THE DEGREE OF KUMMER EXTENSIONS OF NUMBER FIELDS

ANTONELLA PERUCCA, PIETRO SGOBBA AND SEBASTIANO TRONTO

ABSTRACT. Let K be a number field, and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a subgroup of $K^\times$ of rank r. Consider the cyclotomic-Kummer extensions of K given by $K(\zeta_n, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r})$, where n_i divides n for all i. There is an integer x such that these extensions have maximal degree over $K(\zeta_g, \sqrt[g_1]{\alpha_1}, \dots, \sqrt[g_r]{\alpha_r})$, where $g = \gcd(n, x)$ and $g_i = \gcd(n_i, x)$. We prove that the constant x is computable. This result reduces to finitely many cases the computation of the degrees of the extensions $K(\zeta_n, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r})$ over K.

1. INTRODUCTION

Kummer theory is a classical subject in algebraic number theory which was first developed by Kummer in the nineteenth century. General references for the basic results of this theory are [8, Sect. VI.8] and [3].

Given a number field K, we are interested in cyclotomic-Kummer extensions of K. More precisely, let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a multiplicative subgroup of $K^\times$ of positive rank r. Then we are interested in the cyclotomic-Kummer extension

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

where $n_1, \dots, n_r$ are nonnegative integers, m is an integer such that $n_i \mid m$ for all $i \in \{1, \dots, r\}$, and ζ_m denotes a primitive m-th root of unity. The degree of such an extension is "large" because the failure of maximality for the degree, namely the ratio

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

(where φ denotes Euler's totient function), is bounded from above by a constant which does not depend on $m, n_1, \dots, n_r$. This is a classical result of Kummer theory, which also holds more generally (under some assumptions) for products of abelian varieties and tori, see [1, Theorem 1] and [14] (see also [5, Lemme 14] and [2, Theorème 5.2]). Notice that Perucca and Sgobba gave an elementary proof for the existence of this constant, see [11, Theorem 3.1]. As a consequence, we have the following general result:

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

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

2010 *Mathematics Subject Classification.* Primary: 11Y40; Secondary: 11R20, 11R21.
Key words and phrases. Number field, Kummer theory, Kummer extension, degree.

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

In particular, the above result reduces the computation of the cyclotomic-Kummer degree to finitely many cases and hence there exist parametric formulas for the degree (where the parameters are $m, n_1, \dots, n_r$) which involve only a finite case distinction. We prove the following result:

Theorem 1.2. *There is a computable integer constant x satisfying the conclusion of Theorem 1.1.*

For the special case where the parameters $n_1, \dots, n_r$ are all equal, we computed all these cyclotomic-Kummer degrees for the field $\mathbb{Q}$ in [13] (notice that the computation of one single degree was also achieved in [9, Theorem 4.2]), while the case of quadratic fields is treated in [7]. Also notice that for $r = 1$ and m, n_1 powers of a prime number there are explicit formulas for the above degrees, see [10, Section 4].

The structure of the paper is the following: in Sections 2 and 3 we collect preliminary results, in Section 4 we prove the results concerning Kummer degrees related to powers of a prime number, then in Section 5 we prove results about Kummer degrees for general parameters. Finally, in Section 6 we provide some examples of computation of Kummer degrees.

Acknowledgements. We would like to thank the referee, who led the authors to a considerable improvement of the paper.

2. Preliminaries

2.1. **Results for number fields and cyclotomic fields.** Let K be a number field. We say that two finite field extensions F and L of K (contained in one same field) are *linearly disjoint* over K if elements of F which are K-linearly independent are also L-linearly independent. This definition is the same as requiring that the following equality holds:

$$[F : K] \cdot [L : K] = [FL : K] .$$

We say that finitely many field extensions $F_1, \dots, F_r$ of K (contained in one same field) are *linearly disjoint* over K if each of these extensions is linearly disjoint from the compositum of the remaining ones (in other words, if for every i the field F_i is linearly disjoint from $F_1 \cdots \cancel{F_i} \cdots F_r$). Notice that this condition is stronger than requiring the extensions to be pairwise linearly disjoint (consider for example the three quadratic extensions of $\mathbb{Q}$ generated by $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ respectively). The condition is the same as requiring

$$\prod_{i=1}^{r} [F_i : K] = [F_1 \cdots F_r : K] .$$

Lemma 2.1. *Let K be a number field, and let $F_1, \dots, F_r$ be extensions of K which are linearly disjoint over K. For every $i \in \{1, \dots, r\}$ let F_i' be a subextension of F_i/K. Then the extensions $F_1', \dots, F_r'$ are also linearly disjoint over K.*

Proof. We know that for every $i \in \{1, \dots, r\}$ the field $F := F_i$ is linearly disjoint from $L := F_1 \cdots \cancel{F_i} \cdots F_r$. We need to show that for every i the field $F' := F_i'$ is linearly disjoint from $L' := F_1' \cdots \cancel{F_i'} \cdots F_r'$. We have thus reduced the assertion to considering only two fields: prove that if F and L are two extensions of K that are linearly disjoint over K, the same

holds for two subextensions $F' \subseteq F$ and $L' \subseteq L$. Consider a subset of F' consisting of K-linearly independent elements. Since this is also a subset of F, we deduce that the elements are L-linearly independent, and in particular also L'-linearly independent. □

Let us prove a simple lemma in Galois theory:

Lemma 2.2. *Let L_1, L_2 and L_3 be field extensions of K, with $L_1 \subseteq L_2$ and L_2 Galois over K. Then the compositum $L_1(L_2 \cap L_3)$ is equal to the intersection $L_2 \cap (L_1 L_3)$.*

Proof. Let $G = \mathrm{Gal}(\overline{K} \mid K)$ and, for $i \in \{1,2,3\}$, let $G_i := \mathrm{Gal}(\overline{K} \mid L_i)$. The claim is equivalent to $G_1 \cap \langle G_2, G_3\rangle = \langle G_2, G_1 \cap G_3\rangle$, where the inclusion "$\supseteq$" is obvious. Since L_2/K is Galois, the Galois group G_2 is normal in G, so we have $\langle G_2, G_3\rangle = G_2 \cdot G_3$ and $\langle G_2, G_1 \cap G_3\rangle = G_2 \cdot (G_1 \cap G_3)$. Let then $g \in G_1 \cap (G_2 \cdot G_3)$, so that there are $g_1 \in G_1$, $g_2 \in G_2$ and $g_3 \in G_3$ such that $g = g_1 = g_2 g_3$. But then $g_2^{-1} g_1 = g_3 \in G_3$ and, since $G_2 \subseteq G_1$, also $g_2^{-1} g_1 \in G_1$, so that $g = g_2(g_2^{-1} g_1) \in G_2 \cdot (G_1 \cap G_3)$. □

Now we prove two results about cyclotomic extensions, where the field $\mathbb{Q}(\zeta_\infty)$ denotes the compositum of all cyclotomic extensions of $\mathbb{Q}$, and for a prime number ℓ the field $\mathbb{Q}(\zeta_{\ell^\infty})$ is the compositum of all cyclotomic fields $\mathbb{Q}(\zeta_{\ell^n})$ with $n \geqslant 1$.

