PhD-FSTM-2022-070
The Faculty of Science, Technology and Medicine

DISSERTATION

Defence held on 06/07/2022 in Esch-sur-Alzette
to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG EN MATHÉMATIQUES

by

Pietro SGOBBA
Born on 24 August 1994 in Bari (Italy)

REDUCTIONS OF ALGEBRAIC NUMBERS AND ARTIN'S CONJECTURE ON PRIMITIVE ROOTS

Dissertation defence committee

Dr. Antonella Perucca, dissertation supervisor
Professor, Université du Luxembourg

Dr. Gabor Wiese, Chairman
Professor, Université du Luxembourg

Dr. Peter Stevenhagen
Professor, University of Leiden

Dr. Pieter Moree
Professor, Max Planck Institute for Mathematics, Bonn

Dr. Francesco Pappalardi
Professor, Università Roma Tre

PhD-FSTM-2022-070
The Faculty of Science, Technology and Medicine

DISSERTATION

Defence held on 06/07/2022 in Esch-sur-Alzette
to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG EN MATHÉMATIQUES

by

Pietro SGOBBA
Born on 24 August 1994 in Bari (Italy)

REDUCTIONS OF ALGEBRAIC NUMBERS AND ARTIN'S CONJECTURE ON PRIMITIVE ROOTS

Dissertation defence committee

Dr. Antonella Perucca, dissertation supervisor
Professor, Université du Luxembourg

Dr. Gabor Wiese, Chairman
Professor, Université du Luxembourg

Dr. Peter Stevenhagen
Professor, University of Leiden

Dr. Pieter Moree
Professor, Max Planck Institute for Mathematics, Bonn

Dr. Francesco Pappalardi
Professor, Università Roma Tre

Contents

Chapter 1

Introduction

The problems addressed in this thesis are closely related to Artin's conjecture on primitive roots, which is a classical conjecture in number theory. In 1927, Artin claimed that given a rational number g which is neither $0, \pm 1$, nor a square, there are infinitely many prime numbers p such that g is a primitive root modulo p. In 1967, under the assumption of the Generalized Riemann Hypothesis (GRH)[1], Hooley [16] proved the conjecture, as well as an asymptotic formula for the number of primes satisfying the condition. He proved that the number of primes $p \leqslant x$ such that g is a primitive root modulo p is given by

$$\frac{x}{\log x} \sum_{n \geqslant 1} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, g^{1/n}) : \mathbb{Q}]} + O\left(\frac{x \log\log x}{\log^2 x}\right), \tag{1.1}$$

where ζ_n is a primitive n-th root of unity and μ is the Möbius function. It is well-known that a prime q divides the index of the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ generated by $(g \bmod p)$ (assuming that the p-adic valuation of g is zero) if and only if p splits completely in the cyclotomic-Kummer field $\mathbb{Q}(\zeta_q, g^{1/q})$. Therefore, saying that g is a primitive root modulo p is equivalent to saying that there is no prime q dividing $(p-1)$ such that p splits completely in $\mathbb{Q}(\zeta_q, g^{1/q})$. By Chebotarev's density theorem, the density of primes p splitting completely in a number field K is given by $1/[K : \mathbb{Q}]$. Hence, roughly speaking, formula (1.1) is obtained by applying the inclusion-exclusion principle and by making use of the (conditional) quantitative version of Chebotarev's density theorem (e.g. [53, Théorème 4]). See [31, Section 5] for a detailed summary of the proof.

Hooley also showed that the natural density of the above set of primes is equal to a rational number, depending on g, times Artin's constant

$$A := \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558...$$

An unconditional proof does not exist to date. However, in 1986 Heath-Brown [13] proved a result implying that there are at most two prime numbers for which Artin's conjecture fails (taking g to be one of these prime numbers). Similarly, there are at most three positive squarefree integers for which Artin's conjecture fails.

Over the past decades, several variations of the conjecture have been considered, and we refer to Moree's survey [31] for an extensive account on this topic. Some of these variations are set in the context of number fields. Let K be a number field, and for $\alpha \in K^\times$, let us consider the multiplicative order of its reduction modulo all but finitely many primes of K. We discard those primes that appear

[1] By (GRH) it is meant the extended Riemann hypothesis for the Dedekind zeta-function of a number field.

in the prime factorization of the fractional ideal (α), so that for all considered primes $\mathfrak{p}$ the reduction $(\alpha \bmod \mathfrak{p})$ is a well-defined element of $k_{\mathfrak{p}}^{\times}$, where $k_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$. Thus, to each $\mathfrak{p}$ as above we may associate a positive integer, namely the order of $(\alpha \bmod \mathfrak{p})$. One can then study properties of this function and, more specifically, the number of primes $\mathfrak{p}$ such that the order of $(\alpha \bmod \mathfrak{p})$ satisfies certain conditions.

In 1975, Cooke and Weinberger [9] considered the analogue of Artin's conjecture over number fields. For K a number field and $\alpha \in K^{\times}$ not a root of unity, they studied the primes $\mathfrak{p}$ of K such that $(\alpha \bmod \mathfrak{p})$ (as above, we may suppose that this reduction is nonzero) generates $k_{\mathfrak{p}}^{\times}$. Then, assuming (GRH), an analogous asymptotic formula to (1.1) holds, with $\mathbb{Q}$ replaced by K and g by α.

Over $\mathbb{Q}$, Wiertelak [58], and more recently, Pappalardi [36] and Moree [26], investigated the primes p for which the order of $(g \bmod p)$ is divisible by a given integer. More generally, Chinen and Murata [5] and Moree [27] considered the primes p for which the order of $(g \bmod p)$ lies in a given arithmetic progression. Ziegler [59] generalized the latter work to number fields by considering the same condition for the order of $(\alpha \bmod \mathfrak{p})$, where α and $\mathfrak{p}$ are as above.

The main goal of this thesis is studying primes of number fields satisfying conditions on the order of the reductions of some given algebraic numbers. In the rest of the introduction we present our main results. In Section 1.1 we set some general notation. In Section 1.2 we introduce our work on the primes for which the order lies in a given arithmetic progression, and on how they distribute among the residue classes modulo some fixed integer. These results are then developed in Chapters 3 and 4, which consist of the articles [44] (joint with Perucca) and [55], respectively. In Section 1.3 we describe our achievements for primes satisfying some given divisibility properties on the order, such as the order being divisible by a given integer. This is the content of Chapter 5, which consists of the preprint [54].

Chapter 2 concerns Kummer theory for number fields. Indeed, as one can see from (1.1), the degree of number fields of the form $\mathbb{Q}(\zeta_n, g^{1/n})$, for $n \geqslant 1$, play an important role in the computation of the natural densities (i.e. the coefficients of $x/\log x$), and it will be the case also for our problems. Therefore, Chapter 2, which summarizes the articles [47, 49] (joint with Perucca and Tronto), is an essential part of this thesis, and it is devoted to the computation of the degrees of cyclotomic-Kummer extensions of number fields for all parameters at once, e.g. for all integers n in the case above. We refer to Section 2.1 for a complete overview of our methods and achievements.

In Section 1.4 I outline other projects that I have worked on during my Ph.D., but which are not part of this thesis. Namely, some other results in Kummer theory for number fields (joint with Hörmann, Perucca, Tronto), and some results concerning prime divisors of generalizations of the Genocchi numbers (joint with Moree). Notice that these are independent topics on their own.

1.1 Notation

Throughout the thesis we will use the following notation. Let K be a number field, and let $\mathfrak{p}$ be a prime of K. We denote by $v_{\mathfrak{p}}$ the $\mathfrak{p}$-adic valuation over K, and if p is a rational prime, then v_p is the p-adic valuation over $\mathbb{Q}$. For $\alpha \in K^{\times}$, supposing that $v_{\mathfrak{p}}(\alpha) = 0$, we write $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ for the multiplicative order of $(\alpha \bmod \mathfrak{p})$ in $k_{\mathfrak{p}}^{\times}$, where $k_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$. Let G be a finitely generated subgroup of $K^{\times}$. Similarly, supposing that $v_{\mathfrak{p}}(g) = 0$ for all $g \in G$ (it suffices to consider g varying in a set of generators of G), we write $\mathrm{ord}_{\mathfrak{p}}(G)$ for the multiplicative order of $(G \bmod \mathfrak{p})$ in $k_{\mathfrak{p}}^{\times}$, where $(G \bmod \mathfrak{p})$ is the subgroup generated by the reductions $(g \bmod \mathfrak{p})$ for $g \in G$. For $m \geqslant 1$, we denote by ζ_m a primitive m-th root of unity in a fixed algebraic closure $\bar{K}$ of K.

Let $m, n \geqslant 1$ be integers. We write (m, n) for $\gcd(m, n)$, and $[m, n]$ for $\mathrm{lcm}(m, n)$ (unless this

simplified notation would lead to confusion), and similarly $[n_1, \dots, n_r]$ is the least common multiple of the integers $n_1, \dots, n_r$. We write $\mathrm{rad}(n) := \prod_{p|n \text{ prime}} p$ for the radical of n, and n^∞ for the supernatural number $\prod_{p|n \text{ prime}} p^\infty$. Also, $\tau(n)$ is the function counting the positive divisors of n, and as customary, μ is the Möbius function and φ is Euler's totient function (unless stated differently).

1.2 On the distribution of the order over residue classes

Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$. Let $\mathfrak{p}$ run through all primes of K such that $v_\mathfrak{p}(g) = 0$ for all $g \in G$ (it suffices to discard finitely many primes), and consider $\mathrm{ord}_\mathfrak{p}(G)$, namely the multiplicative order of $(G \bmod \mathfrak{p})$. We are interested in the primes $\mathfrak{p}$ such that the order lies in a fixed arithmetic progression, say $\mathrm{ord}_\mathfrak{p}(G) \equiv a \bmod d$ for some integers a and $d \geqslant 2$. For b a nonzero integer different from ± 1, the density of rational primes p for which the multiplicative order of $(b \bmod p)$ satisfies this condition has been studied in various papers by Chinen and Murata [5, 33, 6, 7], and by Moree [27, 28, 29] (for a survey of these papers see Moree [30]). More precisely, Chinen and Murata considered the cases $d = 4$ in [5, 33], d a prime power in [6], and general d in [7], whereas Moree considered the case $d = 3$ in [27], general d in [28], and he showed some properties of the corresponding natural densities in [29]. For $\alpha \in \mathcal{O}_K$ nonzero and not a root of unity, where $\mathcal{O}_K$ is the ring of integers of K, Ziegler [59] considered the condition $\mathrm{ord}_\mathfrak{p}(\alpha) \equiv a \bmod d$. Jointly with Perucca, we proved the following result (as a generalization of [59, Theorem 1]).

Theorem 1.1 ([43, Theorem 1.3])**.** *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$. Let a and $d \geqslant 2$ be integers. Assuming (GRH), the number of primes $\mathfrak{p}$ of K, with norm up to x, such that $\mathrm{ord}_\mathfrak{p}(G) \equiv a \bmod d$ (where $v_\mathfrak{p}(g) = 0$ for all $g \in G$), is given by*

$$\frac{x}{\log x} \sum_{n,t \geqslant 1} \frac{\mu(n) c(n,t)}{[K(\zeta_{[d,n]t}, G^{1/nt}) : K]} + O\left(\frac{x}{\log^{3/2} x}\right), \tag{1.2}$$

where $c(n,t) \in \{0,1\}$, and $c(n,t) = 1$ if and only if $(1+at, d) = 1$, $(d,n) \mid a$ and the automorphism of $\mathbb{Q}(\zeta_{dt})$ which sends ζ_{dt} to ζ_{dt}^{1+at} is the identity on $\mathbb{Q}(\zeta_{dt}) \cap K(\zeta_{nt}, G^{1/nt})$.

The proof of this result consists of several steps which follow Hooley's method for Artin's conjecture. One transforms the condition on the order into conditions on the index and on the Frobenius automorphisms of cyclotomic extensions of K. In particular, the proof requires the assumption of (GRH), in order to apply the stronger version of Chebotarev's density theorem [53, Théorème 4]. Theorem 1.1 can be refined by introducing a condition on the Frobenius conjugacy class at $\mathfrak{p}$.

In Chapter 3, which contains the results of [44] (joint with Perucca), we investigate properties of the natural density in (1.2), such as its rationality and positivity, and some equidistribution properties over the residue classes modulo d, under certain conditions. For instance, writing $\delta(a,d)$ for the considered density, for ℓ a prime number we prove that, if $\ell \mid a$ and $e \geqslant 1$, or $4 \mid a$ and $e \geqslant 2$ for $\ell = 2$, then $\delta(a, \ell^e)$ is a strictly positive rational number, and that for distinct a's with same ℓ-adic valuation the value of the density is the same. If we assume that $\zeta_\ell \in K$ or $\zeta_4 \in K$ for $\ell = 2$, then the same statement holds also for a coprime to ℓ or 2, respectively.

In Chapter 4, which contains the results of [55], we prove (under GRH) a multidimensional variation of Theorem 1.1 by fixing $\alpha_1, \dots, \alpha_r \in K^\times$ generating a group of rank r, and considering the primes $\mathfrak{p}$ of K such that each order $\mathrm{ord}_\mathfrak{p}(\alpha_i)$ lies in a given arithmetic progression depending on i. The following is a special case of Theorem 4.1.

Theorem 1.2. *Let K be a number field and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ generating a group of rank r. For $1 \leqslant i \leqslant r$, let a_i and $d_i \geqslant 2$ be integers. Assuming (GRH), the number of primes $\mathfrak{p}$ of K with norm up to x such that $\mathrm{ord}_{\mathfrak{p}}(\alpha_i) \equiv a_i \bmod d_i$ (where $v_{\mathfrak{p}}(\alpha_i) = 0$) for all i is given by*

$$\frac{x}{\log x} \sum_{t_1,\dots,t_r \geqslant 1} \sum_{n_1,\dots,n_r \geqslant 1} \frac{(\prod_i \mu(n_i)) c(n_1, t_1, \dots, n_r, t_r)}{[K_{n_1,t_1,\dots,n_r,t_r} : K]} + O\left(\frac{x}{(\log x)^{1+\frac{1}{r+1}}} \right),$$

where $K_{n_1,t_1,\dots,n_r,t_r}$ is the compositum of the fields $K(\zeta_{[d_i,n_i]t_i}, \alpha_i^{1/n_i t_i})$ for $1 \leqslant i \leqslant r$, and the coefficient $c(n_1, t_1, \dots, n_r, t_r)$ is either 0 or 1, and it is 1 if and only if there is a K-automorphism σ of $K_{n_1,t_1,\dots,n_r,t_r}$ such that, for all i, σ is the identity on $K(\zeta_{n_i t_i}, \alpha_i^{1/n_i t_i})$ and $\sigma(\zeta_{d_i t_i}) = \zeta_{d_i t_i}^{1+a_i t_i}$. In particular, it is nonzero only if $(1 + a_i t_i, d_i) = 1$ and $(d_i, n_i) \mid a_i$ for all i.

The proof of the previous theorem is a variation of the proof of Theorem 1.1. An essential tool that we need is a multidimensional variation of the estimate $\sum_{n>x} \frac{1}{\varphi(n)n} = O(1/x)$, see Theorem 4.5. Moreover, as a question stemming from the proof, we study the primes $\mathfrak{p}$ for which the multiplicative index of $(\alpha_i \bmod \mathfrak{p})$ equals a given integer for each i. In particular, from our results we can deduce the following, which is a multidimensional version of Artin's conjecture over number fields. This is a special case of Theorem 4.3.

Theorem 1.3. *Let K be a number field and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ generating a group of rank r. Assuming (GRH), the number of primes $\mathfrak{p}$ of K with norm up to x such that α_i is a primitive root modulo $\mathfrak{p}$ for all i is given by*

$$\frac{x}{\log x} \sum_{n_1,\dots,n_r \geqslant 1} \frac{\prod_i \mu(n_i)}{[K(\zeta_{[n_1,\dots,n_r]}, \alpha_1^{1/n_1}, \dots, \alpha_r^{1/n_r}) : K]} + O\left(\frac{x \log\log x}{\log^2 x} \right). \tag{1.3}$$

Notice that this question was considered by Matthews [24] over the rationals. Thanks to the results of Chapter 2 the density in (1.3) can be reduced to a closed formula, namely a rational multiple of a certain absolute constant, see Proposition 4.21.

1.3 Divisibility conditions on the order

Let K be a number field, and let G be a finitely generated (without loss of generality torsion-free) subgroup of $K^\times$. In Chapter 5, which consists of the results of [54], we prove *unconditionally* some asymptotic formulas for the number of primes $\mathfrak{p}$ of K satisfying certain divisibility conditions on $\mathrm{ord}_{\mathfrak{p}}(G)$ (supposing $v_{\mathfrak{p}}(g) = 0$ for all $g \in G$), namely the order being divisible by a given integer, or being k-free for a given $k \geqslant 2$ (for $k = 2$ this means squarefree, and in general it means that all p-adic valuations are less than k), or having prescribed ℓ-adic valuations for finitely many primes ℓ. These questions have been considered over $\mathbb{Q}$ by Pappalardi in [36] for $\mathrm{ord}_p(a)$, with a a rational number, and in [37] for $\mathrm{ord}_p(G)$, with $G \subseteq \mathbb{Q}^\times$ of finite rank. The condition $\mathrm{ord}_p(a)$ being divisible by an integer was also studied by Moree in [29], and previously by Wiertelak [58]. Over number fields, the case of the order being coprime with a given prime number, respectively with a given integer, was considered by Debry and Perucca in [10], respectively by Perucca in [40]. These results also allow to deal with the condition of prescribing finitely many ℓ-adic valuations, but the asymptotics were not considered.

The following is a special case of Theorem 5.1, which is the main result of Chapter 5.

Theorem 1.4. *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 be a positive integer. For all $0 < \varepsilon < 1$, the number of primes $\mathfrak{p}$ of K with norm up to x such that $m \mid \mathrm{ord}_{\mathfrak{p}}(G)$ (and $v_{\mathfrak{p}}(g) = 0$ for all $g \in G$) is given by*

$$\frac{x}{\log x} \sum_{n \mid m^\infty} \sum_{d \mid m} \frac{\mu(d)}{[K(\zeta_{mn}, G^{1/dn}) : K]} + O_\varepsilon \left(x \left(\frac{(\log\log x)^2}{\log x} \right)^{1+\frac{1-\varepsilon}{3(r+1)}} \right).$$

Theorem 1.4 can also be refined by introducing a condition on the Frobenius conjugacy class at $\mathfrak{p}$. The essential tool obtained and applied in the proof of Theorem 1.4 is an unconditional effective version of Chebotarev's density theorem for cyclotomic-Kummer extensions of number fields, see Theorem 5.10, a result which is likely to have further applications for similar questions. Here we state its special case for the primes splitting completely.

Theorem 1.5. *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 $m, n \geqslant 1$ be integers such that $n \mid m$. There exist constants c_1 and c_2 such that, uniformly for*

$$m \leqslant c_1 \left(\frac{\log x}{(\log\log x)^2} \right)^{\frac{1}{3(r+1)}},$$

the number of primes $\mathfrak{p}$ of K with norm up to x which split completely in $K(\zeta_m, G^{1/n})$ is given by

$$\frac{1}{[K(\zeta_m, G^{1/n}) : K]} \mathrm{Li}(x) + O\left(x e^{-c_2 \sqrt[3]{\log x \cdot \log\log x}} \right).$$

The constants c_1 and c_2 and the constant implied by the O-term only depend on K and G.

Thanks to our results in Kummer theory from Chapter 2, the density of Theorem 1.4 as well as the densities of the other sets of primes mentioned above, can be reduced to some rational expression (or to a rational multiple of certain constants for the case of k-free order). The following theorem concerns the primes for which the order is coprime to a given integer. As an example of our results, we also provide a rational formula for the density. This is a special case of Theorem 5.21 combined with Theorem 5.24.

Theorem 1.6. *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 be a positive squarefree integer. For all $0 < \varepsilon < 1$, the number of primes $\mathfrak{p}$ of K with norm up to x such that $\mathrm{ord}_{\mathfrak{p}}(G)$ is coprime to k (and $v_{\mathfrak{p}}(g) = 0$ for all $g \in G$) is given by*

$$\frac{x}{\log x} \sum_{f \mid k} \sum_{n \mid f^\infty} \sum_{d \mid f} \frac{\mu(f)\mu(d)}{[K(\zeta_{fn}, G^{1/dn}) : K]} + O_\varepsilon \left(\tau(k) \cdot x \left(\frac{(\log\log x)^2}{\log x} \right)^{1+\frac{1-\varepsilon}{3(r+1)}} \right).$$

Moreover, there is an integer z (depending only on K and G) such that the natural density is given by the following rational expression:

$$\prod_{\substack{q \mid k \text{ prime} \\ q \nmid z}} \left(1 - \frac{q(q^r - 1)}{(q^{r+1} - 1)(q - 1)} \right) \cdot \sum_{\substack{g \mid z \\ \mathrm{rad}(g) \mid k}} \sum_{h \mid g} \mu\left(\frac{g}{h}\right) \frac{p(g,h)}{[K(\zeta_g, G^{1/h}) : K]},$$

where, for $h \mid g$, we set

$$p(g,h) = \frac{\varphi(g)}{\varphi(g/h)h} \cdot \prod_{\substack{q \mid h \text{ prime} \\ q \nmid (z/h)}} \frac{q^{r+1}}{q^{r+1} - 1} \cdot \prod_{\substack{q \mid h \text{ prime} \\ v_q(h) = v_q(g) < v_q(z)}} \frac{q}{q - 1}.$$

1.4 Related work

1.4.1 Kummer theory

The starting point of this work is my Master thesis *Kummer theory for number fields and applications*, whose results have been published in [43] (joint with Perucca). This article provides on the one hand some explicit results on the failure of maximality for the degrees of Kummer extensions of number fields, on the other hand a result on the primes of number fields for which the order of the reductions of algebraic numbers lies in a given arithmetic progression (see Theorem 1.1).

During my Ph.D., jointly Hörmann, Perucca and Tronto, I have worked on some further projects concerning Kummer theory for number fields. As we will mention in Chapter 2, in [46, 17] we study the degrees of Kummer extensions over $\mathbb{Q}$ and over quadratic fields, respectively, and we provide a procedure to compute them. In [18] we study the cyclic subextensions of $\mathbb{Q}(\zeta_{3p})/\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$, where p is a prime number such that $p \equiv 1 \bmod 3$ and $p \equiv 1 \bmod 4$, respectively.

In [45], which is an addendum to [10], we study how the 2-divisibility properties of G, namely of a finitely generated group of algebraic numbers in a number field K, change if we extend the base field to $K(\zeta_4)$. Notice that what we mean here by divisibility properties is formalized in Section 2.2 in terms of divisibility parameters. Taking $\alpha_1, \dots, \alpha_r \in K^\times$ generating a group G of rank r, in [48] we make use of the ℓ-divisibility parameters of G, where ℓ is a fixed prime number, to compute the degree of the extensions

$$K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})/K(\zeta_{\ell^m})$$

for all $m, n_1, \dots, n_r \geqslant 1$ such that $m \geqslant \max_i(n_i)$. Notice that in this work we provide a different method from the one described in Section 2.3.

1.4.2 Generalized Genocchi numbers

This short section is a brief introduction to the the recent preprint [32] (joint with Moree) about generalizations of the classical Genocchi numbers.

Motivated by an application in the theory of modular forms concerning abundancy of Ramanujan-style congruences of prime level ℓ, we investigate the prime divisors of the sequence of rational numbers $H_n := (1 - \ell^n)B_n/n$ for $n \geqslant 1$, where B_n is the n-th Bernoulli number. By prime divisor of a sequence of rational numbers a_n we intend a prime number p such that $v_p(a_n) \geqslant 1$ and $a_n \neq 0$ for some $n \geqslant 1$. The numbers H_n can be viewed as modified *ℓ-Genocchi numbers* $G_n = \ell(1 - \ell^n)B_n$, which in turn are generalizations of the classical Genocchi numbers $2(1 - 2^n)B_n$, for $n \geqslant 1$. Recall that an odd prime p is B-irregular if p divides the numerator of at least one of the numbers $B_2, B_4, \dots, B_{p-3}$ ($B_n = 0$ for all $n > 1$ odd), else it is called B-regular. Similarly, we say that an odd prime p is *irregular* if p divides at least one of the numbers $G_2, G_4, \dots, G_{p-3}$, otherwise it is called *regular*.

Prime divisors of the sequence H_n can be studied in terms of irregularity for the ℓ-Genocchi numbers. Therefore we study the distribution of the irregular primes (also with the assumption that they lie in a given arithmetic progressions) by expressing the irregularity in terms of B-irregularity and conditions modulo p. Hence we can bound the density of irregular primes by taking advantage of techniques used in the study of Artin's primitive root conjecture, and, making use of Siegel's conjecture on the density of B-irregular primes, we can also obtain conjectures for these densities. For $\ell = 2$ this partially generalizes earlier work by Hu, Kim, Moree and Sha [19].

Chapter 2

Kummer theory for number fields

2.1 The degree of Kummer extensions of number fields

Let K be a number field, and let us work in a fixed algebraic closure $\bar{K}$. Let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a multiplicative subgroup G of $K^\times$ of positive rank r. We are interested in the cyclotomic-Kummer extensions

$$K\big(\zeta_m, \sqrt[n]{G}\big)/K\,,$$

where m, n are integers such that $n \mid m$, and $\sqrt[n]{G}$ is the group of all n-th roots of the elements of G (in particular, it includes all n-th roots of unity). We also keep the notation introduced in Section 1.1. More generally, we consider the extensions

$$K\big(\zeta_m, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r}\big)/K\,,$$

where $m, n_1, \dots, n_r$ are nonnegative integers such that $n_i \mid m$ for all $i \in \{1, \dots, r\}$. More precisely, fixing K and $\alpha_1, \dots, \alpha_r$, we want to compute the degree of these extensions for all $m, n_1, \dots, n_r$ as above. Equivalently, we may study the ratio

$$\frac{\varphi(m) \cdot n_1 \cdots n_r}{\big[K\big(\zeta_m, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r}\big) : K\big]},$$

which we refer to as the failure of maximality for the degree. For all parameters $m, n_1, \dots, n_r$, this ratio is bounded from above by a constant which only depends on K and the α_i's. This is a classical result of Kummer theory, which also holds more generally (under some assumptions) for products of abelian varieties and tori, see [2, Theorem 1] and [50] (see also [14, Lemme 14] and [3, Theorème 5.2]). Notice that Perucca and the author gave an explicit proof for the existence of this constant, see [43, Theorem 3.1]. A classical consequence of this property is the following.

Theorem 2.1 ([47, Theorem 1.1])**.** *Let K be a number field, and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a subgroup of $K^\times$ of rank r. There exists a positive integer x (which depends only on K and $\alpha_1, \dots, \alpha_r$) such that we have*

$$\big[K\big(\zeta_m, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r}\big) : K\big(\zeta_{\gcd(m,x)}, \sqrt[\gcd(n_1,x)]{\alpha_1}, \dots, \sqrt[\gcd(n_r,x)]{\alpha_r}\big)\big] = \frac{\varphi(m)}{\varphi(\gcd(m,x))} \cdot \prod_{i=1}^{r} \frac{n_i}{\gcd(n_i,x)}$$

for all nonnegative integers $n_1, \dots, n_r$ and for all integers m such that $n_i \mid m$ for all i.

In particular, the above result reduces the computation of the cyclotomic-Kummer degree to finitely many cases and hence there exist parametric formulas for the degree (where the parameters are $m, n_1, \dots, n_r$) which involve only a finite case distinction. Therefore, we want to describe explicitly the integer x (Theorem 2.1 only guarantees the existence of x).

We assume that we know how to compute the *cyclotomic failure* of the number field K, namely the ratio $\varphi(m)/[K(\zeta_m) : K]$ for $m \geqslant 1$. Hence we may study the Kummer degrees

$$\left[K\left(\zeta_m, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r}\right) : K(\zeta_m)\right]$$

for all $m, n_1, \dots, n_r \geqslant 1$ such that $n_i \mid m$ for all i. There are essentially two reasons for which this degree might not be maximal, i.e. for which the ratio

$$C(m, n_1, \dots, n_r) := \frac{\prod_{i=1}^{r} n_i}{\left[K\left(\zeta_m, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r}\right) : K(\zeta_m)\right]}, \tag{2.1}$$

which we call the *Kummer failure at* $m, n_1, \dots, n_r$, might be larger than the trivial value 1. If one of the α_i's is an n-th power in K (with $n \mid n_i$), then we lose a factor n from the maximal possible degree $\prod_i n_i$. Similarly, factors are lost also if, for some $n \geqslant 1$, there is a product of powers of the α_i's, with exponents not all divisible by n, which is an n-th power in K. Another reason for the nontriviality of the Kummer failure is that roots of the α_i's might be contained in $K(\zeta_m)$ for some $m \geqslant 1$, and this is related to the abelian radical extensions of K.

In this chapter we are going to consider two ways of approaching the Kummer failure. The first method consists in decomposing $C(m, n_1, \dots, n_r)$ into factors of two types, according to the two phenomena mentioned above. The second method consists in exploiting the theory of entanglement groups, introduced by Lenstra, to study more generally the structure of radical extensions. Let us discuss further both approaches in Sections 2.1.2 and 2.1.3, respectively. Section 2.2 concerns divisibility properties of algebraic numbers, which are preliminaries to our results. In Section 2.3 we discuss in detail our results for the decomposition of the Kummer failure, whereas the results related to entanglement groups are provided in Section 2.4. Finally, in Section 2.5 we provide some examples for the computation of Kummer degrees using both methods.

2.1.1 Notation

Let us fix some notation to be used throughout this chapter, and recall the notation introduced in Section 1.1. Let K be a number field. We denote by μ_K the group of roots of unity in K, and by ω its order, i.e. $\omega = \sharp\mu_K$, so that $\mu_K = \mu_\omega$. Moreover, for a prime number ℓ we set $\omega_\ell := v_\ell(\omega)$. For $n \geqslant 1$, μ_n is the group of n-th roots of unity, and we define $\mu_{\ell^\infty} := \cup_{n \geqslant 1} \mu_n$ and $\mu_{\ell^\infty} := \cup_{n \geqslant 1} \mu_{\ell^n}$. We write both $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\mu_n)$ for the n-th cyclotomic field, and we will also use the notation $\mathbb{Q}(\zeta_\infty)$ for $\mathbb{Q}(\mu_\infty)$, and $\mathbb{Q}(\zeta_{\ell^\infty})$ for $\mathbb{Q}(\mu_{\ell^\infty})$. The notation over K rather than $\mathbb{Q}$ is analogous.

