GALOIS GROUPS OF KUMMER EXTENSIONS OF NUMBER FIELDS

BRYAN ADVOCAAT, CHI WA CHAN, ANTIGONA PAJAZITI,
FLAVIO PERISSINOTTO, AND ANTONELLA PERUCCA

ABSTRACT. Let K be a number field, and let G be a finitely generated subgroup of $K^\times$. For every prime number ℓ and for all positive integers m, n with $m \geqslant n$ we show that the structure of the Galois group of the Kummer extension $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})$ only depends on G through parameters that express divisibility properties over K (respectively, over $K(\zeta_4)$ if $\ell = 2$, $\zeta_4 \notin K$, $m \geqslant 2$). Moreover, we describe an explicit finite procedure to compute at once the Galois group structure for all extensions $K(\zeta_M, \sqrt[N]{G})/K(\zeta_M)$ with M, N positive integers such that $N \mid M$. Our work builds on results in Kummer theory by the last-named author joint with Debry, Hörmann, Perissinotto, Sgobba, and Tronto.

RÉSUMÉ. Soient K un corps de nombres et G un sous-groupe de type fini de $K^\times$. Pour tout nombre premier ℓ et pour tous entiers positifs m, n avec $m \geqslant n$, la structure du groupe de Galois de l'extension de Kummer $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})$ dépend uniquement de G à travers des paramètres qui expriment des propriétés de divisibilité sur K (respectivement, sur $K(\zeta_4)$ si $\ell = 2$, $\zeta_4 \notin K$, $m \geqslant 2$). De plus, nous décrivons une procédure finie explicite pour calculer en une fois la structure du groupe de Galois pour toutes les extensions $K(\zeta_M, \sqrt[N]{G})/K(\zeta_M)$ avec M, N entiers positifs tels que $N \mid M$. Notre travail s'appuie sur des résultats en théorie de Kummer obtenus par le dernier auteur cité en collaboration avec Debry, Hörmann, Perissinotto, Sgobba et Tronto.

1. INTRODUCTION

Kummer theory for number fields is a classical topic in algebraic number theory (see the standard references [6], [1]), and its development is natural and fundamental. Nowadays, Kummer theory is applied, for example, to study questions on the reductions of algebraic numbers, most notably Artin's Conjecture on primitive roots (see the survey article [8]).

The purpose of this paper is solving two problems in Kummer theory for number fields in full generality. The first problem concerns finite *cyclotomic-Kummer extensions* made with ℓ^m-th roots of unity and ℓ^n-th radicals, where $n \leqslant m$ and ℓ is a prime number. The second problem concerns general finite cyclotomic-Kummer extensions made with M-th roots of unity and N-th radicals, where $N \mid M$.

Let K be any number field, and let G be a finitely generated subgroup of $K^\times$ which, without loss of generality, may be taken torsion-free. Let ℓ be a prime number, and let n, m, N, M be positive integers such that $n \leqslant m$ and $N \mid M$.

If $\zeta_{\ell^n} \in K$, then the main theorem of Kummer theory tells us that the Galois group of the Kummer extension $K(\sqrt[\ell^n]{G})/K$ is isomorphic to the group $GK^{\times \ell^n}/K^{\times \ell^n}$. However, without the above assumption, classical Kummer theory cannot be applied. What one can do is adding first to K sufficiently many roots of unity, thus considering the field $L := K(\zeta_{\ell^m})$. Then, by

2000 *Mathematics Subject Classification.* Primary: 11R20; Secondary: 11R18, 11Y40.
Key words and phrases. Number field, Kummer theory, Cyclotomic-Kummer extension, Galois group.

Kummer theory over L, the Galois group of the Kummer extension $L(\sqrt[\ell^n]{G})/L$ is isomorphic to the group $GL^{\times\ell^n}/L^{\times\ell^n}$. What we achieve is showing that we can compute the group structure of this Galois group (of the Kummer extension over L) by only doing computations over K (or over $K(\zeta_4)$ if $\ell = 2$, $m \geqslant 2$, and $\zeta_4 \notin K$). Indeed, there are *parameters for ℓ-divisibility* over K (respectively, over $K(\zeta_4)$) that suffice for the purpose. The structure of the Galois group only depends on G through the divisibility parameters (see Theorem 6). The parameters for ℓ-divisibility have been developed by Perucca and others, see [10, 2, 13], and Section 2.2 is devoted to recalling their definition and properties.

The second problem that we consider is the generalization of the first where the parameters ℓ^n, ℓ^m are replaced by integers N, M that are not necessarily powers of one same prime number. In this full generality we cannot hope to rely on divisibility parameters as before. Our aim, which we were able to fully achieve, is describing an explicit finite procedure for computing at once the structure of the Galois group for all Kummer extensions $K(\zeta_M, \sqrt[N]{G})/K(\zeta_M)$. This procedure is in fact an algorithm which is suitable for mathematical softwares like [15, 7]. This second problem is tackled with in Section 5. Notice that Hörmann, Perissinotto, Perucca, Sgobba, and Tronto were able to compute the degree of the extensions $K(\zeta_M, \sqrt[N]{G})/K(\zeta_M)$ if K is a multiquadratic field (for example, a quadratic field), a quartic field, or a number field without quadratic subfields (in particular, a number field of odd degree), see [3, 9].

Finally, the last section is devoted to examples and explicit computations that show how our general results can be applied in practice.

Acknowledgements. We thank Alexandre Benoist, Fritz Hörmann, and Sergei Iakovenko for their valuable suggestions. Bryan Advocaat, Antigona Pajaziti, and Flavio Perissinotto were kindly supported by the Luxembourg National Research Fund, with the grants PRIDE17 1224660, AFR-PhD 16981197, and PRIDE17 1224660.

