2} \approx 0.594$	$\frac{2641}{2875}A_{4,2} \approx 0.804$	$\frac{17795}{18497}A_{5,2} \approx 0.905$
$\langle 16,27\rangle$	$\frac{1073}{2112}A_{2,2} \approx 0.221$	$\frac{5501}{6512}A_{3,2} \approx 0.620$	$\frac{128873}{138000}A_{4,2} \approx 0.817$	$\frac{286741}{295952}A_{5,2} \approx 0.911$
$\langle 2,27,25\rangle$	$\frac{23323}{953544}A_{2,3}$ ≈ 0.00981	$\frac{79247549}{96766014}A_{3,3}$ ≈ 0.585	$\frac{3234551969}{3500315994}A_{4,3}$ ≈ 0.799	$\frac{109490052089}{113496822354}A_{5,3}$ ≈ 0.903

TABLE 7. Examples of densities β_k over $K = \mathbb{Q}(\zeta_4)$

Finally, recall the notation $\gamma_{k,m}$ from Corollary 23 (which is the density of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_{\mathfrak{p}}(G)$ has ℓ-adic valuation equal to $v_\ell(m)$ for every prime $\ell \mid k$). In Table 8 we provide some examples of these densities.

G	$\gamma_{6,1}$	$\gamma_{6,2}$	$\gamma_{6,3}$	$\gamma_{6,4}$	$\gamma_{6,6}$	$\gamma_{6,9}$	$\gamma_{6,12}$
$\langle 2\rangle$	$35/192$	$35/192$	$7/96$	$5/24$	$7/96$	$7/288$	$1/12$
$\langle 16\rangle$	$55/96$	$5/192$	$11/48$	$5/384$	$1/96$	$11/144$	$1/192$
$\langle 3\rangle$	$13/48$	$1/12$	$1/24$	$13/96$	$1/6$	$1/72$	$1/48$
$\langle 27\rangle$	$5/16$	$1/4$	$1/72$	$5/32$	$1/18$	$1/216$	$1/144$
$\langle 2,3\rangle$	$365/2912$	$423/2912$	$1/364$	$101/728$	$59/364$	$1/1092$	$10/91$
$\langle 16,27\rangle$	$391/1456$	$225/2912$	$15/364$	$785/5824$	$125/728$	$5/364$	$95/4368$
$\langle 2,27,25\rangle$	$801/6400$	$927/6400$	$37/28800$	$443/3200$	$4699/28800$	$37/86400$	$1591/14400$

TABLE 8. Examples of densities $\gamma_{k,m}$ over $K = \mathbb{Q}(\sqrt{-5})$

ACKNOWLEDGMENTS

The author would like to thank Francesco Pappalardi for suggesting the problem and for helpful discussions (Remark 14 is due to him). Also many thanks to Antonella Perucca for her continuous support and valuable feedback. The Sage code used for the examples has been partly adapted from Sebastiano Tronto's code *kummer-degrees* available on GitHub.

REFERENCES

[1] DEBRY, C. - PERUCCA, A., *Reductions of algebraic integers*, J. Number Theory **167** (2016) 259–283.
[2] LAGARIAS, J. C. - ODLYZKO, A. M., *Effective versions of the Chebotarev density theorem*, in Algebraic number fields: L-functions and Galois properties, Proc. Sympos., Univ. Durham, pages 409–464. Academic Press, London, 1977.
[3] MOREE, P., *On primes p for which d divides* $\mathrm{ord}_p(g)$, Funct. Approx. Comment. Math. **33** (2005), 85—95.
[4] MOREE, P., *Artin's primitive root conjecture – a survey*, Integers **12** (2012), no. 6, 1305–1416.
[5] NEUKIRCH, J., *Algebraic Number Theory*, Springer, Berlin Heidelberg, 1999.
[6] PAPPALARDI, F., *Square free values of the order function*, New York J. Math. **9** (2003), 331–344.
[7] PAPPALARDI, F., *Divisibility of reduction in groups of rational numbers*, Math. Comp. **84** (2015), no. 291, 385–407.
[8] PERUCCA, A., *The order of the reductions of an algebraic integer*, J. Number Theory **148** (2015) 121–136.
[9] PERUCCA, A., *Reductions of algebraic integers II*, in *Women in numbers Europe II*, 19-–33, Assoc. Women Math. Ser., 11, Springer, Cham, 2018.

[10] PERUCCA, A. - SGOBBA, P., *Kummer theory for number fields and the reductions of algebraic numbers*, Int. J. Number Theory **15** (2019), no. 8, 1617–1633.
[11] 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.
[12] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *The degree of Kummer extensions of number fields*, Int. J. Number Theory **17** (2021), no. 5, 1091–1110.
[13] ROSSER, J. B. - SCHOENFELD, L., *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), no. 1, 64–94.
[14] *SageMath, the Sage Mathematics Software System (Version 9.2)*, The Sage Developers, 2021, `https://www.sagemath.org`.
[15] SERRE J.-P., *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1), 123–201, 1981.
[16] STARK, H. M., *Some effective cases of the Brauer-Siegel theorem*, Invent. Math. **23** (2), 135–152, 1974.
[17] WIERTELAK, K., *On the density of some sets of primes, IV*, Acta Arith. **43** (1984), no. 2, 177—190.
[18] 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 AV. DE LA FONTE, 4364 ESCH-SUR-ALZETTE, LUXEMBOURG

Email address: `pietro.sgobba@uni.lu`