KUMMER THEORY FOR NUMBER FIELDS VIA ENTANGLEMENT GROUPS

ANTONELLA PERUCCA, PIETRO SGOBBA, SEBASTIANO TRONTO

ABSTRACT. Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. We are interested in computing the degree of the cyclotomic-Kummer extension $K(\sqrt[n]{G})$ over K, where $\sqrt[n]{G}$ consists of all n-th roots of the elements of G. We develop the theory of entanglements introduced by Lenstra, and we apply it to compute the above degrees.

1. INTRODUCTION

Let K be a number field, and let us work in a fixed algebraic closure $\bar{K}$. Let G be a finitely generated subgroup of $K^\times$. For any fixed $n \geqslant 1$, let $\sqrt[n]{G}$ be the group of all n-th roots of the elements of G (which includes the n-th roots of unity). We are interested in computing the degree of the cyclotomic-Kummer extension

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

In [7] Lenstra proposed a theory of *entanglements* to take care of the fact that radicals of elements of G can be contained in cyclotomic extensions of K, and to study this phenomenon we 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 [8, 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 [8, Theorem 1.6] that $E(B_n)$ is an abelian group, and it is clearly finite. In Section 7 we prove the following statement (which in a different form over $\mathbb{Q}$ has been proven by Palenstijn in [8, Proposition 4.3]), where ζ_p denotes a root of unity of order p.

Theorem 1. *Setting* $\Delta_n := \prod_{p \text{ prime},\, p\mid n, \zeta_p\notin K} \frac{p-1}{p}$, *we have*

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

We may compute $[B_n : K^\times]$ with a result by Debry and the first author [3, Theorem 15], so we are left to compute the size of the entanglement group. The following result says in particular that $\#E(B_n)$ 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

2010 *Mathematics Subject Classification.* Primary: 11Y40; Secondary: 11R18, 11R21.
Key words and phrases. Number fields, Kummer theory, Degree, Radical extensions.

only on K and G. This result will be proven using Theorem 36, which is an assertion about the eventual maximal growth of the degrees of cyclotomic-Kummer extensions (notice that in Section 7 we express degrees of Kummer extensions in terms of entanglement groups).

Theorem 2. *There is a computable integer $n_0 \geqslant 1$ (depending only on K and G) such that for every $n \geqslant 1$ we have*

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

Throughout the paper, whenever we talk about about the computability of a certain object depending only on K and G, we mean that there exists a finite procedure that, given as input the field K and the group 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 [5, Chapter 19], which implies that its elements are representable on a computer. Moreover, one should know a finite set generators for the group G. We refer to Remark 41 for more details about the computations.

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, where μ_n denotes the group of n-th roots of unity. Palenstijn proved in [8, 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*, by which we mean those $x \in \bar{K}^\times$ such that $x^\omega \in K^\times$, where ω is the order of the torsion part of $K^\times$. A large portion of the article is thus devoted to express $B_{n,\mathrm{ab}}$ in terms of Kummer radicals and roots of unity (in Sections 5 and 6 we describe $B_{n,\mathrm{ab}}$, first in the special case where n is a prime power and then in general). An example of our results is the following, where μ_K denotes the group of roots of unity contained in K (and 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 3. *Suppose that every element of G has the same divisibility in $K^\times$ and in $K^\times/\mu_K$. Then for every $n \geqslant 1$ 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

$$E(B_n) = \mathrm{Gal}\left(K(H_n) \cap \mathbb{Q}(\mu_n)/\mathbb{Q}(\langle K^\times, H_n\rangle \cap \mu_n)\right) .$$

This result will be a consequence of Theorem 29 in view of Remark 11. Notice that it would not be true without assumptions on G, see Example 26.

Finally in Section 8 we prove the following general statement about the failure of maximality for the cyclotomic-Kummer degree, and in Remark 40 we generalize it to groups which are not necessarily torsion-free.

Theorem 4. *Let G be a finitely-generated and torsion-free subgroup of $K^\times$ of positive rank r. Then there is a computable integer $n_0 \geqslant 1$ (depending only on K and G) such that for every $n \geqslant 1$ we have*

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

where $g := \gcd(n, n_0)$.

This theorem says, in other words, that the degree $[K(\sqrt[n]{G}) : K(\sqrt[g]{G})]$ is maximal.

In Section 9 we present examples of the computation of the degree of cyclotomic-Kummer extensions. Notice that in the case that the base field is $\mathbb{Q}$, Palenstijn computed cyclotomic-Kummer degrees with the theory of entanglements [8, Chapter 4] while the authors computed those degrees by a different method [9].

2. Preliminaries on strongly indivisible elements

2.1. **Notation.** Let K be a number field, and fix some algebraic closure $\bar{K}$. We denote by μ_K the group of roots of unity contained in K and set $\omega := \#\mu_K$. For an integer $n \geqslant 1$ we denote by ζ_n a primitive n-th root of unity in $\bar{K}$, and by μ_n the group of n-th roots of unity in $\bar{K}$. We also define $\mu_\infty := \cup_{n\geqslant 1}\mu_n$. If ℓ is a prime number, then we set $\mu_{\ell^\infty} := \cup_{n\geqslant 1}\mu_{\ell^n}$, we denote by v_ℓ the ℓ-adic valuation on $\mathbb{Q}$, and we write $\omega_\ell := v_\ell(\omega)$.

2.2. **Strong ℓ-independence.** 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 the latter 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.

Lemma 5. *Let $b_1, \dots, b_r \in K^\times$ be strongly ℓ-independent. For every $n \geqslant 1$, if*

$$\zeta \cdot \prod_{i=1}^{r} b_i^{x_i}$$

is an ℓ^n-th power in $K^\times$ for some integers x_i and for some $\zeta \in \mu_K$, then $\ell^n \mid x_i$ for all i.