2. Preliminaries

Notation. We let ℓ be a prime number and denote by v_ℓ the ℓ-adic valuation defined on non-zero integers. We consider a number field K and work within some fixed algebraic closure $\bar{K}$ of K. We let μ_n be the group of n-th roots of unity in $\bar{K}$ and we denote by ζ_n any primitive n-th root of unity.

2.1. Finite abelian groups.

Consider a finite and non-trivial abelian group $\mathcal{G}$. To study its structure as a product of cyclic groups we will suppose that the size of $\mathcal{G}$ is a power of ℓ. If $\mathcal{G}$ is generated by r elements, then the number of cyclic components does not exceed r so the group structure of $\mathcal{G}$ is a decomposition of $\mathcal{G}$ as the product of $r' \leqslant r$ cyclic groups. This amounts to having an isomorphism

$$\mathcal{G} \simeq \prod_{i=1}^{r'} C_{\ell^{e_i}}$$

where the e_i's are a non-increasing list of positive integers. With the identification given by such an isomorphism we may consider $C_{\ell^{e_i}}$ to be a cyclic subgroup $\langle\gamma_i\rangle$ of $\mathcal{G}$. Thus we can write

$$\mathcal{G} = \langle\gamma_1, \dots, \gamma_{r'}\rangle \simeq \langle\gamma_1\rangle \times \cdots \times \langle\gamma_{r'}\rangle\,.$$

To determine the group structure of $\mathcal{G}$ we will apply on several occasions the following well-known result from group theory (see for example [5, Lemma 13.4]):

Remark 1. An element of $\mathcal{G}$ whose order equals the exponent of $\mathcal{G}$ generates a cyclic component C of $\mathcal{G}$. In other words, there is a subgroup $\mathcal{G}'$ of $\mathcal{G}$ such that $\mathcal{G}$ is the internal direct product of C and $\mathcal{G}'$.

2.2. **Parameters for ℓ-divisibility.** We say that an element $a \in K^\times$ is *ℓ-divisible* if $a \in K^{\times \ell}$. If $a\zeta \notin K^{\times \ell}$ holds for every root of unity $\zeta \in K \cap \mu_{\ell^\infty}$, then we say that $a \in K^\times$ is *strongly-ℓ-indivisible*. Elements $a_1, a_2, ..., a_r \in K^\times$ are said to be *strongly ℓ-independent* if $\prod_{i=1}^r a_i^{e_i}$ is strongly ℓ-indivisible for all integers $e_1, e_2, ..., e_r$ that are not all divisible by ℓ.

Every element $a \in K^\times$ that is not a root of unity can be written in the form $a = A^{\ell^d}\zeta$ with $d \in \mathbb{Z}_{\geqslant 0}$, $\zeta \in K \cap \mu_{\ell^\infty}$, and where $A \in K^\times$ is strongly ℓ-indivisible, see [2, Lemma 7]. The non-negative integer d is uniquely determined, while the non-negative integer $h := v_\ell(\operatorname{ord}\zeta)$ may depend on the chosen decomposition. We call (d, h) *parameters for ℓ-divisibility* of a, noting that h might not be unique. By [2, Section 6.1] we have a finite procedure as how to find parameters for ℓ-divisibility.

Let $G = \langle b_1, \dots, b_r \rangle$ be a finitely generated and torsion free subgroup of $K^\times$ of positive rank r. We define the *parameters for ℓ-divisibility* of G as the list of parameters for ℓ-divisibility (d_i, h_i) of b_i, provided that the basis $b_1, \dots, b_r$ is an *ℓ-good basis*. By this we mean that decomposing $b_i = B_i^{\ell^{d_i}} \zeta_{\ell^{h_i}}$ as above with a strongly ℓ-indivisible element B_i, we have the additional property that $B_1, \dots, B_r$ are strongly ℓ-independent. By [2, Theorem 14] we know that an ℓ-good basis exists, and by [2, Section 6.1] we know a finite procedure as how to construct it from a given basis. The *d-parameters* $d_1, \dots, d_r$ are uniquely determined up to reordering by [2, Corollary 16]. The parameters for ℓ-divisibility (d_i, h_i) are not unique up to reordering, however they can be made unique if we impose additional conditions on them, see [2, Propositions 31 and 33]. Recall that the ℓ-good bases are precisely the bases which maximize the sum of their d-parameters; intuitively, this means that ℓ-good bases show all the divisibility of G.

If ℓ is odd or $\zeta_4 \in K$, then the parameters for ℓ-divisibility of G do not change if we extend the field from K to $K(\zeta_{\ell^n})$ for some given n (see [2, Proposition 9]). However, in the case when $\ell = 2$ and $\zeta_4 \notin K$, these parameters may change when extending the field from K to $K(\zeta_4)$, and a precise description of when and how they do change is provided in [13].

Remark 2. Throughout the paper we assume K to be a number field. This is because our results build on [2] by Debry and the last-named author. In particular, the existence of the parameter d of ℓ-divisibility described at the beginning of this section comes from the fact that, if K is a number field, only the roots of unity (of order coprime to ℓ) can be ℓ^n-th powers in $K^\times$ for every positive integer n. Since Kummer theory is valid for all fields, it is likely that our results generalize to some extent in other settings (for example, the last two-named authors are investigating local fields).