2.1.2 The ℓ-adic and ℓ-adelic failure

Let K be a number field, and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a multiplicative subgroup of $K^\times$ of positive rank r. Consider the ratio $C(M, N_1, \dots, N_r)$ from (2.1) for all $M, N_1, \dots, N_r \geqslant 1$ such that $N_i \mid M$ for all i. In order to make formulas more legible, we write $N_i = \prod_\ell \ell^{n_i}$ for the prime factorization of each N_i (each exponent n_i depends on ℓ). Moreover, setting $n := \max_i(n_i)$, we define

$$A_\ell(\ell^{n_1}, \dots, \ell^{n_r}) := \frac{\ell^{\sum_i n_i}}{\left[K\left(\zeta_{\ell^n}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}\right) : K(\zeta_{\ell^n})\right]}$$

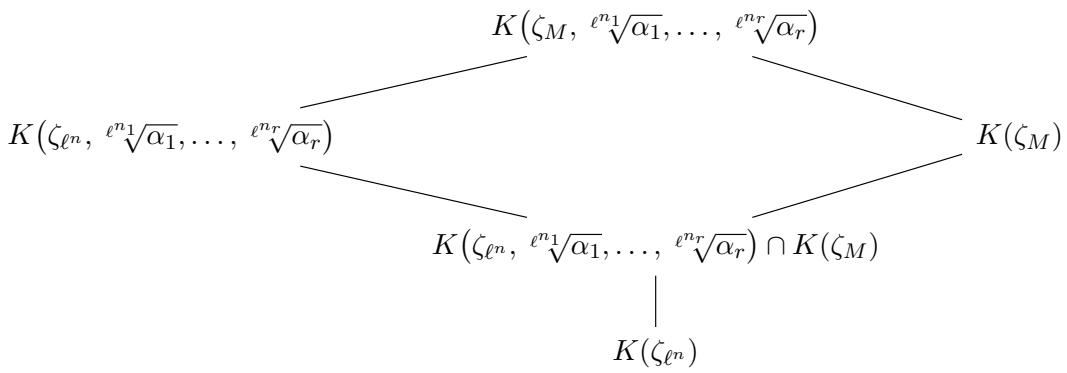
(notice that $A_\ell(\ell^{n_1},\dots,\ell^{n_r}) = C(\ell^n,\ell^{n_1},\dots,\ell^{n_r})$) and

$$B_\ell(M,\ell^{n_1},\dots,\ell^{n_r}) := \left[K\left(\zeta_{\ell^n},\ \sqrt[\ell^{n_1}]{\alpha_1},\dots,\ \sqrt[\ell^{n_r}]{\alpha_r}\right)\cap K(\zeta_M) : K(\zeta_{\ell^n})\right], \tag{2.2}$$

which we call the *ℓ-adic failure* and the *ℓ-adelic failure*, respectively. Notice that the degree (2.2) arises as the ratio of two degrees, namely

$$\frac{[K(\zeta_{\ell^n},\ \sqrt[\ell^{n_1}]{\alpha_1},\dots,\ \sqrt[\ell^{n_r}]{\alpha_r}) : K(\zeta_{\ell^n})]}{[K(\zeta_M,\ \sqrt[\ell^{n_1}]{\alpha_1},\dots,\ \sqrt[\ell^{n_r}]{\alpha_r}) : K(\zeta_M)]}.$$

This is also illustrated in the diagram below:



Thus, we can decompose (2.1) as

$$\begin{aligned} C(M,N_1,\dots,N_r) &= \prod_\ell C(M,\ell^{n_1},\dots,\ell^{n_1}) \\ &= \prod_\ell A_\ell(\ell^{n_1},\dots,\ell^{n_r})\cdot B_\ell(M,\ell^{n_1},\dots,\ell^{n_r}). \end{aligned} \tag{2.3}$$

Therefore the study of the Kummer failure can be reduced to the study of the ℓ-adic and ℓ-adelic failures, separately, where ℓ is a fixed prime number. Thanks to results from [10], the ℓ-adic failure can be computed by making use of certain divisibility parameters, which we introduce in Section 2.2, describing the ℓ-divisibility of the group G generated by the α_i's. In particular, the ℓ-adic failure is bounded because the ℓ-divisibility of the elements of G does not affect the eventual ℓ-adic growth of the degrees (for sufficiently large parameters, increasing a parameter by one corresponds to increasing the degree by a factor ℓ). The ℓ-adelic failure, which concerns the intersections of the ℓ-adic Kummer extensions with cyclotomic extensions of K, is bounded because these extensions are abelian over K, and the roots of G which generate abelian extensions are related to the torsion group of K. We describe how to reduce the computation of the ℓ-adelic failure to finitely many cases.

The main result for this part of the chapter is the following.

Theorem 2.2 ([47, Theorem 5.4])**.** *Let K be a number field, and let $\alpha_1,\dots,\alpha_r \in K^\times$ be such that they generate a multiplicative group of rank r. There are computable integers M_0 and N_0 with $N_0 \mid M_0$, depending only on K and $\alpha_1,\dots,\alpha_r$, such that for all integers $M,N_1,\dots,N_r$ with $N_i \mid M$ for all $i\in\{1,\dots,r\}$ we have*

$$C(M,N_1,\dots,N_r) = C(\gcd(M,M_0),\gcd(N_1,N_0),\dots,\gcd(N_r,N_0)),$$

where $C(M,N_1,\dots,N_r)$ is as in (2.1)*.*

Throughout the chapter, whenever we talk about the computability of a certain object depending only on K and $\alpha_1, \dots, \alpha_r$ (or G), we mean that there exists *an explicit finite procedure* that, given as input the field K and $\alpha_1, \dots, \alpha_r$ (or G), produces as output the desired object. In order to work with our theoretical algorithms in practice, one can assume that the field K is *presented* in the sense of [11, Chapter 19], which implies that its elements are representable on a computer. Moreover, when working with the group G, one should know a finite set of generators for it. We refer to Remark 2.32 for more details about the computations.

A direct consequence of Theorem 2.2 is the following statement.

Corollary 2.3 ([47, Corollary 5.5])**.** *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of rank r. There are computable integers M_0 and N_0, which depend only on K and G (they may be taken as in Theorem 2.2), such that for all integers M, N with $N \mid M$, we have*

$$\frac{N^r}{[K(\zeta_M, \sqrt[N]{G}) : K(\zeta_M)]} = \frac{(N, N_0)^r}{[K(\zeta_{(M,M_0)}, \sqrt[(N,N_0)]{G}) : K(\zeta_{(M,M_0)})]}.$$

Perucca, Tronto and the author provided a procedure to compute explicitly all cyclotomic-Kummer degrees $[K(\zeta_m, \sqrt[n]{G}) : K]$ for all m, n with $n \mid m$, and in particular the ℓ-adelic failure, for $K = \mathbb{Q}$ in [46] (the computation of one single degree over $\mathbb{Q}$ was also achieved in [35, Theorem 4.2]), and for K a quadratic field in [17] (jointly with Hörmann). The case of multiquadratic fields and quartic cyclic fields was considered in [42].

In Section 2.3 we will summarize our achievements and provide proofs for the main results. The content of this section is developed in the article [47].

2.1.3 Entanglement groups

Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. Our goal is computing the degree of the cyclotomic-Kummer extension

$$K\big(\sqrt[n]{G}\big)/K$$

(recall that the group $\sqrt[n]{G}$ includes all n-th roots of unity). As a tool to study the structure of such extensions and to compute with radical expressions, Lenstra introduced the theory of *entanglements* in [23]. This theory takes care, in particular, of the fact that radicals of elements of G can be contained in cyclotomic extensions of K, and to study this phenomenon one may as well suppose that G is torsion-free and of positive rank. Consider the group $\mathrm{Aut}_{K^\times}(B_n)$ consisting of the group automorphisms of $B_n := \langle K^\times, \sqrt[n]{G}\rangle$ which are the identity on $K^\times$. The core of the theory is the so-called *entanglement group* $E(B_n)$, which is the quotient of $\mathrm{Aut}_{K^\times}(B_n)$ by the Galois group of $K(\sqrt[n]{G})/K$ (the latter is a normal subgroup of the former by [35, Theorem 1.6]). The group $E(B_n)$ should measure the additive relations between the radicals in $K(\sqrt[n]{G})$ and the n-th roots of unity. Palenstijn proved in [35, Theorem 1.6] that $E(B_n)$ is an abelian group, and it is clearly finite.

In Section 2.4 we formalize the objects of the theory and we describe and prove our results involving entanglement groups. All these results are published in the article [49], joint with Perucca and Tronto. In particular, we prove the following statement (which has been proven over $\mathbb{Q}$ in a different form by Palenstijn [35, Proposition 4.3]). Recall that ω is the order of the torsion part of $K^\times$.

Theorem 2.4 ([49, Theorem 1])**.** *Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. For $n \geqslant 1$, setting $B_n := \langle K^\times, \sqrt[n]{G}\rangle$ and $\Delta_n := \prod_{p \mid n \text{ prime}, \, p \nmid \omega} \frac{p-1}{p}$, we have*

$$\big[K\big(\sqrt[n]{G}\big) : K\big] = \frac{[B_n : K^\times]}{\sharp E(B_n)} \cdot \Delta_n \,.$$

The index $[B_n : K^\times]$ may be computed with a result by Debry and Perucca [10, Theorem 15], so the computation of the degree is reduced to the computation of the size of the entanglement group. The following result says in particular that $\sharp E(B_n)$ remains bounded as n varies, and that in order to compute the entanglement group $E(B_n)$ for all n it suffices to calculate $E(B_d)$ for all divisors d of some integer depending only on K and G. This result will be proven using Theorem 2.29, which is an assertion about the eventual maximal growth of the degrees of cyclotomic-Kummer extensions.

Theorem 2.5 ([49, Theorem 2])**.** *Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. For $n \geqslant 1$, set $B_n := \langle K^\times, \sqrt[n]{G}\rangle$. There is a computable integer $n_0 \geqslant 1$, depending only on K and G, such that for every $n \geqslant 1$ we have*

$$E(B_n) = E(B_{\gcd(n,n_0)})\,.$$

As a consequence of this result we recover the following assertion on the Kummer failure of the degree $[K(\sqrt[n]{G}) : K]$ (compare with Theorem 2.2).

Theorem 2.6 ([49, Theorem 39])**.** *Let K be a number field, and let G be a finitely generated subgroup of $K^\times$ of rank r. There is a computable integer n_0, which depends only on K and G, such that for every $n \geqslant 1$ we have*

$$\frac{\varphi(n)n^r}{[K(\sqrt[n]{G}) : K]} = \frac{\varphi(\gcd(n,n_0))\gcd(n,n_0)^r}{[K(\sqrt[\gcd(n,n_0)]{G}) : K]}\,.$$

We focus on the subgroup $B_{n,\mathrm{ab}}$ of B_n which consists of *abelian radicals*, by which we mean the elements $x \in \bar{K}^\times$ such that $x^m \in K^\times$ for some integer $m \geqslant 1$ and such that the extension $K(\mu_n, x)/K$ is abelian. Palenstijn proved in [35, Theorem 1.10] that there is a quite explicit description of the entanglement group $E(B_n)$ if $B_{n,\mathrm{ab}} = \langle K^\times, \mu, H\rangle$, where μ is a group of roots of unity and H is a group of *Kummer radicals*, i.e. consisting of all those radicals $x \in \bar{K}^\times$ such that $x^\omega \in K^\times$. Thus we want to express $B_{n,\mathrm{ab}}$ in terms of Kummer radicals and roots of unity, under certain assumptions. This will allow us to achieve the following result (where by 'divisibility' of an element in a group – denoted multiplicatively – we mean the supremum of the natural numbers n such that the element is an n-th power in the group).

Theorem 2.7 ([49, Theorem 3])**.** *Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. Suppose that every element of G has the same divisibility in $K^\times$ and in $K^\times/\mu_K$. For every $n \geqslant 1$, setting $B_n := \langle K^\times, \sqrt[n]{G}\rangle$, we have*

$$B_{n,\mathrm{ab}} = \langle K^\times, \mu_n, H_n\rangle\,,$$

where H_n is a group of Kummer radicals. Moreover, we have

$$E(B_n) = \mathrm{Gal}\left(K(H_n) \cap \mathbb{Q}(\mu_n)/\mathbb{Q}(\mu_{\gcd(n,\omega)})\right).$$

Notice that Theorem 2.7 would not be true without the divisibility assumption, see Example 2.27.

2.2 Strong ℓ-independence and divisibility parameters

2.2.1 Strongly ℓ-independent elements

Let K be a number field, and let ℓ be a prime number. We call $a \in K^\times$ *strongly ℓ-indivisible* if there is no root of unity ζ in K (whose order we may suppose to be a power of ℓ) such that $a\zeta \in K^{\times\ell}$. If

$\zeta_\ell \notin K$, then strongly ℓ-indivisible means not being an ℓ-th power; in general, it means that the class of the element in $K^\times/\mu_K$ is not an ℓ-th power.

If $a \in K^\times$ is not strongly ℓ-indivisible, then we can decompose it as the product of an element of $\mu_{\ell^{\omega_\ell}}$ times the ℓ-th power of some element of $K^\times$; if this element is not strongly ℓ-indivisible, then we can iterate the decomposition. So if $a \in K^\times$ is not a root of unity, then we can write it as $a = \zeta b^{\ell^d}$ for some strongly ℓ-indivisible element $b \in K^\times$, for some integer $d \geqslant 0$ and for some $\zeta \in \mu_{\ell^{\omega_\ell}}$. We refer to d as the *d-parameter for the ℓ-divisibility* of a (it is uniquely determined); we refer to b as the *strongly ℓ-indivisible part* of a (in general, it is only determined up to a root of unity); if ζ has order ℓ^h, then we refer to h as the *h-parameter for the ℓ-divisibility* of a (it may depend on the decomposition, and clearly we have $0 \leqslant h \leqslant \omega_\ell$).

We call $a_1, \dots, a_r \in K^\times$ *strongly ℓ-independent* if $a_1^{x_1} \cdots a_r^{x_r}$ is strongly ℓ-indivisible whenever $x_1, \dots, x_r$ are integers not all divisible by ℓ. If $\zeta_\ell \notin K$, then strongly ℓ-independent means that the classes of the elements in $K^\times/K^{\times\ell}$ are linearly independent in this $\mathbb{F}_\ell$-vector space; in general, we work instead with the $\mathbb{F}_\ell$-vector space $(K^\times/\mu_K)/(K^\times/\mu_K)^\ell$.

Strongly ℓ-independent elements are each strongly ℓ-indivisible, and for a single element the two notions coincide. Notice that if $e_1, \dots, e_r$ are integers coprime to ℓ and $a_1, \dots, a_r \in K^\times$ are strongly ℓ-independent, then also $a_1^{e_1}, \dots, a_r^{e_r}$ are strongly ℓ-independent.

2.2.2 Parameters describing the ℓ-divisibility

Let K be a number field, consider a finitely generated and torsion-free subgroup G of $K^\times$ of positive rank r, and fix some prime number ℓ. Given $g_1, \dots, g_r$ a basis of G as a $\mathbb{Z}$-module, we can write

$$g_i = \zeta_{\ell^{h_i}} \cdot b_i^{\ell^{d_i}}$$

for some strongly ℓ-indivisible element b_i of $K^\times$, for some integer $d_i \geqslant 0$ and for some root of unity $\zeta_{\ell^{h_i}}$ in K of order ℓ^{h_i}. We call $g_1, \dots, g_r$ an *ℓ-good basis* of G if their strongly ℓ-indivisible parts $b_1, \dots, b_r$ are strongly ℓ-independent or, equivalently, if $\sum_i d_i$ is maximal among the possible bases of G, see [10, Section 3.1]. In this case we call d_i and h_i the *d-parameters and the h-parameters for the ℓ-divisibility* of G in K, respectively. These parameters were introduced in [10, Section 3]. The d-parameters are unique up to reordering, while the multiset of the h-parameters may depend on the choice of the g_i's and the b_i's (but one could require additional conditions as to make the pairs (h_i, d_i) unique up to reordering, see [10, Appendix]).

From [10, Theorem 14] we know that an ℓ-good basis of G always exists. As proven there, if $g_1, \dots, g_r$ is not an ℓ-good basis, then there are integers x_i, not all divisible by ℓ, such that $a := \prod_i b_i^{x_i}$ is not strongly ℓ-indivisible. Up to replacing a, we may suppose that all x_i's are either zero or coprime to ℓ. Let $J = \{i : x_i \neq 0\}$, and without loss generality we may suppose that $d_1 = \max_{i \in J}(d_i)$. Since $\ell \nmid x_1$, there is an integer y such that $x_1 y \equiv 1 \bmod \ell$. Hence, replacing a with a^y divided by an ℓ-th power of b_1, we may suppose that $a = b_1 \prod_{j>1} b_j^{z_j}$ for some integers z_j. Then we replace g_1 with

$$g_1' := g_1 \prod_{i>1} g_i^{z_i \ell^{(d_1 - d_i)}} = \zeta \prod_{i>1} b_i^{z_i \ell^{d_1}} = \zeta a^{\ell^{d_1}},$$

where $\zeta \in \mu_K$, which has d-parameter strictly larger than d_1. Moreover, this is a change of basis because g_1'/g_1 is generated by $g_2, \dots, g_r$, and hence g_1 can be expressed in terms of $g_1', g_2, \dots, g_r$. This procedure allows changing the basis of G in such a way that the sum $\sum_i d_i$ increases strictly. The fact that this sum is bounded from above over all possible bases of G is justified in [10, Section 3.1] and is due to the fact that the elements of G are not infinitely many times ℓ-divisible.

Remark 2.8. As shown in [10, Section 6.1], the parameters for the ℓ-divisibility of G are computable. They are zero for all ℓ outside of a finite computable set of primes which depends only on K and G (for the d-parameters this is shown below in Proposition 2.9, while for the h-parameters it suffices that $\ell \nmid \omega$). To apply some of our results, we need to verify that for some given ℓ (with $\ell \mid \omega$) the h-parameters for the ℓ-divisibility can be taken to be zero: this amounts to testing whether the computable h-parameters from [10, Proposition 31] are zero.

Proposition 2.9 ([47, Proposition 4.5])**.** *The parameters for the ℓ-divisibility of G can be taken to be equal to zero for all but finitely many prime numbers ℓ. Moreover, the finite set of primes ℓ for which they might be nonzero can be computed.*

Proof. By [43, Theorem 2.7] there is a basis of G as a $\mathbb{Z}$-module consisting of strongly ℓ-independent elements for all but finitely many primes ℓ, so that parameters for the ℓ-divisibility of G in K might be not all zero only for finitely many primes ℓ.

The finite set S of these primes can be computed by [43, Proof of Theorem 2.7]. Following this reference, the set S consists of the primes ℓ such that $\zeta_\ell \in K$ and those involved in the following computations. Write $G = F \times H$ where F and H are subgroups of $K^\times$ such that $F \cap \mathcal{O}_K^\times = \{1\}$ and $H \subseteq \mathcal{O}_K^\times$ ($\mathcal{O}_K$ is the ring of integers of K), and consider a basis of G consisting of a basis $\{g_i\}$ of F and a basis $\{u_i\}$ of H as $\mathbb{Z}$-modules. We consider the prime ideal factorizations $(g_i) = \prod_j \mathfrak{p}_j^{e_{ij}}$ where the $\mathfrak{p}_j$'s are finitely many distinct primes of K, and without loss of generality we write $u_i = \prod_j b_j^{f_{ij}}$ where the b_j's form a system of fundamental units in K. Then when applying [43, Lemmas 2.4 and 2.5] we obtain that S contains the finitely many rational primes ℓ dividing a nonzero minor corresponding to a maximal square submatrix of the matrices (e_{ij}) and (f_{ij}), respectively. The considered basis of G consists of strongly ℓ-independent elements for all $\ell \notin S$. □

2.3 Reducing the computation of the Kummer failure

Let K be a number field, and let $\alpha_1, \ldots, \alpha_r$ be elements of $K^\times$ which generate a subgroup G of $K^\times$ of positive rank r. In this section we study the Kummer failure (2.1) through the ℓ-adic and ℓ-adelic failures, where ℓ denotes a prime number, as explained in Section 2.1.2.

2.3.1 Kummer extensions of degree a prime power

We fix a prime number ℓ and consider Kummer extensions of the form

$$K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \ldots, \sqrt[\ell^{n_r}]{\alpha_r})/K(\zeta_{\ell^m})$$

where $m, n_1, \ldots, n_r$ are nonnegative integers such that $m \geqslant \max_i(n_i)$, whose degree is a power of ℓ. Recall that for all nonnegative integers n, m with $m \geqslant n$ we write $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})$, and $K(\sqrt[\ell^n]{G})$ if $m = n$, for the field $K(\zeta_{\ell^m}, \sqrt[\ell^n]{\alpha_1}, \ldots, \sqrt[\ell^n]{\alpha_r})$.

Theorem 2.10 ([10, Theorem 18])**.** *Suppose that ℓ is odd or that $\zeta_4 \in K$. Let $\tau \geqslant 1$ be the largest integer satisfying $K(\zeta_\ell) = K(\zeta_{\ell^\tau})$. Let m and n be positive integers such that $m \geqslant \max(n, \tau)$. Then we have*

$$v_\ell[K\big(\zeta_{\ell^m}, \sqrt[\ell^n]{G}\big) : K(\zeta_{\ell^m})] = \max_{i \in \{1,\ldots,r\}}(h_i + \min(n, d_i) - m, 0) + \sum_{i=1}^{r} \max(n - d_i, 0)\,, \qquad (2.4)$$

where $d_1, \ldots, d_r, h_1, \ldots, h_r$ are parameters for the ℓ-divisibility of G in K.

Notice that Theorem 2.10 applies also when $\tau > m \geqslant n$, since $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G}) = K(\zeta_{\ell^\tau}, \sqrt[\ell^n]{G})$ for all $1 \leqslant m < \tau$, so that it is sufficient to replace m with τ in the formula (2.4).

Remark 2.11. If $m \geqslant n$, then the degree

$$\left[K\left(\zeta_{\ell^m}, \sqrt[\ell^n]{G}\right) : K(\zeta_{\ell^m})\right]$$

is computable and it depends only on the integers m, n and on finitely many parameters describing the ℓ-divisibility of G in the considered number field. Indeed, if ℓ is odd or $\zeta_4 \in K$, then it suffices to take the formula provided by Theorem 2.10 (because $m \geqslant \tau$ without loss of generality, the case $m = 0$ being trivial). Now, suppose that $\ell = 2$ and $\zeta_4 \notin K$. If $m \geqslant 2$, then we can extend the base field to $K(\zeta_4)$ and reduce to the previous case (notice that in [45] we proved that the 2-divisibility parameters of G over $K(\zeta_4)$ are determined by properties over K). We are left to compute the degree $[K(\sqrt{G}) : K]$, and this can be achieved with [10, Lemma 19].

Given ℓ, K and G, we set

$$s = \max_{i \in \{1,\dots,r\}} (\varepsilon,\, h_i + d_i)\,, \tag{2.5}$$

where $\varepsilon = 2$ if $\ell = 2$ and $\zeta_4 \notin K$, and $\varepsilon = 0$ otherwise, and where the integers d_i and h_i are parameters for the ℓ-divisibility of G in K (respectively, in $K(\zeta_4)$ if $\ell = 2$ and $\zeta_4 \notin K$). Notice that s is computable (see Remark 2.8) and it depends only on ℓ, K and G. Then it follows from (2.4) that for every $m \geqslant n \geqslant s$ we have (see [47, Lemma 4.3])

$$\left[K\left(\zeta_{\ell^m}, \sqrt[\ell^n]{G}\right) : K(\zeta_{\ell^m})\right] = \ell^{r(n-s)}\left[K\left(\zeta_{\ell^m}, \sqrt[\ell^s]{G}\right) : K(\zeta_{\ell^m})\right]. \tag{2.6}$$

For general parameters, we have that the integer s in (2.5) satisfies the identity

$$\left[K\left(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}\right) : K\left(\zeta_{\ell^m}, \sqrt[\ell^{m_1}]{\alpha_1}, \dots, \sqrt[\ell^{m_r}]{\alpha_r}\right)\right] = \prod_{i=1}^{r} \ell^{\max(n_i - s, 0)}\,, \tag{2.7}$$

for all $n_1, \dots, n_r, m$ with $m \geqslant \max_i(n_i)$, and where we set $m_i := \min(n_i, s)$ for all i (see [47, Proposition 4.8]). The proof of this statement is roughly achieved by first considering the case $n_i \geqslant s$ for all i, and then by dealing with the general case through an argument on the size of the degrees.

Proposition 2.12. *Fixing K and G, the integer s in* (2.5) *can be taken to be equal to zero for all but finitely many prime numbers ℓ, and the finite set of primes ℓ for which s might be nonzero can be computed.*

Proof. It follows directly from Proposition 2.9. □

Remark 2.13. Fix K and $\alpha_1, \dots, \alpha_r$. By (2.7) together with Proposition 2.12 one can deduce that for all but finitely many prime numbers ℓ we have

$$\left[K\left(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}\right) : K\right] = \varphi(\ell^m) \cdot \prod_{i=1}^{r} \ell^{n_i}\,.$$

Notice that we have $[K\left(\zeta_{\ell^m}\right) : K] = \varphi(\ell^m)$ for all but finitely many primes ℓ.

Remark 2.14. From the formula (2.7) we deduce that there is a computable integer A, which depends only on ℓ, K and $\alpha_1, \dots, \alpha_r$, such that

$$\frac{\prod_{i=1}^{r} \ell^{n_i}}{\left[K\left(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}\right) : K(\zeta_{\ell^m})\right]} \quad \text{divides} \quad A \tag{2.8}$$

for all nonnegative integers $n_1, \dots, n_r, m$ with $m \geqslant \max_i(n_i)$. Indeed, setting $m_i := \min(n_i, s)$, the ratio in (2.8) can be written as the product

$$\frac{\prod_{i=1}^r \ell^{n_i - m_i}}{\left[K\left(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}\right) : K\left(\zeta_{\ell^m}, \sqrt[\ell^{m_1}]{\alpha_1}, \dots, \sqrt[\ell^{m_r}]{\alpha_r}\right)\right]} \cdot \\ \cdot \frac{\prod_{i=1}^r \ell^{m_i}}{\left[K\left(\zeta_{\ell^m}, \sqrt[\ell^{m_1}]{\alpha_1}, \dots, \sqrt[\ell^{m_r}]{\alpha_r}\right) : K(\zeta_{\ell^m})\right]},$$

where the former factor equals 1 by (2.7), and the latter factor is a divisor of ℓ^{rs}. Hence, we may take $A = \ell^{rs}$, and by Proposition 2.12 we have $A = 1$ for all but finitely many prime numbers ℓ.

The bound $A = \ell^{rs}$ is in general optimal. Indeed, for the case $\ell \neq 2$ or $\zeta_4 \in K$ it suffices to consider ℓ^s-th powers of strongly ℓ-independent elements of K, so that the parameters for the ℓ-divisibility in (2.5) are $h_i = 0$ and $d_i = s$ for all $i \in \{1, \dots, r\}$.

Remark 2.14 says in particular that the ℓ-adic failure $A_\ell(\ell^{n_1}, \dots, \ell^{n_r})$ is bounded by ℓ^{rs}. In fact, a stronger property holds.

Lemma 2.15 ([47, Lemma 5.1])**.** *Let ℓ be a prime number and let s be as in* (2.5) *for G. For all integers $n_1, \dots, n_r$, we have*

$$A_\ell(\ell^{n_1}, \dots, \ell^{n_r}) = A_\ell(\gcd(\ell^{n_1}, \ell^s), \dots, \gcd(\ell^{n_r}, \ell^s)) .$$

In order to justify this lemma, the only additional step with respect to the argument of Remark 2.14 consists in replacing $n = \max_i(n_i)$ with $\max_i(m_i)$ for the cyclotomic subfield $K(\zeta_{\ell^n})$. This is nontrivial only if $n_j > s$ for some j, in which case we have $\max_i(m_i) = s$. It is sufficient to consider the equality

$$K\left(\zeta_{\ell^s}, \sqrt[\ell^{m_1}]{\alpha_1}, \dots, \sqrt[\ell^{m_r}]{\alpha_r}\right) \cap K(\zeta_{\ell^n}) = K(\zeta_{\ell^s}) ,$$

which holds because $K(\zeta_{\ell^s}, \sqrt[\ell^{m_1}]{\alpha_1}, \dots, \sqrt[\ell^{m_r}]{\alpha_r}) \subseteq K(\sqrt[\ell^s]{G})$ and the intersection of the latter field with $K(\zeta_{\ell^n})$ is equal to $K(\zeta_{\ell^s})$. The last assertion holds because $[K(\zeta_{\ell^m}, \sqrt[\ell^s]{G}) : K(\zeta_{\ell^m})]$ equals $[K(\zeta_{\ell^s}, \sqrt[\ell^s]{G}) : K(\zeta_{\ell^s})]$ by (2.4) (see also [47, Lemma 4.4]).

2.3.2 Intersection with cyclotomic extensions

Let ℓ be a prime number. We study the intersection of the fields $K(\zeta_{\ell^n}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})$ with the cyclotomic fields $K(\zeta_M)$, where $n_1, \dots, n_r$ are nonnegative integers, $M \geqslant 1$, $n = \max_i(n_i)$ and $\ell^n \mid M$.

Remark 2.16. Let $n_1, \dots, n_r, n$ be as above. Since we have

$$K\left(\zeta_{\ell^n}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}\right) \subseteq K\left(\sqrt[\ell^n]{G}\right) ,$$

by [43, Lemma 3.5] the ℓ-adelic failure in (2.2) divides $\ell^{r\omega_\ell}$ for all parameters $n_1, \dots, n_r, M$ with $\ell^n \mid M$ (recall the notation ω_ℓ from Section 2.1.1). In particular, the ℓ-adelic failure equals 1 if $\zeta_\ell \notin K$. This is because $K(\sqrt[\ell^n]{G}) \cap K(\zeta_M)$ is an abelian extension of K containing $K(\zeta_{\ell^n})$, and by Schinzel's theorem on abelian radical extensions [52, Theorem 2] any abelian extension of the form $K(\zeta_n, \sqrt[n]{a})/K$ with $a \in K$ has relative degree over $K(\zeta_n)$ dividing ω.

Remark 2.17. Let $\tau \geqslant 1$ be the largest integer such that $K(\zeta_\ell) = K(\zeta_{\ell^\tau})$ if ℓ is odd, and $K(\zeta_4) = K(\zeta_{2^\tau})$ if $\ell = 2$ (in which case $\tau \geqslant 2$). Clearly, if ℓ is odd and $\zeta_\ell \in K$, or $\ell = 2$ and $\zeta_4 \in K$,

then we have $\tau = \omega_\ell$. If $\ell = 2$ and $\zeta_4 \notin K$, then τ is the smallest integer $\nu \geqslant 2$ such that $K \cap \mathbb{Q}(\zeta_{2^\infty}) \subseteq \mathbb{Q}(\zeta_{2^\nu})$.

Then for any $m \geqslant \tau$ the group $\mathrm{Gal}(K(\zeta_{\ell^m})/K(\zeta_\ell))$ is cyclic of order $m - \tau$. This implies that $[K(\zeta_{\ell^m}) : K] = \ell^{m-\tau}[K(\zeta_{\ell^m}) : K(\zeta_\ell)]$, so that $K(\zeta_{\ell^{m+1}}) \neq K(\zeta_{\ell^m})$, and the largest integer n such that $\zeta_{\ell^n} \in K(\zeta_{\ell^m})$ is equal to m.

Remark 2.18. There exists a computable positive integer M, depending only on K, such that we have $K \cap \mathbb{Q}(\zeta_\infty) \subseteq \mathbb{Q}(\zeta_M)$, and any multiple of M satisfies this inclusion too. Such an M is given by the product of all primes p ramifying in K, with exponents according to the prime factorization of $[K : \mathbb{Q}]$. One can take for $v_p(M)$ the ramification index of p in K, which is at most $[K : \mathbb{Q}]$ and this is not an optimal bound in general.

However, one can do better. Let k be the squarefree product of the odd primes ramifying in K. The intersection $K(\zeta_{4k}) \cap \mathbb{Q}(\zeta_\infty)$ equals $K(\zeta_{4k}) \cap \mathbb{Q}(\zeta_{(2k)^\infty})$ where $\mathbb{Q}(\zeta_{(2k)^\infty})$ is the compositum of the fields $\mathbb{Q}(\zeta_{p^\infty})$ for all $p \mid 2k$ (as a subextension of $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}(\zeta_{4k})$ of degree a power of p lies inside $\mathbb{Q}(\zeta_{p^\infty 4k})$), and this is the compositum of the fields $K(\zeta_{4k}) \cap \mathbb{Q}(\zeta_{p^\infty})$ for $p \mid 2k$. Each field $K(\zeta_{4k}) \cap \mathbb{Q}(\zeta_{p^\infty})$ is of the form $\mathbb{Q}(\zeta_{p^e})$ for some $e \geqslant 1$, and $e \geqslant 2$ for $p = 2$. Hence we may take M such that $v_p(M) = v_p([K(\zeta_{4k}) : \mathbb{Q}]) \leqslant v_p([K : \mathbb{Q}]\varphi(4k))$ for all $p \mid 2k$.

In view of Remark 2.16, in order to study the ℓ-adelic failure, we may suppose that $\ell \mid \omega$. The following statement is part of [47, Proposition 3.2].