Proof. We prove the statement by induction on n. For $n = 1$, the statement holds by definition of strong ℓ-independence. An ℓ^n-th power in $K^\times$ is in particular an ℓ-th power, so by the case

$n = 1$ we can write $x_i = \ell y_i$ for some integers y_i and ζ is an ℓ-th power in $K^\times$. So there is $\xi \in \mu_K$ such that $\xi \cdot \prod_i b_i^{y_i}$ is an ℓ^{n-1}-th power in $K^\times$. By the induction hypothesis we have $\ell^{n-1} \mid y_i$ for all i and we conclude. □

Lemma 6 (Schinzel, [11, Theorem 2])**.** *Let $b \in K^\times$ be strongly ℓ-indivisible. Then the extension $K(\mu_{\ell^n}, \sqrt[\ell^n]{b})/K$ is abelian if and only if $n \leqslant \omega_\ell$.*

Proof. The *if* part is clear because $\mu_{\ell^n} \subseteq K$. Conversely, suppose that the given extension is abelian and that $n > \omega_\ell$. Then $b^{\ell^{\omega_\ell}}$ is an ℓ^n-th power in $K^\times$ by [11, Theorem 2], which is impossible by Lemma 5. □

2.3. **Divisibility parameters.** Consider a finitely generated and torsion-free subgroup G of $K^\times$ of positive rank r, and fix some prime number ℓ. If $g_1, \dots, g_r$ is a basis of G as a $\mathbb{Z}$-module, then 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 [3, 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. 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 [3, Appendix]). Recall from [3, Theorem 14] that an ℓ-good basis of G always exists.

Remark 7. *As shown in* [3, 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 in* [10, Proposition 4.5]*, while for the h-parameters it suffices that $\ell \nmid \omega$). See also Remark 41. 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* [3, Proposition 31] *are zero.*

Lemma 8. *The strongly ℓ-indivisible parts of a basis of G generate a torsion-free subgroup of $K^\times$ of rank r.*

Proof. With the above notation, suppose that $\prod_i b_i^{e_i} = 1$ for some integers e_i. Setting $m = \max_i(h_i + d_i)$, we have $1 = \prod_i b_i^{me_i} = \prod_i g_i^{f_i}$ for some integers f_i. Since G is torsion-free and the b_i's are not roots of unity, we deduce that $f_i = 0$ and hence $e_i = 0$ for all i. □

Lemma 9. *The strongly ℓ-indivisible parts of the elements of G are in the group generated by $\mu_{\ell^{\omega_\ell}}$ and by the strongly ℓ-indivisible parts of the elements of any fixed ℓ-good basis of G.*

Proof. If $g \in G$, write $g = \xi b^{\ell^d}$ where $b \in K^\times$ is strongly ℓ-indivisible and $\xi \in \mu_{\ell^{\omega_\ell}}$. With the above notation, expressing g in terms of the basis g_i, we deduce that

$$b^{\ell^d} = \zeta \prod_{i=1}^{r} b_i^{x_i}$$

for some $\zeta \in \mu_{\ell^{\omega_\ell}}$ and for some integers x_i. By Lemma 5 we have $\ell^d \mid x_i$ for every i and we conclude. □

Lemma 10. *Call d_i the d-parameters for the ℓ-divisibility of G. If an element of G different from 1 has a strictly positive h-parameter, then its d-parameter d satisfies $d < \max_i(d_i) + \omega_\ell$.*

Proof. The given element is of the form $g = \zeta \cdot b^{\ell^d}$, where $b \in K^\times$ is strongly ℓ-indivisible, and where $\zeta \neq 1$ is in $\mu_{\ell^{\omega_\ell}}$. Suppose that $d \geqslant \max_i(d_i) + \omega_\ell$. Then g is not an ℓ^d-th power in $K^\times$. Expressing the elements of an ℓ-good basis of G in terms of their strongly ℓ-indivisible parts b_i, we can write

$$g = \prod_{i=1}^{r} \left(\xi_i b_i^{\ell^{d_i}}\right)^{x_i}$$

where $\xi_i \in \mu_{\ell^{\omega_\ell}}$ and $x_i \in \mathbb{Z}$. Since $g\zeta^{-1}$ is an ℓ^d-th power in $K^\times$, Lemma 5 implies that $\ell^d \mid \ell^{d_i} x_i$. Since $d \geqslant d_i + \omega_\ell$ we have $\xi_i^{x_i} = 1$ and hence g is an ℓ^d-th power in $K^\times$, contradiction. □

Remark 11. *If ℓ is a prime number, then the the following conditions are equivalent:*

1. *Every element of G has the same divisibility in the groups $K^\times$ and $K^\times/\mu_K$.*
2. *Every element of $G \setminus \{1\}$ is the ℓ^d-th power of a strongly ℓ-indivisible element for some integer $d \geqslant 0$.*
3. *The h-parameters for the ℓ-divisibility of G can be taken to be zero (i.e. they are zero for some ℓ-good basis and for some choice of the strongly ℓ-indivisible parts of the elements of this basis).*

Indeed, the first and second condition are clearly equivalent and imply the third. To prove that the third condition implies the second one, suppose that $G = \langle b_i^{\ell^{d_i}} : i = 1, \dots, r\rangle$ where the b_i's are strongly ℓ-independent, and write an element of $G \setminus \{1\}$ as

$$g = \prod_{i \in I} b_i^{\ell^{d_i} x_i}$$

for some non-empty $I \subseteq \{1, \dots, r\}$ and for some integers $x_i \neq 0$. The d-divisibility parameter for g is $d := \min_i(d_i + v_\ell(x_i))$ by Lemma 5, and the above expression implies that $g \in K^{\times \ell^d}$.

3. Preliminaries on 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 $K^\times$.

Proposition 12 (Palenstijn, [8, Lemma 1.9])**.** *If x is a radical such that $x^n \in K^\times$, then the following are equivalent:*

(1) *We have $x^\omega \in \langle K^\times, \mu_\infty \rangle$.*
(2) *The group $\mathrm{Aut}_{K^\times}(\langle K^\times, \mu_n, x\rangle)$ is abelian.*
(3) *The extension $K(\mu_n, x)/K$ is abelian.*

We call a radical *abelian* if it satisfies the conditions of the previous proposition. 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 [8, 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 [8, Corollary 2.27] we know that $E(B) = E(B_{\mathrm{ab}})$.