3. Groups of radicals

In this section we fix some prime number ℓ. We let μ_K be the group of roots of unity in K and we set $z := v_\ell(\#\mu_K)$. We recall the following lemma as it will be used multiple times:

Lemma 3. [12, Lemma 5] *Let $a_1, \dots, a_r$ be strongly ℓ-independent elements of $K^\times$. If $\zeta a_1^{e_1} \dots a_r^{e_r} \in K^{\times \ell^n}$ holds for some positive integer n, for some non-negative integers $e_1, \dots, e_r$ and for some $\zeta \in \mu_K$, then $e_1, \dots, e_r$ are all divisible by ℓ^n.*

Let $I := \{1, \dots, r\}$ and let $G := \langle b_i : i \in I \rangle$ be a finitely generated and torsion free subgroup of $K^\times$ of positive rank r. We suppose that $b_1, ..., b_r$ is an ℓ-good basis of G, and we write $b_i = B_i^{\ell^{d_i}} \zeta_{\ell^{h_i}}$ for some strongly ℓ-independent elements $B_i \in K^\times$ and $\zeta_{\ell^{h_i}} \in K$.

The aim of this section is to prove the following result:

Theorem 4. *The parameters for ℓ-divisibility of G determine the group structure of $GK^{\times \ell^n}/K^{\times \ell^n}$ for all $n \geqslant 1$. Moreover, for any given n, there is an explicit finite procedure to compute the number of non-trivial direct cyclic factors of $GK^{\times \ell^n}/K^{\times \ell^n}$ and each of their sizes. The group structure only depends on n, on $z = v_\ell(\# \mu_K)$ and on the divisibility parameters of G over K.*

Proof. Write $\delta_i := \max(n - d_i, 0)$. Call $b_{i,1}$ the class of b_i modulo $K^{\times \ell^n}$ and call $\mu_{\ell^z,1}$ the image of μ_{ℓ^z} modulo $K^{\times \ell^n}$. Let $\ell^{w_{i,1}}$ be the order of $\zeta_{\ell^{h_i}}$ modulo $K^{\times \ell^n}$, namely $w_{i,1} = \max(0, \min(h_i, h_i + n - z))$. Then, calling $v_{i,1} := v_\ell(\mathrm{ord}(b_{i,1}))$, by Lemma 3 applied to B_i we have $v_{i,1} = \max(\delta_i, w_{i,1})$.

For every i the intersection of $\langle b_{i,1} \rangle$ with $\langle b_{i',1} : i' \neq i \rangle$ is contained in $\mu_{\ell^z,1}$ (by Lemma 3 applied to $B_1, \dots, B_r$). The condition $\langle b_{i,1} \rangle \cap \mu_{\ell^z,1}$ being trivial is equivalent to $v_{i,1} = \delta_i$.

So, if $v_{i,1} = \delta_i$, then in particular we can write

$$GK^{\times \ell^n}/K^{\times \ell^n} = \langle b_{i,1} \rangle \times \langle b_{i',1} : i' \neq i \rangle \, .$$

Write $I_1 = I$, and let $D_1 \subseteq I_1$ consist of those indices i such that $v_{i,1} = \delta_i$. So the groups $\langle b_{i,1} \rangle$ for $i \in D_1$ are direct components of order ℓ^{δ_i} and they can be "detached" and collected, leaving for us to investigate, in case $I_1 \neq D_1$, the indices in $I_1 \setminus D_1$. Let $m_1 \in I_1 \setminus D_1$ be the least index such that $w_{m_1,1} \geqslant w_{i,1}$ for all $i \in I_1 \setminus D_1$, and set $I_2 := I_1 \setminus (D_1 \cup \{m_1\})$. By Remark 1, we have

$$\langle b_{i,1} : i \in I_1 \setminus D_1 \rangle \simeq \langle b_{m_1,1} \rangle \times \langle b_{i,2} : i \in I_2 \rangle \, ,$$

where $b_{i,2}$ stands for the class of b_i modulo $\langle K^{\times \ell^n}, b_{m_1,1} \rangle$. So we are left to investigate the group structure of $\langle b_{i,2} : i \in I_2 \rangle$, in case $I_2 \neq \emptyset$.

We proceed by iteration. At the step $j > 1$, in case $I_j := I_{j-1} \setminus (D_{j-1} \cup \{m_{j-1}\})$ is not empty, we have to investigate the group structure of $\langle b_{i,j} : i \in I_j \rangle$, where $b_{i,j}$ is the class of b_i modulo $H_j := \langle K^{\times \ell^n}, b_{m_1}, \dots, b_{m_{j-1}} \rangle$. Call $\ell^{w_{i,j}}$ the order of $\zeta_{\ell^{h_i}}$ modulo H_j. We claim that

$$w_{i,j} = \max(0, w_{i,j-1} - w_{m_{j-1},j-1} + \delta_{m_{j-1}}) \, . \tag{1}$$

So the cyclic group $\langle b_{i,j} \rangle$ has order $\ell^{v_{i,j}}$, where $v_{i,j} = \max(\delta_i, w_{i,j})$ by Lemma 3.

We then define $D_j \subset I_j$ as the set of indices i satisfying $v_{i,j} = \delta_i$, and as above we collect detachable cyclic components $\langle b_{i,j} \rangle$ for $i \in D_j$, of order ℓ^{δ_i}. If $I_j = D_j$, then we are done. Else, we define $m_j \in I_j \setminus D_j$ as the least index maximizing $w_{i,j}$ and (by Remark 1) collect the cyclic component $\langle b_{m_j,j} \rangle$, of order $\ell^{w_{m_j,j}}$. If $I_j \setminus (D_j \cup \{m_j\})$ is empty, then we are done, else we move on to the next step. The procedure clearly terminates in at most r steps.