Lemma 2.19. *Let ℓ be a prime number such that $\zeta_\ell \in K$. Let $t := \omega_\ell + \max_i(d_i)$, where the d_i's are the d-parameters for the ℓ-divisibility of G in K. Then for all $m \geqslant n \geqslant t$ we have*

$$K\big(\zeta_{\ell^m}, \sqrt[\ell^n]{G}\big) \cap K(\zeta_\infty) = K\big(\zeta_{\ell^m}, \sqrt[\ell^t]{G}\big) \cap K(\zeta_\infty). \tag{2.9}$$

Any $t' \geqslant t$ also satisfies this equality.

Proof. Set $L := K(\zeta_{\ell^m})$. Both intersections of fields in (2.9) are abelian extensions of L of exponent dividing ℓ^n, so by Kummer theory (see [21, Ch.VI, Theorem 8.2]) we have

$$L\big(\sqrt[\ell^n]{G}\big) \cap K(\zeta_\infty) = L\big(\sqrt[\ell^n]{H_1}\big)$$
$$L\big(\sqrt[\ell^t]{G}\big) \cap K(\zeta_\infty) = L\big(\sqrt[\ell^n]{G^{\ell^{n-t}}}\big) \cap K(\zeta_\infty) = L\big(\sqrt[\ell^n]{H_2}\big)$$

where H_1, H_2 are subgroups of $L^\times$ such that $H_1 L^{\times \ell^n} \subseteq G L^{\times \ell^n}$ and $H_2 L^{\times \ell^n} \subseteq G^{\ell^{n-t}} L^{\times \ell^n}$. The inclusion in (2.9) is clear. Suppose that there is $n > t$ such that

$$L\big(\sqrt[\ell^n]{G}\big) \cap K(\zeta_\infty) \supsetneq L\big(\sqrt[\ell^t]{G}\big) \cap K(\zeta_\infty)\,,$$

which implies that $H_1 L^{\times \ell^n} \supsetneq H_2 L^{\times \ell^n}$, again by Kummer theory. Then there is an element $a \in H_1$ (we may suppose that $a \in G$) such that $\sqrt[\ell^n]{a} \notin L(\sqrt[\ell^n]{H_2})$. Since $\sqrt[\ell^n]{a} \in K(\zeta_\infty)$, we deduce $\sqrt[\ell^n]{a} \notin \sqrt[\ell^t]{G}$, which yields $a \notin G^{\ell^{n-t}}$. Let $d \geqslant 0$ be the d-parameter for the ℓ-divisibility of a in K, then by [47, Lemma 3.1] we obtain $d < n - t + \max_i(d_i) = n - \omega_\ell$. On the other hand, since $\sqrt[\ell^n]{a}$ lies in $K(\zeta_\infty)$, the extension $K(\zeta_{\ell^n}, \sqrt[\ell^n]{a})$ is abelian over K. Then by Schinzel's theorem we have $a^{\ell^x} = c^{\ell^n}$ for some $x \leqslant \omega_\ell$ and $c \in K$. This implies that a is at least an $\ell^{n-\omega_\ell}$-th power in K times a root of unity in K, which is a contradiction as $d < n - \omega_\ell$. □

Lemma 2.20. *Let ℓ be a prime number such that $\zeta_\ell \in K$. Let $t := \omega_\ell + \max_i(d_i)$, where the d_i's are the d-parameters for the ℓ-divisibility of G in K. There exists a computable positive integer N, depending only on ℓ, K and G, such that*

$$K\big(\sqrt[\ell^t]{G}\big) \cap K(\zeta_\infty) \subseteq K(\zeta_N). \tag{2.10}$$

Any positive multiple of N also satisfies this inclusion.

Proof. Since $[K(\sqrt[\ell^t]{G}) : K(\zeta_{\ell^t})] \mid \ell^{tr}$ and $[K(\zeta_N) : K] \mid \varphi(N)$, we may take for N a power of ℓ times a squarefree product of primes congruent to 1 modulo ℓ. Let us first consider the ℓ-adic valuation of N. Let n be the largest integer such that $\zeta_{\ell^n} \in K(\zeta_{\ell^{t+\varepsilon}})$, where $\varepsilon = 1$ if $\ell = 2$ and $t = 1$, and $\varepsilon = 0$ otherwise. Then by Remark 2.17 and since $t \geqslant \omega_\ell$, we have $n = t$ if ℓ is odd or $\zeta_4 \in K$, and $n = \max(t, \tau)$ if $\ell = 2$ and $\zeta_4 \notin K$, with τ as in Remark 2.17 for $\ell = 2$. Thus we may take $v_\ell(N) = 2t$ if ℓ is odd or $\zeta_4 \in K$ or $t \geqslant \tau$, respectively $v_2(N) = t + \tau$ otherwise, because the intersection on the left-hand side of (2.10) is an abelian extension of $K(\zeta_{\ell^t})$ (this equals $K(\zeta_{2^\tau})$ in the latter case) of exponent dividing ℓ^t, which leads to the inclusions

$$K(\sqrt[\ell^t]{G}) \cap \mathbb{Q}(\zeta_{\ell^\infty}) \subseteq \mathbb{Q}(\zeta_{\ell^{2t}}), \quad \text{resp. } K(\sqrt[2^t]{G}) \cap \mathbb{Q}(\zeta_{2^\infty}) \subseteq \mathbb{Q}(\zeta_{2^{t+\tau}}).$$

Next we determine the other prime factors of N. By Kummer theory we have

$$K\big(\sqrt[\ell^t]{G}\big) \cap K(\zeta_\infty) = K\big(\sqrt[\ell^t]{H}\big)$$

where H is a subgroup of $K(\zeta_{\ell^t})^\times$ which we may assume to be contained in G. In particular, there is a basis $\{g_i\}$ of H as a $\mathbb{Z}$-module with $g_i \in G$. In order to find the other prime factors of N, by [15, Lemma C.1.7] it is sufficient to consider the finitely many primes which ramify in K or which lie below the primes $\mathfrak{p}$ of K such that the $\mathfrak{p}$-adic valuation of g_i is not divisible by ℓ^t for some i. Among these primes we only need to take those which are congruent to 1 modulo ℓ. Recall that the rational primes below the primes of K in the factorizations of the g_i's can be found by looking at the absolute norm of each g_i. □

The following is a reformulation of [47, Lemma 3.3].

Proposition 2.21. *Let ℓ be a prime number such that $\zeta_\ell \in K$. There exists a computable positive integer M_0, depending only on ℓ, K and G, such that, setting $t_0 = v_\ell(M_0)$, we have $K \cap \mathbb{Q}(\zeta_\infty) \subseteq \mathbb{Q}(\zeta_{M_0})$, and $t_0 \geqslant \omega_\ell + \max_i(d_i)$, where the d_i's are the d-parameters for the ℓ-divisibility of G in K, and*

$$K\big(\sqrt[\ell^{t_0}]{G}\big) \cap K(\zeta_\infty) \subseteq K(\zeta_{M_0}).$$

Moreover, the statement still holds if we replace M_0 with any positive multiple M' of M_0, and t_0 with $v_\ell(M')$.

Proof. Let us take $M_0 := [M, N]$, with M as in Remark 2.18 and N as in Lemma 2.20 (in particular $t_0 \geqslant t$, where $t = \omega_\ell + \max_i(d_i)$). By [47, Proposition 3.2] the intersection $K(\sqrt[\ell^{t_0}]{G}) \cap K(\zeta_\infty)$ is given by the compositum of $K(\sqrt[\ell^t]{G}) \cap K(\zeta_\infty)$ and $K(\zeta_{\ell^{t_0}})$. Therefore it is contained in $K(\zeta_{M_0})$, and the last assertion follows for the same reason. □

Theorem 2.22 ([47, Theorem 5.3])**.** *Let ℓ be a prime number such that $\zeta_\ell \in K$. There is a computable integer M_0, depending only on ℓ, K and $\alpha_1, \ldots, \alpha_r$, such that, setting $t_0 = v_\ell(M_0)$, for all integers $M, n_1, \ldots, n_r$ with $\ell^{n_i} \mid M$ for all i we have*

$$B_\ell(M, \ell^{n_1}, \ldots, \ell^{n_r}) = B_\ell(\gcd(M, M_0), \gcd(\ell^{n_1}, \ell^{t_0}), \ldots, \gcd(\ell^{n_r}, \ell^{t_0}))\,.$$

In particular, this result reduces the computation of the ℓ-adelic failure to the computation of the finitely many degrees $B_\ell(M, \ell^{n_1}, \ldots, \ell^{n_r})$ where $M \mid M_0$ and $n_i \leqslant t_0$ for all i.

Proof. Let M_0 be the integer of Proposition 2.21. If $\ell = 2$ and $\zeta_4 \notin K$, then up to replacing M_0 with a multiple, we may suppose that $t_0 \geqslant s$ with s as in (2.5) for G and $\ell = 2$. Notice that we have $t_0 \geqslant s$ also if ℓ is odd or $\zeta_4 \in K$.

Case 1: Suppose that $n_i \leqslant t_0$ for all i. We only need to check that we may replace M with $\gcd(M, M_0)$ in the degree (2.2). The considered intersection of fields is contained in $K(\sqrt[\ell^{t_0}]{G}) \cap K(\zeta_{M_0})$, by definition of M_0. We may conclude because $K(\zeta_M) \cap K(\zeta_{M_0}) = K(\zeta_{(M,M_0)})$ by [47, Lemma 2.4].

Case 2: Suppose that $n_j > t_0$ for some j. Since $t_0 \geqslant s$ (recall that $s \geqslant 2$ if $\ell = 2$ and $\zeta_4 \notin K$), setting $n := \max_i(n_i)$, by (2.6) we have

$$\left[K\left(\zeta_{\ell^n}, \sqrt[\ell^{t_0+1}]{G}\right) : K\left(\zeta_{\ell^n}, \sqrt[\ell^{t_0}]{G}\right)\right] = \ell^r .$$

This says in particular that each element $\sqrt[\ell^{t_0}]{\alpha_i}$ is strongly ℓ-indivisible in $K(\zeta_{\ell^n}, \sqrt[\ell^{t_0}]{G})$. We prove that, if $n_j > t_0$, then we may replace n_j with t_0 in the degree (2.2). More precisely, setting

$$L_j := K\left(\zeta_{\ell^n}, \sqrt[\ell^{n_1}]{\alpha_1}, \ldots, \sqrt[\ell^{t_0}]{\alpha_j}, \ldots, \sqrt[\ell^{n_r}]{\alpha_r}\right),$$

we prove that

$$L_j\left(\sqrt[\ell^{n_j}]{\alpha_j}\right) \cap K(\zeta_\infty) = L_j \cap K(\zeta_\infty) .$$

We already know that since $L_j(\sqrt[\ell^{n_j}]{\alpha_j}) \subseteq K(\sqrt[\ell^n]{G})$, in view of Proposition 2.21 we have

$$L_j\left(\sqrt[\ell^{n_j}]{\alpha_j}\right) \cap K(\zeta_\infty) = L_j\left(\sqrt[\ell^{n_j}]{\alpha_j}\right) \cap K\left(\zeta_{\ell^n}, \sqrt[\ell^{t_0}]{G}\right) \cap K(\zeta_\infty),$$

so that we may conclude by proving $I := L_j(\sqrt[\ell^{n_j}]{\alpha_j}) \cap K(\zeta_{\ell^n}, \sqrt[\ell^{t_0}]{G}) \subseteq L_j$. Since the extension $L_j(\sqrt[\ell^{n_j}]{\alpha_j})/L_j$ is cyclic, by Kummer theory we have either $I \subseteq L_j$ or $I = L_j(\sqrt[\ell^m]{\alpha_j})$ for some $m \in \{t_0 + 1, \ldots, n_j\}$. As mentioned above the element $\sqrt[\ell^{t_0}]{\alpha_j}$ is strongly ℓ-indivisible in $K(\zeta_{\ell^n}, \sqrt[\ell^{t_0}]{G})$, so that $\sqrt[\ell^m]{\alpha_j}$ does not lie in I if $m > t_0$. Thus we must have $I \subseteq L_j$.

Hence in (2.2) we may replace each ℓ^{n_i} with $\gcd(\ell^{n_i}, \ell^{t_0})$. We conclude by applying [47, Lemma 3.4] which allows us to replace n with t_0, and M with $\gcd(M, M_0)$. □

Proof of Theorem 2.2. In view of the decomposition (2.3), it suffices to combine Theorem 2.22 (applied to all ℓ such that $\zeta_\ell \in K$) with Lemma 2.15 and Remark 2.16. More precisely, for ℓ such that $\zeta_\ell \in K$ let $M_{0,\ell}$ and $t_{0,\ell}$ be the integers of Theorem 2.22, and otherwise let $t_{0,\ell} = s_\ell$, where s_ℓ is the integer of (2.5). Notice that we have $t_{0,\ell} \geqslant s_\ell$ for all ℓ, see the proof of Theorem 2.22. Also, we have $t_{0,\ell} = 0$ for all but finitely many primes ℓ (see Proposition 2.12). Then we may take $N_0 = \prod_\ell \ell^{t_{0,\ell}}$ and M_0 to be the least common multiple of the integers $M_{0,\ell}$ and N_0. □

The following remark takes care of the case of groups with torsion.

Remark 2.23. Let G' be finitely generated subgroup of $K^\times$ with torsion, and write $G' = \langle \zeta_t \rangle \times G$, where G is torsion-free and $t > 1$ with $t \mid \omega$. Then, for $N \mid M$, we may decompose the Kummer degree as follows:

$$[K(\zeta_M, \sqrt[N]{G'}) : K(\zeta_M)] = [K(\zeta_{[M,Nt]}, \sqrt[N]{G}) : K(\zeta_{[M,Nt]})] \cdot [K(\zeta_{[M,Nt]}) : K(\zeta_M)] .$$

The first degree on the right-hand side involves a torsion-free group, whereas the second degree is cyclotomic.

2.4 Kummer theory via entanglement groups

2.4.1 Galois radical groups

Let K be a number field. An element $x \in \bar{K}^\times$ is called a *radical* if $x^n \in K^\times$ for some integer $n \geqslant 1$, i.e. if the class of x in $\bar{K}^\times/K^\times$ is torsion. We call a multiplicative subgroup $B \subseteq \bar{K}^\times$ a *radical group* if $K^\times \subseteq B$ and $B/K^\times$ is torsion (the latter condition means that B consists of radicals). A radical group B is called *Galois* if the exponent of $B/K^\times$ divides the exponent of the torsion part of B (i.e. for every $x \in B$ there is $n \geqslant 1$ such that $x^n \in K^\times$ and $\mu_n \subseteq B$), or equivalently if the extension $K(B)/K$ is Galois.

We denote by $\mathrm{Aut}_{K^\times}(B)$ the group of $K^\times$-automorphisms of B, i.e. the automorphisms of B that are the identity on $K^\times$. By [35, Lemma 1.9] we have that if x is a radical such that $x^n \in K^\times$, then $x^\omega \in \langle K^\times, \mu_\infty\rangle$ holds if and only if the group $\mathrm{Aut}_{K^\times}(\langle K^\times, \mu_n, x\rangle)$ is abelian, and this is equivalent to the extension $K(\mu_n, x)/K$ being abelian. Thus, we call a radical *abelian* if it satisfies any of these conditions. The *abelian radical group* of B, denoted by B_{ab}, consists of the abelian radicals contained in B, and it is again a radical group. We call *Kummer radical* an abelian radical such that $x^\omega \in K^\times$.

If B is a Galois radical group, then the Galois group $\mathrm{Gal}(K(B)/K)$ is a subgroup of $\mathrm{Aut}_{K^\times}(B)$. In particular, by [35, Theorem 1.6] it is a normal subgroup and the quotient

$$E(B) := \mathrm{Aut}_{K^\times}(B)/\,\mathrm{Gal}(K(B)/K)$$

is an abelian group, which is called the *entanglement group* of B over K. By [35, Corollary 2.27] we have that $E(B) = E(B_{\mathrm{ab}})$. The following theorem by Palenstijn provides a way to characterize the entanglement group of B, when B consists of Kummer radicals and roots of unity.

Theorem 2.24 (Palenstijn, [35, Theorem 1.10])**.** *Let B be a Galois radical group, and suppose that $B_{\mathrm{ab}} = \langle \mu, H\rangle$, where μ is a group of roots of unity and H is a radical group of Kummer radicals. Then we have a group isomorphism*

$$E(B) \cong \mathrm{Gal}\left(K(H) \cap \mathbb{Q}(\mu)/\mathbb{Q}(H \cap \mu)\right).$$

In the above result we can take as μ the torsion part of B; then it is possible to choose H such that $H \cap \mu = \mu_K$.

Notice that if $B \subseteq B'$ are two radical groups, then we have $B_{\mathrm{ab}} \subseteq B'_{\mathrm{ab}}$, and the condition $B' = B'_{\mathrm{ab}}$ implies $B = B_{\mathrm{ab}}$.

2.4.2 Maximal abelian extensions

Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. The abelian radicals x such that $x^n \in G$ for some $n \geqslant 1$, together with $K^\times$, form a radical group which we denote by $B_{\infty,\mathrm{ab}}$. If ℓ is a prime number, then we consider the abelian radicals x such that $x^{\ell^n} \in G$ for some $n \geqslant 0$: these, together with $K^\times$, form a radical group which we denote by $B_{\ell^\infty,\mathrm{ab}}$. In fact, the group $B_{\infty,\mathrm{ab}}$ is generated by the groups $B_{\ell^\infty,\mathrm{ab}}$ by varying ℓ. This is a consequence of [49, Lemma 16], which states that, for $n \geqslant 1$, if $a \in K^\times$ and B is a subgroup of $\bar{K}^\times$ containing μ_n, then $\sqrt[n]{a} \in B$ if and only if $\sqrt[\ell^{v_\ell(n)}]{a} \in B$ for every ℓ.

Let ℓ be a prime divisor of ω, and let $b_1, \ldots, b_r$ be the strongly ℓ-indivisible parts associated to an ℓ-good basis of G. We define the group of Kummer radicals

$$S_\ell := \left\langle \sqrt[\ell^{\omega_\ell}]{b_1}, \ldots, \sqrt[\ell^{\omega_\ell}]{b_r} \right\rangle \qquad \text{and} \qquad S := \langle S_\ell : \ell \mid \omega\rangle$$

(for some fixed choice of the ℓ^{ω_ℓ}-th roots). The group S_ℓ is torsion-free because it has rank r (notice that S_ℓ contains G^ω), and that the choice of the ℓ^{ω_ℓ}-th roots will not matter for our results.

We can express $B_{\infty,\mathrm{ab}}$ and $B_{\ell^\infty,\mathrm{ab}}$ in terms of S and S_ℓ in the following way (see [49, Lemma 20]): $B_{\infty,\mathrm{ab}} = \langle K^\times, \mu_\infty, S\rangle$, and

$$B_{\ell^\infty,\mathrm{ab}} = \begin{cases} \langle K^\times, \mu_{\ell^\infty}\rangle & \text{if } \ell \nmid \omega \\ \langle K^\times, \mu_{\ell^\infty}, S_\ell\rangle & \text{if } \ell \mid \omega\,, \end{cases}$$

for every prime ℓ. This is a consequence of Schinzel's theorem on abelian radical extensions for the following reason. Let $b \in K$ be strongly ℓ-independent. If $\ell \nmid \omega$, then the ℓ-th roots of b do not generate an abelian extension of K, whereas if $\ell \mid \omega$, then the extension $K(\mu_{\ell^n}, \sqrt[\ell^n]{b})/K$ is abelian if and only if $n \leqslant \omega_\ell$.

Remark 2.25. There is some computable integer $n \geqslant 1$ (depending only on K and G) such that $K(S) \cap \mathbb{Q}(\mu_\infty) \subseteq \mathbb{Q}(\mu_n)$. Indeed, we can take $n = \prod_{p\in\mathcal{P}} p^{e_p}$, where $\mathcal{P}$ consists of the prime numbers ramifying in $K(S)$, and where e_p is at least the ramification index of p in $K(S)$ (we can take $e_p = [K(S) : \mathbb{Q}] \leqslant \omega^r[K : \mathbb{Q}]$ because $[K(S) : K]$ divides ω^r). Since $K(S)/K$ is the compositum of cyclic Kummer extensions, by a classical result [15, Lemma C.1.7 and its proof] we can take $\mathcal{P}$ to be the set of primes p that divide the discriminant of K or are such that for some prime $\mathfrak{p}$ of K above p and for some $i \in \{1, \dots, r\}$ the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}(b_i)$ is not a multiple of ω (in particular, a prime with the latter property appears in the prime factorization of the absolute norm of the fractional ideal (b_i)). See also Remark 2.32.

The following is a direct consequence of Remarks 2.8 and 2.25.

Proposition 2.26 ([49, Proposition 22])**.** *There is a computable integer $n_0 \geqslant 1$ (depending only on K and G) such that $K(S) \cap \mathbb{Q}(\mu_\infty) \subseteq \mathbb{Q}(\mu_{n_0})$ and $v_\ell(n_0) \geqslant \omega_\ell + \max_i(d_i)$ for every prime number ℓ with $\ell \mid \omega$, where the d_i's are the d-parameters for the ℓ-divisibility of G in K.*

Let us define for every integer $n \geqslant 1$ the radical group

$$B_n := \left\langle K^\times, \sqrt[n]{G}\right\rangle.$$

The radical groups B_n and $B_{n,\mathrm{ab}}$ are Galois and contain μ_n. The entanglement group $E(B_n) = E(B_{n,\mathrm{ab}})$ is finite because $B_n/K^\times$ is finite. For ℓ a prime number, consider the group $B_{\ell^n} = \left\langle K^\times, \sqrt[\ell^n]{G}\right\rangle$, with $n \geqslant 1$. Taking $e_\ell := \omega_\ell + \max_i(d_i)$ for $\ell \mid \omega$, where the d_i's are the d-parameters for the ℓ-divisibility of G, we have (see [49, Lemma 23])

$$B_{\ell^n,\mathrm{ab}} = \begin{cases} \langle K^\times, \mu_{\ell^n}\rangle & \text{if } \ell \nmid \omega \\ \langle K^\times, \mu_{\ell^n}, S_\ell\rangle & \text{if } \ell \mid \omega \text{ and } n \geqslant e_\ell\,. \end{cases}$$

For $n > 1$, writing $n = \prod \ell^e$ for the prime factorization of n, we have that $B_{n,\mathrm{ab}}$ is generated by the groups $B_{\ell^e,\mathrm{ab}}$ ([49, Lemma 28]). Hence, taking $n_1 = \prod_{\ell\mid\omega} \ell^{e_\ell}$, we deduce that

$$B_{n,\mathrm{ab}} = \langle K^\times, \mu_n, S\rangle \qquad \text{for all } n \text{ such that } n_1 \mid n.$$

By Remark 2.8 the integer n_1 is computable and depends only on K and G. Since $\langle K^\times, S\rangle$ consists of Kummer radicals, applying Theorem 2.24 and taking into account that by [49, Proposition 19] all roots of unity in $\langle K^\times, S\rangle$ are contained in μ_K, we obtain

$$E(B_n) = \mathrm{Gal}\left(K(S) \cap \mathbb{Q}(\mu_n)/\mathbb{Q}(\mu_K)\right) \qquad \text{for all } n \text{ such that } n_1 \mid n.$$

Let n_0 be as in Proposition 2.26, so that $n_1 \mid n_0$ and $K(S) \cap \mathbb{Q}(\mu_\infty) \subseteq \mathbb{Q}(\mu_{n_0})$. We further obtain

$$E(B_n) = E(B_{n_0}) = \mathrm{Gal}\left(K(S) \cap \mathbb{Q}(\mu_{n_0})/\mathbb{Q}(\mu_K)\right) \quad \text{for all } n \text{ such that } n_0 \mid n, \tag{2.11}$$

This is a generalization of [35, Theorem 1.4].

Let ℓ be a prime divisor of ω, and consider the group $B_{\ell^n,\mathrm{ab}}$ for $n \geqslant 1$. If we suppose that the h-parameters for the ℓ-divisibility of G can be taken to be zero, then we may express $B_{\ell^n,\mathrm{ab}}$ in terms of Kummer radicals and roots of unity. More precisely, by [49, Proposition 25] we have $B_{\ell^n,\mathrm{ab}} = \langle K^\times, \mu_{\ell^n}, H_{\ell^n}\rangle$, where H_{ℓ^n} can be taken as

$$H_{\ell^n} = \begin{cases} \sqrt[\ell^n]{G} & \text{if } n \leqslant \omega_\ell \\ S_\ell \cap \langle B_{\ell^n}, \mu_{\ell^{n+\omega_\ell}}\rangle & \text{if } n > \omega_\ell\,. \end{cases} \tag{2.12}$$

Notice that by [49, Proposition 24] we have

$$S_\ell \cap \langle B_{\ell^n}, \mu_{\ell^{n+\omega_\ell}}\rangle = \langle \sqrt[\ell^{\max(0,\min(\omega_\ell, n-d_i))}]{b_i} : i = 1, \ldots, r\rangle,$$

where the d_i's are as above. The following example shows that (2.12) does not hold with nonzero h-parameters.

Example 2.27. Let $K = \mathbb{Q}$ and $G = \langle -4\rangle$. The radical group $B_{4,\mathrm{ab}} = \langle \mathbb{Q}^\times, \mu_4, \sqrt[4]{-4}\rangle$ contains only abelian radicals, however $\sqrt[4]{-4}$ is not a Kummer radical. We cannot write $B_{4,\mathrm{ab}} = \langle \mathbb{Q}^\times, \mu, H\rangle$ where $\mu \subseteq \mu_\infty$ and H consists of Kummer radicals, because we would have $\mu \subseteq \mu_4$ and hence $B_{4,\mathrm{ab}}$ would consist of Kummer radicals.

Proof of Theorem 2.7. The assumption that every element of G has the same divisibility in K and in $K^\times/\mu_K$ is equivalent to saying that the h-parameters for the ℓ-divisibility of G can be taken to be zero for every ℓ (see [49, Remark 11] for details).

Write $n = \prod \ell^e$. By the above, since $B_{n,\mathrm{ab}}$ is generated by the groups $B_{\ell^e,\mathrm{ab}}$, we have that $B_{n,\mathrm{ab}}$ is generated by the groups $\langle K^\times, \mu_{\ell^e}\rangle$ for $\ell \nmid \omega$, and $\langle K^\times, \mu_{\ell^e}, H_{\ell^e}\rangle$ for $\ell \mid \omega$, where ℓ runs through the prime factors of n. Hence we obtain

$$B_{n,\mathrm{ab}} = \langle K^\times, \mu_n, H_n\rangle$$

where $H_n = \langle H_{\ell^e} : \ell \mid (n, \omega)\rangle$. Thus the statement follows from Theorem 2.24 as $\langle K^\times, H_n\rangle$ is a group consisting of Kummer radicals. Moreover, we have $\langle K^\times, H_n\rangle \cap \mu_n = \mu_{(n,\omega)}$ because the assumption on G yields $H_n \subseteq \langle \mu_\omega, S\rangle$, and by [49, Proposition 19] we have $\langle K^\times, S\rangle \cap \mu_\infty = \mu_\omega$. □

2.4.3 The Kummer failure via entanglement groups

The formula given in [35, Proposition 4.3] extends to a general number field K.

Theorem 2.28 ([49, Theorem 33])**.** *Let K be a number field. If B is a Galois radical group such that $B/K^\times$ is finite, then we have*

$$[K(B) : K] = \frac{[B : K^\times]}{\sharp E(B)} \cdot \Delta$$

where $\Delta = \prod_{p \text{ prime}, \zeta_p \in B \setminus \mu_K} \frac{p-1}{p}$.

Proof. The assumption on B implies that the quantities involved in the formula are well-defined and finite. From the definition of entanglement group it is clear that

$$[K(B):K] = \frac{\sharp \operatorname{Aut}_{K^\times}(B)}{\sharp E(B)},$$

and by [35, Theorem 2.19] we have $\sharp \operatorname{Aut}_{K^\times}(B) = [B : K^\times] \cdot \Delta$. □

Proof of Theorem 2.4. It suffices to apply Theorem 2.28 with $B = B_n$, where $\Delta = \Delta_n$ by [49, Lemma 27]. □

Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. We define the cyclotomic-Kummer failure for K and G at $n \geqslant 1$ as the ratio

$$D(n) := \frac{\varphi(n) n^r}{[K(\sqrt[n]{G}) : K]}.$$

In this section we take n_0 as in Proposition 2.26.

Theorem 2.29 ([49, Theorem 36])**.** *If n, N are multiples of n_0 with $n \mid N$, then we have $D(N) = D(n)$.*

Proof. We are going to show the identity

$$\frac{[K(\sqrt[N]{G}) : K]}{[K(\sqrt[n]{G}) : K]} = \frac{N^r \varphi(N)}{n^r \varphi(n)},$$

and we may reduce to the case $N = n\ell$, where ℓ is a prime number. In view of our choice of n_0 we have $E(B_n) = E(B_{n\ell})$. We apply Theorem 2.4.

By [49, Proposition 34] for every $m > 1$ we have $[B_m : K^\times] = \prod_{\ell \text{ prime}} [B_{\ell^{v_\ell(m)}} : K^\times]$. Thus, if $\ell \nmid n$, then we have $[B_{n\ell} : K^\times]/[B_n : K^\times] = [B_\ell : K^\times]$. This index equals ℓ^{r+1} by [49, Proposition 35] because $[G : G \cap K^{\times \ell}] = \ell^r$ by [10, Theorem 15] (all d-parameters for the ℓ-divisibility are 0). We conclude that

$$\frac{[K(\sqrt[n\ell]{G}) : K]}{[K(\sqrt[n]{G}) : K]} = [B_\ell : K^\times] \frac{(\ell - 1)}{\ell} = \frac{(n\ell)^r \varphi(n\ell)}{n^r \varphi(n)}.$$

If $\ell \mid n$, set $e := v_\ell(n)$. By [49, Propositions 34 and 35] we have

$$\frac{[B_{n\ell} : K^\times]}{[B_n : K^\times]} = \frac{[B_{\ell^{e+1}} : K^\times]}{[B_{\ell^e} : K^\times]} = \ell \cdot \frac{[G : G \cap (K^\times)^{\ell^{e+1}}]}{[G : G \cap (K^\times)^{\ell^e}]}.$$

The right-hand side equals ℓ^{r+1} by [10, Theorem 15] and hence

$$\frac{[K(\sqrt[n\ell]{G}) : K]}{[K(\sqrt[n]{G}) : K]} = \ell^{r+1} = \frac{(n\ell)^r \varphi(n\ell)}{n^r \varphi(n)}.$$ □

Corollary 2.30 ([49, Corollary 37])**.** *If n, N are multiples of n_0 with $n \mid N$, then the restriction to B_N gives a group isomorphism*

$$\operatorname{Gal}(K(B_N)/K(B_n)) \cong \operatorname{Aut}_{B_n}(B_N).$$

Proof. The restriction to B_N of a $K(B_n)$-automorphism of $K(B_N)$ gives an injective group homomorphism, so we prove that the two finite groups have the same size. By [35, Lemma 1.8] the restriction map $\mathrm{Aut}_{K^\times}(B_N) \to \mathrm{Aut}_{K^\times}(B_n)$ is surjective, and the kernel is $\mathrm{Aut}_{B_n}(B_N)$. We conclude because $E(B_N) = E(B_n)$ by (2.11). □

Proof of Theorem 2.5. Set $g := \gcd(n, n_0)$ and $l := [n, n_0]$. We first prove that for every $n \geqslant 1$ we have $K(B_n) \cap K(B_{n_0}) = K(B_{\gcd(n,n_0)})$. This will follow from the fact that $\mathrm{Gal}(K(B_n)/K(B_g))$ and $\mathrm{Gal}(K(B_l)/K(B_{n_0}))$ have the same size. Consider the bottom row of the following commutative diagram given by restrictions (recall from [35, Lemma 1.8] that the restriction $\mathrm{Aut}_{K^\times}(B') \to \mathrm{Aut}_{K^\times}(B)$ is surjective if $B \subseteq B'$ are Galois radical groups):

$$\begin{array}{ccccccccc}
 & & \mathrm{Gal}(K(B_n)/K(B_g)) & \longrightarrow & \mathrm{Gal}(K(B_n)/K) & \longrightarrow & \mathrm{Gal}(K(B_g)/K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Aut}_{B_g}(B_n) & \longrightarrow & \mathrm{Aut}_{K^\times}(B_n) & \longrightarrow & \mathrm{Aut}_{K^\times}(B_g) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \dfrac{\mathrm{Aut}_{B_g}(B_n)}{\mathrm{Gal}(K(B_n)/K(B_g))} & \longrightarrow & E(B_n) & \longrightarrow & E(B_g) & \longrightarrow & 0
\end{array}$$

By Corollary 2.30 we have

$$\sharp\,\mathrm{Aut}_{B_{n_0}}(B_l) = \sharp\,\mathrm{Gal}(K(B_l)/K(B_{n_0})) \leqslant \sharp\,\mathrm{Gal}(K(B_n)/K(B_g)) \leqslant \sharp\,\mathrm{Aut}_{B_g}(B_n),$$

so it suffices to prove $\sharp\,\mathrm{Aut}_{B_{n_0}}(B_l) \geqslant \sharp\,\mathrm{Aut}_{B_g}(B_n)$. By [35, Theorem 2.19] we have (recall that $\omega \mid n_0$)

$$\sharp\,\mathrm{Aut}_{B_{n_0}}(B_l) = \sharp\frac{B_l}{B_{n_0}} \cdot \prod_{\substack{p \text{ prime} \\ p \mid l,\, p \nmid n_0}} \frac{p-1}{p},$$

$$\sharp\,\mathrm{Aut}_{B_g}(B_n) = \sharp\frac{B_n}{B_g} \cdot \prod_{\substack{p \text{ prime} \\ p \mid n,\, p \nmid \omega g}} \frac{p-1}{p}.$$

Since the two products over p are the same, we conclude because we have

$$\frac{B_n}{B_g} = \frac{B_n}{B_{n_0} \cap B_n} \cong \frac{B_n \cdot B_{n_0}}{B_{n_0}} \subseteq \frac{B_l}{B_{n_0}}\,. \qquad \square$$

We are now ready to prove Theorem 2.6, which states that for every $n \geqslant 1$ we have $D(n) = D(\gcd(n, n_0))$.

