KUMMER THEORY FOR NUMBER FIELDS AND THE REDUCTIONS OF ALGEBRAIC NUMBERS

ANTONELLA PERUCCA AND PIETRO SGOBBA

ABSTRACT. For all number fields the failure of maximality for the Kummer extensions is bounded in a very strong sense. We give a direct proof (without relying on the Bashmakov-Ribet method) of the fact that if G is a finitely generated and torsion-free multiplicative subgroup of a number field K having rank r, then the ratio between n^r and the Kummer degree $[K(\zeta_n, \sqrt[n]{G}) : K(\zeta_n)]$ is bounded independently of n. We then apply this result to generalise to higher rank a theorem of Ziegler from 2006 about the multiplicative order of the reductions of algebraic integers (the multiplicative order must be in a given arithmetic progression, and an additional Frobenius condition may be considered).

1. INTRODUCTION

1.1. **Kummer theory.** Consider a number field K and a finitely generated subgroup G of the multiplicative group $K^\times$. We denote by $K(\zeta_n)$ the n-th cyclotomic extension of K and by $K(\zeta_n, \sqrt[n]{G})$ the n-th Kummer extension of K related to G i.e. the smallest extension of K that contains all algebraic numbers whose n-th power lies in G. We prove the following general result:

Theorem 1. *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank r. There is an integer $C \geqslant 1$ (depending only on K and G) such that for all integers $n \geqslant 1$ the ratio $\frac{n^r}{[K(\zeta_n, \sqrt[n]{G}):K(\zeta_n)]}$ is an integer dividing C.*

The Kummer extension $K(\zeta_n, \sqrt[n]{G})/K(\zeta_n)$ has degree at most n^r, so Theorem 1 shows that the failure of maximality for this extension is bounded in a very strong sense. In particular, for all but finitely many prime numbers ℓ and for every integer $e \geqslant 1$ we have

$$[K(\zeta_{\ell^e}, \sqrt[\ell^e]{G}) : K(\zeta_{\ell^e})] = \ell^e \,.$$

As a consequence of Theorem 1 we obtain a similar result for tori:

Corollary 2. *Let T be a torus over a number field K, and let α be a K-point of T that (over the splitting field) can be identified to a tuple of algebraic numbers which multiplicatively generate a torsion-free group of strictly positive rank r. There is an integer $C \geqslant 1$ (depending only on K, T and α) such that for all integers $n, m \geqslant 1$ the ratio $\frac{n^r}{[K_{nm,n}:K_{nm}]}$ is an integer dividing C, where K_{nm} is the nm-torsion field of the torus and $K_{nm,n}$ is the n-th Kummer extension of K_{nm} related to α.*

2010 *Mathematics Subject Classification.* Primary: 11R44; Secondary: 11R18, 11R21, 11N36.
Key words and phrases. Kummer theory, number field, reduction, multiplicative order, density.

Theorem 1 is proven in Section 3: our proof relies on results by the first author and Debry [4] (combined with Theorem 11, proven in Section 2) and on Schinzel's theorem on abelian radical extensions (Theorem 15). Notice that Theorem 1 also holds more generally (under appropriate assumptions on G) for products of abelian varieties and tori: this was stated by Bertrand in [3, Theorem 1]. A proof for abelian varieties was given by Hindry in [5, Lemme 14] and by Bertrand in [2, Theorème 5.2], see also a result by Banaszak, Gajda and Krason [1, proof of Lemma 2.13]. The proof for tori, although probably not to be found in the literature, should work by the same method used for abelian varieties, which is known as the Bashmakov-Ribet method [12]: this is stated (for split tori) at the end of [7, Section 4 of Chapter 5]. Notice that, in the special case that G has rank 1, Theorem 1 has an explicit constant depending only on K and on divisibility properties of G, see [16, Lemma 3] by Ziegler. In the general case, we similarly find that the constant of Theorem 1 depends only on K, on divisibility properties of G, and on the rank of G.

1.2. **Multiplicative order of the reductions of algebraic numbers.** Consider a number field K and a finitely generated subgroup G of the multiplicative group $K^\times$. We tacitly exclude the finitely many primes $\mathfrak{p}$ of K such that the reduction of G is not a well-defined subgroup of the multiplicative group $k_\mathfrak{p}^\times$ (where $k_\mathfrak{p}$ is the residue field at $\mathfrak{p}$). We write $\mathrm{ord}_\mathfrak{p}(G)$ for the size of G modulo $\mathfrak{p}$ and investigate whether this multiplicative order lies in a given arithmetic progression. Note that this kind of questions are related to Artin's Conjecture on primitive roots, see the survey [9] by Moree.

We make use of the following standard notation: μ is the Möbius function; ζ_n is a primitive n-th root of unity; (X, Y) is the greatest common divisor of X and Y, while $[X, Y]$ is the least common multiple; if S is a set of primes of K, then $S(x)$ is the number of elements of S having norm at most x. For a number field extension K'/K, and integers $n, m \geqslant 1$ with n dividing m, we denote by $K'_m := K'(\zeta_m)$ the m-th cyclotomic extension of K', and by $K'_{m,n} := K'(\zeta_m, \sqrt[n]{G})$ the n-th Kummer extension of G over K'_m. 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 theorem [16, Theorem 2].

Theorem 3. *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank. Fix an integer $d \geqslant 2$, fix an integer a, and consider the following set of primes of K:*

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

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

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

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

$$(1 + at, d) = 1 \qquad \text{and} \qquad (d, n) \mid a$$

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

We refine this result by introducing a condition on the Frobenius conjugacy class with respect to a fixed finite Galois extension of the base field:

Theorem 4. *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank. Let F/K be a finite Galois extension, and let C be a conjugacy-stable subset of $\mathrm{Gal}(F/K)$. Fix an integer $d \geqslant 2$, fix an integer a. Considering only the primes $\mathfrak{p}$ of K that do not ramify in F, define*

$$\mathcal{P} := \{\mathfrak{p} : \mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d\,,\ \mathrm{Frob}_{F/K}(\mathfrak{p}) \subseteq C\}\,.$$

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

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

where

$$c(n,t) := \left|\left\{\sigma \in \mathrm{Gal}(F_{[d,n]t,nt}/K) : \sigma|_F \in C, \sigma|_{K_{nt,nt}} = \mathrm{id}, \sigma(\zeta_{dt}) = \zeta_{dt}^{1+at}\right\}\right| \leqslant |C|$$

and in particular $c(n,t)$ is non-zero only if $(1+at, d) = 1$ and $(d,n) \mid a$ hold.