We are left to prove the claim. By the definition of $w_{i,j}$ in (1), notice that $w_{m_{j-1},j-1} - \delta_{m_{j-1}}$ is the ℓ-adic valuation of the order of the torsion of H_j/H_{j-1} and in particular it is non-negative. Indeed, by construction $H_j = \langle H_{j-1}, b_{m_{j-1}} \rangle$ and $w_{m_{j-1},j-1}$ is by definition the order of $\zeta_{\ell^{h_{m_{j-1}}}}$ modulo H_{j-1}. So by elementary group theory the difference $w_{i,j-1} - w_{i,j}$ (we are comparing the order of one same root of unity modulo H_{j-1} and H_j respectively) is precisely $w_{m_{j-1},j-1} - \delta_{m_{j-1}}$ unless $w_{i,j-1} < w_{m_{j-1},j-1} - \delta_{m_{j-1}}$, in which case $w_{i,j} = 0$. □

Remark 5. Consider the setting of Theorem 4. Write $\delta_i := \max(n-d_i, 0)$. If $z=0$, then $h_i = 0$ for every i, and the group structure is $\prod_{i=1}^r \mathbb{Z}/\ell^{\delta_i}\mathbb{Z}$.

In general, there is some positive integer $k \leqslant r$ such that we can write

$$GK^{\times \ell^n}/K^{\times \ell^n} \cong \prod_{j=1}^{k} G_j$$

where the group G_j is the product of the components of $GK^{\times \ell^n}/K^{\times \ell^n}$ which are collected at the j-th step in the proof of Theorem 4. We have:

$$G_j = (\prod_{i \in D_j} \mathbb{Z}/\ell^{\delta_i}\mathbb{Z}) \times \mathbb{Z}/\ell^{w_{m_j,j}}\mathbb{Z}\,,$$

where the (possibly empty) subsets $D_j \subseteq I$, the indices $m_j \in I$ and the integers δ_i and $w_{m_j,j} > 0$ are as in the proof of Theorem 4. The set $I_k \setminus D_k$ may be empty and, if that is the case, we set the component $\mathbb{Z}/\ell^{w_{m_k,k}}\mathbb{Z}$ of G_k to be the trivial group.

Theorem 6. *Suppose that ℓ is odd or $\zeta_4 \in K$. Let t be the greatest integer satisfying $\zeta_{\ell^t} \in K(\zeta_\ell)$. Let m and n be positive integers such that $m \geqslant n \geqslant 1$. The group structure of the Galois group of the Kummer extension $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})$ only depends on the parameters for ℓ-divisibility of G over K, and the integers $n, \max(m,t)$.*

Proof. By Kummer theory, we have that

$$\mathrm{Gal}(K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})) \cong GK(\zeta_{\ell^m})^{\times \ell^n}/K(\zeta_{\ell^m})^{\times \ell^n}.$$

Since we know by [2, Proposition 9] that the parameters of ℓ-divisibility of the group G do not change if we extend the field from K to $K(\zeta_{\ell^m})$, we can apply Theorem 4 over $K(\zeta_{\ell^m})$. Notice that, in this setting, we have $z = \max(m,t)$. □

Remark 7. For Theorem 6, in the remaining case $\ell = 2$ and $\zeta_4 \notin K$ we can extend the field from K to $K(\zeta_4)$ to reduce to the known case (in particular, we work with the divisibility parameters of G over $K(\zeta_4)$). Taking this field extension is not an issue as soon as one investigates $K(\zeta_{2^m}, \sqrt[2^n]{G})/K(\zeta_{2^m})$ for $m \geqslant 2$. So we are left to investigate $K(\sqrt{G})/K$ when $\zeta_4 \notin K$. The size of the Galois group of this extension is known by [2, Lemma 19 and Theorem 18] hence the group structure is also known because the group is either trivial or it has exponent 2.

Remark 8. In Theorems 4 and 6 the assumption that G is torsion-free is just for convenience. Firstly, adding to G torsion of order coprime to ℓ does not affect the considered questions. Now suppose we have a group G whose torsion subgroup is $\langle \zeta_{\ell^h} \rangle$ for some $h > 0$. The proofs of the two above-mentioned results still hold by choosing $b_1 := \zeta_{\ell^h}$ as a generator of G and defining the parameters of ℓ-divisibility $d_1 := \infty$ and $h_1 := h$ (where d_1 is fixed to be n to determine the group structure of $GK^{\times \ell^n}/K^{\times \ell^n}$ or to study $K(\zeta_{\ell^m}, \sqrt[\ell^n]{G})/K(\zeta_{\ell^m})$).

4. Considerations on the group structure

We collect here several observations on the group structure of $GK^{\times \ell^n}/K^{\times \ell^n}$ computed in the previous section. Remark 9 clarifies what the group structure depends on, Remarks 10 and 11 compare our result with [2], while the others deal with special cases and investigate how the structure changes by varying the parameter n.

Remark 9. The group structure determined in Theorem 4 only depends on G through the divisibility parameters over K. The dependency on K is through $z = v_\ell(\#\mu_K)$ and the divisibility parameters.

In Theorem 6 we work over the base field $K(\zeta_{\ell^m})$, over which the divisibility parameters are unchanged. So if $m \geqslant t$, where t is the integer defined in Theorem 6, the only dependency on K is through the divisibility parameters.