Lemma 2.3. *Let K be a number field, and let M be an integer such that $K \cap \mathbb{Q}(\zeta_\infty) \subseteq \mathbb{Q}(\zeta_M)$. Then for every integer N with $M \mid N$ we have*

$$[K(\zeta_N) : K(\zeta_M)] = [\mathbb{Q}(\zeta_N) : \mathbb{Q}(\zeta_M)]\,.$$

Let ℓ be a prime number. Let m be such that $K \cap \mathbb{Q}(\zeta_{\ell^\infty}) \subseteq \mathbb{Q}(\zeta_{\ell^m})$. Then for every $n \geqslant m$ we have

$$[K(\zeta_{\ell^n}) : K(\zeta_{\ell^m})] = [\mathbb{Q}(\zeta_{\ell^n}) : \mathbb{Q}(\zeta_{\ell^m})]\,.$$

Proof. Call $I = K \cap \mathbb{Q}(\zeta_\infty)$. We have $I = K \cap \mathbb{Q}(\zeta_M) = K \cap \mathbb{Q}(\zeta_N)$. The fields K and $\mathbb{Q}(\zeta_M)$ are linearly disjoint over their intersection I (because $\mathbb{Q}(\zeta_M)/I$ is Galois, see [8, Ch. VI, Theorem 1.12]), and the same holds for K and $\mathbb{Q}(\zeta_N)$. This implies that

$$[K(\zeta_M) : I] = [K : I][\mathbb{Q}(\zeta_M) : I]$$
$$[K(\zeta_N) : I] = [K : I][\mathbb{Q}(\zeta_N) : I]$$

and we may deduce the first assertion. The proof of the second assertion is analogous. □

Lemma 2.4. *Let K be a number field. If M is an integer such that $K \cap \mathbb{Q}(\zeta_\infty) \subseteq \mathbb{Q}(\zeta_M)$, then for every $N \geqslant 1$ we have*

$$K(\zeta_M) \cap K(\zeta_N) = K(\zeta_{\gcd(M,N)})\,,$$

and $[K(\zeta_N) : K(\zeta_{\gcd(M,N)})] = \varphi(N)/\varphi(\gcd(M,N))$.

Proof. Since $\varphi(\mathrm{lcm}(M,N))\varphi(\gcd(M,N)) = \varphi(M)\varphi(N)$, where φ is Euler's totient function, we have

$$[K(\zeta_N) : K(\zeta_M) \cap K(\zeta_N)] = [K(\zeta_{\mathrm{lcm}(M,N)}) : K(\zeta_M)] = \frac{\varphi(N)}{\varphi(\gcd(M,N))}\,, \tag{2.1}$$

where the second equality follows from Lemma 2.3. Since the extension $K(\zeta_N)/K(\zeta_{\gcd(M,N)})$ has degree dividing $\varphi(N)/\varphi(\gcd(M,N))$, and since $K(\zeta_{\gcd(M,N)}) \subseteq K(\zeta_M) \cap K(\zeta_N)$, the statement follows from (2.1). □

2.2. **Results from Kummer theory.**

Lemma 2.5. *Let K be a number field, and let ℓ be a prime number. Consider algebraic numbers $\alpha_1, \dots, \alpha_r$ in $K^\times$. Let $n_1, \dots, n_r, m$ be nonnegative integers such that $m \geqslant \max_i(n_i)$. Then the degree*

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

divides $\prod_{i=1}^r \ell^{n_i}$. Moreover, equality holds if and only if the fields $K(\zeta_{\ell^m}, \sqrt[\ell^{n_i}]{\alpha_i})$ for $i \in \{1, \dots, r\}$ are linearly disjoint over $K(\zeta_{\ell^m})$ and the degree

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

equals ℓ^{n_i} for every i.

Proof. Notice that $K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r})$ is the compositum of the fields $K(\zeta_{\ell^m}, \sqrt[\ell^{n_i}]{\alpha_i})$, and each of these has degree over $K(\zeta_{\ell^m})$ dividing ℓ^{n_i}, because by Kummer theory the degree is a power of ℓ and we have the defining polynomial $x^{\ell^{n_i}} - \alpha_i$. This suffices to conclude. □

Lemma 2.6. *Let K be a number field, and let ℓ be a prime number. Consider algebraic numbers $\alpha_1, \dots, \alpha_r$ in $K^\times$. Let $N_1, \dots, N_r, M$ be nonnegative integers such that $M \geqslant \max_i(N_i)$. If we have*

$$\left[K\left(\zeta_{\ell^M}, \sqrt[\ell^{N_1}]{\alpha_1}, \dots, \sqrt[\ell^{N_r}]{\alpha_r}\right) : K(\zeta_{\ell^M})\right] = \prod_{i=1}^r \ell^{N_i},$$

then we also have

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

for all nonnegative integers $n_1, \dots, n_r, m$ such that $n_i \leqslant N_i$ for all i and such that $\max_i(n_i) \leqslant m \leqslant M$.

Proof. By Lemma 2.5 the extensions $K(\zeta_{\ell^M}, \sqrt[\ell^{N_i}]{\alpha_i})$ for $i \in \{1, \dots, r\}$ are linearly disjoint over $K(\zeta_{\ell^M})$ and each one has maximal degree ℓ^{N_i}. For each i consider the tower of fields

$$F_0 := K(\zeta_{\ell^M}) \qquad F_1 := F_0(\sqrt[\ell^{n_i}]{\alpha_i}) \qquad F_2 := F_0(\sqrt[\ell^{N_i}]{\alpha_i}).$$

The degree of F_1/F_0 divides ℓ^{n_i} and the degree of F_2/F_1 divides $\ell^{N_i - n_i}$. Since the degree of F_2/F_0 is ℓ^{N_i}, we deduce that the degree of $K(\zeta_{\ell^M}, \sqrt[\ell^{n_i}]{\alpha_i})$ over $K(\zeta_{\ell^M})$ equals ℓ^{n_i}. Moreover, by Lemma 2.1 the extensions $K(\zeta_{\ell^M}, \sqrt[\ell^{n_i}]{\alpha_i})$ for $i \in \{1, \dots, r\}$ are linearly disjoint over $K(\zeta_{\ell^M})$, so Lemma 2.5 gives