Proof of Theorem 2.6. Set $g := \gcd(n, n_0)$. By Theorem 2.4, and in view of Theorem 2.5, it suffices to prove that

$$\frac{[B_n : K^\times]\Delta_n}{\varphi(n)n^r} = \frac{[B_g : K^\times]\Delta_g}{\varphi(g)g^r}\,.$$

The assertion is obvious for $n = 1$, so suppose that $n > 1$ and let $n = \prod \ell^e$ be the prime factorization. By [49, Proposition 34 and 35] we have

$$\frac{[B_n : K^\times]\Delta_n}{\varphi(n)n^r} = \prod_{\ell \mid n} \left[G : G \cap K^{\times \ell^e}\right] \ell^{\max(0, e-\omega_\ell)} \Delta_{\ell^e} / \varphi(\ell^e)\ell^{er}\,,$$

and a similar formula holds by replacing the pair (n, e) with $(g, v_\ell(g))$. By the choice of n_0 and by [10, Theorem 15] the ratio $[G : G \cap K^{\times \ell^e}]/\ell^{er}$ does not change if we replace e with $v_\ell(g)$, and the same holds for $\ell^{\max(0,e-\omega_\ell)}\Delta_{\ell^e}/\varphi(\ell^e)$. □

We now consider Kummer extensions for groups which are not necessarily torsion-free.

Remark 2.31. Let $G' = G \times \langle \zeta_m \rangle$, where $m \geqslant 1$ and where G is a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. Then there is some computable positive integer n_0' (depending only on K and G') such that

$$[K(\sqrt[n]{G'}) : K] = \frac{\varphi(nm)n^r}{\varphi(gm)g^r}[K(\sqrt[g]{G'}) : K] \tag{2.13}$$

where $g := \gcd(n, n_0')$. Indeed, taking n_0 as in Proposition 2.26 for G^m and setting $n_0' := n_0/m$ (we have $m \mid n_0$ because the d-parameters for the ℓ-divisibility of G^m are at least $v_\ell(m)$), then we get

$$[K(\sqrt[nm]{G^m}) : K] = \frac{\varphi(nm)(nm)^r}{\varphi(gm)(gm)^r}[K(\sqrt[gm]{G^m}) : K]\,.$$

Formula (2.13) precisely says that the degree of $K(\sqrt[n]{G'})/K(\sqrt[g]{G'})$ is maximal. Indeed, setting $L := K(\sqrt[g]{G'})$, we have

$$[K(\sqrt[n]{G'}) : L] \leqslant [L(\sqrt[n]{\zeta_m}) : L] \cdot [L(\sqrt[n]{G}) : L]$$

and the former degree is at most $[\mathbb{Q}(\sqrt[n]{\zeta_m}) : \mathbb{Q}(\sqrt[g]{\zeta_m})] = \varphi(nm)/\varphi(gm)$ because $\sqrt[g]{\zeta_m} \in L$ while the latter degree is at most n^r/g^r because $L = L(\sqrt[g]{G})$. In particular, for every $n \geqslant 1$ we have

$$K(\sqrt[n]{\zeta_m}) \cap K(\sqrt[n]{G}) \subseteq K(\sqrt[g]{G'})\,.$$

2.5 Examples

In this section, we present some examples from [47, Section 6] and [49, Section 9] to illustrate our results.

In order to work with our theoretical algorithms in practice, we assume that the field K is *presented* in the sense of [11, Chapter 19], which implies that its elements are representable on a computer. Moreover, we assume that a list of generators for the group G is known explicitly.

Remark 2.32. Some more information on K is needed for the computations in Remark 2.8 and Remark 2.25. To compute the parameters for the ℓ-divisibility for G as in [10] we need to tell whether an element $a \in K^\times$ has some ℓ-th root in $K^\times$ (we can factor the polynomial $x^\ell - a$ as in [22]). We have to consider every prime number ℓ, but we may restrict to those dividing all exponents in the factorization of the fractional ideal (a). To factor (a), we first compute its absolute norm $N(a)$ and factor the ideal (p) for every prime number p such that $v_p(N(a)) \neq 0$, as described in [8, §4.8]; we finally determine the correct exponent for each prime ideal using as bound the corresponding exponent in the factorization of the ideal $(N(a))$. Moreover, we need to know μ_K, which can be computed together with the whole unit group of the ring of integers of K, see the algorithm described in [4].

Let us first give examples for the results of Section 2.3.

Remark 2.33. Let K be a number field. Suppose that ℓ is odd or that $\zeta_4 \in K$. Consider elements $\alpha_1, \ldots, \alpha_r$ of $K^\times$ which generate a subgroup of $K^\times$ of positive rank r. Suppose that $\alpha_i = \beta_i^{\ell^{d_i}}$ where $\beta_1, \ldots, \beta_r$ are strongly ℓ-independent elements of K. We have

$$K\big(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1}, \ldots,\ \sqrt[\ell^{n_r}]{\alpha_r}\big) = K\big(\zeta_{\ell^m},\ \sqrt[\ell^{\max(n_1-d_1,0)}]{\beta_1}, \ldots,\ \sqrt[\ell^{\max(n_r-d_r,0)}]{\beta_r}\big)\,.$$

By (2.7) we conclude that

$$\big[K\big(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1}, \ldots,\ \sqrt[\ell^{n_r}]{\alpha_r}\big) : K(\zeta_{\ell^m})\big] = \prod_{i=1}^{r} \ell^{\max(n_i-d_i,0)}$$

for all nonnegative integers $m, n_1, \ldots, n_r$ with $m \geqslant \max_i(n_i)$.

Example 2.34. Consider cyclotomic-Kummer extensions of the form

$$\mathbb{Q}\big(\zeta_M,\ \sqrt[N_1]{2},\ \sqrt[N_2]{-9}\big)/\mathbb{Q}$$

for M, N_1, N_2 positive integers with $N_1, N_2 \mid M$. We can compute the degrees of these extensions via ℓ-adic and ℓ-adelic failures.

Let $G = \langle 2, -9\rangle$. The ℓ-divisibility parameters of G over $\mathbb{Q}$ are all zero for every odd prime ℓ. It follows from Lemma 2.15 that the ℓ-adic failure is 1 for all odd primes ℓ. Moreover, since the only nontrivial root of unity in $\mathbb{Q}$ is $\zeta_2 = -1$, by Remark 2.16 the ℓ-adelic failure is also 1 for every odd prime ℓ.

For $\ell = 2$ we need to compute the 2-divisibility parameters of G over $\mathbb{Q}(i)$ (see Remark 2.11 and (2.6)). Over this field we have $2 = -i(1+i)^2$, and $1+i$ and 3 are strongly 2-independent, so the divisibility parameters are

$$h_1 = 2, \quad d_1 = 1, \quad h_2 = 1, \quad d_2 = 1.$$

It follows from Lemma 2.15 that we have

$$A_2(2^{n_1}, 2^{n_2}) = A_2\big(2^{\min(n_1,3)}, 2^{\min(n_2,3)}\big)\,,$$

so we only need to compute

$$A_2(2^{n_1}, 2^{n_2}) = \frac{2^{n_1+n_2}}{\big[\mathbb{Q}\big(\zeta_{2^{\max(n_1,n_2)}},\ \sqrt[2^{n_1}]{2},\ \sqrt[2^{n_2}]{-9}\big) : \mathbb{Q}(2^{\max(n_1,n_2)})\big]}$$

for $n_1, n_2 \in \{0,1,2,3\}$. These computations are shown in the following table:

	$n_2=0$	$n_2=1$	$n_2=2$	$n_2=3$
$n_1=0$	1	1	2	2
$n_1=1$	1	1	2	4
$n_1=2$	1	2	2	4
$n_1=3$	2	4	4	4

We now compute the 2-adelic failure

$$B_2(M, 2^{n_1}, 2^{n_2}) = \big[\mathbb{Q}\big(\zeta_{2^n},\ \sqrt[2^{n_1}]{2},\ \sqrt[2^{n_2}]{-9}\big) \cap \mathbb{Q}\left(\zeta_M\right) : \mathbb{Q}\left(\zeta_{2^n}\right)\big]$$

for any M, n_1, n_2 with $n_1, n_2 \leqslant v_2(M)$, and where $n = \max(n_1, n_2)$. By Theorem 2.22 we just need to compute such values for $n_1, n_2 \leqslant 3$ and $M \mid 24$. We take into account that:

- We have $\sqrt{2} \in \mathbb{Q}(\zeta_8)$ and there is no M with $8 \nmid M$ such that $\sqrt{2} \in \mathbb{Q}(\zeta_M)$; moreover $\sqrt[2^n]{2} \notin \mathbb{Q}(\zeta_\infty)$ for $n \geqslant 2$. This implies that for M with $2^m \mid M$ we have for $n \geqslant 1$

$$\left[\mathbb{Q}\left(\zeta_{2^m}, \sqrt[2^n]{2}\right) \cap \mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_{2^m})\right] = \begin{cases} 1 & \text{if } 8 \nmid M \text{ or } m \geqslant 3, \\ 2 & \text{if } 8 \mid M \text{ and } m \leqslant 2. \end{cases}$$

- We have $\sqrt{-9} = 3\zeta_4 \in \mathbb{Q}(\zeta_4)$, while $\sqrt[4]{-9} = \zeta_8\sqrt{3} \in \mathbb{Q}(\zeta_{24})$ and there is no M with $24 \nmid M$ such that $\sqrt[4]{-9} \in \mathbb{Q}(\zeta_M)$; moreover $\sqrt[2^n]{-9} \notin \mathbb{Q}(\zeta_\infty)$ for $n \geqslant 3$. This implies that for M with $2^m \mid M$ we have

$$\left[\mathbb{Q}\left(\zeta_{2^m}, \sqrt{-9}\right) \cap \mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_{2^m})\right] = \begin{cases} 1 & \text{if } m \geqslant 2 \text{ or } 4 \nmid M, \\ 2 & \text{if } m = 1 \text{ and } 4 \mid M; \end{cases}$$

  whereas for $m \geqslant n \geqslant 2$

$$\left[\mathbb{Q}\left(\zeta_{2^m}, \sqrt[2^n]{-9}\right) \cap \mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_{2^m})\right] = \begin{cases} 1 & \text{if } 24 \nmid M, \\ 2 & \text{if } 24 \mid M. \end{cases}$$

- We have $\mathbb{Q}(\zeta_4, \sqrt{2}) = \mathbb{Q}(\zeta_8)$ and $\left[\mathbb{Q}(\sqrt{2}, \zeta_8\sqrt{3}) : \mathbb{Q}(\zeta_4)\right] = 4$.

These remarks are sufficient to compute the following table for the 2-adelic failure $B_2(M, 2^{n_1}, 2^{n_2})$:

(n_1, n_2)	$M = 6$	$M = 4$	$M = 12$	$M = 8$	$M = 24$
$(0,1)$	1	2	2	2	2
$(0,2)$		1	1	1	2
$(0,3)$				1	2
$(1,0)$	1	1	1	2	2
$(1,1)$	1	2	2	4	4
$(1,2)$		1	2	2	4
$(1,3)$				1	2
$(2,0)$		1	1	2	2
$(2,1)$		1	1	2	2
$(2,2)$		1	2	2	4
$(2,3)$				1	2
$(3,0)$				1	1
$(3,1)$				1	1
$(3,2)$				1	2
$(3,3)$				1	2

where we have omitted the case $M = 2$ because $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ and hence the 2-adelic failure equals 1. Finally, we have

$$\left[\mathbb{Q}\left(\zeta_M, \sqrt[N_1]{2}, \sqrt[N_2]{-9}\right) : \mathbb{Q}\right] = \frac{\varphi(M)N_1N_2}{A_2(2^{\min(n_1,3)}, 2^{\min(n_2,3)})B_2(\gcd(M,24), 2^{\min(n_1,3)}, 2^{\min(n_2,3)})},$$

where $n_i := v_2(N_i)$ for $i = 1, 2$.

We now give an example for the results of Section 2.4.

Example 2.35. Let $K = \mathbb{Q}(\sqrt{3})$ and $G = \langle 11, 75\rangle$. We compute the degree of $K(\sqrt[n]{G})/K$ for every $n \geqslant 1$. The given basis of G is ℓ-good for every prime ℓ. Moreover, 11 is strongly ℓ-indivisible for every ℓ, while $75 = (5\sqrt{3})^2$ is a square and strongly ℓ-indivisible for every odd ℓ. By [10, Theorem 15] for every prime power ℓ^e we have

$$[G : G \cap K^{\times \ell^e}] = \begin{cases} 2^{2e-1} & \text{if } \ell = 2, \\ \ell^{2e} & \text{otherwise} \end{cases}$$

so we deduce that $[B_n : K^\times] = n^3/\gcd(2,n)^2$. For the computation of the entanglement group, we take into account the following facts:

- $\mu_K = \mu_2$
- $K \subseteq \mathbb{Q}(\mu_{12}) = K(\mu_{12})$, and K is linearly disjoint from $\mathbb{Q}(\mu_n)$ over $\mathbb{Q}$ if $12 \nmid n$
- $\sqrt{11} \in \mathbb{Q}(\mu_{44})$ and $\sqrt{33} \in \mathbb{Q}(\mu_{33})$
- $\sqrt[2^e]{75}$ does not belong to $K(\mu_\infty)$ if $e \geqslant 2$ (because $\sqrt[4]{3} \notin \mathbb{Q}(\mu_\infty)$).

From Theorem 2.7 we deduce that $B_{n,\mathrm{ab}} = \langle K^\times, \mu_n, H_n\rangle$, where

$$H_n = \begin{cases} \langle 1\rangle & \text{if } 2 \nmid n \\ \langle \sqrt{11}\rangle & \text{if } \gcd(4,n) = 2 \\ \langle \sqrt{11}, \sqrt{5\sqrt{3}}\rangle & \text{if } 4 \mid n\,, \end{cases}$$

and for the computation of $\sharp E(B_n)$, setting $L_n := K(H_n) \cap \mathbb{Q}(\mu_n)$, we have $E(B_n) \cong \mathrm{Gal}(L_n/\mathbb{Q})$.

If $12 \mid n$, then we have two cases: if $11 \mid n$, then $L_n = K(\sqrt{11})$, else $L_n = K$. So $\sharp E(B_n)$ is 4 if $11 \mid n$ and it is 2 otherwise. If $12 \nmid n$ and n is even, then we have: $L_n = \mathbb{Q}(\sqrt{11})$ if $44 \mid n$, $L_n = \mathbb{Q}(\sqrt{33})$ if $33 \mid n$, else $L_n = \mathbb{Q}$. Thus $\sharp E(B_n)$ is 2 if $44 \mid n$ or $33 \mid n$ and it is 1 otherwise. If n is odd, then we always have $\sharp E(B_n) = 1$ because $L_n = \mathbb{Q}$.

Noticing that

$$\prod_{\substack{p \text{ odd prime} \\ p \mid n}} \frac{p-1}{p} = \frac{\varphi(n)\gcd(2,n)}{n},$$

we conclude that

$$[K(\sqrt[n]{G}) : K] = \frac{n^2\varphi(n)}{\gcd(2,n)\cdot \sharp E(B_n)} = \begin{cases} n^2\varphi(n) & \text{if } \gcd(132,n) \text{ is odd}, \\ n^2\varphi(n)/2 & \text{if } \gcd(132,n) \in \{2,4,6,22\}, \\ n^2\varphi(n)/4 & \text{if } \gcd(132,n) \in \{12,44,66\}, \\ n^2\varphi(n)/8 & \text{if } \gcd(132,n) = 132. \end{cases}$$

The failure of maximality of the above Kummer degree is due to the following facts: 75 is a square in K; $K \subseteq \mathbb{Q}(\mu_{12})$; $\sqrt{11} \in \mathbb{Q}(\mu_{44})$; $\sqrt{11}\cdot 5\sqrt{3} \in \mathbb{Q}(\mu_{66})$.

Chapter 3

On the distribution of the order of the reductions of algebraic numbers over congruence classes

Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$. We consider the order of the cyclic group $(G \bmod \mathfrak{p})$ for almost all primes $\mathfrak{p}$ of K, and ask whether this number lies in a given arithmetic progression. In this chapter we prove that the density of primes for which the condition holds is, under some general assumptions, a computable rational number which is strictly positive. We have also shown the following equidistribution property: if ℓ^e is a prime power and a is a multiple of ℓ (and a is a multiple of 4 if $\ell = 2$), then the density of primes $\mathfrak{p}$ of K such that the order of $(G \bmod \mathfrak{p})$ is congruent to a modulo ℓ^e only depends on a through its ℓ-adic valuation. The results of this chapter are published in the article [44] by Perucca and Sgobba.

3.1 Main results

Consider a number field K and a multiplicative subgroup G of $K^\times$ which is finitely generated. In this chapter, for positive integers x, y with $y \mid x$ we denote by $K_x := K(\zeta_x)$ the xth cyclotomic extension of K, and by $K_{x,y} := K_x(\sqrt[y]{G})$ the yth Kummer extension of G over K_x. We make use of the notation introduced in Section 1.1. Recall that, if we assume (GRH) we mean the extended Riemann hypothesis for the Dedekind zeta function of number fields.

In [43] Perucca and the author have generalised a result by Ziegler [59, Theorem 1] to higher rank and have proven in particular Theorem 1.1, which we rephrase here for matters of notation.

Theorem 3.1 ([43, Theorem 1.3])**.** *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank. Fix an integer $d \geqslant 2$, fix an integer a, and consider the following set of primes of K:*

$$\mathcal{P} := \{\mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d\}\,.$$

Let $\mathcal{P}(x)$ be the number of primes $\mathfrak{p}$ in $\mathcal{P}$ with norm up to x.

Assuming (GRH), for every $x \geqslant 1$ we have

$$\mathcal{P}(x) = \frac{x}{\log x} \sum_{n,t \geqslant 1} \frac{\mu(n) c(n,a,d,t)}{[K_{[d,n]t,nt} : K]} + O\left(\frac{x}{\log^{3/2} x}\right), \tag{3.1}$$

where $c(n,a,d,t) \in \{0,1\}$*, and where* $c(n,a,d,t) = 1$ *if and only if the following conditions hold:*

(i) $(1+at, d) = 1$*;*

(ii) $(d,n) \mid a$*;*

(iii) the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{dt})/\mathbb{Q})$ *mapping* ζ_{dt} *to* ζ_{dt}^{1+at} *is the identity on* $\mathbb{Q}(\zeta_{dt}) \cap K_{nt,nt}$*.*

From this result it is not clear whether the natural density $\mathrm{dens}_K(G, a \bmod d)$ of the set $\mathcal{P}$ is a rational number, if it is strictly positive, or if it is possible to evaluate it. The main results of this chapter are the following, where K, G, a, and d are as in Theorem 3.1:

Theorem 3.2. *Assume (GRH). Let* $d = \ell^e$ *for some prime number* ℓ *and for some* $e \geqslant 1$*. Suppose that* $K = K_\ell$ *if* ℓ *is odd, or that* $K = K_4$ *if* $\ell = 2$*. Then the density* $\mathrm{dens}_K(G, a \bmod \ell^e)$ *depends on* a *only through its* ℓ*-adic valuation, and it is a computable strictly positive rational number. In particular, it is the same for all* a *coprime to* ℓ*.*

Although the previous result has an assumption on the base field, we do not need that assumption in the following corollary.

Corollary 3.3 (Equidistribution property)**.** *Assume (GRH). Let* K *be any number field, and let* $d = \ell^e$ *for a prime number* ℓ *and* $e \geqslant 1$*. Suppose that* $\ell \mid a$ *if* ℓ *is odd, or that* $4 \mid a$ *and* $e \geqslant 2$ *if* $\ell = 2$*. Then the density* $\mathrm{dens}_K(G, a \bmod \ell^e)$ *depends on* a *only through its* ℓ*-adic valuation, and it is a computable strictly positive rational number.*

The following result concerns the case of composite modulus.

Theorem 3.4. *Assume (GRH). Let* $d \geqslant 2$ *and set* $r := \mathrm{rad}(d)$ *for its radical. Suppose that* $K = K_r$ *if* d *is odd, or that* $K = K_{2r}$ *if* d *is even. Then, for* a *coprime to* d*, the density* $\mathrm{dens}_K(G, a \bmod d)$ *is a computable strictly positive rational number which does not depend on* a*.*

The following result generalizes the positivity assertion of Corollary 3.3.

Theorem 3.5. *Assume (GRH). The density* $\mathrm{dens}_K(G, a \bmod d)$ *is strictly positive for any number field* K *if* d *is a prime power or if* a *is coprime to* d*.*

Theorem 3.2 is proven in Section 3.3.1 for ℓ odd, and in Section 3.3.2 for $\ell = 2$, respectively. We prove Corollary 3.3 in Section 3.3.3. Theorem 3.4 is proven in Section 3.3.4, while Theorem 3.5 is proven in Section 3.3.5. Section 3.4 is devoted to removing from Theorem 3.1 the assumption that the group G is torsion-free. Finally, Section 3.5 contains examples of applications of the above theorems and some numerical data.

Notice that in this chapter we rely on Theorem 3.1 and hence most of our results assume (GRH): if the density in Theorem 3.1 is known unconditionally, then our results would also be unconditional.

3.2 Preliminaries

Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$. In the whole chapter we tacitly assume that the primes $\mathfrak{p}$ of K that we consider are such that the reduction of G modulo $\mathfrak{p}$ is a well-defined subgroup of the multiplicative group of the residue field at $\mathfrak{p}$. Notice that the results of this section are unconditional.

3.2.1 Prescribing valuations for the order

Theorem 3.6. *Let $\ell_1, \dots, \ell_n$ be distinct prime numbers and $x_1, \dots, x_n$ nonnegative integers. Then the density of primes $\mathfrak{p}$ of K such that $v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) = x_i$ for all i is a strictly positive computable rational number.*

Proof. The rationality of the density can be seen by neglecting the condition on the Frobenius in [41, Theorem 18]. For the positivity, apply [38, Proposition 12] to a basis $g_1, \dots, g_r$ of G consisting of $\mathbb{Z}$-independent points of the multiplicative group $K^\times$. □

Corollary 3.7. *Given an integer $d \geqslant 2$ and a positive divisor g of d, the sum of densities*

$$\sum_{\substack{0 \leqslant a < d \\ (a,d)=g}} \mathrm{dens}_K(G, a \bmod d) \tag{3.2}$$

is a strictly positive computable rational number.

Proof. We will express the sum (3.2) as a rational combination of densities as in Theorem 3.6. Write $g = \prod_{i=1}^n \ell_i^{f_i}$, and partition the index set as $\{1, \dots, n\} = I \sqcup J$ such that $f_i < v_{\ell_i}(d)$ for $i \in I$, and $f_i = v_{\ell_i}(d)$ for $i \in J$. Then it is easy to check that

$$\sum_{\substack{0 \leqslant a < d \\ (a,d)=g}} \mathrm{dens}_K(G, a \bmod d) = \mathrm{dens}_K\left(\left\{\mathfrak{p} : \begin{array}{c} v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) = f_i \,, \forall i \in I \\ v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) \geqslant f_i \,, \forall i \in J \end{array}\right\}\right). \tag{3.3}$$

From this expression and Theorem 3.6 we deduce that (3.2) is strictly positive. The density on the right-hand side of (3.3) is given by (applying the inclusion-exclusion principle for the primes up to x and then taking the limit to make the densities)

$$\sum_{s=0}^{|J|} (-1)^s \sum_{\substack{S \subseteq J \\ |S|=s}} \mathrm{dens}_K\left(\left\{\mathfrak{p} : \begin{array}{c} v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) = f_i \,, \forall i \in I \\ v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G)) \leqslant f_i - 1 \,, \forall i \in S \end{array}\right\}\right), \tag{3.4}$$

and each of the densities in (3.4) exists and equals

$$\mathrm{dens}_K\left(\left\{\mathfrak{p} : \begin{array}{c} v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G^h)) = f_i \,, \forall i \in I \\ v_{\ell_i}(\mathrm{ord}_{\mathfrak{p}}(G^h)) = 0 \,, \forall i \in S \end{array}\right\}\right),$$

where $h = \prod_{i \in S} \ell_i^{f_i - 1}$. Such densities are computable rational numbers by Theorem 3.6. Hence the statement is proven. □

Remark 3.8. Corollary 3.7 implies that the density $\mathrm{dens}_K(G, 0 \bmod d)$ is known unconditionally to be a strictly positive computable rational number.

3.2.2 Simplifications by changing the modulus

We keep the notation of Theorem 3.1. By Remark 3.8 we may suppose that $0 < a < d$. The following lemma allows us to reduce to residue classes coprime to d if d is a prime power.

Lemma 3.9. *Let $d = \ell^e$, where ℓ is a prime number and $e \geqslant 1$. Suppose that $a = \ell^x \cdot w$, where w is coprime to ℓ and $0 < x < e$. Set $w_j := w + j\ell^{e-x}$ for $0 \leqslant j < \ell$ (notice that w_j is also coprime to ℓ). Then the primes $\mathfrak{p}$ of K such that $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$ are exactly those such that*

$$\mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) \equiv w \bmod \ell^{e-x} \tag{3.5}$$

minus those such that

$$\mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) \equiv w_j \bmod \ell^{e-x+1} \tag{3.6}$$

for some $0 \leqslant j < \ell$. In particular, we have

$$\mathrm{dens}_K(G, a \bmod \ell^e) =$$
$$\mathrm{dens}_K(G^{\ell^x}, w \bmod \ell^{e-x}) - \sum_{j=0}^{\ell-1} \mathrm{dens}_K(G^{\ell^{x-1}}, w_j \bmod \ell^{e-x+1}) .$$

Proof. Notice that condition (3.6) for any j implies condition (3.5) because w_j is coprime to ℓ and hence we must have $\mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) = \mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}})$.

Let $\mathfrak{p}$ be a prime of K such that $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$. In particular, ℓ^x divides $\mathrm{ord}_{\mathfrak{p}}(G)$. Thus we have

$$\mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) = \frac{\mathrm{ord}_{\mathfrak{p}}(G)}{\ell^x} \qquad \text{and} \qquad \mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) = \frac{\mathrm{ord}_{\mathfrak{p}}(G)}{\ell^{x-1}} .$$

Dividing the congruence $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod \ell^e$ by ℓ^x and ℓ^{x-1}, respectively, we obtain

$$\mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) \equiv w \bmod \ell^{e-x} \qquad \text{and} \qquad \mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) \equiv w\ell \bmod \ell^{e-x+1} .$$

We have proven one containment because $w\ell$ is not congruent to any of the w_j modulo ℓ.

Now suppose that (3.5) holds, and that (3.6) does not hold for any j. In particular we must have $\mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) \neq \mathrm{ord}_{\mathfrak{p}}(G^{\ell^x})$. We deduce $\mathrm{ord}_{\mathfrak{p}}(G^{\ell^{x-1}}) = \ell \cdot \mathrm{ord}_{\mathfrak{p}}(G^{\ell^x})$, and therefore $\mathrm{ord}_{\mathfrak{p}}(G) = \ell^x \cdot \mathrm{ord}_{\mathfrak{p}}(G^{\ell^x})$. We may conclude because multiplying (3.5) by ℓ^x gives

$$\ell^x \cdot \mathrm{ord}_{\mathfrak{p}}(G^{\ell^x}) \equiv a \bmod d . \qquad \square$$

Remark 3.10. Consider the condition $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$. Decompose $(a, d) = sh$ where $s = \prod_{\ell | (a,d)} \ell$ is its radical, and write $a' = \frac{a}{h}$, $d' = \frac{d}{h}$. Notice that $(a', d') = s$ is squarefree. We claim that the following equivalence holds:

$$\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d \qquad \Longleftrightarrow \qquad \mathrm{ord}_{\mathfrak{p}}(G^h) \equiv a' \bmod d' .$$

If the first congruence is satisfied, then (a, d) divides $\mathrm{ord}_{\mathfrak{p}}(G)$, so in particular we have

$$\frac{\mathrm{ord}_{\mathfrak{p}}(G)}{h} \equiv a' \bmod d' .$$

Since h divides $\mathrm{ord}_{\mathfrak{p}}(G)$, we have $\frac{\mathrm{ord}_{\mathfrak{p}}(G)}{h} = \mathrm{ord}_{\mathfrak{p}}(G^h)$ and the second congruence holds. Conversely, if the second congruence is satisfied, then $s = (a', d')$ divides $\mathrm{ord}_{\mathfrak{p}}(G^h)$. Since h introduces no new prime factors, we have

$$\mathrm{ord}_{\mathfrak{p}}(G^h) \cdot h = \mathrm{ord}_{\mathfrak{p}}(G)$$

and hence the congruence $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$ holds.

3.2.3 A general result

We keep the notation from Theorem 3.1, and we denote by $\mathrm{Dens}_K(G,d)$ the density of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_{\mathfrak{p}}(G)$ is coprime to d.

Remark 3.11. From the results in [10] and [40], under the assumptions of Theorems 3.2 and 3.4, the density $\mathrm{Dens}_K(G,d)$ depends on G only through the d-parameters for the ℓ-divisibility of G for each $\ell \mid d$. As a consequence of the results of this chapter, the same holds for the density $\mathrm{dens}_K(G, a \bmod d)$ considered in Theorems 3.2 and 3.4 and in Corollary 3.3.

Theorem 3.12. *Let ℓ be a prime number. Suppose that for every G and for every $e \geqslant 1$ we have*

$$\mathrm{dens}_K(G, w \bmod \ell^e) = \mathrm{dens}_K(G, w' \bmod \ell^e)$$

as long as w, w' are coprime to ℓ. Then for every G and for every $e \geqslant 1$ the density

$$\mathrm{dens}_K(G, a \bmod \ell^e)$$

depends on a only through its ℓ-adic valuation, and it is a computable rational number.