Remark 10. We now investigate the size of the group $\#(GK^{\times \ell^n}/K^{\times \ell^n})$. Indeed, by Remark 5 (setting $w_{m_k,j} = 0$ for all j if m_k does not exists) we have

$$v_\ell(\#(GK^{\times \ell^n}/K^{\times \ell^n})) = \sum_{i \in I \setminus \{m_1,\dots,m_k\}} \delta_i + \sum_{j=1}^{k} w_{m_j,j}\,.$$

Recalling that $w_{i,j} = \max(0, w_{i,j-1} - w_{m_{j-1},j-1} + \delta_{m_{j-1}})$, and applying this formula multiple times, we can write $\sum_j w_{m_j,j} = w_{m_k,1} + \sum_{j<k} \delta_{m_j}$. Moreover, since $w_{m_k,1} - \delta_{m_k} = \max_{i \in I}(w_{i,1} - \delta_i)$ we conclude that

$$v_\ell(\#(GK^{\times \ell^n}/K^{\times \ell^n})) = \sum_{i \in I} \delta_i + \max(0, \max_{i \in I}(w_{i,1} - \delta_i))\,.$$

In the setting of Theorem 6, this formula agrees with [2, Theorem 18] and also with [2, Theorem 15 and Corollary 16] under the assumption that the H_n from loc. cit. is trivial (for example, if $h_i = 0$ for all i) because $v_{i,1} = \delta_i$ for all i. In particular, if $(d_i, h_i) = (0, 0)$ holds for all i (which for any given G happens for almost all ℓ by [11, Theorem 2.7]), then we have $\#(GK^{\times \ell^n}/K^{\times \ell^n}) = \ell^{nr}$. Moreover, still assuming that the group structure is $\prod_{i=1}^{r} \mathbb{Z}/\ell^{\delta_i}\mathbb{Z}$, the following holds: if $n \geqslant d_i$ for all i we have $\#(GK^{\times \ell^{n+1}}/K^{\times \ell^{n+1}}) = \ell^r \cdot \#(GK^{\times \ell^n}/K^{\times \ell^n})$.

Remark 11. The multiset of the pairs (d_i, h_i) depends in general on the choice of the ℓ-good basis of G. Clearly, the group structure determined in Theorem 4 cannot depend on this choice. For the convenience of the reader we verify that the above result is the same even if we pick a different basis. To achieve this, we change the basis of G imposing the conditions listed in [2, Proposition 31] (with these additional conditions, the multiset is unique) and reordering the generators so that $d_i \leqslant d_j$ holds for each $i \leqslant j$. Following the proof of [2, Proposition 31], we then take the following steps, commenting on why the group structure does not change:

(1) *If $h_i \leqslant z - d_i$, we set $h_i = 0$.* Notice that the order of $b_{i,1}$ is still δ_i.

(2) *If $i < j$ and $0 < h_i \leqslant h_j$, we set $h_i = 0$ (in case $h_i = h_j$ we set instead $h_j = 0$).* If $d_i \leqslant d_j$ and $h_i \leqslant h_j$, then we have $w_{i,t} \leqslant w_{j,t}$ for every t: this still holds after this step. In case $h_i \neq h_j$ we preserve the property $i \notin \{m_1, \dots m_k\}$ and $w_{j,t}$ is unchanged; else, we preserve the property $j \notin \{m_1, \dots m_k\}$ and $w_{i,t}$ is unchanged.

(3) *If $i < j$ and if $h_i, h_j > 0$ and $d_i + h_i \geqslant d_j + h_j$, we set $h_j = 0$.* If $d_i \leqslant d_j$ and $d_i + h_i \geqslant d_j + h_j$, then both $w_{i,t} \geqslant w_{j,t}$ (for every t) and $j \notin \{m_1, \dots m_k\}$ hold and are preserved. Moreover, $w_{i,t}$ is unchanged.

Remark 12. We have determined the group structure of $GK^{\times \ell^n}/K^{\times \ell^n}$ so we know the exponent of this group, namely $\ell^{\max_i(v_{i,1})}$. For large n the group structure of $GK^{\times \ell^n}/K^{\times \ell^n}$ does not involve the h-parameters explicitly, and indeed by (1) of the previous remark we may suppose that $h_i = 0$ holds for all i. Moreover, for all $n \gg 0$ (at least, if $n > z + \max(d_1, \cdots, d_r)$), the group $GK^{\times \ell^n}/K^{\times \ell^n}$ has precisely r components, which all grow by a factor ℓ when we increase n by 1 (this is what we call *eventual maximal growth*). This regular growth of the existing components does not hold in general for small n, as we cannot assume the h-parameters to be 0. Because of the eventual maximal growth, we may compute the group structure of $GK^{\times \ell^n}/K^{\times \ell^n}$ for all n by applying the algorithm in Theorem 4 finitely many times.

Remark 13. Supposing $h_i = 0$ for every i, the family of groups $GK^{\times \ell^n}/K^{\times \ell^n}$ can be arbitrary among the family of finite abelian groups of order a power of ℓ, having at most r components and having precisely r components for $n \gg 0$, such that each existing component grows by a factor ℓ by increasing n to $n+1$. Indeed, such groups are of the form $\prod_{i=1}^r \mathbb{Z}/\ell^{\delta_i}\mathbb{Z}$.

Remark 14. In the setting of Theorem 6, set $n_0 \geqslant t$ and consider $m = n = n_0 + x$ for $x \geqslant 0$. We investigate how the group structure of $GK(\zeta_{\ell^m})^{\times \ell^n}/K(\zeta_{\ell^m})^{\times \ell^n}$, and hence the group structure of the Galois group of the Kummer extension, changes when we increase x. We apply our algorithm (see the proof of Theorem 4) for $x = 0$ and then describe how the algorithm varies by increasing x. Let k be the number of steps of the algorithm when $x = 0$. We first notice that the components of $GK(\zeta_{\ell^m})^{\times \ell^n}/K(\zeta_{\ell^m})^{\times \ell^n}$ whose indices are in $\bigcup_{j=1}^k D_j$ (for $x = 0$) give rise to components of order $\ell^{\delta_i + x}$ for every x. The order ℓ^{v_i} of the other components changes according to the following table, where we set $y_i := w_{m_i,i} - \delta_{m_i}$ (here we suppose that $I_k \setminus D_k$ is not empty, else replace k by $k-1$):