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

and we may easily conclude. □

2.3. **The Kummer failure.** Let K be a number field, and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a subgroup G of $K^\times$ of positive rank r. Consider the Kummer degrees

$$\left[K\left(\zeta_M, \sqrt[N_1]{\alpha_1}, \dots, \sqrt[N_r]{\alpha_r}\right) : K(\zeta_M)\right]$$

for all $M, N_1, \dots, N_r$ such that $N_i \mid M$ for all i. More precisely, we consider the ratio

$$C(M, N_1, \dots, N_r) := \frac{\prod_{i=1}^r N_i}{\left[K\left(\zeta_M, \sqrt[N_1]{\alpha_1}, \dots, \sqrt[N_r]{\alpha_r}\right) : K(\zeta_M)\right]}, \tag{2.2}$$

which we call the *Kummer failure at* $M, N_1, \dots, N_r$. For reasons of readability we write $N_i = \prod_\ell \ell^{n_i}$ for the prime factorization of each N_i (each exponent n_i depends on ℓ). Moreover, we set

$$A_\ell(\ell^{n_1}, \dots, \ell^{n_r}) := \frac{\ell^{\sum_i n_i}}{\left[K\left(\zeta_{\ell^n},\ \sqrt[\ell^{n_1}]{\alpha_1}, \dots,\ \sqrt[\ell^{n_r}]{\alpha_r}\right) : K(\zeta_{\ell^n})\right]} \tag{2.3}$$

and

$$B_\ell(M, \ell^{n_1}, \dots, \ell^{n_r}) := \left[K\left(\zeta_{\ell^n},\ \sqrt[\ell^{n_1}]{\alpha_1}, \dots,\ \sqrt[\ell^{n_r}]{\alpha_r}\right) \cap K(\zeta_M) : K(\zeta_{\ell^n})\right], \tag{2.4}$$

with $n := \max_i(n_i)$, which we call the *ℓ-adic failure* and the *ℓ-adelic failure*, respectively. We can decompose (2.2) as

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

because the degree (2.4) is equal to the ratio

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

Proof of Theorem 1.1. As mentioned in the Introduction, there is an integer constant C, which depends only on K and $\alpha_1, \dots, \alpha_r$, such that the ratio

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

divides C for all positive integers $m, n_1, \dots, n_r$ such that $n_i \mid m$ for all i, and we may suppose that this bound is optimal. Notice that if $m', n_1', \dots, n_r'$ are respective multiples of $m, n_1, \dots, n_r$ such that $n_i' \mid m'$ for all i, then we have

$$c(m, n_1, \dots, n_r) \mid c(m', n_1', \dots, n_r').$$

Thus there is a positive integer x such that $c(x, x, \dots, x) = C$. Let $g := \gcd(m, x)$ and $g_i := \gcd(n_i, x)$. We prove that the degree

$$\left[K\left(\zeta_m,\ \sqrt[n_1]{\alpha_1}, \dots,\ \sqrt[n_r]{\alpha_r}\right) : K\left(\zeta_g,\ \sqrt[g_1]{\alpha_1}, \dots,\ \sqrt[g_r]{\alpha_r}\right)\right] \tag{2.5}$$

is maximal, i.e. it equals $\frac{\varphi(m)}{\varphi(g)} \prod_i \frac{n_i}{g_i}$. Let $l := \operatorname{lcm}(m, x)$ and $l_i := \operatorname{lcm}(n_i, x)$ for every i. By definition of x we have

$$c(l, l_1, \dots, l_r) = c(x, x, \dots, x)$$

which implies that

$$\left[K\left(\zeta_l,\ \sqrt[l_1]{\alpha_1}, \dots,\ \sqrt[l_r]{\alpha_r}\right) : K\left(\zeta_x,\ \sqrt[x]{\alpha_1}, \dots,\ \sqrt[x]{\alpha_r}\right)\right] = \frac{\varphi(l)}{\varphi(x)} \prod_i \frac{l_i}{x} = \frac{\varphi(m)}{\varphi(g)} \prod_i \frac{n_i}{g_i}.$$

We may conclude because this degree divides (2.5), considering that

$$K\left(\zeta_m,\ \sqrt[n_1]{\alpha_1}, \dots,\ \sqrt[n_r]{\alpha_r}\right)\left(\zeta_x,\ \sqrt[x]{\alpha_1}, \dots,\ \sqrt[x]{\alpha_r}\right) = K\left(\zeta_l,\ \sqrt[l_1]{\alpha_1}, \dots,\ \sqrt[l_r]{\alpha_r}\right). \qquad \square$$

3. Intersection of Kummer extensions and cyclotomic fields

3.1. **Strongly independent elements.** Let K be a number field, and let ℓ be a prime number. An element $a \in K^\times$ is called *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 ζa is an ℓ-th power in $K^\times$. 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.

Let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. If $g_1, \dots, g_r$ is a basis of G as a free $\mathbb{Z}$-module, we can write

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

for some strongly ℓ-indivisible elements $b_1, \dots, b_r$ of $K^\times$, for some integers $d_i \geqslant 0$ and for some roots of unity $\zeta_{\ell^{h_i}}$ in K of order ℓ^{h_i}. We refer to b_i as the *strongly ℓ-indivisible part* of g_i. We call $g_1, \dots, g_r$ an *ℓ-good basis* of G if $b_1, \dots, b_r$ are strongly ℓ-independent or, equivalently, if the sum $\sum_i d_i$ is maximal among the possible bases of G, see [4, Section 3.1]. In this case we call d_i and h_i the *d-parameters and h-parameters for the ℓ-divisibility* of G in K.

The d-parameters of G are unique up to reordering, while in general the h-parameters are not unique (they may depend on the basis and on the choice of the b_i's, but one could require additional conditions as to make them unique, see [4, Appendix]). Recall from [4, Theorem 14] that an ℓ-good basis of G always exists, and from [4, Section 6.1] that the parameters for the ℓ-divisibility are computable.

Lemma 3.1. *Let $G = \langle g_1, \dots, g_r \rangle$ be a subgroup of $K^\times$, where the given generators form an ℓ-good basis, and let $d_1, \dots, d_r$ be the d-parameters for the ℓ-divisibility. Let $a \in G$, and let $d \geqslant 0$ be the integer such that $a = \zeta b^{\ell^d}$ for some root of unity ζ in K and $b \in K^\times$ strongly ℓ-indivisible. If $a = \prod_{i \in I} g_i^{z_i}$ for some nonzero integers z_i, and where $I \subseteq \{1, \dots, r\}$, then we have $d = \min_{i \in I}(v_\ell(z_i) + d_i)$. Moreover, if $a \notin G^{\ell^y}$, then $d < y + \max_i(d_i)$.*

Proof. We have

$$a = \prod_{i \in I} g_i^{z_i} = \zeta' \prod_{i \in I} b_i^{y_i \ell^{x_i + d_i}},$$

where $x_i = v_\ell(z_i)$, $\ell \nmid y_i$, ζ' is a root of unity in K, and the b_i's are the strongly ℓ-indivisible parts of the g_i's. Without loss of generality, we may suppose that $\min_{i \in I}(x_i + d_i) = x_1 + d_1$. Then, in order to prove that $d = x_1 + d_1$, it is sufficient to notice that the element

$$b_1^{y_1} \cdot \prod_{i \in I,\, i \geqslant 2} b_i^{y_i \ell^{x_i + d_i - (x_1 + d_1)}}$$

is strongly ℓ-indivisible. This holds because if it were an ℓ-th power times a root of unity in K, then we would have $\ell \mid y_1$ as the b_i's are strongly ℓ-independent, which is a contradiction.

To conclude, notice that $x := \min_i(x_i)$ is the greatest integer such that $a \in G^{\ell^x}$. Therefore we obtain that $d \leqslant x + \max_i(d_i)$ and hence if $a \notin G^{\ell^y}$, so that $x < y$, we have $d < y + \max_i(d_i)$. □

3.2. **Intersection with cyclotomic extensions.** Let K be a number field, $G = \langle \alpha_1, \dots, \alpha_r \rangle$ a finitely generated and torsion-free subgroup of $K^\times$ of positive rank (where $\alpha_1, \dots, \alpha_r \in K^\times$ form a basis of G as a $\mathbb{Z}$-module), and ℓ a prime number.