The above theorems imply that the set $\mathcal{P}$ admits a natural density, which is given by the double sum (notice that, since we may reduce to the case of rank 1, by [16, Lemmas 6 and 7] we have absolute convergence for the double sum, so the order of summation does not matter). If G is of rank 1, Theorem 4 is [16, Theorem 1] by Ziegler: the proof given in Section 5 follows closely the one by Ziegler, and relies on Theorem 1 (in the equivalent form of Theorem 13) and Theorem 23. Notice that there are also unconditional results by the first author [11] prescribing the ℓ-adic valuation of $\mathrm{ord}_{\mathfrak{p}}(G)$ for finitely many prime numbers ℓ, and requiring the Frobenius condition.

2. Strongly independent elements

With the usual notation: K is a number field, $K^\times$ is the multiplicative group, $\mathcal{O}_K$ is the ring of integers, $\mathcal{O}_K^\times$ is the group of units of $\mathcal{O}_K$, and μ_K is the group of roots of unity in K.

2.1. Notions of independence.

Definition 5. *If ℓ is a prime number, we call $a \in K^\times$* strongly ℓ–indivisible *if there is no root of unity $\zeta \in \mu_K$ (whose order we may suppose to be a power of ℓ) such that $a\zeta \in (K^\times)^\ell$. 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.*

Strongly ℓ–independent elements are each strongly ℓ–indivisible, and for a single element the two notions coincide. If $\zeta_\ell \notin K$, then strongly ℓ–indivisible just means not being an ℓ-th power.

Lemma 6. *If finitely many vectors with integer coefficients are linearly independent over $\mathbb{Z}$, then for all but finitely many prime numbers ℓ they are linearly independent over $\mathbb{Z}/\ell^n\mathbb{Z}$ for every $n \geqslant 1$ (i.e. if we reduce the vectors modulo ℓ^n, then a linear combination with coefficients in $\mathbb{Z}/\ell^n\mathbb{Z}$ can be zero only if all coefficients are zero).*

Proof. Let M be the matrix with integral entries associated to the considered finitely many vectors. If a minor d of M is non-zero, then d is invertible modulo ℓ for all but finitely many prime numbers ℓ, and it is also invertible modulo ℓ^n for every $n \geqslant 1$. □

Lemma 7. *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank. If there is a $\mathbb{Z}$-basis of G whose elements are strongly ℓ-independent for all but finitely many prime numbers ℓ, then any $\mathbb{Z}$-basis has this property.*

Proof. Let $\{b_j\}_{1\leqslant j\leqslant r}$ be a $\mathbb{Z}$-basis of G, and let ℓ be a prime number such that the elements b_j are strongly ℓ-independent. If $\{a_i\}_{1\leqslant i\leqslant r}$ is another $\mathbb{Z}$-basis of G, we can write

$$a_i = \prod_{j=1}^{r} b_j^{e_{ij}}$$

for some integers e_{ij} such that the vectors $v_i := (e_{ij})$ are linearly independent over $\mathbb{Z}$. Up to discarding finitely many ℓ, we may assume that the vectors v_i are linearly independent over $\mathbb{Z}/\ell\mathbb{Z}$ (cf. Lemma 6), and also that $\zeta_\ell \notin K$. Suppose that for some integers x_i the product

$$a := \prod_{i=1}^{r} a_i^{x_i} = \prod_{j=1}^{r} b_j^{\sum_{i=1}^{r} x_i e_{ij}}$$

is an ℓ-th power in K. Since the elements b_j are strongly ℓ-independent, we know that ℓ divides $\sum_{i=1}^{r} x_i e_{ij}$ for all j. Thus ℓ divides x_i for all i because the vectors v_i are linearly independent over $\mathbb{Z}/\ell\mathbb{Z}$. □

From [4, page 7] we may deduce (less directly) the following stronger assertion: if there exists a basis of G consisting of strongly ℓ-independent elements and $\zeta_\ell \notin K$, then any basis of G consists of strongly ℓ-independent elements.

2.2. **Divisibility results.**

Lemma 8. *Let G be a finitely generated subgroup of $K^\times$ satisfying $G \cap \mathcal{O}_K^\times = \{1\}$ and having strictly positive rank. Then for all but finitely many prime numbers ℓ the following holds: if $g \in G$ is an ℓ^n-th power in K times a unit, then g is an ℓ^n-th power in G, for every $n \geqslant 1$.*

Proof. Fix a $\mathbb{Z}$-basis $\{g_1, \dots, g_r\}$ of G, and let $\{\mathfrak{p}_j\}_{1\leqslant j\leqslant k}$ be the finite set of prime ideals appearing in the factorisation of some principal fractional ideal (g_i), $i = 1, \dots, r$. Thus we can write

$$(g_i) = \prod_{j=1}^{k} \mathfrak{p}_j^{e_{ij}}$$

for some integers e_{ij}. The vectors $v_i := (e_{ij})$ for $1 \leqslant i \leqslant r$ are linearly independent over $\mathbb{Z}$. Indeed, if for some integers z_i we have $\sum_{i=1}^{r} z_i v_i = 0$, we deduce that

$$\Big(\prod_{i=1}^{r} g_i^{z_i}\Big) = \prod_{j=1}^{k} \mathfrak{p}_j^{\sum_{i=1}^{r} z_i e_{ij}} = (1)$$

and hence $z_i = 0$ for every i (because G contains no units apart from 1). Let $g \in G$: writing $g = \prod_{i=1}^r g_i^{x_i}$ for some integers x_i, we have

$$(g) = \prod_{j=1}^k \mathfrak{p}_j^{\sum_{i=1}^r x_i e_{ij}}.$$

So, if g is an ℓ^n-th power in K times a unit, then ℓ^n divides $\sum_{i=1}^r x_i e_{ij}$ for every j. For all but finitely many ℓ the vectors v_i are linearly independent over $\mathbb{Z}/\ell^n\mathbb{Z}$ by Lemma 6 and we deduce that ℓ^n divides x_i for every i. Thus g is an ℓ^n-th power in G. □

Lemma 9. *Let H be a subgroup of $\mathcal{O}_K^\times$. Then for all but finitely many prime numbers ℓ and for every $n \geqslant 1$ the following holds: if $h \in H$ is an ℓ^n-th power in K, then h is an ℓ^n-th power in H (in other words, we have $H \cap K^{\ell^n} \subseteq H^{\ell^n}$).*