Theorem 13 (Palenstijn, [8, 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 $B = B_{\mathrm{ab}}$.

Lemma 14. *If $B \subseteq B'$ are two Galois radical groups, then $E(B)$ is a quotient of $E(B')$.*

Proof. It suffices to prove that $E(B_{\mathrm{ab}})$ is a quotient of $E(B'_{\mathrm{ab}})$, and we have $B_{\mathrm{ab}} \subseteq B'_{\mathrm{ab}}$. So we may reduce to prove the assertion in the special case $B = B_{\mathrm{ab}}$ and $B' = B'_{\mathrm{ab}}$. We have the following commutative diagram of abelian groups given by restrictions:

$$\begin{array}{ccccccc}
 & & \mathrm{Gal}(K(B')/K(B)) & \longrightarrow & \mathrm{Gal}(K(B')/K) & \longrightarrow & \mathrm{Gal}(K(B)/K) \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \ker(\phi) & \longrightarrow & \mathrm{Aut}_{K^\times}(B') & \xrightarrow{\phi} & \mathrm{Aut}_{K^\times}(B)
\end{array}$$

By the Snake Lemma we have an epimorphism between the cokernels of the second and third vertical maps, which gives exactly that $E(B)$ is a quotient of $E(B')$. □

4. On maximal abelian extensions

Let K be a number field, and fix a finitely generated and torsion-free subgroup G of $K^\times$ of positive rank r. We focus on the abelian radicals x such that $x^n \in G$ for some $n \geqslant 1$: these, 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 $B_{\ell^\infty,\mathrm{ab}}$.

Remark 15. *Consider a Galois radical group of the form $\langle K^\times, H\rangle$. If we require that the group $H/(G \cap H)$ is torsion (respectively, an ℓ-group) and that the extension $K(H)/K$ is abelian, then $\langle K^\times, H\rangle$ is a subgroup of $B_{\infty,\mathrm{ab}}$ (respectively, $B_{\ell^\infty,\mathrm{ab}}$).*

As a consequence of the following lemma, the group $B_{\infty,\mathrm{ab}}$ is generated by the groups $B_{\ell^\infty,\mathrm{ab}}$ by varying ℓ.

Lemma 16. *Consider an integer $n > 1$, and let $n = \prod \ell^e$ be the prime factorization. If H is a subgroup of $\bar{K}^\times$ containing μ_n, then for every $a \in K^\times$ we have $\sqrt[n]{a} \in H$ if and only if $\sqrt[\ell^e]{a} \in H$ for all ℓ.*

Proof. The *only if* part is clear. For the *if* part notice that the integers n/ℓ^e are coprime and hence $\sqrt[n]{a}$ can be expressed as a product of powers of the elements $\sqrt[\ell^e]{a}$ for an appropriate choice of the roots. □

Definition 17. Let ℓ be a prime divisor of ω, and let $b_1, \dots, b_r$ be the strongly ℓ-indivisible parts associated to an ℓ-good basis of G. We define the group of Kummer radicals

$$S_\ell := \left\langle \sqrt[\ell^{\omega_\ell}]{b_1}, \dots, \sqrt[\ell^{\omega_\ell}]{b_r} \right\rangle$$

(for some fixed choice of the ℓ^{ω_ℓ}-th roots). We also define $S := \langle S_\ell : \ell \mid \omega\rangle$.

Notice that 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.

Lemma 18. *We have $S_\ell \cap \langle K^\times, \mu_{\ell^\infty}\rangle = \langle b_1, \dots, b_r\rangle$.*

Proof. The former group clearly contains the latter. Let $s \in S_\ell$ be of the form $s = a\zeta$ with $a \in K^\times$ and $\zeta \in \mu_{\ell^\infty}$. Since $s^{\ell^{\omega_\ell}} \in K$, we deduce that $\zeta^{\ell^{\omega_\ell}} \in K$. So we have

$$a^{\ell^{2\omega_\ell}} = s^{\ell^{2\omega_\ell}} = \prod_i b_i^{z_i}$$

for some integers z_i which are all divisible by $\ell^{2\omega_\ell}$ by Lemma 5 . Since S_ℓ is torsion-free, we deduce that s is a product of powers of the b_i's. □

Proposition 19. *We have $\langle K^\times, S\rangle \cap \mu_\infty = \mu_K$.*

Proof. The former group clearly contains the latter, and it suffices to prove that for every prime number ℓ the group $\langle K^\times, S\rangle \cap \mu_{\ell^\infty}$ is contained in K. To study this intersection, we may replace S by S^w, where $w \geqslant 1$ is coprime to ℓ. If $\ell \nmid \omega$, then we choose $w = \omega$ and we conclude. If $\ell \mid \omega$, then we choose $w = \omega/\ell^{\omega_\ell}$ and deduce

$$\left\langle K^\times, S\right\rangle \cap \mu_{\ell^\infty} = \left\langle K^\times, S_\ell\right\rangle \cap \mu_{\ell^\infty}\,.$$

If ζ is in the latter group, then we can write for some $a \in K^\times$ and for some integers z_i

$$\zeta^{\ell^{\omega_\ell}} = a^{\ell^{\omega_\ell}} \prod_i {b_i}^{z_i} \in K\,.$$

By Lemma 5 we have $\ell^{\omega_\ell} \mid z_i$ for every i and hence $\zeta \in K$. □

Lemma 20. *We have $B_{\infty,\mathrm{ab}} = \langle K^\times, \mu_\infty, S\rangle$, and for every prime ℓ we have*