In the following we study the intersection of cyclotomic-Kummer extensions of the form $K(\zeta_{\ell^m},\,\sqrt[\ell^n]{G}) = K(\zeta_{\ell^m},\,\sqrt[\ell^n]{\alpha_1},\dots,\,\sqrt[\ell^n]{\alpha_r})$, where $m \geqslant n$, with $K(\zeta_\infty)$. For m and n fixed, this intersection is abelian over K and clearly contains ζ_{ℓ^m}. However, if ℓ is such that $\zeta_\ell \notin K$, then by Schinzel's theorem on abelian radical extensions (see for instance [11, Theorem 3.3]), an element $a \in K$ is such that the extension $K(\zeta_{\ell^n},\,\sqrt[\ell^n]{a})$ is abelian over K if and only if it is an ℓ^n-th power in K. Therefore, in the remaining part of this section we consider a prime number ℓ such that $\zeta_\ell \in K$.

Proposition 3.2. *There is a computable integer t, which depends only on ℓ, K and G, such that for every $m \geqslant n \geqslant t$ we have*

$$K\big(\zeta_{\ell^m},\,\sqrt[\ell^n]{G}\big) \cap K(\zeta_\infty) = K\big(\zeta_{\ell^m},\,\sqrt[\ell^t]{G}\big) \cap K(\zeta_\infty) \tag{3.1}$$

and for every $M \geqslant 1$ with $\ell^m \mid M$ we have

$$K\big(\zeta_{\ell^m},\,\sqrt[\ell^t]{G}\big) \cap K(\zeta_M) = \Big(K\big(\zeta_{\ell^t},\,\sqrt[\ell^t]{G}\big) \cap K(\zeta_M)\Big)(\zeta_{\ell^m})\,. \tag{3.2}$$

The analogous equality holds with $K(\zeta_\infty)$ in place of $K(\zeta_M)$. Moreover, the above assertions still hold if we replace t with any t' such that $m \geqslant n \geqslant t' \geqslant t$, and (3.2) *also holds if we replace G with any subgroup G' of G.*

Proof. Let $t = \tau + \max_i(d_i)$ where τ is the largest integer such that $\zeta_{\ell^\tau} \in K$ and where the d_i's are the d-parameters for the ℓ-divisibility of G in K. Set $L := K(\zeta_{\ell^m})$. Both intersections of fields in (3.1) are abelian extensions of L of exponent dividing ℓ^n, so by Kummer theory (see [8, Ch.VI, Theorem 8.2]) we have

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

where H_1, H_2 are subgroups of $L^\times$ such that $H_1 L^{\times\ell^n} \subseteq G L^{\times\ell^n}$ and $H_2 L^{\times\ell^n} \subseteq G^{\ell^{n-t}} L^{\times\ell^n}$.

The inclusion in (3.1) is clear. Suppose that there is $n > t$ such that

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

which implies that $H_1 L^{\times\ell^n} \supsetneq H_2 L^{\times\ell^n}$, again by Kummer theory. Then there is an element $a \in H_1$ (we may suppose that $a \in G$) such that $\sqrt[\ell^n]{a} \notin L(\sqrt[\ell^n]{H_2})$. Since $\sqrt[\ell^n]{a} \in K(\zeta_\infty)$, we deduce $\sqrt[\ell^n]{a} \notin \sqrt[\ell^t]{G}$, which yields $a \notin G^{\ell^{n-t}}$. Write $a = \zeta b^{\ell^d}$ where ζ is a root of unity in K of order a power of ℓ, $b \in K^\times$ is strongly ℓ-indivisible and $d \geqslant 0$. Then by Lemma 3.1 we obtain $d < n - t + \max_i(d_i) = n - \tau$.

On the other hand, since $\sqrt[\ell^n]{a}$ lies in $K(\zeta_\infty)$, the extension $K(\zeta_{\ell^n},\,\sqrt[\ell^n]{a})$ is abelian over K. Then by Schinzel's theorem we have $a^{\ell^x} = c^{\ell^n}$ for some $x \leqslant \tau$ and $c \in K$. This implies that a is at least an $\ell^{n-\tau}$-th power in K times a root of unity in K, which is a contradiction as $d < n - \tau$. We may clearly replace t by any larger integer t' as in the statement.

In order to prove (3.2), it is sufficient to apply Lemma 2.2 to the fields $K(\zeta_{\ell^m})$, $K(\zeta_M)$ and $K(\zeta_{\ell^t},\,\sqrt[\ell^t]{G})$, where $K(\zeta_{\ell^m}) \subseteq K(\zeta_M)$ and $K(\zeta_M)/K$ is Galois. The last assertion is clear because the proof of (3.2) only relies on Lemma 2.2. □

As a side remark, observe that in (3.1) we cannot in general replace G by a subgroup G': for example we can take $t = 1$ for $K = \mathbb{Q}$, $\ell = 2$, and $G = \langle 5 \rangle$, but we cannot take $t = 1$ for $G' = \langle 5^2 \rangle$ (the equality fails for $m = n = 2$).

Lemma 3.3. *There exists a computable integer constant M_0, depending only on ℓ, K and G, such that, denoting by t_0 its ℓ-adic valuation, the following hold:*

(i) We have $K \cap \mathbb{Q}(\zeta_\infty) \subseteq \mathbb{Q}(\zeta_{M_0})$.

(ii) We have $t_0 \geqslant t$, where t is the integer of Proposition 3.2, so that for every $m \geqslant n \geqslant t_0$ we have

$$K\big(\zeta_{\ell^m},\, \sqrt[\ell^n]{G}\big) \cap K(\zeta_\infty) = K\big(\zeta_{\ell^m},\, \sqrt[\ell^{t_0}]{G}\big) \cap K(\zeta_\infty)\,.$$

(iii) We have

$$K\big(\zeta_{\ell^{t_0}},\, \sqrt[\ell^{t_0}]{G}\big) \cap K(\zeta_\infty) \subseteq K(\zeta_{M_0})\,. \tag{3.3}$$

Moreover, the above three properties still hold if we replace M_0 with any multiple M' of M_0 and t_0 with $v_\ell(M')$.

Proof. An integer M satisfying $K \cap \mathbb{Q}(\zeta_\infty) \subseteq \mathbb{Q}(\zeta_M)$ is given by the product of all primes p which ramify in K, with exponents according to the prime factorization of $[K : \mathbb{Q}]$. The integer t of condition (ii) is computable by Proposition 3.2.

As for condition (iii), it is sufficient to determine a computable integer N such that

$$K\big(\zeta_{\ell^t},\, \sqrt[\ell^t]{G}\big) \cap K(\zeta_\infty) \subseteq K(\zeta_N)\,. \tag{3.4}$$

Indeed, the inclusion (3.3) would then follow from (3.1) and (3.2). In view of this argument, it is clear that the statement still holds if we replace M_0 by a multiple. Hence we will take $M_0 = \operatorname{lcm}(M, N)$, with $\ell^t \mid N$.