Proof. By Dirichlet's Unit Theorem we can write $\mathcal{O}_K^\times = \mu_K \times \langle b_1, \dots, b_k \rangle$ where $\{b_i\}_{1 \leqslant i \leqslant k}$ is a fundamental system of units. By Lemma 10 we may suppose that H is contained in the free group $F := \langle b_1, \dots, b_k \rangle$. The group H has then a $\mathbb{Z}$-basis $\{h_i\}_{1 \leqslant i \leqslant r}$ where $r \leqslant k$, and each h_i can be uniquely written as

$$h_i = \prod_{j=1}^k b_j^{e_{ij}} \tag{2}$$

for some integers e_{ij}. If $h \in H$ is an ℓ^n-th power in K then, being a unit, it is an ℓ^n-th power in $\mathcal{O}_K^\times$. Since $h \in F$, there is also an ℓ^n-th root of h inside F, so we can write

$$h = \prod_{j=1}^k b_j^{\ell^n x_j} \tag{3}$$

for some integers x_j. Recalling (2), we also have

$$h = \prod_{i=1}^r h_i^{y_i} = \prod_{j=1}^k b_j^{\sum_{i=1}^r e_{ij} y_i} \tag{4}$$

for some integers y_i. Comparing (3) and (4), we deduce that ℓ^n divides $\sum_{i=1}^r e_{ij} y_i$ for every j. The vectors $v_i := (e_{ij})$ for $1 \leqslant i \leqslant r$ are linearly independent over $\mathbb{Z}$ and hence by Lemma 6 they are also linearly independent over $\mathbb{Z}/\ell^n\mathbb{Z}$ for all but finitely many prime numbers ℓ: in this case ℓ^n divides y_i for every i and hence h is an ℓ^n-th power in H. □

Lemma 10. *Let H be a subgroup of $\mathcal{O}_K^\times$, and let $\tilde{H} \subseteq H$ be a subgroup of finite index. For all integers $n \geqslant 1$ coprime to this index, the property $\tilde{H} \cap K^n \subseteq \tilde{H}^n$ implies the property $H \cap K^n \subseteq H^n$.*

Proof. Suppose that $\tilde{H} \cap K^n \subseteq \tilde{H}^n$ holds, and call $m := [H : \tilde{H}]$. If $\alpha \in H \cap K^n$, then $\alpha^m \in \tilde{H} \cap K^n$. So we know that $\alpha^m \in \tilde{H}^n$ and hence there is $\beta \in H$ such that $\alpha^m = \beta^n$. Since n and m are coprime, there are integers x, y with $nx + my = 1$. Thus we can write $\alpha = (\alpha^x \beta^y)^n$, which yields $\alpha \in H^n$. □

2.3. **Basis with strongly ℓ-independent elements.**

Theorem 11. *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank. Then there is a $\mathbb{Z}$-basis of G whose elements are strongly ℓ-independent for all but finitely many prime numbers ℓ.*

Proof. Writing $H := G \cap \mathcal{O}_K^\times$, the quotient G/H is clearly finitely generated, and it is torsion-free (because if the power of an element is a unit, then the element itself is a unit). Thus G/H is free, and there is a finitely generated and torsion-free subgroup F of G such that $F \cap \mathcal{O}_K^\times = \{1\}$ and $G = F \times H$. Take a $\mathbb{Z}$-basis of G consisting of a $\mathbb{Z}$-basis $\{g_i\}_{1 \leqslant i \leqslant r}$ of F and of a $\mathbb{Z}$-basis $\{u_j\}_{1 \leqslant j \leqslant r'}$ of H. Let $g \in G$, and express it with respect to the given basis:

$$g = \prod_{i=1}^{r} g_i^{x_i} \cdot \prod_{j=1}^{r'} u_j^{y_j} \,. \tag{5}$$

If g is an ℓ-th power in K (where ℓ is a prime number), then $f := \prod g_i^{x_i} \in F$ is an ℓ-th power in K times a unit hence by Lemma 8 (for all but finitely many ℓ) it is an ℓ-th power in F. We deduce that $h := \prod u_j^{y_j} \in H$ is an ℓ-th power in K hence by Lemma 9 (for all but finitely many ℓ) it is an ℓ-th power in H. Up to discarding finitely many ℓ, we have found that all exponents in (5) are divisible by ℓ, and we may suppose $\zeta_\ell \notin K$. So the elements of the given basis of G are strongly ℓ-independent. □

In fact *any* $\mathbb{Z}$-basis of G consists of elements that are strongly ℓ-independent for almost all ℓ:

Theorem 12. *Let K be a number field. If $\alpha_1, \ldots, \alpha_r \in K$ generate a torsion-free subgroup of $K^\times$ of rank r, then they are strongly ℓ-independent for all but finitely many prime numbers ℓ.*

Proof. It suffices to combine Theorem 11 and Lemma 7. □

3. On the maximality of Kummer extensions

Fix a finitely generated and torsion-free subgroup G of $K^\times$ of strictly positive rank. If $x, y \geqslant 1$ are integers such that $y \mid x$, then as usual K_x is the x-th cyclotomic extension of K, and we denote by $K_{x,y} := K_x(\sqrt[y]{G})$ the y-th Kummer extension of G over K_x. The aim of this section is proving the following result (which for $m = 1$ gives Theorem 1):

Theorem 13. *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank r. There is an integer $C \geqslant 1$ (depending only on K and G) such that for all integers $n, m \geqslant 1$ the ratio $\frac{n^r}{[K_{nm,n} : K_{nm}]}$ divides C.*

Lemma 14. *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank r. If ℓ is a prime number, then there is some integer $A_\ell \geqslant 1$ which is a power of ℓ (depending only on K and G) such that for every integer $n \geqslant 1$ the ratio $\frac{\ell^{nr}}{[K_{\ell^n,\ell^n} : K_{\ell^n}]}$ is an integer dividing A_ℓ. Moreover, A_ℓ equals 1 for all but finitely many ℓ.*

Proof. We know that A_ℓ exists for every ℓ because by [4, Section 3.3] we have the eventual maximal growth in n of the ℓ^n-th Kummer extension over K_{ℓ^n}. For all but finitely many ℓ, by

Theorem 11 there is a $\mathbb{Z}$-basis of G consisting of strongly ℓ-independent elements and hence by [4, Section 3.3] (for $\ell \neq 2$) we can take $A_\ell = 1$. □

Theorem 15 (Schinzel [13, Thm. 2], with an alternative proof in [8, 15])**.** *Let K be a number field, and let $a \in K^\times$. If $N \geqslant 1$ is an integer, then the extension $K_N(\sqrt[N]{a})/K$ is abelian if and only if $a^T = b^N$ holds for some $b \in K^\times$ and for some divisor T of N satisfying $K = K_T$.*

Corollary 16. *Let K be a number field, let ℓ be a prime number, and call τ the largest integer satisfying $K = K_{\ell^\tau}$. Fix an integer $n \geqslant 1$.*

(i) *Let $a \in K^\times$. If the extension $K_{\ell^n}(\sqrt[\ell^n]{a})/K$ is abelian, then its relative degree over K_{ℓ^n} divides ℓ^τ.*
(ii) *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank r. An abelian subextension of $K_{\ell^n,\ell^n}/K$ that contains K_{ℓ^n} has a relative degree over K_{ℓ^n} which divides $\ell^{\tau r}$.*