Proof. We know from [10, Theorem 3] that the quantity

$$\mathrm{Dens}_K(G,\ell) = 1 - \mathrm{dens}_K(G, 0 \bmod \ell)$$

is a computable rational number. Then for every a coprime to ℓ, by the assumption on the equidistribution, we have

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \frac{1}{\varphi(\ell^e)} \cdot \mathrm{Dens}_K(G,\ell)\,,$$

so that $\mathrm{dens}_K(G, a \bmod \ell^n)$ is a computable rational number which does not depend on a.

For $0 < a < \ell^e$ not coprime to ℓ we apply Lemma 3.9, which allows us to compute the density $\mathrm{dens}_K(G, a \bmod \ell^e)$ as the difference of densities which we know to be computable rational numbers. More precisely, by the equidistribution condition the formula given in Lemma 3.9 becomes

$$\begin{aligned}&\mathrm{dens}_K(G, a \bmod \ell^e) = \\ &\mathrm{dens}_K(G^{\ell^x}, w \bmod \ell^{e-x}) - \ell \cdot \mathrm{dens}_K(G^{\ell^{x-1}}, w \bmod \ell^{e-x+1})\,,\end{aligned}$$

where $a = w\ell^x$ and $x = v_\ell(a)$. In particular, this formula shows that what matters about a is only its ℓ-adic valuation.

Finally the density for $a = 0$ is given as the complementary density of all the considered cases, and hence it is also a computable rational number. □

Remark 3.13. Notice that for $0 < a < \ell^e$ with some fixed valuation $v_\ell(a) = x$ where $0 \leqslant x < e$, the previous theorem says that we have the following density:

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \frac{1}{\varphi(\ell^{e-x})} \cdot \mathrm{dens}_K\left(\{\mathfrak{p} : v_\ell(\mathrm{ord}_{\mathfrak{p}}(G)) = x\}\right)\,. \tag{3.7}$$

Proposition 3.14. *With the assumptions of Theorem 3.12, we have that the density $\mathrm{dens}_K(G, a \bmod \ell^e)$ is strictly positive for every a.*

Proof. For $a = 0$ we know this unconditionally by Remark 3.8. For $0 < a < \ell^e$, by Theorem 3.6 the densities (3.7) in Remark 3.13 are strictly positive. □

We say that a prime $\mathfrak{p}$ of K is of degree 1 if both its ramification index and its residue class degree over $\mathbb{Q}$ are equal to 1.

Lemma 3.15. *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$. Let a, d be integers with $d \geqslant 2$ and let $r := \prod_{\ell \mid d} \ell$ be the radical of d. Let $m = r$ if d is odd, and $m = 2r$ otherwise. Consider the following set of primes $\mathfrak{p}$ of K:*

$$\mathcal{S} := \{\mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d,\ \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m\}\,.$$

Then the density of the set $\mathcal{S}$ exists and it is equal to

$$\frac{1}{[K_m : K]} \cdot \mathrm{dens}_{K_m}(G, a \bmod d)\,. \tag{3.8}$$

Remark 3.16. Notice that, assuming (GRH), a formula for the density of the set $\mathcal{S}$ is given in [43, Corollary 5.2]. By Theorems 3.2 and 3.4 it follows that the density (3.8) is a computable strictly positive rational number if d is a prime power or if a is coprime to d. Moreover, if $d = \ell^e$ for a prime ℓ, then the density of $\mathcal{S}$ depends on a only through its ℓ-adic valuation, while if d is composite and $(a, d) = 1$, then it does not depend on a.

Proof of Lemma 3.15. We may assume that the primes $\mathfrak{p}$ of $\mathcal{S}$ are of degree 1 and unramified in K_m. Hence for a prime $\mathfrak{p}$ in $\mathcal{S}$ we have $\mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m$ if and only if $\mathfrak{p}$ splits completely in K_m. Therefore, the set of primes of K_m lying above the primes of $\mathcal{S}$ is the set

$$\{\mathfrak{P} \subseteq K_m \text{ of degree } 1 : \mathrm{ord}_{\mathfrak{P}}(G) \equiv a \bmod d\}\,,$$

which has density $\mathrm{dens}_{K_m}(G, a \bmod d)$. Thus we obtain that the density of the set $\mathcal{S}$ exists and it is equal to $1/[K_m : K]$ times $\mathrm{dens}_{K_m}(G, a \bmod d)$ (see for instance [40, Proposition 1]). □

3.3 Proof of the main results

We keep the notation of Theorem 3.1.

3.3.1 Proof of Theorem 3.2 for ℓ odd

Lemma 3.17. *Let ℓ be an odd prime number. Suppose that $K = K_\ell$. For every G and for every $e \geqslant 1$ we have*

$$c(n, x, \ell^e, t) = c(n, x', \ell^e, t)$$

as long as x, x' are coprime to ℓ.

Proof. Let $d = \ell^e$. Let a vary among the integers strictly between 0 and d and coprime to ℓ. Since a is coprime to ℓ and $d = \ell^e$, the condition $(d, n) \mid a$ means $\ell \nmid n$ and it is independent of a. If $c(n, a, d, t)$ is non-zero, then the integer t must be divisible by ℓ because $\zeta_\ell \in K$ and hence it must be fixed if raised to the power $1 + at$ (recall that a is coprime to ℓ). In particular, the condition $(1 + at, d) = 1$ holds independently of a.

We are left to check that Condition (iii) of Theorem 3.1 does not depend on a, provided that Conditions (i) and (ii) hold. Write $F := K_{nt,nt}$ and define $\tau := v_\ell(t)$. We thus have to show that the following is independent of a: the Galois group of $F_{\ell^{e+\tau}}/F$ contains the automorphism σ_{1+at} satisfying $\zeta_{\ell^{e+\tau}} \mapsto \zeta_{\ell^{e+\tau}}^{1+at}$. Since $K = K_\ell$, we have some largest integer $x \geqslant \tau \geqslant 1$ such that

F contains $\mathbb{Q}_{\ell^x}$, and this integer determines the Galois group of $F_{\ell^{e+\tau}}/F$, which is a finite cyclic ℓ-group.

If $x \geqslant e+\tau$, then the field extension $F_{\ell^{e+\tau}}/F$ is trivial and the coefficient $c(n,a,\ell^e,t)$ is 0 independently of a. Now suppose that $\tau \leqslant x < e+\tau$. The exponents for the action on $\zeta_{\ell^{e+\tau}}$ are those corresponding to the automorphisms of order dividing $\ell^{e+\tau-x}$. Since $v_\ell(at)$ does not depend on a, we have that

$$v_\ell((1+at)^{\ell^n}-1) = \tau+n$$

independently of a and we conclude. □

Proof of Theorem 3.2 for ℓ odd. Lemma 3.17 implies that the conditions of Theorem 3.12 are satisfied if $K = K_\ell$ (compare with formula (3.1)). Thus the density $\mathrm{dens}_K(G, a \bmod d)$ depends on a only through its ℓ-adic valuation, and it is a computable rational number. By Proposition 3.14 this rational number must be strictly positive. □

3.3.2 Proof of Theorem 3.2 for $\ell = 2$

Lemma 3.18. *Suppose $K = K_4$. For every G and for every $e \geqslant 1$ we have*

$$c(n,x,2^e,t) = c(n,x',2^e,t)$$

as long as x, x' are odd.

Proof. Let $d = 2^e$. Notice that the claim is clear for $e = 1$, so suppose $e \geqslant 2$. Let a vary in the odd integers strictly between 0 and d. Similarly to the proof of Lemma 3.17, the condition $(n,d) \mid a$ means that $2 \nmid n$ and is independent of a. Moreover, t must be an even integer and hence the condition $(1+at,d) = 1$ is satisfied independently of a. Now suppose that the above conditions are satisfied, and let us focus on Condition (iii) of Theorem 3.1.

Set $\tau := v_2(t)$, and call F the field $K_{nt,nt}$. Similarly to the proof of Lemma 3.17, we check that the following condition is independent of a: the Galois group of $F_{2^{e+\tau}}/F$ contains the automorphism σ_{1+ta} satisfying $\zeta_{2^{e+\tau}} \mapsto \zeta_{2^{e+\tau}}^{1+at}$.

Recall that $K = K_4$, and call $x \geqslant 2$ the largest integer such that F contains $\mathbb{Q}_{2^x}$ (we clearly have $x \geqslant \tau$). We then need to investigate the cyclic group $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_{2^x})$.

If $x \geqslant e+\tau$, then this field extension is trivial and we have $c(n,a,2^e,t) = 0$ independently of a (where a is odd). If $x = \tau$ then $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_{2^x})$ contains 2^e automorphisms acting distinctly on $\zeta_{2^{e+\tau}}$ and fixing ζ_{2^τ}: we deduce that $c(n,a,2^e,t) = 1$ independently of a (where a is odd).

From now on, suppose $\tau < x < e+\tau$. We see $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_{2^x})$ as a subgroup of the cyclic Galois group $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_4)$. That subgroup contains the elements of order dividing $2^{e+\tau-x}$. The Galois automorphisms are determined by the image of $\zeta_{2^{e+\tau}}$, and they are determined by the exponent to which they raise this element.

If $\tau = 1$, then we do not have the automorphism σ_{1+at} in $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_4)$ (independently of a) because a is odd and hence $\zeta_4^{1+at} \neq \zeta_4$. This means that in this case $c(n,a,2^e,t) = 0$ independently of a (for a odd).

Finally suppose $1 < \tau < x < e+\tau$. Since $\tau > 1$, the automorphism $\sigma_{1+at} \in \mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_4)$ is well-defined. We have to check whether σ_{1+at} also belongs to $\mathrm{Gal}(\mathbb{Q}_{2^{e+\tau}}/\mathbb{Q}_{2^x})$ or not independently of a. It is then sufficient to show that the order of σ_{1+at} does not depend on a. This order is a power of 2, namely the smallest power 2^n such that $v((1+at)^{2^n}-1) \geqslant e+\tau$. Since $v_2(at) \geqslant 2$, then for every $n \geqslant 1$ we have $v_2((1+at)^{2^n}-1) = \tau+n$ independently of a and hence the order of the automorphism σ_{1+at} does not depend on a. □

Proof of Theorem 3.2 for $\ell = 2$. Analogously to the proof for the odd case, it suffices to combine Lemma 3.18 with Theorem 3.12 and Proposition 3.14. □

3.3.3 Proof of Corollary 3.3

Proof of Corollary 3.3. Let $m = \ell$ if ℓ is odd, and $m = 4$ if $\ell = 2$. Let $\mathfrak{p}$ be a prime of K of degree 1, and which does not ramify in K_m. In view of our hypothesis on a, we have that if $\mathfrak{p}$ is such that $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod \ell^e$, then $\mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m$. We deduce from Lemma 3.15 that

$$\mathrm{dens}_K(G, a \bmod \ell^e) = \frac{1}{[K_m : K]} \cdot \mathrm{dens}_{K_m}(G, a \bmod \ell^e)\,.$$

By Theorem 3.2 we conclude that $\mathrm{dens}_K(G, a \bmod \ell^e)$ depends on a only through its ℓ-adic valuation and that it is a computable strictly positive rational number. □

3.3.4 Proof of Theorem 3.4

Lemma 3.19. *Let $d \geqslant 2$ be an integer and write $d = \prod \ell^e$ for its prime decomposition. For the coefficients of Theorem 3.1, with respect to any fixed group G, we have*

$$c(n, a, d, t) = \prod_{\ell \mid d} c(n, a, \ell^e, t)\,.$$

Proof. We prove that $c(n, a, d, t) = 1$ if and only if $c(n, a, \ell^e, t) = 1$ for every prime divisor ℓ of d. It is clear that $(1 + at, d) = 1$ and $(d, n) \mid a$ if and only if $(1 + at, \ell^e) = 1$ and $(\ell^e, n) \mid a$ for every ℓ. Now suppose that these conditions hold. Let σ be the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{dt})/\mathbb{Q})$ such that $\sigma(\zeta_{dt}) = \zeta_{dt}^{1+at}$, and let σ_ℓ be the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^e t})/\mathbb{Q})$ such that $\sigma_\ell(\zeta_{\ell^e t}) = \zeta_{\ell^e t}^{1+at}$. We are left to show that σ is the identity on $\mathbb{Q}(\zeta_{dt}) \cap K_{nt,nt}$ if and only if σ_ℓ is the identity on $\mathbb{Q}(\zeta_{\ell^e t}) \cap K_{nt,nt}$ for every ℓ. This follows from the fact that $\mathbb{Q}(\zeta_{dt})$ is the compositum of the fields $\mathbb{Q}(\zeta_{\ell^e t})$, and σ_ℓ is the restriction of σ to $\mathbb{Q}(\zeta_{\ell^e t})$ for each ℓ. □

Lemma 3.20. *Let $d \geqslant 2$ be an integer and let $r := \prod_{\ell \mid d} \ell$ be its radical. Suppose that $K = K_r$ if d is odd, or that $K = K_{2r}$ if d is even. For the coefficients of Theorem 3.1, with respect to any fixed group G, we then have*

$$c(n, x, d, t) = c(n, x', d, t)$$

as long as x, x' are coprime to d.

Proof. We have to show that, whenever a is coprime to d, the coefficient $c(n, a, d, t)$ is independent of a. By Lemma 3.19 we may reduce to the case in which d is a prime power, and then we may conclude by Lemma 3.17 if d is odd, and Lemma 3.18 if d is even. □

Proof of Theorem 3.4. By [40, Corollary 12] and [10, Theorem 3] the density $\mathrm{Dens}_K(G, d)$ of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_{\mathfrak{p}}(G)$ is coprime to d is an explicitly computable rational number. This density can be decomposed as the sum over a, with a coprime to d, of the densities $\mathrm{dens}_K(G, a \bmod d)$. Since $K_r = K$ if d is odd, and $K_{2r} = K$ if d is even, by Lemma 3.20 the above densities have equal value, so that for every a coprime to d we have

$$\mathrm{dens}_K(G, a \bmod d) = \frac{1}{\varphi(d)} \cdot \mathrm{Dens}_K(G, d)\,,$$

which is then a computable rational number. Moreover, this density is also strictly positive because by Theorem 3.6 the density $\mathrm{Dens}_K(G, d)$ is strictly positive. □

3.3.5 Proof of Theorem 3.5

Proof of Theorem 3.5. Let r be the radical of d, and let $m = r$ if d is odd, and $m = 2r$ otherwise. Consider the following set of primes $\mathfrak{p}$ of K of degree 1, and unramified in K_m:

$$\mathcal{S} := \{\mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d,\ \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m\}\,.$$

By Lemma 3.15 the set $\mathcal{S}$ has density equal to

$$\frac{1}{[K_m : K]} \cdot \mathrm{dens}_{K_m}(G, a \bmod d)\,.$$

By Theorems 3.2 and 3.4, the density $\mathrm{dens}_{K_m}(G, a \bmod d)$ is strictly positive if d is a prime power or if a is coprime to d, so the same holds for the density of $\mathcal{S}$. Consequently, the density $\mathrm{dens}_K(G, a \bmod d)$ is also strictly positive. □

3.4 Multiplicative groups with torsion

Stating Theorem 3.1 for a finite group is trivial (the given density is either 0 or 1). However it is not trivial to remove the assumption that the multiplicative group is torsion-free: this is what we achieve in this section. As a side remark, notice that our strategy also applies to the density considered in [43, Theorem 1.4], i.e. if we introduce a condition on the Frobenius conjugacy class with respect to a fixed finite Galois extension of the base field.

Let K be a number field, and let G' be a finitely generated (and not necessarily torsion-free) multiplicative subgroup of $K^\times$ of positive rank. Then we can write G' as $G' = \langle\zeta\rangle \times G$, where ζ is a root of unity of K generating the torsion part of G' and G is torsion-free. Let us exclude finitely many primes $\mathfrak{p}$ of K so that the reduction of G' is well-defined and we have $\mathrm{ord}_{\mathfrak{p}}(\zeta) = \mathrm{ord}(\zeta)$. The order of G' modulo $\mathfrak{p}$ is then the least common multiple between the order of G modulo $\mathfrak{p}$ and a fixed integer:

$$\mathrm{ord}_{\mathfrak{p}}(G') = [\mathrm{ord}_{\mathfrak{p}}(G), \mathrm{ord}(\zeta)]\,.$$

We may then reformulate the given problem.

Remark 3.21. Let G be a finitely generated and torsion-free subgroup of $K^\times$, and fix some integer $n \geqslant 2$. Given two integers a and $d \geqslant 2$, we investigate the density of primes $\mathfrak{p}$ of K for which

$$[\mathrm{ord}_{\mathfrak{p}}(G), n] \equiv a \bmod d\,. \tag{3.9}$$

Assuming (GRH), the case $n = 1$ is known, and our aim is reducing to this case. Notice that our method also shows that the considered density exists. We denote this density by $\mathrm{dens}'_K(G, n; a \bmod d)$.

Let ℓ be a prime divisor of n. The aim is finding a way to replace n with $\frac{n}{\ell}$ (or to conclude directly). We distinguish various cases.

Case (i): If $\ell \mid d$ and $\ell \nmid a$, then we have $\mathrm{dens}'_K(G, n; a \bmod d) = 0$ because ℓ divides $[\mathrm{ord}_{\mathfrak{p}}(G), n]$ and (3.9) cannot hold.

Case (ii): If $\ell \mid d$ and $\ell \mid a$, then the congruence $[\mathrm{ord}_{\mathfrak{p}}(G), n] \equiv a \bmod d$ is equivalent to

$$\big[\,\mathrm{ord}_{\mathfrak{p}}(G^\ell), \frac{n}{\ell}\big] \equiv \frac{a}{\ell} \bmod \frac{d}{\ell}\,,$$

so we have

$$\mathrm{dens}'_K(G, n; a \bmod d) = \mathrm{dens}'_K\left(G^\ell, \frac{n}{\ell}; \frac{a}{\ell} \bmod \frac{d}{\ell}\right).$$

Case (iii): Suppose that $\ell \nmid d$. Let $\tilde{\ell}$ be a multiplicative inverse for ℓ modulo d, and set $v := v_\ell(n)$. If $\ell^v \mid \mathrm{ord}_\mathfrak{p}(G)$, then we have

$$[\mathrm{ord}_\mathfrak{p}(G), n] \equiv a \bmod d \quad \Longleftrightarrow \quad \left[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\right] \equiv a \bmod d\,. \tag{3.10}$$

If $\ell^v \nmid \mathrm{ord}_\mathfrak{p}(G)$, then we have

$$[\mathrm{ord}_\mathfrak{p}(G), n] \equiv a \bmod d \quad \Longleftrightarrow \quad \left[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\right] \equiv a\tilde{\ell} \bmod d\,.$$

The condition $\ell^v \mid \mathrm{ord}_\mathfrak{p}(G)$ amounts to

$$\left[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\right] \equiv 0 \bmod \ell^v$$

and hence (recalling that ℓ and d are coprime) we can easily combine this congruence and the congruence in (3.10) with the Chinese Remainder Theorem. The first subcase thus amounts to

$$\left[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\right] \equiv a\tilde{\ell}^v\ell^v \bmod d\ell^v\,.$$

Similarly, the second subcase amounts to letting $\left[\mathrm{ord}_\mathfrak{p}(G), \frac{n}{\ell}\right]$ be in the difference of congruence classes

$$(a\tilde{\ell} \bmod d) \setminus (a\tilde{\ell}^{v+1}\ell^v \bmod d\ell^v)\,.$$

Notice that the congruence classes for the first and second subcase are distinct. Thus if $\ell \nmid d$ we can explicitly write

$$\begin{aligned}\mathrm{dens}'_K(G, n; a \bmod d) = &\,\mathrm{dens}'_K\left(G, \frac{n}{\ell}; a_0 \bmod d\ell^v\right) + \mathrm{dens}'_K\left(G, \frac{n}{\ell}; a\tilde{\ell} \bmod d\right)\\ &- \mathrm{dens}'_K\left(G, \frac{n}{\ell}; a_0\tilde{\ell} \bmod d\ell^v\right),\end{aligned}$$

where we have set $a_0 := a\tilde{\ell}^v\ell^v \bmod d\ell^v$.

We have thus proven the following result.

Theorem 3.22. *Assume (GRH). Let K be a number field, and let G' be a finitely generated subgroup of $K^\times$ of positive rank. Let $n \geqslant 1$ be the order of the torsion of G', and let G be a torsion-free subgroup of G' such that $G' = G \times \langle\zeta_n\rangle$. Let a and $d \geqslant 2$ be fixed integers. The density of the set of primes $\mathfrak{p}$ of K*

$$\{\mathfrak{p} : \mathrm{ord}_\mathfrak{p}(G') \equiv a \bmod d\}$$

exists and can be expressed as a finite sum of terms of the type

$$\pm\,\mathrm{dens}_K(G^m, a' \bmod d')$$

where m, a', d' are integers and $m \mid n$.

3.5 Examples

In this last section we work out some examples and collect some numerical data to illustrate our results.

Example 3.23. Let $K = \mathbb{Q}(\zeta_3)$ and consider the group $G = \langle 5, 7\rangle \leqslant \mathbb{Q}(\zeta_3)^\times$. We compute the density $\mathrm{dens}_K(G, a \bmod 9)$ for $0 \leqslant a < 9$. Since $\zeta_3 \in K$, we can use [10, Theorem 2] to compute the density of primes $\mathfrak{p}$ of K for which the order of $G \bmod \mathfrak{p}$ is coprime to 3, and we have

$$\mathrm{Dens}_K(G, 3) = \frac{1}{13}\,.$$

Then by Theorem 3.2 we have:

$$\mathrm{dens}_K(G, a \bmod 9) = \frac{1}{78} \qquad \text{for } a \in \{1, 2, 4, 5, 7, 8\}\,.$$

For $a = 3$ or $a = 6$, by [10, Theorem 3] we have

$$\mathrm{Dens}_K(G^3, 3) = \frac{9}{13}$$

and applying Lemma 3.9 we obtain by the equidistribution property

$$\begin{aligned}\mathrm{dens}_K(G, a \bmod 9) &= \mathrm{dens}_K(G^3, 1 \bmod 3) - 3\,\mathrm{dens}_K(G, 1 \bmod 9)\\ &= \frac{9}{2 \cdot 13} - 3 \cdot \frac{1}{78} = \frac{4}{13}\,.\end{aligned}$$

For $a = 0$ we get the complementary density of $\mathrm{Dens}_K(G^3, 3)$ and hence

$$\mathrm{dens}_K(G, 0 \bmod 9) = \frac{4}{13}\,.$$

Example 3.24. Let $K = \mathbb{Q}(\zeta_4)$ and consider the group $G = \langle 3, 5\rangle \leqslant \mathbb{Q}(\zeta_4)^\times$. We compute the density of primes $\mathrm{dens}_K(G, a \bmod 8)$ for $0 \leqslant a < 8$. Since $\zeta_4 \in K$, by [10, Theorem 2] the density of primes $\mathfrak{p}$ of K for which the order of $G \bmod \mathfrak{p}$ is odd is given by

$$\mathrm{Dens}_K(G, 2) = \frac{1}{28}\,.$$

Then by Theorem 3.2 we have:

$$\mathrm{dens}_K(G, a \bmod 8) = \frac{1}{112} \qquad \text{for } a \in \{1, 3, 5, 7\}\,.$$

For $a = 2$ or $a = 6$, by [10, Theorem 3] we have

$$\mathrm{Dens}_K(G^2, 2) = \frac{1}{7}\,,$$

and applying Lemma 3.9 we obtain by the equidistribution property

$$\begin{aligned}\mathrm{dens}_K(G, a \bmod 8) &= \mathrm{dens}_K(G^2, 1 \bmod 4) - 2\,\mathrm{dens}_K(G, 1 \bmod 8)\\ &= \frac{1}{14} - 2 \cdot \frac{1}{112} = \frac{3}{56}\,.\end{aligned}$$

For $a = 4$ we proceed similarly. By [10, Theorem 3] we have

$$\mathrm{Dens}_K(G^4, 2) = \frac{4}{7},$$

and then, by Lemma 3.9, we obtain by the equidistribution property

$$\begin{aligned}\mathrm{dens}_K(G, 4 \bmod 8) &= \mathrm{dens}_K(G^4, 1 \bmod 2) - 2\,\mathrm{dens}_K(G^2, 1 \bmod 4)\\ &= \frac{4}{7} - \frac{1}{7} = \frac{3}{7}.\end{aligned}$$

Finally for $a = 0$ we obtain the complementary density

$$\mathrm{dens}_K(G, 0 \bmod 8) = \frac{3}{7}.$$

Example 3.25. Let $K = \mathbb{Q}(\zeta_{12})$ and consider the group $G = \langle 7, 11\rangle \leqslant \mathbb{Q}(\zeta_{12})^\times$. We compute the density of primes $\mathrm{dens}_K(G, a \bmod 12)$ for $a \in \{1, 5, 7, 11\}$, which are all equal by Theorem 3.4 as $\zeta_{12} \in K$. By [40, Corollary 12] the density of primes $\mathfrak{p}$ of K for which the order of $(G \bmod \mathfrak{p})$ is coprime to 12 can be computed as in the previous examples:

$$\mathrm{Dens}_K(G, 12) = \mathrm{Dens}_K(G, 4) \cdot \mathrm{Dens}_K(G, 3) = \frac{1}{364}.$$

Hence we obtain by the equidistribution

$$\mathrm{dens}_K(G, a \bmod 12) = \frac{1}{1456}.$$

In the following two examples we also compute with SageMath [57] approximated densities to support the validity of the equidistribution property of Corollary 3.3.

Example 3.26. Consider the group $\langle 2\rangle \leqslant \mathbb{Q}^\times$. Focusing on the set of primes up to 10^6, we find with SageMath the following approximated values for the density $\mathrm{dens}_{\mathbb{Q}}(2, a \bmod d)$:

$a \bmod d$	$\mathrm{dens}_{\mathbb{Q}}(2, a \bmod d)$	primes up to 10^6
$4 \bmod 16$	$1/6 \approx 0.1667$	0.1676
$12 \bmod 16$	$1/6 \approx 0.1667$	0.1652
$3 \bmod 9$	$1/8 = 0.125$	0.1236
$6 \bmod 9$	$1/8 = 0.125$	0.1266
$9 \bmod 27$	$1/24 \approx 0.0417$	0.0422
$18 \bmod 27$	$1/24 \approx 0.0417$	0.0411
$3 \bmod 27$	$1/24 \approx 0.0417$	0.0416
$6 \bmod 27$	$1/24 \approx 0.0417$	0.0421
$15 \bmod 27$	$1/24 \approx 0.0417$	0.0420
$21 \bmod 27$	$1/24 \approx 0.0417$	0.0405

For instance, by Corollary 3.3, for $3 \mid a$ and $d = 9$ or $d = 27$ we have

$$\mathrm{dens}_{\mathbb{Q}}(2, a \bmod d) = \frac{1}{[\mathbb{Q}(\zeta_3) : \mathbb{Q}]} \cdot \mathrm{dens}_{\mathbb{Q}(\zeta_3)}(2, a \bmod d),$$

and similarly for $4 \mid a$ and $d = 16$. Thus we can compute these densities by following the same procedure as in the previous examples.

Example 3.27. Let $G = \langle 2, 3\rangle \leqslant \mathbb{Q}^\times$. We compute all the densities $\mathrm{dens}_{\mathbb{Q}}(G, a \bmod d)$ using the methods of the previous examples. Again we study the set of primes up to 10^6 and find with SageMath the following approximated values for the considered densities:

$a \bmod d$	$\mathrm{dens}_{\mathbb{Q}}(G, a \bmod d)$	primes up to 10^6
$4 \bmod 16$	$17/112 \approx 0.1518$	0.1522
$12 \bmod 16$	$17/112 \approx 0.1518$	0.1508
$3 \bmod 9$	$2/13 \approx 0.1538$	0.1538
$6 \bmod 9$	$2/13 \approx 0.1538$	0.1540
$9 \bmod 27$	$2/39 \approx 0.0513$	0.0513
$18 \bmod 27$	$2/39 \approx 0.0513$	0.0513
$3 \bmod 27$	$2/39 \approx 0.0513$	0.0518
$6 \bmod 27$	$2/39 \approx 0.0513$	0.0512
$15 \bmod 27$	$2/39 \approx 0.0513$	0.0513
$21 \bmod 27$	$2/39 \approx 0.0513$	0.0507

Example 3.28. Let $K = \mathbb{Q}(\zeta_3)^\times$, and let G be a finitely generated and torsion-free subgroup of $\mathbb{Q}(\zeta_3)^\times$. Consider the group $G' = G \times \langle \zeta_6 \rangle$. We study the density of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_{\mathfrak{p}}(G') \equiv a \bmod 10$, as considered in Section 3.4. For $a = 1, 3, 5, 7, 9$, we have $\mathrm{dens}'_K(G, 6; a \bmod 10) = 0$. For $a = 4$ we have

$$\begin{aligned}
&\mathrm{dens}'_K(G, 6; 4 \bmod 10)\\
&= \mathrm{dens}'_K(G, 2; 24 \bmod 30) + \mathrm{dens}'_K(G, 2; 8 \bmod 10) - \mathrm{dens}'_K(G, 2; 18 \bmod 30)\\
&= \mathrm{dens}_K(G^2, 12 \bmod 15) + \mathrm{dens}_K(G^2, 4 \bmod 5) - \mathrm{dens}_K(G^2, 9 \bmod 15)\,,
\end{aligned}$$

and also

$$\begin{aligned}
&\mathrm{dens}'_K(G, 6; 4 \bmod 10) = \mathrm{dens}'_K(G^2, 3; 2 \bmod 5)\\
&= \mathrm{dens}_K(G^2, 12 \bmod 15) + \mathrm{dens}_K(G^2, 4 \bmod 5) - \mathrm{dens}_K(G^2, 9 \bmod 15)\,,
\end{aligned}$$

where the difference in the two calculations consists only in whether we consider the prime 2 or the prime 3 first for the method described in Section 3.4. For $a = 2, 6, 8$ we can make a similar computation. Finally, for $a = 0$ we have

$$\mathrm{dens}'_K(G, 6; 0 \bmod 10) = \mathrm{dens}_K(G, 0 \bmod 5)\,,$$

as 2 always divides $\mathrm{ord}_{\mathfrak{p}}(G')$, and $\mathrm{ord}_{\mathfrak{p}}(G') \equiv 0 \bmod 5$ if and only if $\mathrm{ord}_{\mathfrak{p}}(G) \equiv 0 \bmod 5$.

Chapter 4

On the distribution of the order and index for the reductions of algebraic numbers

Let K be a number field, and let $\alpha_1, \dots, \alpha_r$ be algebraic numbers in 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, and they are published in [55], except for Section 4.7 which contains some new results.

4.1 Main results and overview

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, recalling the notation from Section 1.1, we will prove under GRH the existence of the density of primes $\mathfrak{p}$ satisfying $\mathrm{ord}_\mathfrak{p}(\alpha_i) \equiv a_i \bmod d_i$ for each i, where a_i, d_i are some fixed integers. In Theorem 4.1 we give an asymptotic formula for the number of such primes. We also study the density of primes satisfying conditions on the index. Write $\mathrm{ind}_\mathfrak{p}(\alpha_i)$ for the index of the subgroup generated by $(\alpha_i \bmod \mathfrak{p})$ in $k_\mathfrak{p}^\times$. Notice that $\mathrm{ind}_\mathfrak{p}(\alpha_i) = (\mathrm{N}\,\mathfrak{p} - 1)/\,\mathrm{ord}_\mathfrak{p}(\alpha_i)$. We prove the existence of the density of primes $\mathfrak{p}$ such that $\mathrm{ind}_\mathfrak{p}(\alpha_i) = t_i$ for each i, where the t_i's are positive integers, and more generally such that $\mathrm{ind}_\mathfrak{p}(\alpha_i)$ 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 [59], which concerns the case of rank 1. Moreover, in [43] 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 [44] they have investigated properties of the density of this set (see Chapter 3). Notice that problems of this kind have been studied in various papers by Chinen and

Murata, and by Moree, see for instance [7, 29], and that they are related to Artin's Conjecture on primitive roots, see the survey [31] by Moree.