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

Proof. The assertion on $B_{\infty,\mathrm{ab}}$ follows from the description of $B_{\ell^\infty,\mathrm{ab}}$. In both cases $B_{\ell^\infty,\mathrm{ab}}$ contains the given group, so we are left to prove the inclusion. If $\ell \nmid \omega$, then by Lemma 6 the abelian radicals x such that $x^{\ell^n} \in K^\times$ for some $n \geqslant 0$ are contained in $\langle K^\times, \mu_{\ell^\infty}\rangle$. Now let $\ell \nmid \omega$ and consider an abelian radical x such that $x^{\ell^n} \in G$ for some $n \geqslant 0$. If $x^{\ell^n} = 1$, then $x \in \mu_{\ell^\infty}$, else we can write

$$x^{\ell^n} = \zeta b^{\ell^d}$$

for some $\zeta \in \mu_{\ell^{\omega_\ell}}$, for some integer $d \geqslant 0$, and for some $b \in K^\times$ which is strongly ℓ-indivisible. If $n \leqslant d$, then we have $x \in \langle K^\times, \mu_{\ell^\infty}\rangle$. If $n > d$, then $\sqrt[\ell^{n-d}]{b}$ is an abelian radical and hence by Lemma 6 we must have $n - d \leqslant \omega_\ell$. By Lemma 9 we conclude that $\sqrt[\ell^{n-d}]{b}$, and hence x, is contained in $\langle \mu_{\ell^\infty}, S_\ell\rangle$. □

Remark 21. *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 $n = \prod_{\ell\in\mathcal{P}} \ell^{e_\ell}$, where $\mathcal{P}$ consists of the prime numbers ramifying in $K(S)/\mathbb{Q}$, and where e_ℓ is at least the ramification index of ℓ (we can take $e_\ell = \omega^r[K:\mathbb{Q}]$ because $[K(S):K]$ divides ω^r). Since $K(S)/K$ is the compositum of cyclic Kummer extensions, by a classical result* [4, Lemma C.1.7 and its proof] *we can take $\mathcal{P}$ to be the set of primes ℓ that divide the discriminant of K or are such that for some prime $\mathfrak{p}$ of K above ℓ and for some $i \in \{1,\dots,r\}$ the $\mathfrak{p}$-adic valuation $\mathrm{ord}_\mathfrak{p}(b_i)$ 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 41.*

To obtain various results we will work with an integer satisfying two properties: that such an integer exists and is computable is explained by the following proposition.

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 $v_\ell(n_0) \geqslant \max_i(d_i) + \omega_\ell$ for every prime number ℓ, where the d_i's are the d-parameters for the ℓ-divisibility of G.*

Proof. It suffices to combine Remarks 7 and 21, recalling that the d-parameters for the ℓ-divisibility of G are computable. □

5. Radical groups with ℓ-radicals

We keep the previous notation, and define for every integer $n \geqslant 0$ the radical group

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

where $\sqrt[\ell^n]{G}$ denotes the group of all ℓ^n-th roots of the elements of G. Notice that B_{ℓ^n} and $B_{\ell^n,\mathrm{ab}}$ are Galois radical groups containing μ_{ℓ^n}.

Lemma 23. *If ℓ is a prime number, then there is some computable integer e_0 (depending only on K, G, and ℓ) such that*

$$B_{\ell^n,\mathrm{ab}} = \begin{cases} \langle K^\times, \mu_{\ell^n} \rangle & \text{if } \ell \nmid \omega \\ \langle K^\times, \mu_{\ell^n}, S_\ell \rangle & \text{if } \ell \mid \omega \text{ and } n \geqslant e_0 \,. \end{cases}$$

Proof. The assertion for $\ell \nmid \omega$ follows from Lemma 20, so suppose that $\ell \mid \omega$ and set $e_0 := \max_i(d_i) + \omega_\ell$, where the d_i's are the d-parameters for the ℓ-divisibility of G. Thus $B_{\ell^{e_0},\mathrm{ab}}$ contains S_ℓ and we are left to prove that $B_{\ell^n,\mathrm{ab}}$ is contained in $\langle K^\times, \mu_{\ell^n}, S_\ell \rangle$ for every $n \geqslant e_0$. By Lemma 20 it suffices to prove that any root of unity $\zeta \in B_{\ell^n,\mathrm{ab}} \cap \mu_{\ell^\infty}$ is contained in μ_{ℓ^n}. The property $\zeta^{\ell^n} \in K^{\times \ell^n}$ is enough to conclude because $n \geqslant \omega_\ell$.

Write $\zeta^{\ell^n} = a^{\ell^n} g$ for some $a \in K^\times$ and for some $g \in G$. If $g = 1$ we are done, so suppose that $g \neq 1$ and write $g = \xi b^{\ell^d}$ for some $\xi \in \mu_{\ell^\infty} \cap K$, for some integer $d \geqslant 0$, and for some $b \in K^\times$ which is strongly ℓ-indivisible. Since ξ/ζ^{ℓ^n} is in μ_K, Lemma 5 implies that $d \geqslant n$. If $\xi = 1$, then we are done, and we cannot have $\xi \neq 1$ because Lemma 10 would imply $d < \max_i(d_i) + \omega_\ell \leqslant n$. □

Proposition 24. *Let ℓ be a prime divisor of ω and let $n \geqslant 0$. For the Galois radical group*

$$B'_{\ell^n} := \langle B_{\ell^n}, \mu_{\ell^{n+\omega_\ell}} \rangle$$

we have

$$B'_{\ell^n,\mathrm{ab}} = \langle K^\times, \mu_{\ell^{n+\omega_\ell}}, S_\ell \cap B'_{\ell^n} \rangle \,.$$

The group $S_\ell \cap B'_{\ell^n}$ consists of Kummer radicals. More precisely, we have

$$S_\ell \cap B'_{\ell^n} = \langle \sqrt[\ell^{\max(0,\min(\omega_\ell, n-d_i))}]{b_i} : i = 1, \dots, r \rangle \tag{1}$$

where the b_i's are the strongly ℓ-indivisible parts of an ℓ-good basis for G and the d_i's are the divisibility parameters of the corresponding generator (and the roots of the b_i's are chosen so that they are in S_ℓ).

Notice that, if G contains $\zeta_{\ell^{\omega_\ell}}$ times an ℓ^n-th power in $K^\times$, then $B'_{\ell^n} = B_{\ell^n}$.