Since $K(\zeta_{\ell^t},\, \sqrt[\ell^t]{G})/K(\zeta_{\ell^t})$ has degree dividing ℓ^{tr} (where r is the rank of G) and $[K(\zeta_N) : K]$ divides $\varphi(N)$, we may take for N a power of ℓ times a squarefree product of primes congruent to 1 modulo ℓ (indeed, if $N = x\ell^t$ and $N' = x'\ell^t$ are such that $x' \mid x$ and $\varphi(x)$ and $\varphi(x')$ have the same ℓ-adic valuation, then we may replace N by N'). The ℓ-adic valuation of N can be taken to be $t+\omega$, where ω is the largest integer such that $\zeta_{\ell^\omega} \in K(\zeta_{\ell^t})$, because the intersection on the left-hand side of (3.4) is an abelian extension of $K(\zeta_{\ell^t})$ of exponent dividing ℓ^t. As we argued in the proof of Proposition 3.2, by Kummer theory we have

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

where H is a subgroup of $K(\zeta_{\ell^t})^\times$ which we may assume to be contained in G. In particular, there is a basis $\{g_i\}$ of H as a $\mathbb{Z}$-module with $g_i \in G$. In order to find the other prime factors of N, by [6, Lemma C.1.7] it is sufficient to consider the finitely many primes which ramify in K or which lie below the primes $\mathfrak{p}$ of K such that the $\mathfrak{p}$-adic valuation of g_i is not divisible by ℓ^t for some i. Among these primes we only need to take those which are congruent to 1 modulo ℓ. Notice that the rational primes below the primes of K in the factorizations of the g_i's can be found by looking at the absolute norm of each g_i. □

Lemma 3.4. *Let M_0 and t_0 be as in Lemma 3.3. Then for every $m \geqslant t_0$ and $M \geqslant 1$ with $\ell^m \mid M$ we have*

$$\big[K\big(\zeta_{\ell^m},\, \sqrt[\ell^{t_0}]{G}\big) \cap K(\zeta_M) : K(\zeta_{\ell^m})\big] = \big[K\big(\zeta_{\ell^{t_0}},\, \sqrt[\ell^{t_0}]{G}\big) \cap K(\zeta_{\gcd(M,M_0)}) : K(\zeta_{\ell^{t_0}})\big]\,.$$

Moreover, the same holds if we replace G by a subgroup (keeping the same M_0 and t_0).

Proof. Let $g = \gcd(M, M_0)$. We first prove that

$$K\big(\zeta_{\ell^m},\, \sqrt[\ell^{t_0}]{G}\big) \cap K(\zeta_M) = \Big(K\big(\zeta_{\ell^{t_0}},\, \sqrt[\ell^{t_0}]{G}\big) \cap K(\zeta_g)\Big)(\zeta_{\ell^m})\,.$$

It is sufficient to apply (3.2) and make use of the equality

$$K\big(\zeta_{\ell^{t_0}},\ \sqrt[\ell^{t_0}]{G}\big)\cap K(\zeta_M)=K\big(\zeta_{\ell^{t_0}},\ \sqrt[\ell^{t_0}]{G}\big)\cap K(\zeta_g)\,,$$

which we obtain by applying Lemma 2.4 for M_0 in view of (3.3). Next, the fields $K(\zeta_{\ell^{t_0}},\ \sqrt[\ell^{t_0}]{G})\cap K(\zeta_g)$ and $K(\zeta_{\ell^m})$ are disjoint over $K(\zeta_{\ell^{t_0}})$ because we have

$$K(\zeta_g)\cap K(\zeta_{\ell^m})=K(\zeta_{\ell^{t_0}})\,.$$

Indeed, the intersection on the left-hand side is contained in $K(\zeta_{M_0})$ and by Lemma 2.4 we have $K(\zeta_{M_0})\cap K(\zeta_{\ell^m})=K(\zeta_{\ell^{t_0}})$. From this, we deduce the assertion on the degree.

The last assertion in the statement holds because all the arguments used in the proof are still valid in this case. Indeed, the only step which uses a result related to G is the application of (3.2), but we can rely on the last assertion of Proposition 3.2. □

4. KUMMER EXTENSIONS: POWERS OF A PRIME

Let K be a number field, and let $\alpha_1,\dots,\alpha_r$ be elements of $K^\times$ which generate a subgroup G of $K^\times$ of positive rank r. In this section we fix some prime number ℓ and consider cyclotomic-Kummer extensions of the form $K(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1},\dots,\ \sqrt[\ell^{n_r}]{\alpha_r})$ where $m,n_1,\dots,n_r$ are nonnegative integers such that $m\geqslant\max_i(n_i)$. By Lemma 2.5 the degree of this extension over $K(\zeta_{\ell^m})$ is a power of ℓ. Recall that for all nonnegative integers n, m with $m\geqslant n$ we write $K(\zeta_{\ell^m},\ \sqrt[\ell^n]{G})$ for the field $K(\zeta_{\ell^m},\ \sqrt[\ell^n]{\alpha_1},\dots,\ \sqrt[\ell^n]{\alpha_r})$.

4.1. **Results for equal parameters.**

Theorem 4.1 ([4, Theorem 18])**.** *Suppose that ℓ is odd or that $\zeta_4\in K$. Let $\omega\geqslant 1$ be the largest integer satisfying $K(\zeta_\ell)=K(\zeta_{\ell^\omega})$. Let m and n be positive integers such that $m\geqslant\max(n,\omega)$. Then we have*

$$v_\ell\Big[K\big(\zeta_{\ell^m},\ \sqrt[\ell^n]{G}\big):K(\zeta_{\ell^m})\Big]=\max_{i\in\{1,\dots,r\}}(h_i+\min(n,d_i)-m,0)+\sum_{i=1}^{r}\max(n-d_i,0)\,,\tag{4.1}$$

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

Notice that Theorem 4.1 applies also when $\omega>m\geqslant n$, since $K(\zeta_{\ell^m},\ \sqrt[\ell^n]{G})=K(\zeta_{\ell^\omega},\ \sqrt[\ell^n]{G})$ for all $1\leqslant m<\omega$, so that it is sufficient to replace m with ω in the formula (4.1).

Remark 4.2. *If $m\geqslant n$, then the degree*

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

is computable and it depends only on the integers m,n and on finitely many parameters describing the ℓ-divisibility of G in the considered number field. Indeed, if ℓ is odd or $\zeta_4\in K$ it suffices to take the formula provided by Theorem 4.1 (because $m\geqslant\omega$ without loss of generality, the case $m=0$ being trivial). Now, suppose that $\ell=2$ and $\zeta_4\notin K$. If $m\geqslant 2$, then we can extend the base field to $K(\zeta_4)$ and reduce to the previous case (notice that in [12] *we proved that the 2-divisibility parameters of G over $K(\zeta_4)$ are determined by properties over K). We are left to compute the degree $[K(\sqrt{G}):K]$, and this can be achieved with* [4, Lemma 19].