4.1.1 Notation

As mentioned above, we make use of the notation from Section 1.1. 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 $\mathfrak{p}$.

4.1.2 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 [59, 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 4.1. *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

$$\mathcal{P}(x) = \frac{x}{\log x} \sum_T \sum_N \frac{(\prod_i \mu(n_i)) c(N,T)}{[F_{w,N,T} : K]} + O\left(\frac{x}{(\log x)^{1+\frac{1}{r+1}}}\right), \tag{4.1}$$

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* $(1+a_i t_i, d_i) = 1$ *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.*

Taking $F = K$ in Theorem 4.1 yields Theorem 1.2 in the Introduction.

Remark 4.2. The multiple series involved in the asymptotic formula (4.1) converges. This statement is a consequence of the results of Section 4.2: more precisely, the convergence follows by Proposition 4.9 and Theorem 4.5, and we prove this property in Corollary 4.12. Notice that the same remark applies to the series in the formulas (4.3) and (4.5) below (see also Corollary 4.11).

Theorem 4.3. *Let* F/K *be a finite Galois extension, and let* C *be a union of conjugacy classes of* $\mathrm{Gal}(F/K)$*. Let* $T = (t_1,\dots,t_r)$ *be an* r*-tuple of positive integers. Define the following set of primes of* K*:*

$$\mathcal{R} := \left\{\mathfrak{p} : \mathrm{ind}_{\mathfrak{p}}(\alpha_i) = t_i\ \forall i,\ \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C\right\} . \tag{4.2}$$

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

$$\mathcal{R}(x) = \frac{x}{\log x}\sum_N \frac{(\prod_i \mu(n_i))c'(N,T)}{[F_{N,T}:K]} + O\left(\frac{x}{\log^2 x} + \sum_{i=1}^r \frac{x\log\log x}{\varphi(t_i)\log^2 x}\right), \tag{4.3}$$

where

$$c'(N,T) = \left|\left\{\sigma \in \mathrm{Gal}(F_{N,T}/K) : \sigma|_{K_{N,T}} = \mathrm{id},\ \sigma|_F \in C\right\}\right| . \tag{4.4}$$

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

Notice that applying Theorem 4.3 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. This is stated in Theorem 1.3 and developed further in Proposition 4.21.

Moreover, in Theorem 4.22, for $F = K$, we reduce the natural density in (4.3) to a closed formula consisting of a rational multiple of a constant depending only on r.

Theorem 4.4. *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* S_i *be some nonempty sets of positive integers. Define the following set of primes of* K*:*

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

Assuming (GRH), we have

$$\mathcal{S}(x) = \frac{x}{\log x}\sum_{\substack{T\\ t_i\in S_i}}\sum_N \frac{(\prod_i \mu(n_i))c'(N,T)}{[F_{N,T}:K]} + O\left(\frac{x}{(\log x)^{1+\frac{1}{r+1}}}\right) , \tag{4.5}$$

where

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

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. A small generalization of Theorem 4.4 is provided by Corollary 4.24.

Notice that if we take $r = 1$ in Theorems 4.1 and 4.3, then we obtain the same formulas as in [59, Theorem 1, Proposition 1], respectively.

4.1.3 Overview

In order to generalize Ziegler's proofs [59] to obtain Theorems 4.1, 4.3 and 4.4, some crucial results are needed. The first one is Theorem 4.5 which is an estimate for a multiple series involving Euler's totient function φ. Section 4.2 is devoted to the proof of this theorem. The other two results concern Kummer extensions of number fields and are proven in Section 4.3. More precisely, Proposition 4.9 states that the failure of maximality of their degree is bounded in a strong way, whereas Proposition 4.13 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 4.1.2.

In Section 4.4 we prove Theorem 4.3, and then we use this result in Section 4.5 to set more general conditions on the index and achieve Theorem 4.4. In Section 4.6 we prove Theorem 4.1 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 us to apply the previous results.

Finally, in Section 4.7 we consider the multidimensional variation of Artin's conjecture obtained thanks to Theorem 4.3 and, making use of the results of Chapter 2, we reduce the corresponding natural density to a rational multiple of a certain constant.

4.2 On Euler's totient function

In this section we estimate some expressions involving Euler's totient function. We keep the notation introduced in Section 4.1.1. 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:

$$\tau(n) = O\left(n^{\varepsilon}\right) \quad \forall \varepsilon > 0\,, \tag{4.6}$$

(see [25, Formula (2.20)]);

$$\frac{n}{\varphi(n)} = O\left(n^{\varepsilon}\right) \quad \forall \varepsilon > 0\,, \tag{4.7}$$

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);

$$\sum_{n \leqslant x} \frac{n}{\varphi(n)} = O\left(x\right)\,, \tag{4.8}$$

(see for instance [25, Formula (2.32)]).

Our goal is to prove a multidimensional variant of the estimate $\sum_{n>x} \frac{1}{\varphi(n)n} = O\left(\frac{1}{x}\right)$ (see for instance [59, Lemma 7]), namely

Theorem 4.5 (Pollack)**.** *We have*

$$\sum_{\substack{N \\ n_1 > x}} \frac{1}{\varphi([n_1, n_2, \dots, n_r]) n_1 n_2 \cdots n_r} = O\left(\frac{1}{x}\right)\,. \tag{4.9}$$

Lemma 4.6. *Let z be a positive integer, then for every $\varepsilon > 0$ we have*

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

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 (4.8) 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 (4.6) and (4.7) 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 4.7. *We have*

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

Proof. We may assume $r \geqslant 2$, the case $r = 1$ being just (4.8). 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

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

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

$$\sum_{\substack{N\\ n_1\leqslant x}}\frac{(n_1,[n_2,\dots,n_r])}{[n_2,\dots,n_r]n_2\cdots n_r}\prod_{i=1}^{r}\prod_{p|n_i}\left(1-\frac{1}{p}\right)^{-1}$$
$$= \sum_{n_2,\dots,n_r\geqslant 1}\frac{1}{[n_2,\dots,n_r]n_2\cdots n_r}\prod_{i=2}^{r}\frac{n_i}{\varphi(n_i)}\cdot\sum_{n_1\leqslant x}(n_1,[n_2,\dots,n_r])\frac{n_1}{\varphi(n_1)}.$$

Taking $n = n_1$, $z = [n_2,\dots,n_r]$ and $\varepsilon = 1/2$, Lemma 4.6 says that the inner sum is estimated by $O\left(x[n_2,\dots,n_r]^{1/2}\right)$. Applying the obvious inequalities

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

we can then estimate the series by

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

where in the first equality we used the estimates $\frac{n_i}{\varphi(n_i)} = O(n_i^{1/4r})$ in view of (4.7), 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 4.5.

Proof of Theorem 4.5. We may assume $r \geqslant 2$. We decompose the series considered in (4.9) into the sums over n_1 lying in dyadic intervals, i.e. we express it as

$$\sum_{j \geqslant 0} \sum_{\substack{N \\ 2^j x < n_1 \leqslant 2^{j+1} x}} \frac{1}{\varphi([n_1, \dots, n_r]) n_1 \cdots n_r} . \tag{4.10}$$

We now estimate each inner series on the multi-indices N in (4.10). For $j \geqslant 0$, each of them equals

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

where the estimate is due to Lemma 4.7. Finally, we conclude by summing the obtained error terms over j, so that (4.10) equals $O\left(1/x\right)$. □

The following result is an immediate consequence of Theorem 4.5.

Corollary 4.8. *Let $x_1, \dots, x_r \geqslant 1$. Then we have*

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

Proof. Up to swapping the variables, we may suppose that $x_1 = \max_i(x_i)$ and apply Theorem 4.5. □

4.3 Preliminaries from Kummer theory

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.

4.3.1 Bounded failure of maximality for Kummer degrees

In [43, 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 4.9. *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*

$$\frac{\prod_{i=1}^r t_i}{\left[K\left(\zeta_n, \alpha_1^{1/t_1}, \dots, \alpha_r^{1/t_r}\right) : K(\zeta_n)\right]} \mid B\,. \tag{4.11}$$

Proof. Let $n, t_1, \dots, t_r$ be arbitrary with $t := [t_1, \dots, t_r] \mid n$. Then by [43, Theorem 3.1] there is $B \geqslant 1$ (depending only on K and the α_i's) such that

$$\frac{t^r}{\left[K\left(\zeta_n, \alpha_1^{1/t}, \dots, \alpha_r^{1/t}\right) : K(\zeta_n)\right]} \mid B\,. \tag{4.12}$$

We show that this bound B satisfies also (4.11). We have

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

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 (4.11) is a divisor of the ratio in (4.12), and hence it divides B. □

Proposition 4.9 is also a consequence of Theorem 2.2 ([47, Theorem 5.4]), which provides a stronger statement. The bound B considered in the proof is not optimal in general, but it is suitable for our purposes. It can be computed thanks to the results of Chapter 2 or [43, 47].

Corollary 4.10. *For all positive integers $n, t_1, \dots, t_r$, where n is a common multiple of the t_i's, we have*

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

where $B \geqslant 1$ is the integer from Proposition 4.9 associated to K and the α_i's.

Proof. By (4.11) 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 4.1.1 and Theorem 4.1, where N, T are r-tuples of positive integers and $w = w(T) := [d_1 t_1, \dots, d_r t_r]$ for some positive integers $d_1, \dots, d_r$.

Corollary 4.11. *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 4.10 we can bound

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

Then the convergence follows by Theorem 4.5. □

Corollary 4.12. *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 $[n_1 t_1, \dots, n_r t_r]$ is divisible by $[n_1, t_1, \dots, n_r, t_r]$, applying Corollary 4.10 we can bound

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

The convergence follows again by Theorem 4.5. □

4.3.2 Estimates for the discriminant

In the following we prove an estimate for the discriminant of a cyclotomic-Kummer extension of the type $K(\zeta_n, \alpha_1^{1/t_1}, \dots, \alpha_r^{1/t_r})$. In fact, we give a variant of [43, 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 [34, Ch. III, Corollary 2.10]):

$$d_{K''/K} = \mathrm{N}_{K'/K}(d_{K''/K'}) \cdot d_{K'/K}^{[K'':K']}\,. \tag{4.13}$$

Proposition 4.13. *Let K be a number field, and let $\gamma_1, \dots, \gamma_r \in K^\times$ be algebraic numbers which are not roots of unity. Let $t_1, \dots, t_r$ be positive integers and let n be a common multiple of the t_i's. Setting $F := K(\zeta_n, \gamma_1^{1/t_1}, \dots, \gamma_r^{1/t_r})$, 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

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

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 [43, 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

$$d_{F/K} \mid (d_{K(\zeta_n)/K})^t \cdot \prod_{i=1}^{r} (d_{L_i/K})^{\varphi(n)t/t_i} . \tag{4.14}$$

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 [43, Theorem 4.2], formulas (4.5) and (4.6), respectively). Combining these two divisibilities with (4.14) we obtain

$$d_{F/K} \mid \left(n^{\varphi(n)t} \cdot \prod_{i=1}^{r} \left((\alpha_i\beta_i)^{2t_i} t_i^{t_i} \right)^{\varphi(n)t/t_i} \right) \mathcal{O}_K = \left((nt)^{\varphi(n)t} \cdot A^{2\varphi(n)t} \right) \mathcal{O}_K , \tag{4.15}$$

where we set $A := \prod_{i=1}^{r} \alpha_i\beta_i$. In view of the identity (4.13), 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 (4.15) 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

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

4.4 The asymptotic formula for the index

The aim of this section is proving Theorem 4.3 with the method of [59, Section 3]. We keep the notation of the introduction and, in particular, of Theorem 4.3. 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 4.4-4.6 we may assume $r \geqslant 2$, as the case $r = 1$ was proven in [59]. 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 [59, 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 4.14. The defining conditions of the set $\mathcal{R}$ (see (4.2)), 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:

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

If $\mathfrak{p}$ is of degree 1, then by [59, Lemma 2] the condition $n_i t_i \mid \operatorname{ind}_{\mathfrak{p}}(\alpha_i)$ holds if and only if $\mathfrak{p}$ splits completely in $K(\zeta_{n_i t_i}, \alpha_i^{1/n_i t_i})$. 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

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

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

(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 $\operatorname{ind}_{\mathfrak{p}}(\alpha_i) \mid \mathrm{N}\,\mathfrak{p} - 1 < \lfloor x \rfloor$, 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 $t_i q \nmid \operatorname{ind}_{\mathfrak{p}}(\alpha_i)$ for all i and for all prime numbers $q < \xi$ but with $t_i q \mid \operatorname{ind}_{\mathfrak{p}}(\alpha_i)$ 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

$$\mathcal{R}(x) = \mathcal{M}_\xi(x) + O\big(\mathcal{M}_{\xi,\eta}(x)\big). \tag{4.16}$$

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

Lemma 4.15. *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 (4.4)*.*

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 4.14 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 (4.4)).

Since we are assuming (GRH), by the effective Chebotarev density theorem (see for instance [59, 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

$$\mathrm{Li}(x)\sum_{\substack{N\\ n_i\in E}}\frac{(\prod_i \mu(n_i))c'(N,T)}{[F_{N,T}:K]} + O\left(\sum_{\substack{N\\ n_i\in E}}\frac{\sqrt{x}\log\left(x^{[F_{N,T}:\mathbb{Q}]}\cdot\left|d_{F_{N,T}}\right|\right)}{[F_{N,T}:K]}\right). \tag{4.17}$$

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 (4.17) includes $O\left(\sqrt{x}/\log x\right)$.

As for the second part of the O-term, applying Corollary 4.10 first and then Proposition 4.13, we obtain

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

By assumption we have $\log t_i = O(\log x)$ 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 [12, 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 (4.17) 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

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

Since $c'(N,T) \leqslant [F : K]$, applying Corollary 4.10 and Theorem 4.5, we can estimate each series by $O(1/\xi) = O(1/\log x)$. Using that $\mathrm{Li}(x) = O(x/\log x)$ 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 main term of $\mathcal{M}_\xi(x)$ as the multiple series converges by Corollary 4.11. □

Let us now focus on the error term of (4.16).

Lemma 4.16. *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 [59, page 73]) which are estimated in [59, Lemmas 9, 10, 11]. Notice that our different value for ξ does not change the proof of [59, Lemma 11], whereas [59, Lemmas 9, 10] do not depend on ξ.

Moreover, it is straightforward to see that these lemmas hold also for algebraic numbers (see also [43, Proof of Proposition 5.1]). In fact, in [59, 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 4.3. The statement follows by invoking formula (4.16) and applying Lemmas 4.15 and 4.16. □

4.5 Putting conditions on the index

In this section we prove Theorem 4.4, keeping the notation of the introduction. The following result is a variant of [59, Lemma 13].

Lemma 4.17. *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 [59, 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 4.4. 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 (4.2) 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

$$\sum_{\substack{T \\ t_i \in S_i}} \mathcal{R}_T(x) - \sum_{\substack{T \\ t_i \leqslant y,\, t_i \in S_i}} \mathcal{R}_T(x) \leqslant \sum_{\substack{T \\ t_1 > y}} \mathcal{R}_T(x) + \ldots + \sum_{\substack{T \\ t_r > y}} \mathcal{R}_T(x). \tag{4.18}$$

Applying Lemma 4.17, 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

$$\mathcal{S}(x) = \sum_{\substack{T \\ t_i \leqslant y,\, t_i \in S_i}} \mathcal{R}_T(x) + O\left(\frac{x}{(\log x)^{1+\rho}}\right). \tag{4.19}$$

We now replace the asymptotic (4.3) for the functions $\mathcal{R}_T(x)$ in (4.19), as $x > y^3$. Let us first focus on the main term that we obtain, namely

$$\frac{x}{\log x} \sum_{\substack{T \\ t_i \leqslant y,\, t_i \in S_i}} \sum_{N} \frac{(\prod_i \mu(n_i)) c'(N,T)}{[F_{N,T} : K]}. \tag{4.20}$$

Call D_T the (inner) multiple series on the multi-indices N appearing in (4.20) and notice that $D_T \geqslant 0$. Similarly to (4.18), we have

$$\sum_{\substack{T \\ t_i \in S_i}} D_T - \sum_{\substack{T \\ t_i \leqslant y,\, t_i \in S_i}} D_T \leqslant \sum_{\substack{T \\ t_1 > y}} D_T + \ldots + \sum_{\substack{T \\ t_r > y}} D_T. \tag{4.21}$$

Since $[n_1t_1, \dots, t_rn_r]$ is a multiple of $[t_1, n_1, \dots, t_r, n_r]$, applying Corollary 4.10 we have

$$\frac{1}{[F_{N,T} : F]} \leqslant \frac{B[F : \mathbb{Q}]}{\varphi([t_1, n_1, \dots, t_r, n_r])t_1n_1 \cdots t_rn_r},$$

and hence by Theorem 4.5 each series on the right-hand side of (4.21), 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 (4.19). The first part of the O-term of (4.3) 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 $2 - \rho r > 1$. Recall the formula $\sum_{k<y} 1/\varphi(k) = O(\log y)$ (see for instance [59, Lemma 8]). Then, for each $j \in \{1, \dots, r\}$, the second part of the O-term of (4.3) 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. □

4.6 The asymptotic formula for the order

In this section we obtain an asymptotic formula for the function $\mathcal{P}(x)$ of Theorem 4.1 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 $\mathrm{ord}_{\mathfrak{p}}(\alpha_i) \cdot \mathrm{ind}_{\mathfrak{p}}(\alpha_i) = \mathrm{N}\,\mathfrak{p} - 1$, the condition $\mathrm{ord}_{\mathfrak{p}}(\alpha_i) \equiv a_i \bmod d_i$ is equivalent to $\mathrm{ind}_{\mathfrak{p}}(\alpha_i) = t_i$ and $p \equiv 1 + a_it_i \bmod d_it_i$. We define the sets of primes of K satisfying these conditions by setting

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

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

$$\mathcal{P}(x) = \sum_T \mathcal{V}_T(x) + O\left(\frac{\sqrt{x}}{\log x}\right). \tag{4.22}$$

Given T such that $1 + a_i t_i$ 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 $1 + a_i t_i$ 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 (4.22) to the multi-indices T with $(1 + a_i t_i, d_i) = 1$ for every i.

Recall the notation $w = w(T) := [d_1 t_1, \dots, d_r t_r]$.

Lemma 4.18. *Fix T such that $(1 + a_i t_i, d_i) = 1$ for all i. Then the set $\mathcal{V}_T$ can be written as*

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

where

$$C_w := \left\{ \sigma \in \mathrm{Gal}(F(\zeta_w)/K) : \forall i \; \sigma(\zeta_{d_i t_i}) = \zeta_{d_i t_i}^{1+a_i t_i}, \, \sigma|_F \in C \right\}.$$

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

$$\mathcal{V}_T(x) = \frac{x}{\log x} \sum_N \frac{(\prod_i \mu(n_i)) c(N,T)}{[F_{w,N,T} : K]} + O\left(\frac{x}{\log^2 x} + \sum_{i=1}^r \frac{x \log\log x}{\varphi(t_i) \log^2 x}\right), \tag{4.23}$$

where $F_{w,N,T}$ and $c(N,T)$ are as in Theorem 4.1. 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 $1 + a_i t_i$ and d_i are coprime for all i, if $\mathfrak{p} \in \mathcal{V}_T$ and $\mathrm{N}\,\mathfrak{p} = p$, then $p \nmid d_i t_i$ for all i and we have the equivalence

$$p \equiv 1 + a_i t_i \bmod d_i t_i \quad \Longleftrightarrow \quad \left(\frac{p}{\mathbb{Q}(\zeta_{d_i t_i})/\mathbb{Q}}\right) \text{ satisfies } \zeta_{d_i t_i} \mapsto \zeta_{d_i t_i}^{1+a_i t_i}. \tag{4.24}$$

The first part of the statement is now clear, because the condition on the right of (4.24) holds for all i if and only if $(\mathfrak{p}, K(\zeta_w)/K)$ acts as the exponentiation by $1 + a_i t_i$ on $\zeta_{d_i t_i}$ for all i.

In order to get an asymptotic formula for $\mathcal{V}_T(x)$, it is sufficient to apply Theorem 4.3 to the field extension $F(\zeta_w)/K$ and C_w. Notice that in this application of Theorem 4.3 the number $c'(N,T)$ coincides with the number $c(N,T)$ of Theorem 4.1. 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 $1 + a_i t_i$.

As for the constant implied by the O-term, one can check easily that applying Theorem 4.3 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 4.15 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 4.13. □

We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1. Let $\mathcal{V}_T$ be as above. We follow the proof of Theorem 4.4 closely. Take $0 < \rho \leqslant 1/2$ and set $y := (\log x)^\rho$. Consider formula (4.22). 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 (4.18) and then applying Lemma 4.17 (we may take S_i to be the set of all positive integers for all i). We obtain

$$\mathcal{P}(x) = \sum_{\substack{T \\ t_i \leqslant y}} \mathcal{V}_T(x) + O\left(\frac{x}{(\log x)^{1+\rho}}\right), \tag{4.25}$$

where we may restrict the indices t_i to those satisfying $(1 + a_i t_i, d_i) = 1$ 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 4.18 we may replace in (4.25) $\mathcal{V}_T(x)$ by the asymptotic (4.23). 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 (4.21) (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 4.4, i.e. by applying Theorem 4.5 (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 [59, Theorem 1].

Remark 4.19. 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 $[t_1, \ldots, t_r] \mid y$ 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 $v = v(N,T) := [n_1 t_1, \ldots, n_r t_r]$, 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 $i, j \in \{1, \ldots, r\}$ (because $y \equiv a_i t_i \bmod d_i t_i$).

Remark 4.20. Let K be a number field, and let $G_1, \ldots, G_r$ be finitely generated subgroups of $K^\times$ of finite positive rank $s_1, \ldots, s_r$, 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 4.1, 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 [59] to finite rank in [43], so that one could use the latter work to achieve directly all the steps of the present chapter 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 4.3 and 4.4 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.

4.7 A multidimensional variation of Artin's conjecture and further results

In this section we provide some additional results which fit with the topic of the article [55] and will be published in an oncoming work.

Let K be a number field, and let $\alpha_1, \dots, \alpha_r$ be algebraic numbers in $K^\times$ which generate a multiplicative subgroup of $K^\times$ of positive rank r. We investigate the primes $\mathfrak{p}$ of K for which α_i is a primitive or near-primitive root modulo $\mathfrak{p}$ (and $v_\mathfrak{p}(\alpha_i) = 0$) for all $1 \leqslant i \leqslant r$, in other words for which $\mathrm{ind}_\mathfrak{p}(\alpha_i)$ is 1 or a given integer for all i. We also consider the case of tuple of indices $\mathrm{ind}_\mathfrak{p}(\alpha_i)$ lying in a given set, generalizing Theorem 4.4, and we provide an application of this result.

As we mentioned before, the case $\mathrm{ind}_\mathfrak{p}(\alpha_i) = 1$ for all i is a special case of Theorem 4.3, and Theorem 1.3 provides an asymptotic formula for the number of such primes. Our goal is providing a closed formula for the natural density of this set of primes, in both cases. In the following, ℓ always denotes a prime.

Proposition 4.21. *There is an integer z, which depends only on K and the α_i's, such that the series in the formula* (1.3)*, namely*

$$\sum_N \frac{\prod_i \mu(n_i)}{[K(\zeta_{[n_1,\dots,n_r]}, \alpha_1^{1/n_1}, \dots, \alpha_r^{1/n_r}) : K]} \tag{4.26}$$

(assuming (GRH), this is the density of primes $\mathfrak{p}$ of K such that $\mathrm{ind}_\mathfrak{p}(\alpha_i) = 1$ for all i), is given by

$$\prod_{\ell \nmid z} \left(1 + \frac{1}{\ell - 1}\left(\left(1 - \frac{1}{\ell}\right)^r - 1\right)\right) \cdot \sum_{g \mid z} \sum_{\substack{h_1,\dots,h_r \mid g \\ [h_1,\dots,h_r]=g}} \frac{\prod_{i=1}^r \mu(h_i)}{[K(\zeta_g, \alpha_1^{1/h_1}, \dots, \alpha_r^{1/h_r}) : K]}. \tag{4.27}$$

Setting

$$A_r := \prod_\ell \left(1 + \frac{1}{\ell - 1}\left(\left(1 - \frac{1}{\ell}\right)^r - 1\right)\right) \tag{4.28}$$

for $r \geqslant 1$, the densities (4.27) are given by rational multiples of A_r. The constants A_r can be seen as multidimensional generalizations of Artin's constant (for $r = 1$ we have $A_1 = \prod_\ell \left(1 - \frac{1}{\ell(\ell-1)}\right)$.

Proof of Proposition 4.21. Let us denote by δ the series (4.26). By Theorem 2.1 there is an integer z, which depends only on K and on the α_i's, such that for all $m, n_1, \dots, n_r$ with $[n_1, \dots, n_r] \mid m$ we have

$$[K(\zeta_m, \alpha_1^{1/n_1}, \dots, \alpha_r^{1/n_r}) : K] = \frac{\varphi(m)}{\varphi((m,z))} \prod_i \frac{n_i}{(n_i, z)} \cdot [K(\zeta_{(m,z)}, \alpha_1^{1/(n_1,z)}, \dots, \alpha_r^{1/(n_r,z)}) : K]\,.$$

Therefore, we obtain

$$\begin{aligned}
\delta &= \sum_{\substack{g \mid z \\ h_i \mid g \forall i}} \frac{1}{[K(\zeta_g, \alpha_1^{1/h_1}, \dots, \alpha_r^{1/h_r}) : K]} \sum_{\substack{N \\ ([n_i],z)=g \\ (n_i,z)=h_i \forall i}} \frac{\prod_i \mu(n_i)}{\varphi([n_1,\dots,n_r])/\varphi(g) \cdot \prod_i n_i/h_i} \\
&= \prod_{\ell \nmid z} p_\ell \cdot \sum_{\substack{g \mid z \\ h_i \mid g \forall i}} \frac{1}{[K(\zeta_g, \alpha_1^{1/h_1}, \dots, \alpha_r^{1/h_r}) : K]} \sum_{\substack{N,\ n_i \mid z \\ ([n_i],z)=g \\ (n_i,z)=h_i \forall i}} \frac{\prod_i \mu(n_i)}{\varphi([n_1,\dots,n_r])/\varphi(g) \cdot \prod_i n_i/h_i},
\end{aligned} \tag{4.29}$$

where, for $\ell \nmid z$, we have

$$p_\ell = \sum_{s_1,\dots,s_r\in\{0,1\}} \frac{\prod_i \mu(\ell^{s_i})}{\varphi(\ell^{\max_i(s_i)})\ell^{\sum_i s_i}}$$
$$= 1 + \frac{1}{\ell-1}\sum_{j=1}^{r} C_j^r \frac{(-1)^j}{\ell^j} = 1 + \frac{1}{\ell-1}\left(\left(1-\frac{1}{\ell}\right)^r - 1\right),$$

with C_n^m, for m, n, the binomial coefficient $\frac{m!}{n!(m-n)!}$.

Let us focus on the inner sum in (4.29). We may restrict the indices n_i to the squarefree divisors of z, so that g and the h_i's must also be squarefree. The conditions on the n_i's become $[n_1,\dots,n_r] = g$ and $n_i = h_i$ for all i. Hence the considered sum reduces either to $\prod_i \mu(h_i)$ if $g = [h_1,\dots,h_r]$, or to 0 otherwise. □

More generally, for near-primitive roots we have the following.

Theorem 4.22. *Let $T = (t_1,\dots,t_r)$ be an r-tuple of positive integers, and set $t := [t_1,\dots,t_r]$. Consider the series*

$$D_T := \sum_N \frac{\prod_i \mu(n_i)}{[K_{N,T} : K]},$$

which is, assuming (GRH), the density of primes $\mathfrak{p}$ of K such that $\mathrm{ind}_{\mathfrak{p}}(\alpha_i) = t_i$ for all i by Theorem 4.3. Then there is an integer z, which depends only on K and the α_i's, such that

$$D_T = \frac{1}{\varphi(t)\prod_i t_i} \cdot \prod_{\ell\nmid zt}\left(1+\frac{1}{\ell-1}\left(\left(1-\frac{1}{\ell}\right)^r - 1\right)\right) \cdot \prod_{\substack{\ell\nmid z\\ \ell\mid t}}\left(1-\frac{1}{\ell}\right)^{r-k_1+1}\left(1+\frac{1}{\ell}\left(1-\frac{1}{\ell}\right)^{k_1-1}\right)\cdot$$
$$\cdot \sum_{\substack{g\mid z\\ (t,z)\mid g\mid t\,\mathrm{rad}(z)}} \sum_{\substack{h_1,\dots,h_r\mid g\\ (t_i,z)\mid h_i\mid t_i\,\mathrm{rad}(z)\forall i\\ [h_1,\dots,h_r]=g}} \frac{\varphi(g)\big(\prod_{i=1}^r h_i\big)p(g,h_1,\dots,h_r)}{[K(\zeta_g,\alpha_1^{1/h_1},\dots,\alpha_r^{1/h_r}) : K]}, \tag{4.30}$$

where for $\ell \mid t$ we set $k_1 := \sharp\{i : v_\ell(t/t_i) = 0\}$, and we have

$$p(g,h_1,\dots,h_r) = \prod_{\substack{\ell\mid g\\ v_\ell(t)\geqslant v_\ell(z)}} \left(1+\frac{1}{\ell}\left(1-\frac{1}{\ell}\right)^{k_1-1}\right)\left(1-\frac{1}{\ell}\right)^{k_2+1}\cdot\prod_{\ell\mid g}\left(\frac{-1}{\ell}\right)^{k_3}\cdot\prod_{\substack{\ell\mid g\\ \ell\nmid t}}\frac{1}{\ell-1}\cdot \prod_{\substack{\ell\mid(g,t)\\ v_\ell(g/t)=1\\ v_\ell(t)<v_\ell(z)}}\frac{1}{\ell},$$

with

$$k_2 := \sharp\{i : v_\ell(z) \leqslant v_\ell(t_i) < v_\ell(t)\}, \qquad k_3 := \sharp\{i : v_\ell(t_i)+1 = v_\ell(h_i)\}.$$

Notice that the integers k_1, k_2, k_3 depend on ℓ.

The densities D_T in (4.30) are given by the constants A_r defined in (4.28) times rational numbers (depending on T, K and the α_i's).

Proof of Theorem 4.22. Recall that

$$D_T = \sum_N \frac{\prod_i \mu(n_i)}{[K(\zeta_{[n_1t_1,\dots,n_rt_r]}, \alpha_1^{1/n_1t_1},\dots,\alpha_r^{1/n_rt_r}) : K]}.$$

By Theorem 2.1 there is an integer z, which depends only on K and on the α_i's, such that we may write

$$D_T = \frac{1}{\prod_i t_i} \sum_{\substack{g \mid z \\ h_i \mid g \forall i}} \frac{\varphi(g) \prod_i h_i}{[K(\zeta_g, \alpha_1^{1/h_1}, \dots, \alpha_r^{1/h_r}) : K]} \sum_{\substack{N \\ ([n_i t_i], z) = g \\ (n_i t_i, z) = h_i \forall i}} \frac{\prod_i \mu(n_i)}{\varphi([n_1 t_1, \dots, n_r t_r]) \cdot \prod_i n_i}.$$

Notice that we may restrict the indices g to those such that $[h_1, \dots, h_r] = g$, and also satisfying $(t, z) \mid g$ and $g \mid t \operatorname{rad}(z)$, as well as $(t_i, z) \mid h_i$ and $h_i \mid t_i \operatorname{rad}(z)$ for all i. Therefore, writing $z_\ell := v_\ell(z)$ for a prime ℓ, and similarly for g_ℓ, t_ℓ, $h_{i,\ell}$, $t_{i,\ell}$ for all i, we may suppose

$$\begin{gathered} \min(t_\ell, z_\ell) \leqslant g_\ell \leqslant \min(t_\ell + 1, z_\ell) \\ \min(t_{i,\ell}, z_\ell) \leqslant h_{i,\ell} \leqslant \min(t_{i,\ell} + 1, g_\ell) \text{ for all } i. \end{gathered} \tag{4.31}$$

We may express the inner series on N in D_T as $\prod_\ell p_\ell$ where

$$p_\ell = p_\ell(g, h_1, \dots, h_r) = \sum_{\substack{S \in \{0,1\}^r \\ \min(\max_i(s_i + t_{i,\ell}), z_\ell) = g_\ell \\ \min(s_i + t_{i,\ell}, z_\ell) = h_{i,\ell} \ \forall i}} \frac{1}{\varphi(\ell^{\max_i(s_i + t_{i,\ell})})} \Big(\frac{-1}{\ell}\Big)^{\sum_i s_i},$$

with S denoting the tuple $(s_1, \dots, s_r) \in \{0,1\}^r$. We will then take

$$p(g, h_1, \dots, h_r) = \prod_{\ell \mid z} \varphi(\ell^{t_\ell}) p_\ell.$$

Given a prime ℓ, in the following we denote $S_1 = \{i : t_{i,\ell} = t_\ell\}$ and $k_1 = |S_1|$. Notice that $t_\ell = \max_i(t_{i,\ell})$.