Proof. For the first assertion, since $B'_{\ell^n,\mathrm{ab}}$ clearly contains the given group, it suffices to prove that the abelian radicals in $\sqrt[\ell^n]{G}$ are contained in $\langle K^\times, \mu_{\ell^{n+\omega_\ell}}, S_\ell \rangle$. So let $g \in G$, and suppose that $K(\mu_{\ell^n}, \sqrt[\ell^n]{g})/K$ is abelian. We may suppose that $g \neq 1$, so we can write $g = \zeta b^{\ell^d}$ for some $\zeta \in \mu_{\ell^{\omega_\ell}}$, for some integer $d \geqslant 0$, and for some $b \in K^\times$ which is strongly ℓ-indivisible. If $n \leqslant d$, then we have $\sqrt[\ell^n]{g} \in \langle K^\times, \mu_{\ell^{n+\omega_\ell}} \rangle$, so let $n > d$. It is enough to prove that $\sqrt[\ell^{n-d}]{b} \in \langle \mu_{\ell^{n+\omega_\ell}}, S_\ell \rangle$. Since this is an abelian radical, Lemma 6 implies $n - d \leqslant \omega_\ell$. We can write

$$b^{\ell^d} = \zeta^{-1} g = \xi \prod_i b_i^{\ell^{d_i} z_i}$$

for some $\xi \in \mu_K$ and for some integers z_i. By Lemma 5 we have $d_i + v_\ell(z_i) \geqslant d$. Recalling that $n - d \leqslant \omega_\ell$, we deduce that $\sqrt[\ell^{n-d}]{b}$ is, up to an element in $\mu_{\ell^{n+\omega_\ell}}$, the product of powers of the elements $\sqrt[\ell^{\omega_\ell}]{b_i}$.

Now consider (1). The inclusion $\supseteq$ is clear because, for each i, the given root of b_i is in S_ℓ and it is, up to an element of $\mu_{\ell^{n+\omega_\ell}}$, the ℓ^n-th root of an element of G. For the inclusion $\subseteq$, by Lemma 18 it suffices to prove that

$$S_\ell \cap B'_{\ell^n} \subseteq \langle K^\times, \mu_{\ell^{n+\omega_\ell}}, \sqrt[\ell^{\max(0,\min(\omega_\ell, n-d_i))}]{b_i} : i = 1, \dots, r \rangle .$$

Noticing that $S_\ell \cap B'_{\ell^n}$ consists of abelian radicals, this inclusion follows from the fact that the element $\sqrt[\ell^{n-d}]{b}$ considered above is also in

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

□

Proposition 25. *Let ℓ be a prime divisor of ω and let $n \geqslant 0$. Suppose that the h-parameters for the ℓ-divisibility of G can be taken to be zero. Then we have*

$$B_{\ell^n,\mathrm{ab}} = \langle K^\times, \mu_{\ell^n}, H_{\ell^n} \rangle$$

where H_{ℓ^n} is a group consisting of Kummer radicals. We may take for H_{ℓ^n} the computable groups

$$H_{\ell^n} = \begin{cases} \sqrt[\ell^n]{G} & \text{if } n \leqslant \omega_\ell \\ S_\ell \cap \langle B_{\ell^n}, \mu_{\ell^{n+\omega_\ell}} \rangle & \text{if } n > \omega_\ell . \end{cases} \tag{2}$$

Proof. If $n \leqslant \omega_\ell$, then $\sqrt[\ell^n]{G}$ consists of Kummer radicals and we may easily conclude. Now let $n > \omega_\ell$ and take for H_{ℓ^n} the group in (1) (which consists of Kummer radicals and is computable). Notice that $B_{\ell^n,\mathrm{ab}}$ contains $K^\times$ and μ_{ℓ^n}. Moreover, it contains H_{ℓ^n} because this group consists of abelian radicals, which are in B_{ℓ^n} by our assumption on the h-parameters. We are left to prove that $B_{\ell^n,\mathrm{ab}} \subseteq \langle K^\times, \mu_{\ell^n}, H_{\ell^n} \rangle$. An element $x \in B_{\ell^n,\mathrm{ab}} \subseteq B'_{\ell^n,\mathrm{ab}}$ is such that $x^{\ell^n} = y^{\ell^n} g$, where $y \in K^\times$ and $g \in G$. By Proposition 24 we can write

$$x = a\xi h \qquad \text{where} \qquad a \in K^\times \quad \xi \in \mu_{\ell^{n+\omega_\ell}} \quad h \in H_{\ell^n} .$$

Because of our assumption on the h-parameters we have $g \in \langle b_1, \dots, b_r \rangle$ and hence ξ^{ℓ^n} is an ℓ^n-th power in $K^\times$ times $\prod_i b_i^{z_i}$ for some integers z_i. By Lemma 5 we have $\ell^n \mid z_i$ for every i, and we conclude that $\xi \in \langle K^\times, \mu_{\ell^n} \rangle$. □

To justify the assumptions of the previous proposition, consider the following example.

Example 26. 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.

6. Radical groups in the general case

We keep the previous notation, and define for every integer $n \geqslant 1$ the radical group

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

where $\sqrt[n]{G}$ denotes the group of all n-th roots of the elements of G. 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.

Lemma 27. *If ℓ is a prime number, then we have*

$$B_n \cap \mu_\ell = \begin{cases} \mu_\ell & \text{if } \ell \mid n\omega \\ 1 & \text{otherwise}. \end{cases}$$

Proof. If $\ell \mid n\omega$, then clearly $\zeta_\ell \in B_n$. Now suppose that $\ell \nmid n\omega$, and that $\zeta_\ell = a\sqrt[n]{g}$ for some $a \in K^\times$ and $g \in G$. We deduce that $\zeta_\ell^n \in K$ and hence $\zeta_\ell \in K$, contradiction. □

Lemma 28. *Consider an integer $n > 1$, and let $n = \prod \ell^e$ be the prime factorization. Then $B_{n,\mathrm{ab}}$ is generated by the groups $B_{\ell^e,\mathrm{ab}}$.*

Proof. We clearly have $B_{\ell^e,\mathrm{ab}} \subseteq B_{n,\mathrm{ab}}$. Conversely, consider an abelian radical of the form $a\sqrt[n]{g}$ where $a \in K^\times$ and $g \in G$. Since $K(\mu_n, \sqrt[n]{g})/K$ is abelian, the same holds for $K(\mu_{\ell^e}, \sqrt[\ell^e]{g})/K$, and we deduce that $\sqrt[\ell^e]{g}$ is in $B_{\ell^e,\mathrm{ab}}$. We conclude by Lemma 16. □