Proof. We may clearly suppose that $n \geqslant \tau$. The first assertion is immediate by the special case of prime powers in Theorem 15. Now consider the second assertion. By Kummer theory the Galois group of the given abelian extension over K_{ℓ^n} is the product of at most r cyclic ℓ-groups. If the assertion is false, then there is a cyclic quotient of degree $\ell^{\tau+1}$ and hence there is a cyclic extension of K_{ℓ^n} of degree $\ell^{\tau+1}$ which is abelian over K. By Kummer theory this is of the form $K_{\ell^n}(\sqrt[\ell^n]{a})$ for some $a \in K^\times$, contradicting (i). □

Lemma 17. *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank. If ℓ is a prime number, then there is some integer $B_\ell \geqslant 1$ which is a power of ℓ (depending only on K and G) such that for every integer $n, m \geqslant 1$ we have*

$$\frac{[K_{\ell^n,\ell^n} : K_{\ell^n}]}{[K_{\ell^n m,\ell^n} : K_{\ell^n m}]} \mid B_\ell \,.$$

We can take $B_\ell = \ell^{\tau r}$, where τ is the largest integer satisfying $K = K_{\ell^\tau}$ (even though this is not necessarily optimal). In particular, we may take $B_\ell = 1$ for all but finitely many ℓ (for example, if $\zeta_\ell \notin K$).

Proof. The intersection of the fields K_{ℓ^n,ℓ^n} and $K_{\ell^n m}$ is an abelian extension of K (it is contained in a cyclotomic extension) so by Corollary 16 (ii) its degree over K_{ℓ^n} divides $\ell^{\tau r}$ (and $\tau = 0$ if $\zeta_\ell \notin K$). □

Proof of Theorem 13. It suffices to prove that for every prime number ℓ there is an integer $C_\ell \geqslant 1$ that equals 1 for almost all ℓ, and that satisfies

$$\frac{\ell^{er}}{[K_{\ell^e h,\ell^e} : K_{\ell^e h}]} \mid C_\ell \tag{6}$$

for all integers $e, h \geqslant 1$ with h coprime to ℓ. Indeed, since Kummer extensions related to powers of distinct primes have coprime degrees, we may take $C := \prod_\ell C_\ell$. Notice that we may suppose that h and ℓ are coprime because if $m = h\ell^{e'}$ and $E = e + e'$ for some integer

$e' \geqslant 0$, then we have $\ell^E h = \ell^e m$ and (since a bound for the failure of maximality for the ℓ^E-Kummer extension is also a bound for the ℓ^e-Kummer extension) the following holds:

$$\frac{\ell^{Er}}{[K_{\ell^E h,\ell^E} : K_{\ell^E h}]} \mid C_\ell \qquad \Rightarrow \qquad \frac{\ell^{er}}{[K_{\ell^e m,\ell^e} : K_{\ell^e m}]} \mid C_\ell \,.$$

By Lemmas 14 and 17 we may set $C_\ell := A_\ell \cdot B_\ell$, where the integers A_ℓ and B_ℓ equal 1 for almost all ℓ, are independent of $e, h \geqslant 1$ (where h is coprime to ℓ), and satisfy

$$\frac{\ell^{er}}{[K_{\ell^e,\ell^e} : K_{\ell^e}]} \mid A_\ell \qquad \text{and} \qquad \frac{[K_{\ell^e,\ell^e} : K_{\ell^e}]}{[K_{\ell^e h,\ell^e} : K_{\ell^e h}]} \mid B_\ell \,.$$

□

Remark 18. *Theorem 1 is a special case of Theorem 13, and the two results are in fact equivalent. Indeed, by Theorem 1 the ratio between $(nm)^r$ and $[K_{nm,nm} : K_{nm}]$ divides C, and the degree of the m-th Kummer extension $K_{nm,nm}/K_{nm,n}$ clearly divides m^r. We deduce that the ratio between n^r and $[K_{nm,n} : K_{nm}]$ divides C.*

Proof of Corollary 2. Up to multiplying C by a finite positive integer, we may replace K by the splitting field and then apply Theorem 13. □

Remark 19. *In Theorem 13 (and hence also in Corollary 2) we could remove the assumption "torsion-free". Indeed, if $G = \langle \zeta_t \rangle \times G'$ where $t \geqslant 1$ and where G' is a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank, then we have $K_{mn}(\sqrt[n]{G}) = K_{[m,t]n}(\sqrt[n]{G'})$ and hence*

$$[K_{mn}(\sqrt[n]{G}) : K_{mn}] = [K_{[m,t]n}(\sqrt[n]{G'}) : K_{[m,t]n}] \cdot [K_{[m,t]n} : K_{mn}] \,.$$

The degree of the Kummer extension for G' is evaluated in Theorem 13. The degree of the cyclotomic extension is at most t (for example it is 1 if n is coprime to t).

Remark 20. *To compute a constant C for Theorem 13, recall from its proof that we may take $C = \prod_\ell A_\ell \cdot B_\ell$, where A_ℓ is as in Lemma 14, and where B_ℓ is as in Lemma 17 (with the further restriction that m is coprime to ℓ). Notice that if A_ℓ and B_ℓ as above are optimal, then C is also optimal. Choose a $\mathbb{Z}$-basis of G: for all but finitely many prime numbers ℓ, the elements of the basis are strongly ℓ-independent and hence (for $\ell \neq 2$) we have $A_\ell = 1$ by* [4, Theorem 18]*; for the remaining finitely many ℓ we can apply the results of* [4] *to evaluate the Kummer degrees and determine the optimal A_ℓ. If $\zeta_\ell \notin K$, then $B_\ell = 1$. For the remaining finitely many ℓ, by Lemma 17 we may take $B_\ell = \ell^{\tau r}$ (this may not be the optimal value for B_ℓ though).*

Example 21. We follow the strategy outlined in the previous remark. Consider the subgroup G of $\mathbb{Q}^\times$ with $\mathbb{Z}$-basis $\{3, 5\}$. These elements are clearly strongly ℓ-independent for every prime number ℓ and hence $A_\ell = 1$ for $\ell \neq 2$. By results on the Gaussian integers they are also strongly 2-independent over $\mathbb{Q}(\zeta_4)$ and hence $A_2 = 1$. For $\ell \neq 2$ we have $B_\ell = 1$, and we may take $B_2 = 4$. Since we have $\mathbb{Q}(\zeta_{60}, \sqrt{G}) = \mathbb{Q}(\zeta_{60})$, the value $C = 4$ is optimal. This example can be generalised as follows: if G is generated by r distinct odd prime numbers, then $C = 2^r$ is optimal ($A_\ell = 1$ for all ℓ, $B_\ell = 1$ for all $\ell \neq 2$, and $B_2 = 2^r$). If we replace one of the generators by 2, then again $C = 2^r$ is optimal. Now $A_2 = 2$ is optimal (we have to take into

account that $\sqrt{2} \in \mathbb{Q}(\zeta_8)$). Moreover, we may take $B_2 = 2^r$. The ratio in Lemma 17 for $n = 1$ already attains the maximal value 2^r with $n = 1$ and with $m = 4\prod_p p$, where the product runs over the odd prime generators of G. However, one of the factors 2 is due to A_2 and hence we may take $C = 2^r$.