Case 1: $\ell \nmid z$. The sum p_ℓ is independent of g and the h_i's, and we have

$$p_\ell = \sum_{S \in \{0,1\}^r} \frac{1}{\varphi(\ell^{\max_i(s_i + t_{i,\ell})})} \Big(\frac{-1}{\ell}\Big)^{\sum_i s_i}.$$

Case 1.1: $t_{i,\ell} = 0$ for all i. This case is analogous to the computation in the proof of Proposition 4.21, hence we obtain

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

Case 1.2: $t_{i,\ell} \neq 0$ for some i. We have

$$\begin{aligned} p_\ell &= \frac{1}{\varphi(\ell^{t_\ell})} \Bigg(\sum_{\substack{S \in \{0,1\}^r \\ s_i = 0 \forall i \in S_1}} \Big(\frac{-1}{\ell}\Big)^{\sum_i s_i} + \frac{1}{\ell} \sum_{\substack{S \in \{0,1\}^r \\ \exists i \in S_1 : s_i \neq 0}} \Big(\frac{-1}{\ell}\Big)^{\sum_i s_i} \Bigg) \\ &= \frac{1}{\varphi(\ell^{t_\ell})} \Bigg(1 + \frac{1}{\ell} \sum_{i=1}^{k_1} C_i^{k_1} \Big(\frac{-1}{\ell}\Big)^i \Bigg) \Big(1 - \frac{1}{\ell}\Big)^{r - k_1} \\ &= \frac{1}{\varphi(\ell^{t_\ell})} \Big(1 - \frac{1}{\ell}\Big)^{r - k_1} \Big(1 + \frac{1}{\ell} \Big(\Big(1 - \frac{1}{\ell}\Big)^{k_1} - 1 \Big) \Big) \\ &= \frac{1}{\varphi(\ell^{t_\ell})} \Big(1 - \frac{1}{\ell}\Big)^{r - k_1 + 1} \Big(1 + \frac{1}{\ell} \Big(1 - \frac{1}{\ell}\Big)^{k_1 - 1} \Big). \end{aligned}$$

Case 2: $\ell \mid z$. We set $S_2 = \{i : z_\ell \leqslant t_{i,\ell} < t_\ell\}$, $S_3 = \{i : h_{i,\ell} = t_{i,\ell} + 1\}$, and $k_i = |S_i|$ for all i.

Case 2.1: $t_\ell = 0$. The conditions on the indices are reduced to $\max_i(s_i) = g_\ell$ and $s_i = h_{i,\ell}$ for all i, and we must have $0 \leqslant h_{i,\ell} \leqslant g_\ell \leqslant 1$ for all i and $\max_i(h_{i,\ell}) = g_\ell$. Hence, if $g_\ell = 0$, then all s_i's must be zero and we have $p_\ell = 1$. If $g_\ell = 1$ and $h_{i,\ell} = 1$ for some i, then $p_\ell = \frac{1}{\ell-1}(\frac{-1}{\ell})^{k_3}$.

Case 2.2: $t_\ell \geqslant z_\ell$. From (4.31) we deduce $z_\ell = g_\ell$ and $h_{i,\ell} = z_\ell$ for all $i \in S_1 \cup S_2$, and $h_{i,\ell} \in \{t_{i,\ell}, t_{i,\ell} + 1\}$ for all other i. Then we obtain

$$\begin{aligned} p_\ell &= \frac{1}{\varphi(\ell^{t_\ell})}\Big(1 + \frac{1}{\ell}\Big(\Big(1 - \frac{1}{\ell}\Big)^{k_1} - 1\Big)\Big)\Big(1 - \frac{1}{\ell}\Big)^{k_2}\Big(-\frac{1}{\ell}\Big)^{k_3} \\ &= \frac{1}{\varphi(\ell^{t_\ell})}\Big(1 + \frac{1}{\ell}\Big(1 - \frac{1}{\ell}\Big)^{k_1-1}\Big)\Big(1 - \frac{1}{\ell}\Big)^{k_2+1}\Big(-\frac{1}{\ell}\Big)^{k_3}. \end{aligned}$$

Case 2.3: $0 < t_\ell < z_\ell$. From (4.31) we deduce $g_\ell \in \{t_\ell, t_\ell + 1\}$ and $h_{i,\ell} \in \{t_{i,\ell}, t_{i,\ell} + 1\}$ for all i. If $g_\ell = t_\ell + 1$ (we must have $h_{i,\ell} = t_\ell + 1$ for at least one i), then we obtain $p_\ell = \frac{1}{\varphi(\ell^{t_\ell})\ell}(\frac{-1}{\ell})^{k_3}$. If $g_\ell = t_\ell$ (and hence $h_{i,\ell} = g_\ell$ for all $i \in S_1$), then we obtain $p_\ell = \frac{1}{\varphi(\ell^{t_\ell})}(\frac{-1}{\ell})^{k_3}$. □

Remark 4.23. Taking $T = (1, \dots, 1)$ in (4.30) yields the formula (4.27). This is an easy check. In particular, with this assumption we obtain that $g, h_1, \dots, h_r$ are squarefree and such that $g = [h_1, \dots, h_r]$, and we have

$$p(g, h_1, \dots, h_r) = \frac{1}{\varphi(g)} \prod_{\ell \mid g} \Big(\frac{-1}{\ell}\Big)^{v_\ell(\prod_i h_i)} = \frac{\prod_i \mu(h_i)}{\varphi(g) \prod_i h_i}.$$

We also provide here a generalization of Theorem 4.4.

Corollary 4.24. *Let F/K be a finite Galois extension, and let C be a union of conjugacy classes of $\mathrm{Gal}(F/K)$. Let S be a non-empty set of r-tuples of positive integers, i.e. $S \subseteq \mathbb{N}_{>0}^r$. Define the following set of primes of K:*

$$\mathcal{S}' := \left\{\mathfrak{p} : (\mathrm{ind}_{\mathfrak{p}}(\alpha_1), \dots, \mathrm{ind}_{\mathfrak{p}}(\alpha_r)) \in S,\ \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C\right\}.$$

Assuming (GRH), we have

$$\mathcal{S}'(x) = \frac{x}{\log x} \sum_{T \in S} \sum_{N} \frac{(\prod_i \mu(n_i)) c'(N, T)}{[F_{N,T} : K]} + O\left(\frac{x}{(\log x)^{1+\frac{1}{r+1}}}\right), \tag{4.32}$$

where

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

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

Proof. The proof of the statement is essentially the same as for Theorem 4.4. Keeping the same notation as there, it is enough to notice that we have

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

and similarly

$$\sum_{T \in S} D_T - \sum_{\substack{T \in S \\ t_i \leqslant y}} D_T \leqslant \sum_{\substack{T \\ t_1 > y}} D_T + \ldots + \sum_{\substack{T \\ t_r > y}} D_T.$$

□

As an application of Corollary 4.24 we have the following result.

Corollary 4.25. *Let G be a finitely generated and torsion-free subgroup $K^\times$ of positive rank s. Let ℓ be a fixed prime number. Consider the set of primes $\mathfrak{p}$ of K*

$$\mathcal{L} := \{\mathfrak{p} : \mathrm{ind}_{\mathfrak{p}}(G) \mid \ell^\infty\}.$$

Assuming (GRH), there is a squarefree integer z, which depends only on K and G, such that

$$\mathcal{L}(x) = \frac{x}{\log x}\prod_{p\nmid z\ell}\left(1-\frac{1}{p^s(p-1)}\right)\cdot\sum_{g\mid \frac{z}{(z,\ell)}}\frac{\mu(g)}{[K(\zeta_g,G^{1/g}):K]}+O\left(\frac{x}{\log^{3/2}x}\right).$$

Setting

$$A'_s := \prod_p\left(1-\frac{1}{p^s(p-1)}\right) \tag{4.33}$$

for $s\geqslant 1$, the densities in the formulas for $\mathcal{L}(x)$ are given A'_s times rational numbers depending on K, G and ℓ. The constants A'_s can be seen as generalizations of Artin's constant, in different way with respect to (4.28).

Proof of Corollary 4.25. Let us denote δ_ℓ the density appearing in (4.32) with $r=1$ and $S=\{n\geqslant 1 : n\mid \ell^\infty\}$ for G, namely

$$\delta_\ell = \sum_{k\geqslant 0}\sum_{n\geqslant 1}\frac{\mu(n)}{[K(\zeta_{n\ell^k},G^{1/n\ell^k}):K]}.$$

By Theorem 2.1 there is an integer z', which depends only on K and G, such that we may write

$$\delta_\ell = \sum_{g\mid z'}\frac{\varphi(g)g^s}{[K(\zeta_g,G^{1/g}):K]}\sum_{\substack{k\geqslant 0\\ n\geqslant 1\\ (n\ell^k,z')=g}}\frac{\mu(n)}{\varphi(n\ell^k)(n\ell^k)^s}.$$

Since we may restrict the indices n to squarefree integers, we may suppose that $g\mid \mathrm{rad}(z')\ell^{v_\ell(z')}$. Let us set $z:=\mathrm{rad}(z')$, and for p a prime, $z_p=v_p(z')$, and $g_p=v_p(g)$. The inner sum on the indices k,n can be expressed as $\prod_p a_p(g)$ with

$$a_\ell(g)=\sum_{\substack{k\geqslant 0,\ t\in\{0,1\}\\ \min(t+k,z_\ell)=g_\ell}}\frac{\mu(\ell^t)}{\varphi(\ell^{t+k})\ell^{s(t+k)}},\quad\text{and}\quad a_p(g)=\sum_{\substack{t\in\{0,1\}\\ \min(t,z_p)=g_p}}\frac{\mu(p^t)}{\varphi(p^t)p^{st}}\ \text{if } p\neq\ell.$$

For $p\nmid z\ell$ we have $a_p=1-1/(p^s(p-1))$ (a_p does not depend on g). Supposing that $\ell\nmid z$ we have $a_\ell=1$. Let $p\mid z$. If $p\nmid g$, then $a_p(g)=1$. If $p\mid g$ and $p\neq\ell$ we have $g_p=1$ and $a_p(g)=-1/(p^s(p-1))$. Supposing that $\ell\mid g$, we have $a_\ell(g)=0$. Hence, we obtain

$$\delta_\ell=\prod_{p\nmid z\ell}\left(1-\frac{1}{p^s(p-1)}\right)\cdot\sum_{g\mid z}\frac{\varphi(g)g^s a_\ell(g)}{[K(\zeta_g,G^{1/g}):K]}\prod_{\substack{p\mid g\\ p\neq\ell}}\frac{-1}{p^s(p-1)}.$$

In view of the definition of $a_\ell(g)$, the index g can be supposed to be coprime with ℓ. Hence, since g is also squarefree, the last product can be expressed as $\mu(g)/(g^s\varphi(g))$. This yields the formula in the statement. □

We conclude the section by providing some numerical examples for the proven formulas. In Table 4.1 we show some values for the constants A_k and A'_k defined in (4.28) and (4.33), respectively. In Tables 4.2 and 4.3 we show examples for the densities of Proposition 4.21 and Theorem 4.22. Table 4.4 gives examples for the densities of Corollary 4.25. All values have been verified with SageMath [57] by computing the approximated density that considers only primes up to a certain bound. The Sage codes used to compute the density formulas have been partly adapted from Sebastiano Tronto's code *kummer-degrees*, available on GitHub.

k	A_k	A'_k
1	0.373956	0.373956
2	0.147349	0.697501
3	0.0608217	0.856540
4	0.0261075	0.931265
5	0.0115658	0.966669
6	0.00525176	0.983683

Table 4.1: Examples of constants A_k and A'_k approximated ($\ell < 10^6$)

α_1, α_2	$2, 3$	$3, 7$	$-3, 5$
$T = (1, 1)$	$A_2 \approx 0.147$	$\frac{286}{281}A_2 \approx 0.150$	$\frac{1800}{1183}A_2 \approx 0.224$
$T = (1, 2)$	$\frac{11}{13}A_2 \approx 0.125$	$\frac{2382}{3653}A_2 \approx 0.0961$	$\frac{1107}{1183}A_2 \approx 0.138$
$T = (2, 1)$	$\frac{17}{26}A_2 \approx 0.0963$	$\frac{3000}{3653}A_2 \approx 0.121$	$\frac{600}{1183}A_2 \approx 0.0747$
$T = (2, 3)$	$\frac{16}{117}A_2 \approx 0.0202$	$\frac{784}{10959}A_2 \approx 0.0105$	$\frac{800}{3549}A_2 \approx 0.0332$
$T = (3, 7)$	$\frac{512}{178997}A_2 \approx 0.000421$	$\frac{1024}{178997}A_2 \approx 0.000843$	0
$T = (1, 4)$	$\frac{2}{13}A_2 \approx 0.0227$	$\frac{1809}{7306}A_2 \approx 0.0365$	$\frac{1107}{4732}A_2 \approx 0.0345$
$T = (5, 4)$	$\frac{192}{29575}A_2 \approx 0.000957$	$\frac{86832}{8310575}A_2 \approx 0.00154$	$\frac{648}{29575}A_2 \approx 0.00323$

α_1, α_2	$5, 9$	$11, 3$	$-2, 7$
$T = (1, 1)$	0	$\frac{15562}{15457}A_2 \approx 0.148$	$A_2 \approx 0.147$
$T = (1, 2)$	$\frac{2200}{1183}A_2 \approx 0.274$	$\frac{12932}{15457}A_2 \approx 0.123$	$\frac{214}{281}A_2 \approx 0.112$
$T = (2, 1)$	0	$\frac{10096}{15457}A_2 \approx 0.0962$	$\frac{415}{562}A_2 \approx 0.109$
$T = (2, 3)$	0	$\frac{19360}{139113}A_2 \approx 0.0205$	$\frac{3320}{32877}A_2 \approx 0.0149$
$T = (3, 7)$	0	$\frac{598016}{212827433}A_2 \approx 0.000414$	$\frac{512}{178997}A_2 \approx 0.000421$
$T = (1, 4)$	$\frac{300}{1183}A_2 \approx 0.0374$	$\frac{1815}{15457}A_2 \approx 0.0173$	$\frac{67}{281}A_2 \approx 0.0351$
$T = (5, 4)$	0	$\frac{34848}{7032935}A_2 \approx 0.000730$	$\frac{6432}{639275}A_2 \approx 0.00148$

Table 4.2: Examples for the densities of rational primes p such that $(\mathrm{ind}_p(\alpha_1), \mathrm{ind}_p(\alpha_2)) = T$

$\alpha_1, \alpha_2, \alpha_3$	$2, 3, 5$	$3, 7, 2$	$11, 3, 5$
$T = (1, 1, 1)$	$\frac{500}{439} A_3 \approx 0.0693$	$\frac{69998}{67585} A_3 \approx 0.0630$	$\frac{46055400}{39884467} A_3 \approx 0.0703$
$T = (2, 1, 2)$	$\frac{1593}{4390} A_3 \approx 0.0221$	$\frac{52824}{67585} A_3 \approx 0.0475$	$\frac{10360116}{28488905} A_3 \approx 0.0221$
$T = (3, 3, 2)$	$\frac{88}{2195} A_3 \approx 0.00244$	$\frac{79376}{1824795} A_3 \approx 0.00265$	$\frac{1113024}{28488905} A_3 \approx 0.00238$
$T = (5, 2, 3)$	0	$\frac{401408}{105963625} A_3 \approx 0.000230$	0

Table 4.3: Examples for the densities of rational primes p such that the indices $\mathrm{ind}_p(\alpha_i)$ for all $i = 1, 2, 3$ are given by the entries of T, respectively

G	$\langle 2, 3 \rangle$	$\langle 3, 7 \rangle$	$\langle 5, 9 \rangle$	$\langle 11, 3 \rangle$
$\ell = 2$	$\frac{4}{3} A_2' \approx 0.930$	$\frac{4}{3} A_2' \approx 0.930$	$\frac{4}{3} A_2' \approx 0.930$	$\frac{4}{3} A_2' \approx 0.930$
$\ell = 3$	$\frac{18}{17} A_2' \approx 0.739$	$\frac{18}{17} A_2' \approx 0.739$	$\frac{400}{561} A_2' \approx 0.497$	$\frac{18}{17} A_2' \approx 0.739$
$\ell = 5$	$\frac{100}{99} A_2' \approx 0.705$	$\frac{1494200}{1479357} A_2' \approx 0.705$	$\frac{200}{297} A_2' \approx 0.470$	$\frac{6165800}{6104241} A_2' \approx 0.705$
$\ell = 7$	$\frac{294}{293} A_2' \approx 0.700$	$\frac{294}{293} A_2' \approx 0.700$	$\frac{19600}{29007} A_2' \approx 0.471$	$\frac{6042484}{6022029} A_2' \approx 0.700$

Table 4.4: Examples for the densities of rational primes p such that $\mathrm{ind}_p(G) \mid \ell^\infty$

Chapter 5

Divisibility conditions on the order of the reductions of algebraic numbers

Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. In this chapter, 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 Chebotarev's density theorem for Kummer extensions of number fields. The results of this chapter are available in the paper [54].

5.1 Main results

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 chapter 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, recalling the notation set in Section 1.1, in Theorem 5.1 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 5.2, 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 chapter we do not rely on the Generalized Riemann Hypothesis (GRH). In fact, Theorem 5.10 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 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 [36, 37] (also replacing g with a group of rational numbers), by Moree [26], and previously by Wiertelak [58]. We provide 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 [10, 40]. As discussed in the Introduction, 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, see [59] by Ziegler and [43] by Perucca and the author. For more references and historical background we refer to [31, Sect. 9.2 and 9.3].

5.1.1 Notation

As mentioned above, we make us of the notation from Section 1.1. 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.

5.1.2 Outline of the main results

The main result is the following.

Theorem 5.1. *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

$$\mathcal{P}_m(x) = \frac{x}{\log x} \varrho_{C,m} + O_\varepsilon \left(x \left(\frac{(\log\log x)^2}{\log x} \right)^{1+\frac{1-\varepsilon}{3(r+1)}} \right) \tag{5.1}$$

where

$$\varrho_{C,m} := \sum_{n \mid m^\infty} \sum_{d \mid m} \frac{\mu(d) c(mn, dn)}{[F_{mn,dn} : K]} \tag{5.2}$$

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

$$c(a,b) := |C \cap \mathrm{Gal}(F/F \cap K_{a,b})|. \tag{5.3}$$

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 5.16 we explain how to deal with the general case. Also notice that the series in (5.2) is convergent by Proposition 5.15. The coefficient $c(a,b)$ in (5.3) is always at most $|C| \leqslant [F : K]$, and it is equal to 1 if the condition on the Frobenius is trivial. For this case see Theorem 1.4, which follows directly.

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 5.2 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 5.3 is devoted to the proof of Theorem 5.1, whereas in Section 5.4 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 5.18.

Sections 5.5 and 5.6 are devoted to proving applications of Theorem 5.1. In Section 5.5 we apply Theorem 5.1 to prove the following result on the primes $\mathfrak{p}$ of K for which $\mathrm{ord}_{\mathfrak{p}}(G)$ is k-free.

Theorem 5.2. *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

$$\mathcal{N}_k(x) = \frac{x}{\log x} \sum_{m \geqslant 1} \mu(m) \varrho_{C,m^k} + O_k\left(\frac{x}{(\log x)^{1+\frac{k-1}{3(r+1)(k+1)}}} \right), \tag{5.4}$$

where ϱ_{C,m^k} is as in (5.2)*. 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 (5.3)*. 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 5.15. In Section 5.6, from Theorem 5.1 we also derive Theorem 5.21, 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 5.7, under (GRH), we derive some improvements on the error terms of formulas (5.1) and (5.4). Finally, in Section 5.8 we provide several numerical examples for the densities considered in this chapter.

5.2 Chebotarev's 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 5.1.1).

5.2.1 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, as customary, $\mathrm{Li}(x) = \int_2^x \frac{dx}{\log x}$ is the logarithmic integral function.

5.2.2 Chebotarev's density theorem

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

Theorem 5.3 (Effective Chebotarev's density theorem, unconditional, [20, Theorem 1.2] and [53, 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*

$$\log x \geqslant c_1 [L:\mathbb{Q}] \log^2 |d_L|\,, \tag{5.5}$$

then

$$\pi(L/K, C)(x) = \frac{|C|}{[L:K]} \mathrm{Li}(x) + O\left(\frac{|C|}{[L:K]} \mathrm{Li}(x^\beta) + |\tilde{C}| x \exp\left(- c_2 \sqrt{\frac{\log x}{[L:\mathbb{Q}]}} \right) \right), \tag{5.6}$$

where $|\tilde{C}|$ denotes the number of conjugacy classes contained in C, and where β is the exceptional zero of $\zeta_L(s)$, i.e. the unique real zero in the range

$$1 - \frac{1}{4 \log |d_L|} \leqslant \alpha \leqslant 1$$

(if it exists, otherwise the term $\frac{|C|}{[L:K]} \mathrm{Li}(x^\beta)$ is deleted).

Remark 5.4. 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. [59, Lemma 1], the same asymptotic formula (5.6) 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 [56, 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 5.8. However, for the general case we need to deduce from Stark's results some improvement which is suitable for our goal.

5.2.3 On a possible zero of the Dedekind zeta function

Lemma 5.5 ([56, 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*

$$\left\{ s \in \mathbb{C} : 1 - \frac{1}{4 \log |d_L|} \leqslant \mathrm{Re}(s) \leqslant 1 \text{ and } |\mathrm{Im}(s)| \leqslant \frac{1}{4 \log |d_L|} \right\}. \tag{5.7}$$

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

Lemma 5.6. *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*

$$1 - \frac{1}{4(2[K:\mathbb{Q}])! \cdot \log |d_L|} \leqslant \beta \leqslant 1, \tag{5.8}$$

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 (5.8).

Proof. If $K = \mathbb{Q}$, then the statement holds by [56, Lemma 8], hence we suppose $K \neq \mathbb{Q}$. If $\zeta_L(s)$ has a zero with real part lying in the range (5.8), then by Lemma 5.5 it must be real, simple, and unique in that range. Since L/K is normal, by [56, 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 $\zeta_K(\beta) = 0$ or $\zeta_F(\beta) = 0$ for some quadratic extension F/K with $F \subseteq L$. We conclude by applying [56, Lemma 8] either to K or F, noticing that the range of the cited result contains the interval (5.8). □

Proposition 5.7. *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* (5.7) *is real and simple, and we have*

$$\frac{1}{2} \leqslant \beta \leqslant \max\left\{1 - \frac{1}{4(2[K:\mathbb{Q}])! \log|d_L|}, 1 - \frac{1}{c_3 |d_L|^{1/[L:\mathbb{Q}]}}\right\}, \tag{5.9}$$

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 (5.8), then β satisfies (5.9). We follow the same argument as in [56, 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 (5.8) by Lemma 5.6 and hence (5.9) is satisfied. If L contains a quadratic field, suppose that $\zeta_L(\beta) = 0$ for some β in the range (5.8). By Lemma 5.6 there must be a quadratic subfield M of L such that $\zeta_M(\beta) = 0$. By [56, 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 5.8. In fact, if in the proof of Lemma 5.6 we have $\zeta_K(\beta) = 0$, then the lower bound of (5.8) 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 (5.8) may be taken to be $1 - (4\log|d_L|)^{-1}$ or $1 - (16\log|d_L|)^{-1}$, respectively (see [56, Lemmas 8 and 10]). Accordingly, the factor $4(2[K:\mathbb{Q}])!$ in (5.9) can be replaced by 4 or 16 in the respective cases, by following the same argument of the proof of Proposition 5.7.

5.2.4 Chebotarev's density theorem for cyclotomic-Kummer extensions

Proposition 5.9. *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

$$d_{K_{m,n}/\mathbb{Q}} = \mathrm{N}_{K/\mathbb{Q}}(d_{K_{m,n}/K}) \cdot d_{K/\mathbb{Q}}^{[K_{m,n}:K]}, \tag{5.10}$$

see [34, Ch.III, Corollary 2.10]. By [53, Proposition 5], since $K_{m,n}/K$ is Galois, we have

$$\log\left|\mathrm{N}_{K/\mathbb{Q}}(d_{K_{m,n}/K})\right| \leqslant [K_{m,n}:\mathbb{Q}]\Big(\log[K_{m,n}:K] + \sum_{p \in P(K_{m,n}/K)} \log p\Big) \tag{5.11}$$

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 [43, 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

$$\sum_{p \in P(K_{m,n}/K)} \log p \leqslant \log m + \sum_{p \in P(G)} \log p\,. \tag{5.12}$$

We conclude by taking the logarithm of $\big|d_{K_{m,n}}\big|$, making use of (5.10), and by applying the bounds (5.11), (5.12) 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 [37, Lemma 4] to number fields.

Theorem 5.10 (Effective Chebotarev's density theorem for cyclotomic-Kummer extensions)**.** *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*

$$C_{m,n} := \{\sigma \in \mathrm{Gal}(F_{m,n}/K) : \sigma|_F \in C,\, \sigma|_{K_{m,n}} = \mathrm{id}\}\,, \tag{5.13}$$

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

$$m \leqslant c_4 \left(\frac{\log x}{(\log\log x)^2}\right)^{\frac{1}{3(r+1)}}\,, \tag{5.14}$$

we have

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

If the condition on the Frobenius is trivial, then Theorem 5.10 reduces to Theorem 1.5.

Proof. We apply Theorem 5.3 to $F_{m,n}/K$ and $C_{m,n}$. By Proposition 5.9 and since $[F_{m,n} : F] \leqslant m^{r+1}$ we have

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

($c_{F,G}$ is a constant depending only on F and G). Thus, from (5.14) we deduce $m^{3(r+1)} \log^2 m \ll \log x$, hence (5.5) is satisfied.

We now focus on the error terms of (5.6). In order to bound the second one, it is enough to notice that

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

Let us consider the first one. 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 5.7 separately. On the one hand, by Proposition 5.9 we have

$$\left|d_{F_{m,n}}\right|^{1/[F_{m,n}:\mathbb{Q}]} \leqslant \exp\left(\log m^{r+2} + c_{F,G}\right) \ll_{F,G} m^{r+2} \ll \left(\frac{\log x}{(\log\log x)^2}\right)^{2/3},$$

which yields

$$\begin{aligned}\frac{x^\beta}{\log x} &\leqslant \frac{x}{x^{1/(c_3\left|d_{F_{m,n}}\right|^{1/[F_{m,n}:\mathbb{Q}]})}\log x} \leqslant \frac{x}{\exp\left(c_6\left(\frac{(\log\log x)^2}{\log x}\right)^{2/3}\log x\right)\log x} \\ &\leqslant \frac{x}{\exp\left(c_6(\log x)^{1/3}(\log\log x)^{4/3}\right)\log x} \leqslant \frac{x}{\exp\left(c_5\sqrt[3]{\log x\cdot\log\log x}\right)}.\end{aligned}$$

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

$$\frac{x^\beta}{\log x} \leqslant \frac{x}{x^{1/(4(2[K:\mathbb{Q}])!\log\left|d_{F_{m,n}}\right|)}\log x} \leqslant \frac{x}{\exp\left(c_7\sqrt{\log x}\right)\log x} \leqslant \frac{x}{\exp\left(c_5\sqrt[3]{\log x\cdot\log\log x}\right)}.$$

The constants c_5, c_6, c_7 depend only on F and G. Collecting all error terms gives the asymptotic formula. □

5.3 The order being divisible by a given integer

In this section we prove Theorem 5.1. We first set some notation. Recall also the notation introduced in Sections 5.1.1 and 5.2.1.

5.3.1 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 (5.13) (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.

5.3.2 Proof of Theorem 5.1

The proof of Theorem 5.1 is based on [37, Theorem 1] and [26, 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

$$\pi^1_{m,n} = \left\{ \mathfrak{p} : \mathfrak{p} \text{ of degree } 1,\ \mathrm{N}\,\mathfrak{p} \equiv 1 \bmod m,\ n \mid \mathrm{ind}_{\mathfrak{p}}(G),\ \left(\frac{\mathfrak{p}}{F/K}\right) \subseteq C \right\}, \tag{5.15}$$

see also [59, Lemma 2].

Lemma 5.11. *If $\mathcal{P}_m$ is as in Theorem 5.1, 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 [26, 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

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

We conclude by (5.15) that

$$\mathcal{B}_n(x) = \sum_{d \mid m} \mu(d) \pi^1_{mn,dn}(x). \tag{5.16}$$

□

Remark 5.12. Notice that, in the proof of Lemma 5.11 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 (5.16), and by the Chebotarev density theorem we deduce

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

We are now ready to prove Theorem 5.1.

Proof of Theorem 5.1. 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 5.11 and Theorem 5.10. For $n \mid m^\infty$ let $\mathcal{B}_n$ be as in the proof of Lemma 5.11, and recall (5.16). Set $y := c_4(\log x/(\log\log x)^2)^{1/3(r+1)}$, where c_4 is the constant of Theorem 5.10. Thus, we have

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

In order to estimate the tail of the series in the main term we make use of Remark 5.12 and obtain

$$\mathcal{P}_m(x) = \mathrm{Li}(x)\sum_{n\mid m^\infty}\sum_{d\mid m}\frac{\mu(d)c(mn,dn)}{[F_{mn,dn}:K]} + O\left(\frac{x}{\log x}\sum_{\substack{n\mid m^\infty\\ mn>y}}\frac{1}{[K_{mn,n}:K]}\right) \tag{5.17}$$

$$+ O_{F,G}\left(\frac{x\cdot y}{e^{c_5\sqrt[3]{\log x\cdot\log\log x}}}\right) + O\bigg(\sum_{\substack{n\mid m^\infty\\ nm>y}}\mathcal{B}_n(x)\bigg). \tag{5.18}$$

The first error term in (5.18) is negligible with respect to the error term in the statement. Let us estimate the error term in (5.17). Since $[K(\zeta_{mn}):K] \gg_K \varphi(mn)$ and $mn/\varphi(mn) = m/\varphi(m)$ (as $\mathrm{rad}(n) \mid m$), applying [36, Lemma 3.3] for some $0 < \varepsilon < 1$, we can bound

$$\sum_{\substack{n\mid m^\infty\\ mn>y}}\frac{1}{[K_{mn,n}:K]} \ll_K \sum_{\substack{n\mid m^\infty\\ nm>y}}\frac{1}{\varphi(mn)} \ll_\varepsilon \frac{m}{\varphi(m)}\frac{1}{y^{1-\varepsilon}}. \tag{5.19}$$

Since $m/\varphi(m) = O(\log\log m)$, see e.g. [51, Theorem 15], and $m \leqslant x$ without loss of generality, we then have

$$\frac{x}{\log x}\sum_{\substack{n\mid m^\infty\\ mn>y}}\frac{1}{[K_{mn,n}:K]} \ll_{K,\varepsilon} \frac{x\log\log x}{y^{1-\varepsilon}\log x}. \tag{5.20}$$

Next we focus on the second error term in (5.18). In view of Remark 5.12, and by applying the Brun-Titchmarsh Theorem and the same estimates as above, for $z := (\log x)^{2/(1-\varepsilon)}$ we have

$$\begin{aligned}\sum_{\substack{n\mid m^\infty\\ nm\leqslant y}}\mathcal{B}_n(x) &\ll_K \sum_{\substack{n\mid m^\infty\\ y<nm\leqslant z}}|\{p\leqslant x : p\equiv 1 \bmod mn\}| + \sum_{\substack{n\mid m^\infty\\ nm>z}}|\{k\leqslant x : mn\mid k\}|\\ &\ll \sum_{\substack{n\mid m^\infty\\ y<nm\leqslant z}}\frac{x}{\varphi(mn)\log(x/mn)} + \sum_{\substack{n\mid m^\infty\\ nm>z}}\frac{x}{mn} \ll_\varepsilon \frac{x\log\log x}{\log(x/z)}\frac{1}{y^{1-\varepsilon}} + \frac{x}{\log^2 x}.\end{aligned} \tag{5.21}$$

Both expressions (5.20) and (5.21) are bounded by the error term in the statement. □

5.3.3 Properties and remarks

Remark 5.13. One can see from [36, Proof of Lemma 3.3] that the constant depending on ε arising in (5.19) 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 5.1.