x	v_{m_1}	v_{m_2}	$\cdots$	v_{m_k}
0	$w_{m_1,1}$	$w_{m_2,2}$	$\cdots$	$w_{m_k,k}$
$0 < x \leqslant y_1$	$w_{m_1,1}$	$w_{m_2,2} + x$	$\cdots$	$w_{m_k,k} + x$
$y_1 < x \leqslant y_2$	$\delta_1 + x$	$w_{m_2,2} + y_1$	$\cdots$	$w_{m_k,k} + x$
$y_2 < x \leqslant y_3$	$\delta_1 + x$	$\delta_2 + x$	$\cdots$	$w_{m_k,k} + x$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$y_{k-1} < x \leqslant y_k$	$\delta_1 + x$	$\delta_2 + x$	$\cdots$	$w_{m_k,k} + y_{k-1}$
$x > y_k$	$\delta_1 + x$	$\delta_2 + x$	$\cdots$	$\delta_k + x$

In particular, for each interval $y_i < x \leqslant y_{i+1}$ all components of the group but one increase in size, and the stable component corresponds to the index m_i. Moreover, we have maximal growth starting from $x = y_k$.

Remark 15. If there exists a choice of indices such that the parameters of divisibility of the group G satisfy $w_{1,1} > w_{2,1} > \cdots > w_{r,1}$ and $0 < w_{1,1} - \delta_1 < w_{2,1} - \delta_2 < \cdots < w_{r,1} - \delta_r$, then the algorithm in the proof of Theorem 4 ends after r steps, with $D_j = \emptyset$ for all j.

5. Galois groups of Kummer extensions

Let G be a finitely generated and (without loss of generality) torsion free subgroup of $K^\times$ of positive rank r. Let $N \mid M$ be positive integers. Our aim is to compute the structure of the Galois group of all Kummer extensions relative to a cyclotomic extension, namely all groups

$$\mathcal{G}_{M,N} := \mathrm{Gal}\left(\frac{K(\zeta_M, \sqrt[N]{G})}{K(\zeta_M)}\right).$$

Notice that $\mathcal{G}_{M,N}$ is a finite abelian group, whose exponent divides N, and that has at most r cyclic components. Considering the prime decomposition $N = \prod \ell^e$, we may identify $\mathcal{G}_{M,N}$

with a product of ℓ-groups, as done in [12, Lemma 28]:

$$\mathcal{G}_{M,N} \simeq \prod_{\ell} \mathrm{Gal}\left(\frac{K(\zeta_{\ell^e},\ \sqrt[\ell^e]{G})}{K(\zeta_{\ell^e},\ \sqrt[\ell^e]{G}) \cap K(\zeta_M)}\right).$$

We consider the Galois group $\mathcal{G}_{\ell^e,\ell^e} = \mathrm{Gal}(K(\zeta_{\ell^e},\ \sqrt[\ell^e]{G})/K(\zeta_{\ell^e}))$ and we call the positive integer $\ell^{er}/\#\mathcal{G}_{\ell^e,\ell^e}$ the *ℓ-adic failure of maximality* (for the degree of the Kummer extension). The structure of $\mathcal{G}_{\ell^e,\ell^e}$ for all $e \geqslant 1$ can be computed as in Section 3, as we are in the situation of Theorem 6 with $m = n = e$ (or we may apply Remark 7 if $\ell = 2$ and $\zeta_4 \notin K$).

Similarly, we consider the Galois group

$$\mathcal{H}_{M,\ell^e} := \mathrm{Gal}((K(\zeta_{\ell^e},\ \sqrt[\ell^e]{G}) \cap K(\zeta_M)/K(\zeta_{\ell^e}))$$

and we call its cardinality the *ℓ-adelic failure of maximality*. By Schinzel's Theorem on Abelian radical extensions (see, for example, [11, Theorem 3.5]) the exponent of $\mathcal{H}_{\ell^e,M}$ divides the ℓ-part of $\#\mu_K$. In particular, $\mathcal{H}_{M,\ell^e}$ is trivial if $\zeta_\ell \notin K$. If we suppose that $\zeta_\ell \in K$, by [11, Theorem 3.1 and Remark 3.8] (see also [14, Proposition 3.5]) there exist computable positive integers e_0, M_0 that only depend on K, G, and ℓ for which we have

$$K(\zeta_{\ell^e},\ \sqrt[\ell^e]{G}) \cap K(\zeta_M) = K(\zeta_{\ell^{\min(e,e_0)}},\ \sqrt[\ell^{\min(e,e_0)}]{G}) \cap K(\zeta_{\gcd(M,M_0)})$$

which implies that $\mathcal{H}_{M,\ell^e}$ does not change if we replace e by $\min(e, e_0)$ and M by $\gcd(M, M_0)$. In particular, computing the structure of this group for all e and M amounts to only finitely many computations. Now fix $e \leqslant e_0$ and $M \mid M_0$. To compute $\mathcal{H}_{M,\ell^e}$, we may first compute the largest subgroup H of G which is contained in $K(\zeta_M)^{\times\ell^e}$ and then apply the method discussed in Section 3 to compute the group structure of $HK(\zeta_{\ell^e})^{\times\ell^e}/K(\zeta_{\ell^e})^{\times\ell^e}$.

To conclude, by Galois theory $\mathcal{H}_{M,\ell^e}$ is a quotient of $\mathcal{G}_{\ell^e,\ell^e}$ and hence by the third isomorphism theorem of groups we can write

$$\mathcal{G}_{M,N} \simeq \prod_{\ell} \mathcal{G}_{\ell^e,\ell^e}/\mathcal{H}_{M,\ell^e} \simeq \prod_{\ell} GK(\zeta_{\ell^e})^{\times\ell^e}/HK(\zeta_{\ell^e})^{\times\ell^e}\,. \tag{2}$$

To compute the ℓ-part of the group $\mathcal{G}_{M,N}$, we can apply Theorem 4 on the group G over the field $K(\zeta_{\ell^e},\ \sqrt[\ell^e]{H})$.