Theorem 29. *Let $n > 1$ be an integer, and suppose that for every prime divisor ℓ of n the h-parameters for the ℓ-divisibility of G can be taken to be zero. Then we can write*

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

where H_n is a group consisting of Kummer radicals. We have

$$E(B_n) = \mathrm{Gal}\left(K(H_n) \cap \mathbb{Q}(\mu_n)/\mathbb{Q}(\langle K^\times, H_n\rangle \cap \mu_n)\right).$$

If $n = \prod \ell^e$ is the prime factorization, then we can take for H_n the group generated by the groups H_{ℓ^e} from (2) *for $\ell \mid \omega$. With this choice we have $\langle K^\times, H_n\rangle \cap \mu_n = \mu_{\gcd(n,\omega)}$.*

Proof. We apply Lemma 28. If $\ell \nmid \omega$, then $B_{\ell^e,\mathrm{ab}} = \langle K^\times, \mu_{\ell^e}\rangle$ by Lemma 23; if $\ell \mid \omega$, then we can apply Proposition 25 to get the description of $B_{\ell^e,\mathrm{ab}}$.

The assertion on $E(B_{n,\mathrm{ab}})$ follows from Theorem 13 because $\langle K^\times, H_n\rangle$ is a group of Kummer radicals. Notice that with our choice of H_n we have $\langle K^\times, H_n\rangle \cap \mu_n = \mu_{\gcd(n,\omega)}$ by Proposition 19 because our assumption on the h-parameters implies that $H_n \subseteq \langle \mu_K, S\rangle$. □

Proof of Theorem 3. The statement follows from Theorem 29, in view of Remark 11. □

Lemma 30. *There is some computable integer $n_0 \geqslant 1$ (depending only on K and G) such that $B_{n,\mathrm{ab}} = \langle K^\times, \mu_n, S\rangle$ holds for every multiple n of n_0. It suffices to take n_0 as in Proposition 22.*

Proof. Combine Lemma 28 with Lemma 23. □

The following result is a generalization of [8, Theorem 1.4].

Theorem 31. *There is some computable integer $n_0 \geqslant 1$ (depending only on K and G) such that*

$$E(B_n) = \mathrm{Gal}\left(K(S) \cap \mathbb{Q}(\mu_{n_0})/\mathbb{Q}(\mu_K)\right)$$

holds for every multiple n of n_0. It suffices to take n_0 as in Proposition 22.

Proof. Take n_0 as in Proposition 22. We have $\mu_K \subseteq \mu_{n_0}$ and hence $\langle K^\times, S\rangle \cap \mu_n = \mu_K$ by Proposition 19. Since $\langle K^\times, S\rangle$ is a group of Kummer radicals, combining Lemma 30 with Theorem 13 gives the statement. □

The following proposition should be compared with Theorem 29 (we now have no additional assumptions on G).

Proposition 32. *Consider an integer $n > 1$. We have*

$$\langle B_n, \mu_{n\omega}\rangle_{\mathrm{ab}} = \langle K^\times, \mu_{n\omega}, R_n\rangle\,,$$

where R_n is a group consisting of Kummer radicals. Let $n = \prod \ell^e$ be the prime factorization. Then we can take R_n to be the group generated by the groups $R_{\ell^e} := S_\ell \cap B'_{\ell^e}$ as in (1) *if $\ell \mid \omega$. With this choice, we have*

$$E(\langle B_n, \mu_{n\omega}\rangle) = \mathrm{Gal}\left(K(R_n)\cap\mathbb{Q}(\mu_{n\omega})/\mathbb{Q}(\mu_K)\right).$$

Proof. By Lemma 28 the group $\langle B_n, \mu_{n\omega}\rangle_{\mathrm{ab}}$ is generated by the groups $\langle B_{\ell^e}, \mu_{\ell^{e+\omega_\ell}}\rangle_{\mathrm{ab}}$. If $\ell \nmid \omega$, then the latter group is $\langle K^\times, \mu_{\ell^e}\rangle$ by Lemma 6, while for $\ell \mid \omega$ we can apply Proposition 24. Finally we can apply Theorem 13 because $\langle K^\times, R_n\rangle$ is a group of Kummer radicals and we have $\langle K^\times, R_n\rangle \cap \mu_{n\omega} = \mu_K$ by Proposition 19 noticing that $R_n \subseteq S$. □

7. Kummer degrees via entanglement groups

The formula given in [8, Proposition 4.3] extends to a general number field K.

Theorem 33. *If B is a Galois radical group such that $B/K^\times$ is finite, then we have*

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

where $\Delta = \prod_{p\text{ prime},\zeta_p\in B\setminus\mu_K} \frac{p-1}{p}$. In particular, $\#E(B)$ is a divisor of $[B:K^\times]\cdot\Delta$.

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

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

and by [8, Theorem 2.19] we have $\#\operatorname{Aut}_{K^\times}(B) = [B:K^\times]\cdot\Delta$. □

Proof of Theorem 1. It suffices to apply Theorem 33 with $B = B_n$, where $\Delta = \Delta_n$ by Lemma 27. □

The following result implies that for every $n > 1$ we have $[B_n : K^\times] = \prod_{\ell\text{ prime}}[B_{\ell^{v_\ell(n)}} : K^\times]$.