4. Estimates for the relative discriminant

The aim of this section is proving Theorem 23, which is an estimate for the discriminant of a cyclotomic/Kummer extension of a given number field: we first recall some basic facts from [10]. Let L/K be a finite extension of number fields, and denote by $N_{L/K}$ the relative norm for fractional ideals of L, which is multiplicative. If $a \in \mathcal{O}_L$, then we define the *relative different* $\delta_{L/K}(a)$ of a to be $f'(a)$ (where f is the minimal polynomial of a over K) if $L = K(a)$, and zero otherwise. We see the *relative different* $\mathcal{D}_{L/K}$ of L/K as the ideal of $\mathcal{O}_L$ generated by $\delta_{L/K}(a)$ for $a \in \mathcal{O}_L$. The *relative discriminant* $d_{L/K}$ of L/K is the ideal of $\mathcal{O}_K$ which is generated by the discriminants $d(\beta_1, \dots, \beta_n)$ of all bases $\beta_1, \dots, \beta_n$ of L/K which are contained in $\mathcal{O}_L$. It is the norm of the relative different, namely $d_{L/K} = N_{L/K}(\mathcal{D}_{L/K})$. We call d_K the *absolute discriminant* of K. For a tower of number fields $K'' \supset K' \supset K$ we have the chain relation of the norm $N_{K''/K} = N_{K'/K} \circ N_{K''/K'}$. We also have the chain relation of relative differents

$$\mathcal{D}_{K''/K} = \mathcal{D}_{K''/K'}\mathcal{D}_{K'/K} \tag{7}$$

and hence the following relation of relative discriminants

$$d_{K''/K} = N_{K'/K}(d_{K''/K'}) \cdot d_{K'/K}^{[K'':K']}\,. \tag{8}$$

Lemma 22. *Let L be a finite extension of a number field K. If L_1 and L_2 are two subextensions of L with compositum L, then we have:*

(i) *for the relative differents, the containment $\mathcal{D}_{L_2/K}\mathcal{O}_L \subseteq \mathcal{D}_{L/L_1}$;*
(ii) *for the relative discriminants, the divisibility relation*

$$d_{L/K} \mid d_{L_1/K}^{[L:L_1]} \cdot d_{L_2/K}^{[L:L_2]}\,.$$

(iii) *If $L_1, \dots, L_n$ are subextensions of L with compositum L, then we have for the relative discriminants the divisibility relation*

$$d_{L/K} \mid \prod_{i=1}^{n} d_{L_i/K}^{[L:L_i]}\,.$$

Proof. To prove the first assertion, fix $a \in \mathcal{O}_{L_2}$ such that $L_2 = K(a)$, and write $\delta_{L_2/K}(a) = f'(a)$ where f is the minimal polynomial of a over K. Since $a \in \mathcal{O}_L$, its minimal polynomial g over L_1 divides f. By the Gauss Lemma we have $f = gh$ for some monic polynomial h with coefficients in $\mathcal{O}_{L_1}$. Thus $f'(a) = g'(a)h(a)$ is an element of $\mathcal{D}_{L/L_1}$ because $h(a) \in \mathcal{O}_L$ and because $L = L_1(a)$ implies $g'(a) = \delta_{L/L_1}(a)$.

The third assertion easily follows (by induction) from the second. To prove the latter, by (7) and (i) we have

$$\mathcal{D}_{L/K} = \mathcal{D}_{L/L_1}\mathcal{D}_{L_1/K} \mid \mathcal{D}_{L_1/K}\mathcal{D}_{L_2/K}\mathcal{O}_L\,,$$

and by definition we know $N_{L/K}(\mathcal{D}_{L/K}) = d_{L/K}$. Since the norm is multiplicative, by a straightforward computation we obtain

$$N_{L/K}(\mathcal{D}_{L_1/K}\mathcal{D}_{L_2/K}\mathcal{O}_L) = d_{L_1/K}^{[L:L_1]} \cdot d_{L_2/K}^{[L:L_2]}\,.$$

□

We will make use of the formula

$$\prod_{\substack{1\leqslant i,j\leqslant n\\ i\neq j}} (\zeta_n^i - \zeta_n^j) = (-1)^{n-1}n^n\,, \tag{9}$$

which can be shown by an easy computation considering the derivative of the polynomial $X^n - 1 = \prod_{j=1}^n (X - \zeta_n^j)$ and evaluating it at ζ_n^i for each $1 \leqslant i \leqslant n$.

Theorem 23 (cf. [16, Lemma 5])**.** *Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of strictly positive rank r. For all integers $m, n \geqslant 1$ we have*

$$\frac{\log\left|d_{K_{nm,n}}\right|}{n^r\varphi(nm)} \leqslant [K:\mathbb{Q}]((r+1)\log(n) + \log(m)) + O(1)\,.$$

In particular, for every integer $t \geqslant 1$ we have

$$\frac{\log\left|d_{K_{t,t}}\right|}{t^r\varphi(t)} \leqslant [K:\mathbb{Q}](r+1)\log(t) + O(1)\,.$$

Choose a $\mathbb{Z}$-basis $\gamma_1, \dots, \gamma_r$ of G and, for $1 \leqslant i \leqslant r$, write $\gamma_i = \alpha_i/\beta_i$ with $\alpha_i, \beta_i \in \mathcal{O}_K$ (non-zero and not both roots of unity). Then the constant implied by the O-term can be taken to be

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

Proof. Write L_i for the extension of K generated by some fixed root $\sqrt[n]{\gamma_i}$. Since $K_{nm,n}$ is the compositum of K_{nm} and the fields L_i, by Lemma 22 (iii) we have

$$d_{K_{nm,n}/K} \mid (d_{K_{nm}/K})^{n^r} \cdot \prod_i (d_{L_i/K})^{n^{r-1}\varphi(nm)}\,. \tag{10}$$