Remark 16. There may be radicals in $\sqrt[\ell^e]{G}$ that are in $K(\zeta_M)$ and in $K(\zeta_{\ell^{e+1}})$ but not in $K(\zeta_{\ell^e})$, where we suppose $\ell^e|M$. For example, take $K = \mathbb{Q}(\sqrt{3})$, $G = \langle -25\rangle$, $\ell^e = 2$: the element -25 is a square in $K(\zeta_4) = K(\zeta_3)$ but not in $K(\zeta_2) = K$. Such elements contribute to the ℓ-adelic failure of maximality for (M, e) but not to the ℓ-adic failure for larger values of e. So $\mathcal{H}_{M,\ell^e}$ may reduce in size by increasing e.

Remark 17. The following answers a question of Sergei Iakovenko (from an email to the last-named author in 2021): There is a constant c such that for every prime number ℓ and for every $n, M \geqslant 1$ the Galois group of

$$K(\zeta_{\ell^n}, \sqrt[\ell^n]{G}, \zeta_M)/K(\zeta_{\ell^n}, \zeta_M)$$

contains a subgroup isomorphic to $(\gcd(c, \ell^n)\mathbb{Z}/\ell^n\mathbb{Z})^r$. We can take $c = \#\mu_K \cdot \prod_\ell \ell^{D_\ell}$, where D_ℓ is the maximum of the multiset of d-parameters for ℓ-divisibility (hence $D_\ell = 0$ holds for almost all ℓ). Indeed, for any fixed ℓ the group $GK^{\times\ell^n}/K^{\times\ell^n}$ contains a subgroup of the form $(\ell^{D_\ell}\mathbb{Z}/\ell^n\mathbb{Z})^r$ by Remark 12. We conclude because the exponent of $\mathcal{H}_{M,\ell^e}$ divides $\#\mu_K$.

Remark 18. The Galois group of $K(\zeta_M, \sqrt[\ell^n]{G})/K(\zeta_M)$ has $r' \leqslant r$ components, where (fixing K and G) the number r' depends on ℓ, n, M. By construction, it is generated by r' radicals of elements that can be expanded to a set of generators for G. Notice that there are finitely many possibilities for r'. By construction, the set of elements of G whose radicals generate the above Galois group can be taken in a finite family of sets by varying ℓ, n, M.

6. Examples

We keep the notation of Sections 3 and 5. The following three examples show explicit computations of the group structure of $GK^{\times \ell^n}/K^{\times \ell^n}$.

Example 19. Let $\ell = 3$ and $K = \mathbb{Q}(\zeta_9)$, so that $z = 2$. Consider $G = \langle 18, 6^3 \rangle$. By [2, Example 27] (or with a direct check) this is a 3-good basis for G, with divisibility parameters $d_2 = 1$ and $d_1 = h_1 = h_2 = 0$. Fixing $n \geqslant 1$, we have $\delta_1 = n$ and $\delta_2 = n - 1$ and $w_{1,1} = w_{2,1} = 0$ and hence $v_{i,1} = \delta_i$ for $i = 1, 2$. We conclude that

$$GK^{\times 3^n}/K^{\times 3^n} \simeq \mathbb{Z}/3^n\mathbb{Z} \times \mathbb{Z}/3^{n-1}\mathbb{Z}\,.$$

Example 20. Suppose that the parameters for ℓ-divisibility of the group G are

$$(d_1, d_2, d_3, d_4, d_5) = (1, 3, 3, 3, 5) \quad \text{and} \quad (h_1, h_2, h_3, h_4, h_5) = (2, 3, 1, 0, 2)\,.$$

Let $z = 5$ and $n = 4$. Then we get the following tuples:

$$\begin{aligned} \underline{\delta} &= (3, 1, 1, 1, 0), \\ \underline{w_{\cdot,1}} &= (1, 2, 0, 0, 1), \\ \underline{v_{\cdot,1}} &= (3, 2, 1, 1, 1). \end{aligned}$$

We see that $v_{1,1} = \delta_{1,1}$, $v_{3,1} = \delta_{3,1}$ and $v_{4,1} = \delta_{4,1}$, so we conclude that $b_{1,1}$, $b_{3,1}$ and $b_{4,1}$ generate direct components of order ℓ^3, ℓ and ℓ respectively. If we then consider the indices in $I_1 \setminus D_1 = \{2, 5\}$, the maximal $w_{i,1}$ is given by $w_{2,1} = 2$, hence we get a direct component generated by $b_{2,1}$. This leaves us to investigate $b_{5,2}$, which will generate a direct component $\langle b_{5,2} \rangle$. We have $w_{5,2} = w_{5,1} - w_{2,1} + \delta_2 = 0$, hence $b_{5,2} = 0$.

Notice that for $z = n \geqslant 7$ we find the following values

$$\begin{aligned} \underline{\delta} &= (n - 1, n - 3, n - 3, n - 3, n - 5), \\ \underline{w_{\cdot,1}} &= (2, 3, 1, 0, 2) = \underline{h} \end{aligned}$$

and hence $v_{i,1} = \delta_i$ for all i. We can then conclude that each $b_{i,1}$ generates a direct component of order ℓ^{δ_i}. The parameters h_i are not involved in the group structure as n is big enough, as pointed out in Remark 12.