Lemma 4.3. *There is a computable integer s, which depends only on ℓ, K and G, such that for every $m\geqslant n\geqslant s$ we have*

$$\big[K\big(\zeta_{\ell^m},\ \sqrt[\ell^n]{G}\big):K(\zeta_{\ell^m})\big]=\ell^{r(n-s)}\big[K\big(\zeta_{\ell^m},\ \sqrt[\ell^s]{G}\big):K(\zeta_{\ell^m})\big]\,.\tag{4.2}$$

We may take

$$s = \max_{i\in\{1,\dots,r\}} (\varepsilon,\, h_i + d_i)\,, \tag{4.3}$$

where $\varepsilon = 2$ if $\ell = 2$ and $\zeta_4 \notin K$, and $\varepsilon = 0$ otherwise, and where the integers d_i and h_i are parameters for the ℓ-divisibility of G in K (respectively, in $K(\zeta_4)$ if $\ell = 2$ and $\zeta_4 \notin K$).

Proof. It is sufficient to apply (4.1) with our choice of s. For $\ell = 2$ and $\zeta_4 \notin K$ we take $s \geqslant 2$, so that the Kummer degrees appearing in (4.2) can be computed by Theorem 4.1. Notice that the equality (4.2) holds also in the case $s < \omega$ (where ω is as in Theorem 4.1) because if $1 \leqslant m < \omega$ we may replace m by ω. □

Lemma 4.4. *The integer s of Lemma 4.3 is such that for every $m \geqslant s$ we have*

$$K\big(\zeta_{\ell^s},\, \sqrt[\ell^s]{G}\big) \cap K(\zeta_{\ell^m}) = K(\zeta_{\ell^s})\,.$$

Proof. Applying (4.1) it is easy to check that the integer s as in (4.3) (or any larger integer) satisfies

$$\big[K\big(\zeta_{\ell^m},\, \sqrt[\ell^s]{G}\big) : K(\zeta_{\ell^m})\big] = \big[K\big(\zeta_{\ell^s},\, \sqrt[\ell^s]{G}\big) : K(\zeta_{\ell^s})\big]$$

for all $m \geqslant s$ (recall that $s \geqslant 2$ if $\ell = 2$ and $\zeta_4 \notin K$). We deduce that the fields $K(\zeta_{\ell^s},\, \sqrt[\ell^s]{G})$ and $K(\zeta_{\ell^m})$ are linearly disjoint over $K(\zeta_{\ell^s})$. □

Proposition 4.5. *Fixing K and G, the integer s of Lemma 4.3 can be taken to be equal to zero for all but finitely many prime numbers ℓ. Moreover, the finite set of primes ℓ for which s might be nonzero can be computed.*

Proof. Let s be as in (4.3). By [11, Theorem 2.7] there is a basis of G as a $\mathbb{Z}$-module consisting of strongly ℓ-independent elements for all but finitely many primes ℓ, so that parameters for the ℓ-divisibility of G in K might be not all zero only for finitely many primes ℓ.

The finite set S of these primes can be computed by [11, Proof of Theorem 2.7]. Following this reference, the set S consists of the primes ℓ such that $\zeta_\ell \in K$ and those involved in the following computations. Write $G = F \times H$ where F and H are subgroups of $K^\times$ such that $F \cap \mathcal{O}_K^\times = \{1\}$ and $H \subseteq \mathcal{O}_K^\times$ ($\mathcal{O}_K$ is the ring of integers of K), and consider a basis of G consisting of a basis $\{g_i\}$ of F and a basis $\{u_i\}$ of H as $\mathbb{Z}$-modules. We consider the prime ideal factorizations $(g_i) = \prod_j \mathfrak{p}_j^{e_{ij}}$ where the $\mathfrak{p}_j$'s are finitely many distinct primes of K, and without loss of generality we write $u_i = \prod_j b_j^{f_{ij}}$ where the b_j's form a system of fundamental units in K. Then when applying [11, Lemmas 2.4 and 2.5] we obtain that S contains the finitely many rational primes ℓ dividing a nonzero minor corresponding to a maximal square submatrix of the matrices (e_{ij}) and (f_{ij}), respectively. The considered basis of G consists of strongly ℓ-independent elements for all $\ell \notin S$, and hence $s = 0$ for all these primes. □

4.2. **Results for general parameters.**

Proposition 4.6. *There is a computable integer s, which depends only on K, ℓ, and $\alpha_1, \dots, \alpha_r$, such that if $n_1, \dots, n_r, m$ are integers with $\min_i(n_i) \geqslant s$ and $m \geqslant \max_i(n_i)$, then we have*

$$v_\ell\left[K\big(\zeta_{\ell^m},\, \sqrt[\ell^{n_1}]{\alpha_1}, \dots,\, \sqrt[\ell^{n_r}]{\alpha_r}\big) : K\big(\zeta_{\ell^m},\, \sqrt[\ell^s]{G}\big)\right] = \sum_{i=1}^{r} (n_i - s)\,.$$

Proof. Let s be as in Lemma 4.3, and let $n = \max_i(n_i)$: we then have

$$\left[K\left(\zeta_{\ell^m},\ \sqrt[\ell^n]{G}\right) : K\left(\zeta_{\ell^m},\ \sqrt[\ell^s]{G}\right)\right] = \ell^{r(n-s)}\,. \tag{4.4}$$

Let $F = K(\zeta_{\ell^m},\ \sqrt[\ell^s]{G})$, and write $\beta_i = \sqrt[\ell^s]{\alpha_i}$. Formula (4.4) implies by Lemma 2.6 that

$$\left[F\left(\sqrt[\ell^{n_1-s}]{\beta_1}, \ldots,\ \sqrt[\ell^{n_r-s}]{\beta_r}\right) : F\right] = \prod_{i=1}^{r} \ell^{n_i-s}\,. \qquad \square$$

Remark 4.7. *Fix K and $\alpha_1, \ldots, \alpha_r$. By Proposition 4.6 together with Proposition 4.5 and Lemma 2.3 one can easily deduce that for all but finitely many prime numbers ℓ we have*

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

Indeed, if $s = 0$, then Proposition 4.6 reduces the computation of the above degree to the cyclotomic degree $[K\left(\zeta_{\ell^m}\right) : K]$, which equals $\varphi(\ell^m)$ by Lemma 2.3 for all but finitely many primes ℓ.

Proposition 4.8. *There is a computable integer s, which depends only on K, ℓ, and $\alpha_1, \ldots, \alpha_r$, such that if $n_1, \ldots, n_r, m$ are integers with $m \geqslant \max_i(n_i)$, then setting $m_i := \min(n_i, s)$ for all i we have*

$$v_\ell\left[K\left(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1}, \ldots,\ \sqrt[\ell^{n_r}]{\alpha_r}\right) : K\left(\zeta_{\ell^m},\ \sqrt[\ell^{m_1}]{\alpha_1}, \ldots,\ \sqrt[\ell^{m_r}]{\alpha_r}\right)\right] = \sum_{i=1}^{r} \max(n_i - s, 0)\,. \tag{4.5}$$

Proof. Let s be as in Proposition 4.6, and set $v_i := \max(n_i, s)$ for all i, so that

$$\left[K\left(\zeta_{\ell^m},\ \sqrt[\ell^{v_1}]{\alpha_1}, \ldots,\ \sqrt[\ell^{v_r}]{\alpha_r}\right) : K\left(\zeta_{\ell^m},\ \sqrt[\ell^s]{G}\right)\right] = \prod_{i=1}^{r} \ell^{v_i-s} = \prod_{i=1}^{r} \ell^{\max(n_i-s,0)}\,. \tag{4.6}$$

We may conclude because the degree in (4.6) divides the degree in (4.5), and the latter degree clearly divides $\prod_i \ell^{\max(n_i-s,0)}$. $\square$

Recall the notation of Section 2.3.