Proposition 34. *Consider an integer $n > 1$, and let $n = \prod \ell^e$ be the prime factorization. Then we have*

$$B_n/K^\times \cong \prod_\ell B_{\ell^e}/K^\times\,.$$

Proof. The groups $B_{\ell^e}/K^\times$ generate the finite abelian group $B_n/K^\times$, and their orders are pairwise coprime. □

Proposition 35. *If ℓ is a prime number and $e > 0$, then we have*

$$\left[B_{\ell^e} : K^\times\right] = \left[G : G \cap K^{\times \ell^e}\right] \cdot \ell^{\max(0, e-\omega_\ell)}\,.$$

Proof. Let $H = \langle \mu_{\ell^e}, \sqrt[\ell^e]{G}\rangle$, and hence $B_{\ell^e} = \langle K^\times, H\rangle$. By the fundamental isomorphism theorem we then have

$$\frac{B_{\ell^e}}{K^\times} \cong \frac{H}{K^\times \cap H}.$$

Considering the map $[\ell^e]$ raising an element to the ℓ^e-th power, we have

$$\ker([\ell^e] : H \to G) = \mu_{\ell^e} \quad \text{and} \quad \ker([\ell^e] : K^\times \cap H \to (K^\times \cap H)^{\ell^e}) = \mu_{\ell^{\min(e,\omega_\ell)}}\,.$$

Thus we obtain

$$\left[H : K^\times \cap H\right] = \left[G : (K^\times \cap H)^{\ell^e}\right] \cdot \ell^{\max(0, e-\omega_\ell)}$$

and we are left to prove that $G \cap K^{\times \ell^e} = (K^\times \cap H)^{\ell^e}$. The former group contains the latter because any element of $(K^\times \cap H)^{\ell^e}$ is in $K^{\times \ell^e}$ and in $H^{\ell^e} = G$. Now consider $g \in G \cap K^{\times \ell^e}$, and write $g = a^{\ell^e}$ for some $a \in K^\times$. Since $a^{\ell^e} \in G$ we must have $a \in H$ and hence $g \in (K^\times \cap H)^{\ell^e}$. □

One can find $\left[G : G \cap K^{\times \ell^e}\right]$ using [3, Theorem 15] because the parameters for the ℓ-divisibility of G are computable.

8. The eventual maximal growth of the Kummer degrees

Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r.

Theorem 36. *There is a computable integer $n_0 \geqslant 1$ (depending only on K and G) such that, if n, N are multiples of n_0 with $n \mid N$, then we have*

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

It suffices to take n_0 as in Proposition 22.

Proof. We may reduce to the case $N = n\ell$, where ℓ is a prime number. Our choice of n_0 is as in the proof of Theorem 31, so n_0 is computable and we have $E(B_n) = E(B_{n\ell})$. We apply Theorem 1.

If $\ell \nmid n$, then by Proposition 34 we have $[B_{n\ell} : K^\times]/[B_n : K^\times] = [B_\ell : K^\times]$. This index equals ℓ^{r+1} by Proposition 35 because $[G : G \cap K^{\times \ell}] = \ell^r$ by [3, Theorem 15] (all d-divisibility parameters are 0). We conclude that

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

If $\ell \mid n$, set $e := v_\ell(n)$. By 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 [3, Theorem 15] and hence

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

Corollary 37. *There is a computable integer $n_0 \geqslant 1$ (depending only on K and G) such that, if n, N are multiples of n_0 with $n \mid N$, then the restriction to B_N gives a group isomorphism*

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

It suffices to take n_0 as in Proposition 22.

Proof. The restriction to B_N gives an injective group homomorphism, so we prove that the two finite groups have the same size. By [8, 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 Theorem 31. $\square$

Theorem 38. *There is a computable integer $n_0 \geqslant 1$ (depending only on K and G) such that for every $n \geqslant 1$ we have*

$$K(B_n) \cap K(B_{n_0}) = K(B_{\gcd(n,n_0)})$$

and $E(B_n) = E(B_{\gcd(n,n_0)})$. It suffices to take n_0 as in Proposition 22.

Proof. Set $g := \gcd(n, n_0)$ and $l := \mathrm{lcm}(n, n_0)$. The first assertion 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 [8, 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 37 we have

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

so it suffices to prove $\#\operatorname{Aut}_{B_{n_0}}(B_l) \geqslant \#\operatorname{Aut}_{B_g}(B_n)$. By [8, Theorem 2.19] we have

$$\#\operatorname{Aut}_{B_{n_0}}(B_l) = \#\frac{B_l}{B_{n_0}} \cdot \prod_{\substack{p \text{ prime}, \zeta_p \notin K \\ p|l,\, p\nmid n_0}} \frac{p-1}{p},$$

$$\#\operatorname{Aut}_{B_g}(B_n) = \#\frac{B_n}{B_g} \cdot \prod_{\substack{p \text{ prime}, \zeta_p \notin K \\ p|n,\, p\nmid g}} \frac{p-1}{p}.$$

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

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

□

Proof of Theorem 2. This is a consequence of Theorem 38. □

Theorem 39. *There is a computable integer $n_0 \geqslant 1$ (depending only on K and G) such that for every $n \geqslant 1$ we have*

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

where $g := \gcd(n, n_0)$. It suffices to take n_0 as in Proposition 22.

Proof. By Theorem 1, and in view of Theorem 38, 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 Propositions 34 and 35 we have

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

and a similar formula holds by replacing the pair (n, e) by $(g, v_\ell(g))$. By the choice of n_0 and by [3, Theorem 15] the ratio $[G : G \cap K^{\times \ell^e}]/\ell^{er}$ does not change if we replace e by $v_\ell(g)$, and the same holds for $\ell^{\max(0,e-\omega_\ell)}\Delta_{\ell^e}/\varphi(\ell^e)$. □

Proof of Theorem 4. This is a consequence of Theorem 39. □

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

Remark 40. *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*

$$[K(\sqrt[n]{G'}) : K] = \frac{\varphi(nm)n^r}{\varphi(gm)g^r}[K(\sqrt[g]{G'}) : K] \tag{3}$$

where $g := \gcd(n, n_0')$. *Indeed, taking* n_0 *as in Proposition 22 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 (3) *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*

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

9. EXAMPLES

In order to work with our theoretical algorithms in practice, we assume that the field K is *presented* in the sense of [5, 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 41. *Some more information on* K *is needed for the computations in Remark 7 and Remark 21. To compute the parameters for the* ℓ*-divisibility for* G *as in* [3] *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* [6]*). 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* (p) *for every prime number* p *such that* $v_p(N(a)) \neq 0$*, as described in* [2, §4.8]*; we finally determine the correct exponent for each prime ideal using as bound the corresponding exponent in the factorization of* $(N(a))$*. 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* [1].