Example 21. Let $K = \mathbb{Q}(\zeta_4)$ and $G = \langle -15 + 20\zeta_4, 14\zeta_4 \rangle$. If $M = N = 4$, we have $\mathcal{G}_{4,4} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ because the group $\mathcal{H}_{4,4}$ is trivial and the 2-divisibility parameters of the group are all 0. Set now $M = 140$ and $N = 4$. Since $\sqrt[4]{-15 + 20\zeta_4}$ generates $\mathbb{Q}(\zeta_{20})/\mathbb{Q}(\zeta_4)$ (by [4, Theorem 2]) and $14\zeta_4$ is a square in $\mathbb{Q}(\zeta_{28})$, then

$$H = G \cap K(\zeta_{140})^{\times 4} = \langle -15 + 20\zeta_4, (14\zeta_4)^2 \rangle$$

and hence by (2) the Galois group of the Kummer extension $\mathcal{G}_{140,4}$ is $\mathbb{Z}/2\mathbb{Z}$. Indeed, the d parameters of 2-divisibility of G in $K(\zeta_{140})$ are respectively $d_1 = 2$ and $d_2 = 1$. In general, the group H can be computed for every M and $N = 2^n$:

$$H = \begin{cases} G^{2^n} & \text{if } 5,7 \nmid M \\ \langle (-15+20\zeta_4)^{2^n}, (14\zeta_4)^{2^{n-1}} \rangle & \text{if } 7 \mid M, 5 \nmid M \\ \langle (-15+20\zeta_4)^{2^{n-2}}, (14\zeta_4)^{2^n} \rangle & \text{if } 5 \mid M, 7 \nmid M, n \geqslant 2 \\ \langle (-15+20\zeta_4)^{2^{n-2}}, (14\zeta_4)^{2^{n-1}} \rangle & \text{if } 35 \mid M, n \geqslant 2 \\ \langle -15+20\zeta_4, (14\zeta_4)^2 \rangle & \text{if } 5 \mid M, 7 \nmid M, n = 1 \\ G & \text{if } 35 \mid M, n = 1 \end{cases}$$

Hence we can compute by (2) the Galois group $\mathcal{G}_{M,N} = G/H$ for every M and $N = 2^n$.

The following example shows the feature presented in Remark 16.

Example 22. Let $\ell = 2$, $K = \mathbb{Q}(\zeta_{16}\sqrt{5})$ and $G = \langle 5, 6 \rangle$. The divisibility parameters are $(1, 3)$ for the former generator and $(0, 0)$ for the latter. By Theorem 4 we calculate that $\mathcal{G}_{8,8} = (\mathbb{Z}/8\mathbb{Z})^2$ and that $\mathcal{G}_{16,16} = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$. Since $\sqrt{5} \in K(\zeta_5)$ and $\sqrt{6} \in K(\zeta_3)$, for $M = 120$ we have $H = G \cap K(\zeta_{120})^{\times 8} = \langle 5^4, 6^4 \rangle$ and we can compute $\mathcal{H}_{120,8} = (\mathbb{Z}/2\mathbb{Z})^2$ and $\mathcal{G}_{120,8} = (\mathbb{Z}/4\mathbb{Z})^2$. Since $\sqrt{5} \in K(\zeta_{16})$, for $M = 48$ we have $H = G \cap K(\zeta_{48})^{\times 16} = \langle 5^8, 6^8 \rangle$. This implies that, for $M = 240$, $\mathcal{H}_{48,16} = \mathcal{H}_{240,16} = \mathbb{Z}/2\mathbb{Z}$ and, by (2), $\mathcal{G}_{48,16} = \mathcal{G}_{240,16} = (\mathbb{Z}/8\mathbb{Z})^2$.

REFERENCES

[1] J. CASSELS, A. FRÖHLICH, *Algebraic Number Theory*. Thompson Book Company, Washington D.C. (1967), 85–94.

[2] C. DEBRY, A. PERUCCA, *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283.

[3] F. HÖRMANN, A. PERUCCA, P. SGOBBA, S. TRONTO, *Explicit Kummer theory for quadratic fields*, JP J. Algebra, Number Theory Appl. **49** (2021), no. 2, 151–178.

[4] F. HÖRMANN, A. PERUCCA, P. SGOBBA, S. TRONTO, *Explicit Kummer generators of cyclotomic extensions*, JP J. Algebra, Number Theory Appl. **53** (2022), no. 1, 69–84.

[5] T. JUDSON, *Abstract Algebra: Theory and Application*. Virginia Commonwealth University, Math Department (2011).

[6] S. LANG, *Algebra*, Springer New York (2011).

[7] W. BOSMA, J. CANNON, C. PLAYOUST, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.

[8] P. MOREE, *Artin's primitive root conjecture – a survey*. Integers. **12** (2005).

[9] F. PERISSINOTTO, A. PERUCCA, *Kummer theory for multiquadratic or quartic cyclic number fields*, Unif. Distrib. Theory **17** (2022), no. 2, 165–194.

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

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

[12] A. PERUCCA, P. SGOBBA, S. TRONTO, *Kummer theory for number fields via entanglement groups*, Manuscripta Math. **169** (2022), 251–270.

[13] A. PERUCCA, P. SGOBBA, S. TRONTO, *Addendum to: Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283.

[14] O. JÄRVINIEMI, A. PERUCCA, *Unified treatment of Artin-type problems*. Res. number theory **9** (2023), no. 10, https://doi.org/10.1007/s40993-022-00418-6

[15] *SageMath, the Sage Mathematics Software System (Version 9.8)*, The Sage Developers (2023), https://www.sagemath.org.

University of Luxembourg, Department of Mathematics
6, avenue de la Fonte, L-4364, Esch-sur-Alzette, Luxembourg.