We know $d_{K_{nm}/K} \mid d_{\mathbb{Q}(\zeta_{nm})/\mathbb{Q}}\mathcal{O}_K$ because $\{\zeta_{nm}^i\}$ for $0 \leqslant i < \varphi(nm)$ is a $\mathbb{Z}$-basis of the ring of integers of $\mathbb{Q}(\zeta_{nm})$, while $\{\zeta_{nm}^i\}$ for $0 \leqslant i < [K_{nm}:K]$ is a basis of K_{nm}/K consisting of algebraic integers. We deduce the following estimate (which is not optimal, but it is sufficient for the purpose of the proof):

$$d_{K_{nm}/K} \mid (nm)^{\varphi(nm)}\mathcal{O}_K. \tag{11}$$

Let $\alpha_i, \beta_i \in \mathcal{O}_K$ be as in the statement and notice that the elements $\beta_i(\sqrt[n]{\gamma_i})^j = \sqrt[n]{\alpha_i^j\beta_i^{n-j}}$, with $0 \leqslant j < [L_i : K]$, form a basis of L_i/K which is contained in $\mathcal{O}_{L_i}$. Therefore the discriminant of this basis (which is an element of the relative discriminant $d_{L_i/K}$) divides

$$\beta_i^{2n} \cdot \prod_{1\leqslant j<k\leqslant n} (\sqrt[n]{\gamma_i}\zeta_n^j - \sqrt[n]{\gamma_i}\zeta_n^k)^2 = \alpha_i^{n-1}\beta_i^{n+1} \cdot \prod_{1\leqslant j<k\leqslant n} (\zeta_n^j - \zeta_n^k)^2 \mid (\alpha_i\beta_i)^{2n} \cdot n^n\,,$$

where the latter divisibility follows by (9). We thus have

$$d_{L_i/K} \mid (\alpha_i\beta_i)^{2n} n^n \mathcal{O}_K \tag{12}$$

(which is not an optimal estimate, but again it is sufficient for the purpose of the proof).

Combining (10) with (11) and (12) we obtain

$$d_{K_{nm,n}/K} \mid \left((nm)^{n^r\varphi(nm)} \cdot \prod_{i=1}^{r} \left((\alpha_i\beta_i)^{2n} n^n \right)^{n^{r-1}\varphi(nm)} \right) \mathcal{O}_K \ .$$

Setting $A := \prod_i \alpha_i\beta_i$, we have

$$d_{K_{nm,n}/K} \mid \left((nm)^{n^r\varphi(nm)} \cdot A^{2n^r\varphi(nm)} \cdot n^{rn^r\varphi(nm)} \right) \mathcal{O}_K \ . \tag{13}$$

If I is an ideal of $\mathbb{Z}$, then write $|I|$ for its non-negative generator. By (8) we have

$$\left|d_{K_{nm,n}}\right| = \left|N_{K/\mathbb{Q}}(d_{K_{nm,n}/K})\right| |d_K|^{[K_{nm,n}:K]} \tag{14}$$

and hence applying (13) we can estimate $\log \left|d_{K_{nm,n}}\right|$ from above with the sum of the following four terms:

$$\begin{aligned}
\log \left|N_{K/\mathbb{Q}}((nm)^{n^r\varphi(nm)}\mathcal{O}_K)\right| &= n^r\varphi(nm) \cdot [K:\mathbb{Q}] \cdot \log(nm) \\
\log \left|N_{K/\mathbb{Q}}(A^{2n^r\varphi(nm)}\mathcal{O}_K)\right| &= n^r\varphi(nm) \cdot 2\textstyle\sum_{i=1}^{r} \log \left|N_{K/\mathbb{Q}}(\alpha_i\beta_i)\right| \\
\log \left|N_{K/\mathbb{Q}}(n^{rn^r\varphi(nm)}\mathcal{O}_K)\right| &= n^r\varphi(nm) \cdot [K:\mathbb{Q}] \cdot r\log(n) \\
\log |d_K|^{[K_{nm,n}:K]} &\leqslant n^r\varphi(nm) \cdot \log |d_K| \ .
\end{aligned}$$

We then have

$$\frac{\log \left|d_{K_{nm,n}}\right|}{n^r\varphi(nm)} \leqslant [K:\mathbb{Q}] \left(\log(nm) + r\log(n)\right) + \log|d_K| + 2\sum_{i=1}^{r} \log \left|N_{K/\mathbb{Q}}(\alpha_i\beta_i)\right| \ .$$

□

5. Generalization of Ziegler's proof

The aim of this section is proving Theorem 4: we refer to Theorem 4 for the notation, and to [16, proof of Theorem 1] for the parts of the proof that do not require modifications with respect to the case of rank 1 (a full proof can be found in [14, Chapter 4]). Recall that we assume (GRH).

Step 1: We tacitly exclude the primes of K that ramify in F, and those whose ramification index or inertial degree over $\mathbb{Q}$ is not 1: the excluded primes count as $O\left(\sqrt{x}/\log x\right)$ by [16, Lemma 1]. We also tacitly exclude the finitely many primes $\mathfrak{p}$ of K such that the reduction of G modulo $\mathfrak{p}$ is not a well-defined subgroup of the multiplicative group $k_\mathfrak{p}^\times$. We write $\mathrm{ord}_\mathfrak{p}(G)$ for the size of G modulo $\mathfrak{p}$, and $\mathrm{ind}_\mathfrak{p}(G)$ for its index in $k_\mathfrak{p}^\times$. Since G modulo $\mathfrak{p}$ is cyclic, as in [16, Lemma 2] (where we may ignore the primes that ramify in $K_{t,t}$ by [6, Lemma C.1.7]) we have for every integer $t \geqslant 1$:

$$t \mid \mathrm{ind}_\mathfrak{p}(G) \iff \mathfrak{p} \text{ splits completely in } K_{t,t} \, . \tag{15}$$

Step 2: Since $\mathrm{ord}_{\mathfrak{p}}(G)\,\mathrm{ind}_{\mathfrak{p}}(G) = \mathrm{N}\,\mathfrak{p} - 1$, we may turn the condition on the order into a condition on the index. Indeed, we may write

$$\mathcal{P}(x) = \sum_{t=1}^{\infty} V_t(x) + O\left(\frac{\sqrt{x}}{\log x}\right), \tag{16}$$

where (recalling that we only consider primes of K whose ramification index and inertial degree over $\mathbb{Q}$ are 1, and that are unramified in F)

$$V_t := \left\{\mathfrak{p} :\ \mathrm{ind}_{\mathfrak{p}}(G) = t,\ \mathrm{N}\,\mathfrak{p} \equiv at + 1 \bmod dt,\ \mathrm{Frob}_{F/K}(\mathfrak{p}) \subseteq C\right\}$$

because if $t := \mathrm{ind}_{\mathfrak{p}}(G)$, then the condition $\mathrm{ord}_{\mathfrak{p}}(G) \equiv a \bmod d$ becomes $\mathrm{N}\,\mathfrak{p} - 1 \equiv at \bmod dt$. We may easily combine the condition on the norm and the Frobenius condition, and write

$$V_t = \left\{\mathfrak{p} :\ \mathrm{ind}_{\mathfrak{p}}(G) = t,\ \mathrm{Frob}_{F(\zeta_{dt})/K}(\mathfrak{p}) \subseteq C_t\right\}, \tag{17}$$

where C_t consists of those $\sigma \in \mathrm{Gal}(F(\zeta_{dt})/K)$ such that $\sigma|_F \in C$ and $\sigma(\zeta_{dt}) = \zeta_{dt}^{1+at}$.