Remark 4.9. *Proposition 4.8 implies that there is a computable integer A, which depends only on ℓ, K and $\alpha_1, \ldots, \alpha_r$, such that the ℓ-adic failure $A_\ell(\ell^{n_1}, \ldots, \ell^{n_r})$ divides A. More generally, there is a computable integer A such that*

$$\frac{\prod_{i=1}^{r} \ell^{n_i}}{\left[K\left(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1}, \ldots,\ \sqrt[\ell^{n_r}]{\alpha_r}\right) : K(\zeta_{\ell^m})\right]} \mid A \tag{4.7}$$

for all nonnegative integers $n_1, \ldots, n_r, m$ with $m \geqslant \max_i(n_i)$. Indeed, by Proposition 4.8 we may replace each n_i in (4.7) *by $\min(n_i, s)$, where s can be taken as in* (4.3)*. Thus we may take $A = \ell^{rs}$, and hence by Proposition 4.5 we have $A = 1$ for all but finitely many prime numbers ℓ.*

Notice that the bound $A = \ell^{rs}$ is in general optimal. Indeed, for the case $\ell \neq 2$ or $\zeta_4 \in K$ it suffices to consider ℓ^s-th powers of strongly ℓ-independent elements of K, so that the parameters for the ℓ-divisibility in (4.3) *are $h_i = 0$ and $d_i = s$ for all $i \in \{1, \ldots, r\}$.*

5. KUMMER EXTENSIONS: THE GENERAL CASE

Let K be a number field, and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a subgroup G of $K^\times$ of positive rank r. In this section we study the Kummer degrees

$$\left[K\left(\zeta_M, \sqrt[N_1]{\alpha_1}, \dots, \sqrt[N_r]{\alpha_r}\right) : K(\zeta_M)\right],$$

for all $M, N_1, \dots, N_r$ such that $N_i \mid M$ for all i. Recall the notation of Section 2.3.

5.1. The ℓ-adic and ℓ-adelic failure.

Lemma 5.1. *Let ℓ be a prime number and let s be the computable integer of Lemma 4.3 for G. For all integers $n_1, \dots, n_r$, we have*

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

Proof. As we argued in Remark 4.9, in view of Proposition 4.8 we may replace each n_i in the ratio (2.3) by $\min(n_i, s)$. So, we are left to check that if $n_j > s$ for some j, then setting $n = \max_i(n_i)$ and $m_i := \min(n_i, s)$ we have

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

This is a consequence of the equality

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

which is true because $K(\zeta_{\ell^s}, \sqrt[\ell^{m_1}]{\alpha_1}, \dots, \sqrt[\ell^{m_r}]{\alpha_r}) \subseteq K(\zeta_{\ell^s}, \sqrt[\ell^s]{G})$ and the intersection of the latter field with $K(\zeta_{\ell^n})$ is equal to $K(\zeta_{\ell^s})$ by Lemma 4.4. Hence $n = \max_i(n_i)$ can be replaced by $\min(n, s)$ in the ratio (2.3). □

Remark 5.2. *Let ℓ be a prime number, let $n_1, \dots, n_r$ be nonnegative integers, and set $n = \max_i(n_i)$. Since we have*

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

by [11, Lemma 3.5] *the ℓ-adelic failure divides $\ell^{\tau r}$, where τ is the largest integer such that $\zeta_{\ell^\tau} \in K$. In particular, the ℓ-adelic failure equals 1 if $\zeta_\ell \notin K$.*

Theorem 5.3. *Let ℓ be a prime number such that $\zeta_\ell \in K$. There are computable integer constants M_0 and t, depending only on ℓ, K and $\alpha_1, \dots, \alpha_r$, with $\ell^t \mid M_0$, such that for all integers $M, n_1, \dots, n_r$ with $\ell^{n_i} \mid M$ for all i we have*

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

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

Proof. Let t_0 and M_0 be as in Lemma 3.3 and s as in Lemma 4.3 for G. Take $t = \max(t_0, s)$, and by Lemma 3.3 we may suppose $\ell^t \mid M_0$, up to replacing M_0 with a multiple. Notice that t and M_0 are computable.

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

Case 2: Suppose that $n_j > t$ for some j. Since $t \geqslant s$ (recall that $s \geqslant 2$ if $\ell = 2$ and $\zeta_4 \notin K$), setting $n := \max_i(n_i)$, by Lemma 4.3 we have

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

This says in particular that each element $\sqrt[\ell^t]{\alpha_i}$ is strongly ℓ-indivisible in $K(\zeta_{\ell^n}, \sqrt[\ell^t]{G})$. We prove that, if $n_j > t$, then we may replace n_j by t in the degree (2.4). More precisely, setting

$$L_j := K\big(\zeta_{\ell^n}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^t]{\alpha_j}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}\big)\,,$$

we prove that

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

We already know that since $L_j(\sqrt[\ell^{n_j}]{\alpha_j}) \subseteq K(\zeta_{\ell^n}, \sqrt[\ell^n]{G})$, in view of Lemma 3.3 we have

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

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

Hence in (2.4) we may replace each ℓ^{n_i} by $\gcd(\ell^{n_i}, \ell^t)$. We conclude by applying Lemma 3.4 which allows us to replace n by t, and M by $\gcd(M, M_0)$. □

5.2. **The Kummer failure.**

Theorem 5.4. *There are computable integer constants M_0 and N_0 with $N_0 \mid M_0$, depending only on K and $\alpha_1, \dots, \alpha_r$, such that for all integers $M, N_1, \dots, N_r$ where $N_i \mid M$ for all $i \in \{1, \dots, r\}$ we have*

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

Proof. It suffices to combine Theorem 5.3 (applied to all ℓ such that $\zeta_\ell \in K$) with Lemma 5.1 and Remark 5.2. More precisely, for ℓ such that $\zeta_\ell \in K$ let $M_{0,\ell}$ and t_ℓ be the integers of Theorem 5.3, and otherwise let $t_\ell = s_\ell$, where s_ℓ is the integer of Lemma 5.1. Notice that in the former case we are supposing $t_\ell \geqslant s_\ell$, as we did in the proof of Theorem 5.3. Also, we have $t_\ell = 0$ for all but finitely many primes ℓ (see Proposition 4.5). Then we may take $N_0 = \prod_\ell \ell^{t_\ell}$ and M_0 to be the least common multiple of the integers $M_{0,\ell}$ and N_0. □