Remark 5.14. Let $m \geqslant 1$, and $\omega(m)$ be the number of prime factors of m. One can show that for $T \geqslant 1$ and $0 < c < 1$ we have

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

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 [36, Lemma 3.3] we have

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

Taking $c = 1 - 1/\log\log x$ and making use of this inequality in the proof of Theorem 5.1 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 [37, Theorem 1].

Proposition 5.15. *The series $\varrho_{C,m}$ from Theorem 5.1 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 5.12 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 5.16. The assumption that the group G is torsion-free allows some simplifications throughout the proof of Theorem 5.1. 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 5.17. 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

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

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 $m \mid \mathrm{ord}_{\mathfrak{P}}(G)$.

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 5.2 and $\gamma_{C,k,m}$ of Theorem 5.21.

5.4 A rational formula for the density

As a special case of Corollary 3.7 ([44, Corollary 7]), the natural density $\varrho_{C,m}$ of the set $\mathcal{P}_m$ from Theorem 5.1 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 5.17). In the rest of the chapter, ℓ will always represent a prime number (also when not mentioned explicitly). Notice that, over $\mathbb{Q}$, Pappalardi [37] provided an explicit rational formula for ϱ_m for G consisting of positive rationals, whereas the case of groups with negative rationals was considered in [1] by Abdullah, Ali Mustafa and Pappalardi.

Theorem 5.18. *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*

$$\varrho_m = \frac{1}{\varphi(m)} \prod_{\substack{\ell \mid m \\ \ell \nmid z}} \frac{\ell(\ell^r - 1)}{\ell^{r+1} - 1} \cdot \sum_{\substack{g \mid z \\ \mathrm{rad}(g) \mid (m,z) \mid g}} \sum_{h \mid g} \frac{p(g,h)}{[K_{g,h} : K]}, \tag{5.22}$$

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 [47] (see e.g. [47, 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 [47, 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

$$\varrho_m = \sum_{n \mid m^\infty} \sum_{d \mid m} \frac{\mu(d)}{[K_{mn,dn} : K]} = \frac{1}{\varphi(m)} \sum_{\substack{g \mid z \\ h \mid g}} \frac{\varphi(g) h^r}{[K_{g,h} : K]} \sum_{\substack{n \mid m^\infty \\ (mn,z)=g}} \sum_{\substack{d \mid m \\ (dn,z)=h}} \frac{\mu(d)}{n^{r+1} d^r}. \tag{5.23}$$

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 (5.23) 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

$$p_\ell(g,h) := \sum_{\substack{s \geqslant 0 \\ \min(m_\ell + s, z_\ell) = g_\ell}} \sum_{\substack{e \in \{0,1\} \\ \min(s+e, z_\ell) = h_\ell}} \frac{\mu(\ell^e)}{\ell^{s(r+1)} \ell^{er}}. \tag{5.24}$$

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 (5.22). 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 (5.24) 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

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

□

5.5 The order being k-free

In this section we prove Theorem 5.2. The proof relies on ideas from [36, Theorem 1.2] (see also [37, Remark (8), p.388]).

Proof of Theorem 5.2. 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 (5.1) as for $\mathcal{P}_m(x)$. Then, for $0 < a < 1$ and $z := \log^a x$ we have

$$\begin{aligned}
\mathcal{N}_k(x) &= \sum_{m \leqslant z} \mu(m) \mathcal{P}^1_{m^k}(x) + O\left(\sum_{m > z} \mathcal{P}^1_{m^k}(x)\right) + O\left(\frac{\sqrt{x}}{\log x}\right) \\
&= \frac{x}{\log x} \beta_{C,k} + O\left(\frac{x}{\log x} \sum_{m > z} \varrho_{C,m^k}\right) + O\left(\sum_{m > z} \mathcal{P}^1_{m^k}(x)\right) \qquad (5.25) \\
&\quad + O\left(\sum_{m \leqslant z} x \left(\frac{(\log\log x)^2}{\log x}\right)^{1 + \frac{1-\varepsilon}{3(r+1)}}\right) + O\left(\frac{\sqrt{x}}{\log x}\right). \qquad (5.26)
\end{aligned}$$

By Proposition 5.15 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 (5.25) by

$$\frac{x}{\log x} \sum_{m > z} \frac{1}{m^{k-\eta}} = O_\eta\left(\frac{x}{(\log x)^{1+a(k-1-\eta)}}\right). \qquad (5.27)$$

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 (5.25) 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 (5.27).

Next, we can bound the first error term in (5.26) by

$$(\log x)^a \cdot x\left(\frac{(\log\log x)^2}{\log x}\right)^{1+\frac{1-\varepsilon}{3(r+1)}} \leqslant \frac{x(\log\log x)^3}{(\log x)^{1+\frac{1-\varepsilon}{3(r+1)}-a}}, \tag{5.28}$$

and we may choose $a = \frac{1-\varepsilon}{3(r+1)(k-\eta)}$, so that (5.28) can be bounded by (5.27). With a suitable choice of ε and η (depending on k), the exponent in the denominator of (5.27) can be reduced to $1+\frac{k-1}{3(r+1)(k+1)}$. Collecting the errors yields the result. □

Remark 5.19. In the context of Theorem 5.2, 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 5.2 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.

Theorem 5.20. *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*

$$\beta_k = \prod_{\ell\nmid z}\Big(1-\frac{\ell^r-1}{(\ell-1)(\ell^{r+1}-1)\ell^{k-2}}\Big)\cdot \sum_{\substack{g\mid z\\ (\mathrm{rad}(g)^k,z)\mid g}}\sum_{h\mid g}\frac{p(g,h)}{[K_{g,h}:K]}, \tag{5.29}$$

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

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

Notice that, setting

$$A_{k,r} := \prod_{\ell \text{ prime}}\Big(1-\frac{\ell^r-1}{(\ell-1)(\ell^{r+1}-1)\ell^{k-2}}\Big), \tag{5.30}$$

a constant which only depends on the integer k and on the rank r of G, the infinite product in (5.29) 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 [47, Theorem 1.1] as in the proof of Theorem 5.18 we obtain

$$\beta_k = \sum_{m\geqslant 1}\sum_{\substack{n\mid m^\infty\\ d\mid m}} \frac{\mu(m)\mu(d)}{[K_{nm^k,dn}:K]} = \sum_{\substack{g\mid z\\ h\mid g}} \frac{\varphi(g)h^r}{[K_{g,h}:K]} \sum_{m\geqslant 1} \sum_{\substack{n\mid m^\infty\\ (nm^k,z)=g}} \sum_{\substack{d\mid m\\ (dn,z)=h}} \frac{\mu(m)\mu(d)}{n^{r+1}d^r\varphi(m^k)}$$

$$= \sum_{\substack{g\mid z\\ h\mid g}} \frac{\varphi(g)h^r}{[K_{g,h}:K]} \prod_{\ell \text{ prime}} p_\ell(g,h) \tag{5.31}$$

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

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

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

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

We take $p(g,h) := \varphi(g)h^r \prod_{\ell\mid g} p_\ell(g,h)$ (and make use of the identity $\varphi(g)/\varphi(\operatorname{rad}(g)^k) = g/\operatorname{rad}(g)^k$). 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 (5.31) to the divisors g such that $(\operatorname{rad}(g)^k, z) \mid g$.

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 $k \geqslant 2$). 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, $p_\ell(g,h) = 0$. □

5.6 Prescribing valuations for the order

In this section we apply Theorem 5.1 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 5.21. *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 $\operatorname{Gal}(F/K)$. 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 (5.2)*, 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 (5.3)*). The constant implied by the O-term depends only on ε, F, K, G.*

It follows from Proposition 5.15 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 5.1 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 5.22. 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 5.1 and it is a special case of Theorem 5.21. The case of trivial condition on the Frobenius is stated in Theorem 1.6.

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

Theorem 5.23. *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

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

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

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

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

Proof. The proof is similar to that of Theorem 5.18 and does not contain new ingredients: one needs to first apply [47, 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.

Nevertheless, for the convenience of the reader we provide here the details. We apply [47, Theorem 1.1] as we did in the proof of Theorem 5.18 to obtain

$$\begin{aligned}\gamma_{k,m} &= \sum_{f \mid k} \sum_{n \mid (fm)^\infty} \sum_{d \mid fm} \frac{\mu(f)\mu(d)}{[K_{fmn,dn} : K]} \\ &= \sum_{\substack{g \mid z \\ h \mid g}} \frac{\varphi(g)h^r}{[K_{g,h} : K]} \sum_{f \mid k} \sum_{\substack{n \mid (fm)^\infty \\ (fmn,z)=g}} \sum_{\substack{d \mid fm \\ (dn,z)=h}} \frac{\mu(f)\mu(d)}{\varphi(fmn)(nd)^r}.\end{aligned}$$

Write $m = \prod_{\ell \mid k} \ell^{a_\ell}$ with $a_\ell \geqslant 0$. Notice that the inner sums do not vanish only if $(m,z) \mid g$ and $\mathrm{rad}(g) \mid k$. Thus we reduce the formula to

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

where for $\ell \mid k$ prime and $a_\ell = 0$ we define $p_\ell(g,h)$ according to a case distinction on the prime factors ℓ of k. Set $z_\ell := v_\ell(z)$, and similarly for g_ℓ, h_ℓ.

Case 1: $\ell \mid k$ and $a_\ell = 0$. If $\ell \nmid z$, then we set

$$p_\ell(g,h) := 1 - \frac{1}{\ell-1} \sum_{s \geqslant 0} \sum_{t \in \{0,1\}} \frac{\mu(\ell^t)}{\ell^{s(r+1)+tr}} = 1 - \frac{\ell(\ell^r-1)}{(\ell-1)(\ell^{r+1}-1)};$$

if $\ell \mid z$ and $\ell \nmid g$, then $p_\ell(g,h) := 1$; if $\ell \mid g$, then we set

$$p_\ell(g,h) := -\frac{1}{\ell-1} \sum_{\substack{s \geqslant 0 \\ \min(s+1,z_\ell)=g_\ell}} \sum_{\substack{t \in \{0,1\} \\ \min(s+t,z_\ell)=h_\ell}} \frac{\mu(\ell^t)}{\ell^{s(r+1)+tr}}.$$

We take $q_1(g,h) := \prod_{\ell \mid (k,g), a_\ell = 0} p_\ell(g,h)\ell^{h_\ell(r+1)}$, and we compute $p_\ell(g,h)$ depending on the prime factor ℓ of (k,g).

Case 1.1: $\ell \nmid h$. We must have $s = t = 0$, hence $p_\ell(g,h) = -1/(\ell-1)$ if $g_\ell = 1$, otherwise $p_\ell(g,h) = 0$.

Case 1.2: $\ell \mid h$, $h_\ell = g_\ell = z_\ell$. The conditions on the indices hold only for $s + t \geqslant z_\ell$. We obtain $p_\ell(g,h) = \frac{1}{\ell^{h_\ell(r+1)}} \frac{\ell^{r+1}}{\ell^{r+1}-1}$.

Case 1.3: $\ell \mid h$, $h_\ell < g_\ell = z_\ell$. We must have $s + t = h_\ell$ and $s + 1 \geqslant z_\ell$, hence $p_\ell(g,h) = -1/(\ell^{h_\ell(r+1)}(\ell-1))$ if $g_\ell - h_\ell = 1$, and $p_\ell(g,h) = 0$ otherwise.

Case 1.4: $\ell \mid h$, $g_\ell < z_\ell$. We must have $s = g_\ell - 1$. Thus, we obtain: $p_\ell(g,h) = -1/(\ell^{h_\ell(r+1)}(\ell-1))$ if $g_\ell - h_\ell = 1$; $p_\ell(g,h) = \ell/(\ell^{h_\ell(r+1)}(\ell-1))$ if $g_\ell = h_\ell$; $p_\ell(g,h) = 0$ otherwise.

Case 2: $\ell \mid k$ *and* $a_\ell > 0$. Recall that g is such that $g_\ell \geqslant \min(a_\ell, z_\ell)$. We set

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

If $\ell \nmid z$, then we have $p_\ell(g,h) = \frac{(\ell-1)(\ell^r-1)}{\ell^{r+1}-1}$ if $a_\ell > 0$. Before dealing with the case $\ell \mid z$, we set $q_2(g,h) := \prod_{\ell \mid (k,z), a_\ell > 0} p_\ell(g,h)\ell^{h_\ell(r+1)}$, and we compute $p_\ell(g,h)$ depending on the prime factor ℓ of (k,z).

Case 2.1: $\ell \nmid h$. We must have $s = t = 0$ and hence we have: $p_\ell(g,h) = 0$ if $g_\ell \notin \{z_\ell, a_\ell, a_\ell + 1\}$, or $g_\ell = z_\ell > a_\ell + 1$; $p_\ell(g,h) = 1$ if $g_\ell = a_\ell < z_\ell$; $p_\ell(g,h) = -1/\ell$ if $g_\ell = a_\ell + 1$; $p_\ell(g,h) = 1 - 1/\ell$ if $g_\ell = z_\ell \leqslant a_\ell$.

Case 2.2: $\ell \mid h$ *and* $h_\ell = g_\ell = z_\ell$. The conditions on the indices hold only for $s \geqslant h_\ell$, or $s = h_\ell - 1$ and $t = 1$ (as $a_\ell \geqslant 1$). We obtain

$$p_\ell(g,h) = \Big(1 - \frac{1}{\ell}\Big)\Big(\Big(1 - \frac{1}{\ell^r}\Big)\frac{1}{\ell^{h_\ell(r+1)}} \sum_{s \geqslant 0} \frac{1}{\ell^{s(r+1)}} - \frac{\ell}{\ell^{h_\ell}}\Big) = -\frac{\ell^r(\ell-1)^2}{\ell^{h_\ell(r+1)}(\ell^{r+1}-1)}.$$

Case 2.3: $\ell \mid h$ *and* $h_\ell < g_\ell = z_\ell$. Then the conditions are satisfied only if $s + e + a_\ell \geqslant z_\ell$. We deduce that $p_\ell(g,h)$ equals: $-(\ell-1)^2/\ell^{h_\ell(r+1)+1}$ if $g_\ell - h_\ell < a_\ell$; $(2\ell-1)/\ell^{h_\ell(r+1)+1}$ if $g_\ell - h_\ell = a_\ell$; $-1/\ell^{h_\ell(r+1)+1}$ if $g_\ell - h_\ell = a_\ell + 1$; 0 if $g_\ell - h_\ell > a_\ell + 1$.

Case 2.4: $\ell \mid h$ *and* $g_\ell < z_\ell$. The conditions are satisfied only if $a_\ell + s + e = g_\ell$. Thus, $p_\ell(g,h)$ equals: 0 if $g_\ell - h_\ell \notin \{a_\ell - 1, a_\ell, a_\ell + 1\}$; $-\ell/\ell^{h_\ell(r+1)}$ if $g_\ell - h_\ell = a_\ell - 1$; $2/\ell^{h_\ell(r+1)}$ if $g_\ell - h_\ell = a_\ell$; $-1/\ell^{h_\ell(r+1)+1}$ if $g_\ell - h_\ell = a_\ell + 1$.

Finally, take $p(g,h) := (\varphi(g)/h) \cdot q_1(g,h)q_2(g,h)$. □

Theorem 5.24. *Let K be a number field and let G be a torsion-free subgroup of $K^\times$ of positive rank r. Let $k \geqslant 1$ be a squarefree integer. There is an integer z, which depends only on K and G, such that the natural density of the set of primes $\mathfrak{p}$ of K with $\mathrm{ord}_{\mathfrak{p}}(G)$ coprime to k (where $\mathfrak{p} \notin \mathcal{P}(G)$) is given by*

$$\prod_{\substack{\ell \mid k \\ \ell \nmid z}} \Big(1 - \frac{\ell(\ell^r - 1)}{(\ell^{r+1}-1)(\ell-1)}\Big) \cdot \sum_{\substack{g \mid z \\ \mathrm{rad}(g) \mid k}} \sum_{h \mid g} \mu\Big(\frac{g}{h}\Big) \frac{p(g,h)}{[K_{g,h} : K]},$$

where, for $h \mid g$, we set

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

Proof. It suffices to take $m = 1$ in Theorem 5.23. Clearly we have $q_2(g,h) = 1$. We obtain that $p(g,h) = 0$ if and only if g/h is not squarefree, and this together with the factor $\prod_{\ell|g/h}(-1)$ in $q_1(g,h)$ yields the term $\mu(g/h)$ in the formula. Also, the factor $\prod_{\ell|g/h} 1/(\ell-1)$ in $q_1(g,h)$ is equal to $1/\varphi(g/h)$. □

5.7 Conditional results assuming GRH

In this section we show how Theorems 5.1 and 5.2 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 [53, Théorème 4] or [59, Theorem 2], and we obtain smaller error terms. Let us first apply this theorem to cyclotomic-Kummer extensions of K.

Lemma 5.25. *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* (5.13)*) is given by*

$$\pi(F_{m,n}/K, C_{m,n})(x) = \frac{|C_{m,n}|}{[F_{m,n} : K]} \operatorname{Li}(x) + O_{F,G}\left(\sqrt{x}\log(mx)\right). \tag{5.32}$$

Proof. Applying [53, 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 Proposition 5.9, 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 5.26. *With the setup of Theorem 5.1, 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 5.1. Recall (5.16), where $\mathcal{B}_n$ was defined in the proof of Lemma 5.11. Applying first Lemma 5.11, and then Lemma 5.25 to the functions $\pi^1_{mn,dn}(x)$ (notice that (5.32) also holds if we restrict to the primes of K of degree 1), setting $y := x^{1/4}$ we obtain:

$$\mathcal{P}_m(x) = \operatorname{Li}(x)\varrho_{C,m} + O\left(\sum_{n\leqslant y/m}\sum_{d\mid m}\sqrt{x}\log(mnx)\right) + O\left(\frac{\sqrt{x}}{\log x}\right) \tag{5.33}$$

$$+ O\left(\operatorname{Li}(x)\sum_{\substack{n\mid m^\infty\\ nm>y}}\sum_{d\mid m}\frac{\mu(d)c(mn,dn)}{[F_{mn,dn} : K]}\right) + O\left(\sum_{\substack{n\mid m^\infty\\ nm>y}}\mathcal{B}_n(x)\right). \tag{5.34}$$

The first O-term in (5.33) 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 (5.34) 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. □

Corollary 5.27. *Assume (GRH). With the setup of Theorem 5.2, we have*

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

Moreover, with the setup of Theorem 5.21, for all $0 < \varepsilon < 1/4$ we have

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

Proof. As for the first assertion, it is sufficient to follow the proof of Theorem 5.2, making use of Theorem 5.26 instead of Theorem 5.1. This yields

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

We may conclude by taking $a = 1/(k-1-\eta)$ (with η, ε sufficiently small). The second assertion is a direct consequence of Theorem 5.26. □

5.8 Numerical data

In this section we provide several examples of densities computed with the formulas of Theorems 5.18, 5.20 and 5.23. All values have been verified with SageMath [57] by computing the approximated density that considers only primes up to a certain bound. The Sage codes used to compute the density formulas have been partly adapted from Sebastiano Tronto's code *kummer-degrees*, available on GitHub. In particular, we have tested these formulas for K and G as in the several numerical examples from [39, 10, 40, 37, 36] (notice that in [10, 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 5.18. In Tables 5.1-5.4 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 5.1: 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 5.2: 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 5.3: 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 5.4: Examples of densities ϱ_m with $K = \mathbb{Q}(\zeta_4)$

Recall the notation β_k from Theorem 5.20 (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 (5.30). In Table 5.5 we show some values for these constants $A_{k,r}$, approximated by considering only the primes ℓ up to 10^5. In Tables 5.6 and 5.7 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 5.5: 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 5.6: 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 5.7: Examples of densities β_k over $K = \mathbb{Q}(\zeta_4)$

Finally, recall the notation $\gamma_{k,m}$ from Theorem 5.23 (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 5.8 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 5.8: Examples of densities $\gamma_{k,m}$ over $K = \mathbb{Q}(\sqrt{-5})$

Bibliography

[1] H. Abdullah, A. Ali Mustafa, and F. Pappalardi. Density of the quasi r-rank Artin problem. *Funct. Approx. Comment. Math.*, 65(1):73 – 93, 2021.

[2] D. Bertrand. Galois representations and transcendental numbers. In *New advances in transcendence theory (Durham, 1986)*, pages 37–55. Cambridge Univ. Press, Cambridge, 1988.

[3] D. Bertrand. Galois descent in Galois theories. In *Arithmetic and Galois theories of differential equations*, volume 23 of *Sémin. Congr.*, pages 1–24. Soc. Math. France, Paris, 2011.

[4] J. Buchmann. Complexity of algorithms in algebraic number theory. In *Number theory (Banff, AB, 1988)*, pages 37–53. de Gruyter, Berlin, 1990.

[5] K. Chinen and L. Murata. On a distribution property of the residual order of $a \pmod p$. I. *J. Number Theory*, 105(1):60–81, 2004.

[6] K. Chinen and L. Murata. On a distribution property of the residual order of $a \pmod p$. III. *J. Math. Soc. Japan*, 58(3):693–720, 2006.

[7] K. Chinen and L. Murata. On a distribution property of the residual order of $a \pmod p$. IV. In *Number theory*, volume 15 of *Dev. Math.*, pages 11–22. Springer, New York, 2006.

[8] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[9] G. Cooke and P. J. Weinberger. On the construction of division chains in algebraic number rings, with applications to SL_2. *Comm. Algebra*, 3:481–524, 1975.

[10] C. Debry and A. Perucca. Reductions of algebraic integers. *J. Number Theory*, 167:259–283, 2016.

[11] M. D. Fried and M. Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.

[12] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. The Clarendon Press, Oxford University Press, New York, fifth edition, 1979.

[13] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)*, 37(145):27–38, 1986.

[14] M. Hindry. Autour d'une conjecture de Serge Lang. *Invent. Math.*, 94(3):575–603, 1988.

[15] M. Hindry and J. H. Silverman. *Diophantine geometry: An introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[16] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[17] F. Hörmann, A. Perucca, P. Sgobba, and S. Tronto. Explicit Kummer theory for quadratic fields. *JP J. Algebra, Number Theory Appl.*, 49(2):151–178, 2021.

[18] F. Hörmann, A. Perucca, P. Sgobba, and S. Tronto. Explicit Kummer generators for cyclotomic extensions. *JP J. Algebra, Number Theory Appl.*, 53(1):69–84, 2022.

[19] S. Hu, M.-S. Kim, P. Moree, and M. Sha. Irregular primes with respect to Genocchi numbers and Artin's primitive root conjecture. *J. Number Theory*, 205:59–80, 2019.

[20] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464, 1977.

[21] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[22] A. K. Lenstra. Factoring polynomials over algebraic number fields. In *Computer algebra (London, 1983)*, volume 162 of *Lecture Notes in Comput. Sci.*, pages 245–254. Springer, Berlin, 1983.

[23] A. K. Lenstra. Factoring radicals. In *Colloquium Lectures, AMS 112th Annual Meeting, San Antonio, January 12–15*. 2006.

[24] K. R. Matthews. A generalisation of Artin's conjecture for primitive roots. *Acta Arith.*, 29:113–146, 1976.

[25] H. L. Montgomery and R. C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

[26] P. Moree. On primes p for which d divides $\mathrm{ord}_p(g)$. *Funct. Approx. Comment. Math.*, 33:85–95, 2005.

[27] P. Moree. On the distribution of the order and index of $g \pmod p$ over residue classes. I. *J. Number Theory*, 114(2):238–271, 2005.

[28] P. Moree. On the distribution of the order and index of $g \pmod p$ over residue classes. II. *J. Number Theory*, 117(2):330–354, 2006.

[29] P. Moree. On the distribution of the order and index of $g \pmod p$ over residue classes. III. *J. Number Theory*, 120(1):132–160, 2006.

[30] P. Moree. On the distribution of the order over residue classes. *Electron. Res. Announc. Amer. Math. Soc.*, 12:121–128, 2006.

[31] P. Moree. Artin's primitive root conjecture—a survey. *Integers*, 12(6):1305–1416, 2012.

[32] P. Moree and P. Sgobba. Prime divisors of ℓ-Genocchi numbers and the ubiquity of Ramanujan-style congruences of level ℓ. Preprint, `http://hdl.handle.net/10993/51204`, 2022.

[33] L. Murata and K. Chinen. On a distribution property of the residual order of $a \pmod p$. II. *J. Number Theory*, 105(1):82–100, 2004.

[34] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[35] W. J. Palenstijn. *Radicals in arithmetic*. PhD thesis, University of Leiden, 2014.

[36] F. Pappalardi. Square free values of the order function. *New York J. Math.*, 9:331–344, 2003.

[37] F. Pappalardi. Divisibility of reduction in groups of rational numbers. *Math. Comp.*, 84(291):385–407, 2015.

[38] A. Perucca. Prescribing valuations of the order of a point in the reductions of abelian varieties and tori. *J. Number Theory*, 129(2):469–476, 2009.

[39] A. Perucca. The order of the reductions of an algebraic integer. *J. Number Theory*, 148:121–136, 2015.

[40] A. Perucca. Reductions of algebraic integers II. In *Women in numbers Europe II*, volume 11 of *Assoc. Women Math. Ser.*, pages 19–33. Springer, 2018.

[41] A. Perucca. Multiplicative order and Frobenius symbol for the reductions of number fields. In *Research directions in number theory—Women in Numbers IV*, volume 19 of *Assoc. Women Math. Ser.*, pages 161–171. Springer, Cham, 2019.

[42] A. Perucca and F. Perissinotto. Kummer theory for multiquadratic or quartic cyclic number fields. Preprint, submitted for publication, `http://hdl.handle.net/10993/46603`, 2021.

[43] A. Perucca and P. Sgobba. Kummer theory for number fields and the reductions of algebraic numbers. *Int. J. Number Theory*, 15(8):1617–1633, 2019.

[44] A. Perucca and P. Sgobba. Kummer theory for number fields and the reductions of algebraic numbers II. *Unif. Distrib. Theory*, 15(1):75–92, 2020.

[45] A. Perucca, P. Sgobba, and S. Tronto. Addendum to: Reductions of algebraic integers [J. Number Theory 167 (2016) 259–283]. *J. Number Theory*, 209:391–395, 2020.

[46] A. Perucca, P. Sgobba, and S. Tronto. Explicit Kummer theory for the rational numbers. *Int. J. Number Theory*, 16(10):2213–2231, 2020.

[47] A. Perucca, P. Sgobba, and S. Tronto. The degree of Kummer extensions of number fields. *Int. J. Number Theory*, 17(5):1091–1110, 2021.

[48] A. Perucca, P. Sgobba, and S. Tronto. Divisibility parameters and the degree of Kummer extensions of number fields. *Unif. Distrib. Theory*, 16(2):71–88, 2021.

[49] A. Perucca, P. Sgobba, and S. Tronto. Kummer theory for number fields via entanglement groups. *Manuscripta Math.*, 169:251–270, 2022.

[50] K. A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.

[51] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[52] A. Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arith.*, 32(3):245–274, 1977.

[53] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[54] P. Sgobba. Divisibility conditions on the order of the reductions of algebraic numbers. Preprint, submitted for publication, `https://arxiv.org/abs/2110.08911`, 2021.

[55] P. Sgobba. On the distribution of the order and index for the reductions of algebraic numbers. *J. Number Theory*, 223:132–152, 2021.

[56] H. M. Stark. Some effective cases of the Brauer-Siegel theorem. *Invent. Math.*, 23:135–152, 1974.

[57] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2021. `https://www.sagemath.org`.

[58] K. Wiertelak. On the density of some sets of primes. IV. *Acta Arith.*, 43(2):177–190, 1984.

[59] V. Ziegler. On the distribution of the order of number field elements modulo prime ideals. *Unif. Distrib. Theory*, 1(1):65–85, 2006.

Acknowledgments

First of all, I would like to thank my supervisor Antonella Perucca for accepting me as a PhD student and for supervising my work during these years. I am grateful to her for introducing me to beautiful problems in number theory, for pushing me to be curious in our research area, and for teaching me what it means to be a researcher in mathematics. I thank Antonella also for her constant support and for her valuable help and feedback throughout my PhD.

I would like to express my sincere gratitude to the other members of my PhD defense committee, not only for accepting to evaluate my work, but also for their feedback and the mathematical exchanges. I thank Gabor Wiese for his continuous support and help, and for stimulating my interest in number theory since the beginning of my university studies in Luxembourg. I thank Peter Stevenhagen for being a member of my CET and for his constant feedback and advice over the years. I thank Pieter Moree for the several meetings in Luxembourg and for our fruitful collaborations. He pointed out some improvements to my work, such as on the error term of Theorem 5.10. I thank Francesco Pappalardi for welcoming me at the University Roma Tre in 2018, for suggesting the main problem of Chapter 5 and for many helpful discussions (Remark 5.14 is due to him).

I would like to thank Paul Pollack for our discussions while attending a summer camp in China and for the subsequent exchanges. In particular, I thank him for his considerable help with the results of Section 4.2. I would like to thank Leo Murata for the useful meetings during his visit in Luxembourg and for his encouragement. I thank Gerard van der Geer for his beautiful lectures and the nice conversations during his regular stays in Luxembourg.

Next, I would like to thank all the members of the research group in number theory at the University of Luxembourg for contributing to such a nice mathematical and social environment. In particular, I thank Sebastiano for our countless discussions, for our collaborations and for sharing the journey of our PhDs from the very beginning. I thank Bryan for being such a great friend and colleague, for his mathematical feedback and for all the nice time spent together. I thank Flavio for our conversations, while working in the same research area and sharing the same office. Thanks to Emiliano for all his advice and encouragement, and for being a great older brother in my PhD life. I also thank Alexandre, Andrea, Lassina, Luca, Mariagiulia, Daniel and all other members of our research group.

Thanks to Oskar for being not just a colleague, but also a supportive and caring friend. Thanks to Robert and Guenda, whom I have shared my office with for a long part of my PhD. Thanks to all other members of our department, among which I specially thank Hanh, Minh, Nina, Thilo, Alisa, Massimo, Shiwi and Pallavi. I also thank the secretaries of our department, Katharina Heil and Marie Leblanc, as well as the secretary of our doctoral program, Catherine Violet, for their constant help and for their kindness and efficiency.

I would also like to thank Yujuan and Ariane, two special friends and colleagues from other departments at the University of Luxembourg, for sharing their experience as PhD students with me and for their reliability over the years.

Finally, I would like to thank my parents Mimmo and Rosa, and my sister Enrica, for always believing in me and supporting me. I am deeply grateful to them for the opportunity to live and study in Luxembourg, which has shaped my life and the person I am today.