Step 3: If F'/K is any finite Galois extension, and if we fix a conjugacy-stable subset C' of its Galois group, then we define the set

$$R_t := \left\{\mathfrak{p} :\ \mathrm{ind}_{\mathfrak{p}}(G) = t,\ \mathrm{Frob}_{F'/K}(\mathfrak{p}) \subseteq C'\right\}. \tag{18}$$

Proposition 24 (cf. [16, Proposition 1])**.** *If $t \leqslant x^{1/3}$ is a positive integer, then we have*

$$R_t(x) = \mathrm{Li}(x) \sum_{n=1}^{\infty} \frac{\mu(n) c'(n,t)}{[F'_{nt,nt} : K]} + O\left(\frac{x}{\log^2(x)}\right) + O\left(\frac{x \log(\log(x))}{\varphi(t)\log^2(x)}\right),$$

where $c'(n,t) := \left|\left\{\sigma \in \mathrm{Gal}(F'_{nt,nt}/K) : \sigma|_{F'} \in C', \sigma|_{K_{nt,nt}} = \mathrm{id}\right\}\right| \leqslant |C'|$.

Proof of Proposition 24. The condition $\mathrm{ind}_{\mathfrak{p}}(G) = t$ is equivalent to

$$t|\,\mathrm{ind}_{\mathfrak{p}}(G) \ \text{ and } \ qt \nmid \mathrm{ind}_{\mathfrak{p}}(G) \text{ for every prime number } q\,.$$

We apply (15) and the inclusion exclusion principle to obtain

$$R_t(x) = \sum_{n=1}^{\infty} \mu(n) \left|\left\{\mathfrak{p} : \mathrm{N}\,\mathfrak{p} \leqslant x,\ \mathrm{Frob}_{K_{nt,nt}/K}(\mathfrak{p}) = \{\mathrm{id}\},\ \mathrm{Frob}_{F'/K}(\mathfrak{p}) \subseteq C'\right\}\right| + O\left(\frac{\sqrt{x}}{\log(x)}\right).$$

Consider the following auxiliary sets

$$M(t,\xi) := \left\{\mathfrak{p} :\ t|\,\mathrm{ind}_{\mathfrak{p}}(G),\ tq \nmid \mathrm{ind}_{\mathfrak{p}}(G)\ \forall q \leqslant \xi \text{ prime},\ \mathrm{Frob}_{F'/K}(\mathfrak{p}) \subseteq C'\right\}$$

$$M(t,\xi,\eta) := \left\{\mathfrak{p} :\ tq|\,\mathrm{ind}_{\mathfrak{p}}(G) \text{ for some } \xi \leqslant q \leqslant \eta \text{ prime},\ \mathrm{Frob}_{F'/K}(\mathfrak{p}) \subseteq C'\right\}$$

and define $\xi_1 := \frac{1}{6}\log(x)$, $\xi_2 := \frac{\sqrt{x}}{\log^2(x)}$ and $\xi_3 := \sqrt{x}\log(x)$. It is not difficult to check that

$$M(t,\xi_1)(x) - M(t,\xi_1,x-1)(x) \leqslant M(t,x-1)(x) \leqslant M(t,\xi_1)(x)\,.$$

Since we may restrict to $\mathrm{ind}_{\mathfrak{p}}(G) \leqslant x - 1$, then we have

$$\begin{aligned} R_t(x) &= M(t,x-1)(x) + O\left(\frac{\sqrt{x}}{\log(x)}\right) \\ &= M(t,\xi_1)(x) + O\Big(M(t,\xi_1,x-1)(x)\Big) + O\left(\frac{\sqrt{x}}{\log(x)}\right). \end{aligned} \tag{19}$$

As in [16, Lemma 12], we may estimate the main term of (19) as

$$M(t,\xi_1)(x) = \mathrm{Li}(x)\sum_{n=1}^{\infty}\frac{\mu(n)c'(n,t)}{[F'_{nt,nt}:K]} + O\left(\frac{x}{\log^2(x)}\right)$$

because we can apply Theorem 23 in place of [16, Lemma 5] (to rewrite the error term of the Chebotarev Density Theorem), and by Theorem 13 there is a constant B such that (to estimate the rewritten error term) we have

$$\frac{c'(n,t)\varphi(nt)(nt)^r}{[F'_{nt,nt}:K]} \leqslant B$$

and hence (this is for the last estimate of Ziegler's proof)

$$\frac{c'(n,t)}{[F'_{nt,nt}:K]} \leqslant \frac{B}{\varphi(nt)(nt)^r} = O\Big(\frac{1}{n\varphi(n)}\Big)\,.$$

We may also estimate the O-term of (19) as

$$O\left(M(t,\xi_1,x-1)(x)\right) = O\left(\frac{x}{\log^2(x)}\right) + O\left(\frac{x\log(\log x)}{\varphi(t)\log^2(x)}\right)$$

by considering the inequality

$$M(t,\xi_1,x-1)(x) \leqslant M(t,\xi_1,\xi_2)(x) + M(t,\xi_2,\xi_3)(x) + M(t,\xi_3,x-1)(x)$$

and by straight-forwardly generalising [16, Lemmas 9, 10, and 11] as follows: we use Theorems 13 and 23 in place of [16, Lemmas 3 and 5]; for [16, Lemma 9] it suffices to work with some fixed $\alpha \in G\setminus\{1\}$ because we have

$$M(t,\xi_3,x-1)(x) \leqslant \left|\left\{\mathfrak{p} : \mathrm{N}\,\mathfrak{p}\leqslant x,\ \alpha^{(\mathrm{N}\,\mathfrak{p}-1)/tq}\equiv 1 \bmod \mathfrak{p},\ \text{for some } \xi_3\leqslant q\leqslant x-1\right\}\right|\,.$$

□

Step 4: As in [16, Proposition 3] (since the generalisation of [16, Lemma 13] is straightforward) we can prove that

$$\mathcal{P}(x) = \sum_{\substack{t\leqslant\sqrt{\log x}\\(1+at,d)=1}} V_t(x) + O\left(\frac{x}{\log^{3/2}(x)}\right)\,. \tag{20}$$

As in [16, Proposition 2] we can prove by (17) and Proposition 24 that, if $t\leqslant x^{1/3}$, then

$$V_t(x) = \mathrm{Li}(x)\sum_{\substack{n=1\\(d,n)|a}}^{\infty}\frac{\mu(n)c(n,t)}{[F_{[d,n]t,nt}:K]} + O\left(\frac{x}{\log^2(x)}\right) + O\left(\frac{x\log(\log(x))}{\varphi(t)\log^2(x)}\right)\,. \tag{21}$$