Example 42. Let $K = \mathbb{Q}(\sqrt{5})$ and $G = \langle g \rangle$, where $g = (2 - 2\sqrt{5}) \cdot \sqrt{5}$. We compute the degree of $K(\sqrt[n]{G})/K$ for every $n \geqslant 1$ by applying Theorem 1.

Since $g = \varepsilon 2^2\sqrt{5}$, where $\varepsilon = \frac{1-\sqrt{5}}{2}$ is a fundamental unit, g is strongly ℓ-indivisible for all primes ℓ. From [3, Theorem 15] we see that $\left[G : G \cap K^{\times \ell^e}\right] = \ell^e$ for all prime powers ℓ^e, thus Propositions 34 and 35 give $[B_n : K^\times] = n^2/\gcd(2, n)$.

Since $\mu_K = \mu_2$, we immediately get $B_{n,\mathrm{ab}} = \langle K^\times, \mu_n, H_n \rangle$, where

$$H_n = \begin{cases} \langle 1 \rangle & \text{if } n \text{ is odd,} \\ \langle \sqrt{g} \rangle & \text{if } n \text{ is even.} \end{cases}$$

The expressions of sine and cosine of $2\pi/5$ in terms of radicals show that $K(\sqrt{g}) = \mathbb{Q}(\mu_5)$. Setting $L_n := K(H_n) \cap \mathbb{Q}(\mu_n)$, by Theorem 13 we have $E(B_{n,\mathrm{ab}}) \cong \mathrm{Gal}(L_n/\mathbb{Q})$.

If $5 \mid n$, then we have $K(H_n) \subseteq \mathbb{Q}(\mu_n)$ and hence $L_n = K(H_n)$. In this case we deduce that $\#E(B_n) = \#E(B_{n,\mathrm{ab}}) = 2\gcd(2, n)$.

If $5 \nmid n$, then K and $\mathbb{Q}(\mu_n)$ are linearly disjoint over $\mathbb{Q}$. Moreover $\sqrt{g} \notin K(\mu_n)$, so we get $L_n = \mathbb{Q}$ and thus $\#E(B_n) = 1$.

Notice that we have

$$\prod_{\substack{p \text{ odd prime} \\ p \mid n}} \frac{p-1}{p} = \frac{\varphi(n)\gcd(2,n)}{n}\,. \tag{4}$$

We conclude that

$$\left[K(\sqrt[n]{G}) : K\right] = \frac{n^2/\gcd(2,n)}{\#E(B_n)} \cdot \frac{\varphi(n)\gcd(2,n)}{n} = \begin{cases} n\varphi(n) & \text{if } 5 \nmid n, \\ n\varphi(n)/2 & \text{if } \gcd(10,n) = 5, \\ n\varphi(n)/4 & \text{if } 10 \mid n. \end{cases}$$

The failure of maximality of the above Kummer degree is due to the following two facts: $K \subseteq \mathbb{Q}(\mu_5)$ and $\sqrt{g} \in \mathbb{Q}(\mu_5)$.

Example 43. 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 an ℓ-good basis of G 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 [3, 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 $\sqrt[4]{3} \notin \mathbb{Q}(\mu_\infty)$ by Lemma 6).

From Theorem 29 we deduce that $B_{n,\mathrm{ab}} = \langle K^\times, \mu_n, H_n\rangle$, where

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

For the computation of $\#E(B_n)$ we apply Theorem 29. We have $\mathbb{Q}(\mu_n \cap K) = \mathbb{Q}$. 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 $\#E(B_n)$ is 4 if $11 \mid n$ and it is 2 otherwise.

If $12 \nmid n$ but 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 $\#E(B_n)$ is 2 if $44 \mid n$ or $33 \mid n$ and it is 1 otherwise.

If n is odd, then we always have $\#E(B_n) = 1$ because $L_n = \mathbb{Q}$.

By (4) we conclude that

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

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

DECLARATIONS AND ACKNOWLEDGMENTS

No funding was received to assist with the preparation of this manuscript. The authors have no conflicts of interest to declare that are relevant to the content of this article. Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

We would like to thank Peter Stevenhagen for introducing us to the work of Lenstra on radical entanglements, and the referee for many useful comments.

REFERENCES

[1] J. BUCHMANN, *Complexity of algorithms in algebraic number theory*, Proceedings of the first conference of the Canadian Number Theory Association, De Gruyter (1990), 37–53.

[2] H. COHEN, *A course in computational algebraic number theory*, Springer Science and Business Media, 2013.

[3] DEBRY, C. - PERUCCA, A., *Reductions of algebraic integers*, J. Number Theory **167** (2016) no. 1, 259–283.

[4] HINDRY, M. - SILVERMAN, J. H.: *Diophantine geometry - An introduction*, Graduate Texts in Mathematics, **201**, Springer-Verlag, New York, 2000.

[5] FRIED, M. D. - JARDEN, M. *Field arithmetic*, Third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge, A Series of Modern Surveys in Mathematics, **11**, Springer-Verlag, Berlin, 2008.

[6] LENSTRA, H. W. JR., *Factoring polynomials over algebraic number fields*, Computer Algebra (1983), 245–254.

[7] LENSTRA, H. W. JR., *Entangled radicals*, Colloquium Lectures, AMS 112th Annual Meeting, San Antonio, January 12–15, 2006, available at `https://www.math.leidenuniv.nl/~hwl/papers/rad.pdf`.

[8] PALENSTIJN, W. J., *Radicals in arithmetic*, PhD thesis, University of Leiden (2014), available at `https://openaccess.leidenuniv.nl/handle/1887/25833`.

[9] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Explicit Kummer theory for the rationals*, Int. J. Number Theory **16** (2020) no. 10, 2213–2231.

[10] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *The degree of Kummer extensions of number fields*, Int. J. Number Theory **17** (2021), no. 5, 1091–1110.

[11] SCHINZEL, A., *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), no. 3, 245–274. Addendum, ibid. **36** (1980) no. 1,101–104. See also Andrzej Schinzel Selecta Vol.II, European Mathematical Society, Zürich, 2007, 939–970.

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

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