Corollary 5.5. *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. There are computable integer constants M_0 and N_0, depending only on K and G, such that for all integers M, N with $N \mid M$, the Kummer failure*

$$C'(M, N) := \frac{N^r}{\big[K\big(\zeta_M, \sqrt[N]{G}\big) : K(\zeta_M)\big]}$$

satisfies

$$C'(M, N) = C'(\gcd(M, M_0), \gcd(N, N_0))\,.$$

Proof. This is a direct consequence of Theorem 5.4. □

Proof of Theorem 1.2. Take $x := M_0$, where M_0 is the computable integer of Theorem 5.4. Notice that x satisfies $K \cap \mathbb{Q}(\zeta_\infty) \subseteq \mathbb{Q}(\zeta_x)$, so that by Lemma 2.4 we have

$$\big[K\big(\zeta_m\big) : K\big(\zeta_{\gcd(m,x)}\big)\big] = \frac{\varphi(m)}{\varphi(\gcd(m,x))}\,.$$

By Theorem 5.4 we have

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

and hence we may easily conclude. □

6. Examples

In this section, we collect various examples to illustrate our results.

Example 6.1. Let $K = \mathbb{Q}$ and $\ell = 3$. Consider the elements $\alpha_1 = 2$, $\alpha_2 = 3$, and $\alpha_3 = 5$. The 3-divisibility parameters of the group $G = \langle 2, 3, 5\rangle$ over $\mathbb{Q}$ are all zero, so by (4.3) we can take $s = 0$ in Lemma 4.3 and hence also in Propositions 4.6 and 4.8. We deduce that we have

$$\big[K\big(\zeta_{3^m},\ \sqrt[3^{n_1}]{2},\ \sqrt[3^{n_2}]{3},\ \sqrt[3^{n_3}]{5}\big) : K(\zeta_{3^m})\big] = 3^{n_1+n_2+n_3}$$

for all nonnegative integers m, n_1, n_2, n_3 with $m \geqslant \max(n_1, n_2, n_3)$.

A generalization of the above example is the following remark:

Remark 6.2. *Let K be a number field. Suppose that ℓ is odd or that $\zeta_4 \in K$. Consider elements $\alpha_1, \dots, \alpha_r$ of $K^\times$ which generate a subgroup of $K^\times$ of positive rank r. Suppose that $\alpha_i = \beta_i^{\ell^{d_i}}$ where $\beta_1, \dots, \beta_r$ are strongly ℓ-independent elements of K. We have*

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

We conclude that

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

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

Example 6.3. Let $K = \mathbb{Q}$ and $\ell = 2$. Consider the elements $\alpha_1 = -4$, $\alpha_2 = 5$. The 2-divisibility parameters of the group $G = \langle -4, 5\rangle$ over $\mathbb{Q}(\zeta_4)$ are $(d_1, d_2; h_1, h_2) = (2, 0; 0, 0)$ because $-4 = (1+i)^4$ (and $1+i$ generates a prime ideal, hence it is strongly 2-indivisible). Then by (4.3) we can take $s = 2$ in Lemma 4.3 and hence also in Propositions 4.6 and 4.8.

For all nonnegative integers m, n_1, n_2 with $m \geqslant \max(n_1, n_2)$ denote by $\deg(m, n_1, n_2)$ the degree of $\mathbb{Q}(\zeta_{2^m},\ \sqrt[2^{n_1}]{-4},\ \sqrt[2^{n_2}]{5})$ over $\mathbb{Q}(\zeta_{2^m})$. By Proposition 4.8 it suffices to compute $\deg(m, n_1, n_2)$ for $n_1, n_2 \leqslant 2$ in order to deduce formulas that cover all cases. In the end we get the following:

- for $m = 0, 1$ we find $\deg(m, n_1, n_2) = 2^{n_1+n_2}$ case by case;
- for $m \geqslant 2$ and $n_1 = 0, 1$, since $\sqrt[4]{-4} \in \mathbb{Q}(\zeta_{2^m})$, we find $\deg(m, n_1, n_2) = 2^{n_2}$;
- for $m \geqslant 2$ and $n_1 \geqslant 2$ we have $\deg(m, n_1, n_2) = 2^{n_1+n_2-2}$.

Example 6.4. Consider cyclotomic-Kummer extensions of the form

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

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

Let $G = \langle 2, -9\rangle$. The ℓ-divisibility parameters of G over $\mathbb{Q}$ are all zero for every odd prime ℓ. It follows from Lemma 5.1 that the ℓ-adic failure is 1 for all odd primes ℓ. Moreover, since the only nontrivial root of unity in $\mathbb{Q}$ is $\zeta_2 = -1$, by Remark 5.2 it follows that the ℓ-adelic failure is also 1 for every odd prime ℓ.

For $\ell = 2$ we need to compute the 2-divisibility parameters of G over $\mathbb{Q}(i)$ (see Remark 4.2 and Lemma 4.3). Over this field we have $2 = -i(1+i)^2$, and $1+i$ and 3 are strongly 2-independent, so the divisibility parameters are

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

It follows from Lemma 5.1 that we have

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

so we only need to compute

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

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

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

We now compute the 2-adelic failure

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

for any M, n_1, n_2 with $n_1, n_2 \leqslant v_2(M)$, and where $n = \max(n_1, n_2)$. By Theorem 5.3 we just need to compute such values for $n_1, n_2 \leqslant 3$ and $M \mid 24$. We take into account that:

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

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

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

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

whereas for $m \geqslant n \geqslant 2$

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

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

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

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

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

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

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

REFERENCES

[1] BERTRAND, D., *Galois representations and transcendental numbers*, in: A. Baker (ed.), New Advances in Transcendence Theory (Durham 1986), Cambridge University Press, 1988, 37–55.

[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] BIRCH, B.J., *Cyclotomic fields and Kummer extensions*, in Algebraic Number Theory, edited by J.W.S. Cassels and A. Fröhlich, Academic Press, London, 1967, 85–93.

[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. H.: *Diophantine geometry - An introduction*, Graduate Texts in Mathematics, Vol. 201, Springer-Verlag, New York, 2000.

[7] HÖRMANN, F. - PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Explicit Kummer theory for quadratic fields*, preprint available on ORBilu: `http://hdl.handle.net/10993/42266`.

[8] LANG, S., *Algebra*, Revised third edition, Graduate Texts in Mathematics, Vol. 211, Springer-Verlag, New York (2002).

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

[10] PERUCCA, A., *The order of the reductions of an algebraic integer*, J. Number Theory **148** (2015) 121–136.

[11] PERUCCA, A. - SGOBBA, P.: *Kummer theory for number fields and the reductions of algebraic numbers*, Int. J. Number Theory **15** (2019), no. 8 , 1617–1633.

[12] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Addendum to: Reductions of algebraic integers [J. Number Theory 167 (2016) 259–283]*, J. Number Theory **209** (2020) 391–395.
[13] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Explicit Kummer theory for the rational numbers*, Int. J. Number Theory **16** (2020), no. 10, 2213-2231.
[14] RIBET, K., *Kummer theory on extensions of abelian varieties by tori*, Duke Math. J. **46** (1979) 745–761.

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