Notice that we may replace $\mathrm{Li}(x)$ by $x/\log(x)$ in (21) because (this follows from the case of rank 1) we have

$$\sum_{\substack{n=1\\(d,n)|a}}^{\infty}\frac{\mu(n)c(n,t)}{[F_{[d,n]t,nt}:K]} = O\left(\sum_{n=1}^{\infty}\frac{1}{[F_{[d,n]t,nt}:K]}\right) = O\left(1\right)\,.$$

Step 5: As in the proof of [16, Theorem 1], we then find the formula for $\mathcal{P}(x)$ by combining (20) and (21). To write down the main term of (1), notice that by Theorem 13 we have

$$\sum_{\substack{t=1\\(1+at,d)=1}}^{\infty}\sum_{\substack{n=1\\(d,n)|a}}^{\infty}\frac{\mu(n)c(n,t)}{[F_{[d,n]t,nt}:K]}-\sum_{\substack{t\leqslant\sqrt{\log x}\\(1+at,d)=1}}\sum_{\substack{n=1\\(d,n)|a}}^{\infty}\frac{\mu(n)c(n,t)}{[F_{[d,n]t,nt}:K]}=$$

$$O\left(\sum_{\substack{t>\sqrt{\log x}\\n\geqslant 1}}\frac{1}{[F_{[d,n]t,nt}:F]}\right)=O\left(\sum_{\substack{t>\sqrt{\log x}\\n\geqslant 1}}\frac{1}{n\varphi(n)t\varphi(t)}\right)=$$

$$O\left(\sum_{t>\sqrt{\log x}}\frac{1}{t\varphi(t)}\right)=O\left(\frac{1}{\sqrt{\log(x)}}\right)$$

where in the last line we applied [16, Lemma 7].

Step 6: The inequality $c(n,t)\leqslant|C|$ holds because we know the restriction of the automorphisms to $K_{[d,n]t,nt}$. If $c(n,t)$ is non-zero, then we have $(1+at,d)=1$ because the order of ζ_{dt}^{1+at} must be dt, while the condition $(d,n)\mid a$ is evident by comparing the restrictions of σ to K_{nt} and K_{dt}. We additionally remark that in Theorem 4 the constant implied by the O-term depends neither on C nor on a (this can be verified by going through the proof).

Corollary 25. *Let K,G,a,d be as in Theorem 4. Fix integers z,m with $m\geqslant 2$. Assuming (GRH), the number of primes $\mathfrak{p}$ of K with $\mathrm{N}\,\mathfrak{p}\leqslant x$ satisfying*

$$\mathrm{N}\,\mathfrak{p}\equiv z \bmod m \qquad \textit{and} \qquad \mathrm{ord}_{\mathfrak{p}}(G)\equiv a \bmod d$$

is given by

$$\frac{x}{\log(x)}\sum_{n,t\geqslant 1}\frac{\mu(n)c(n,t)}{[K_{[nt,dt,m],nt}:K]}+O\left(\frac{x}{\log^{3/2}(x)}\right), \tag{22}$$

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

$$(z,m)=(1+at,dt)=1 \qquad \textit{and} \qquad (d,n)\mid a \qquad \textit{and} \qquad 1+at\equiv z \bmod (m,dt)$$

and the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_{[m,dt]})/\mathbb{Q})$ such that $\zeta_m\mapsto\zeta_m^z$ and $\zeta_{dt}\mapsto\zeta_{dt}^{1+at}$ is the identity on $\mathbb{Q}(\zeta_{[m,dt]})\cap K_{nt,nt}$.

Proof. This generalisation of [16, Corollary 2] can easily be shown by setting $F=K_m$ in Theorem 4, and by taking C to be the set of those automorphisms in $\mathrm{Gal}(F/K)$ that map ζ_m to ζ_m^z (notice that $|C|\leqslant 1$). □

ACKNOWLEDGMENTS

We thank the outstanding referee for their considerable help with generalising the results from algebraic integers to algebraic numbers (Theorem 23). Many thanks to Gabor Wiese and Samuele Anni for checking some of the proofs. The authors would also like to thank Daniel

Bertrand, Marc Hindry, and Ken Ribet for providing useful references related to Kummer theory.

REFERENCES

[1] BANASZAK, G. - GAJDA, W. - KRASOŃ P., *Detecting linear dependence by reduction maps*, J. Number Theory **115** (2005), 322–342.
[2] BERTRAND, D., *Galois descent in Galois theories*, in: L. Di Vizio - T. Rivoal (Eds.), Arithmetic and Galois theory of differential equations, Séminaires et Congrès **23** (2011), 1–24.
[3] BERTRAND, D., *Galois representations and transcendental numbers*, in: A. Baker (Ed.), New Advances in Transcendence Theory (Durham 1986), Cambridge University Press, 1988, 37–55.
[4] DEBRY, C. - PERUCCA, A., *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283.
[5] HINDRY, M., *Autour d'une conjecture de Serge Lang*, Invent. math. **94** (1988), 575–603.
[6] HINDRY, M. - SILVERMAN, J., *Diophantine Geometry. An Introduction*, Graduate Texts in Mathematics 201, Springer-Verlag, New York, 2000.
[7] LANG, S., *Elliptic Curves - Diophantine Analysis*, Grundlehren der mathematischen Wissenschaften 231, Springer-Verlag, Berlin Heidelberg, 1970.
[8] LENSTRA, H. W. JR., *Commentary on H: Divisibility and congruences*. Andrzej Schinzel Selecta Vol.II, European Mathematical Society, Zürich, 2007, 901–902.
[9] MOREE, P., *Artin's primitive root conjecture – a survey*, Integers **12** (2012), no. 6, 1305–1416.
[10] NEUKIRCH, J., *Algebraic Number Theory*. Springer, Berlin Heidelberg, 1999.
[11] PERUCCA, A., *Multiplicative order and Frobenius symbol for the reductions of number fields*, to appear in the Proceedings of WIN4 (2019).
[12] RIBET, K., *Kummer theory on extensions of abelian varieties by tori*, Duke Math. J. **46** (1979), 745–761.
[13] SCHINZEL, A., *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), no. 3, 245–274. Addendum, ibid. **36** (1980),101–104. See also Andrzej Schinzel Selecta Vol.II, European Mathematical Society, Zürich, 2007, 939–970.
[14] SGOBBA, P., *Kummer theory for number fields and applications*, Master Thesis (supervised by A. Perucca), University of Luxembourg, June 2018.
[15] WÓJCIK, J., *Criterion for a field to be abelian*, Colloq. Math. **68** (1995), no. 2, 187–191.
[16] ZIEGLER, V., *On the distribution of the order of number field elements modulo prime ideals*, Uniform Distribution Theory **1** (2006), no.1, 65–85.

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

Email address: antonella.perucca@uni.lu, pietro.sgobba@uni.lu