KUMMER EXTENSIONS OF NUMBER FIELDS (THE CASE OF RANK 2)

ANTONELLA PERUCCA

ABSTRACT. Let K be a number field, and let ℓ be a prime number. Fix some elements α_1, α_2 of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of rank 2. Let n_1, n_2, m be positive integers with $m \geqslant \max(n_1, n_2)$. We show that there exist parametric formulas (involving only a finite case distinction) to express the degree of the Kummer extension $K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \sqrt[\ell^{n_2}]{\alpha_2})$ over $K(\zeta_{\ell^m})$ for all n_1, n_2, m. The parameters appearing in the formulas are explicitly computable.

1. INTRODUCTION

Let K be a number field, and let ℓ be a prime number. Let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of rank r. If n, m are positive integers with $m \geqslant n$ (and if ζ_{ℓ^m} denotes a primitive ℓ^m-th root of unity) then we are interested in the degree of the Kummer extension

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

over $K(\zeta_{\ell^m})$ for all n and m. Together with Debry [1] and with Sgobba and Tronto [5] the author proved that there are finitely many divisibility parameters such that the above Kummer degree can be expressed with parametric formulas for all n and m. There is only a small case distinction if $\ell = 2$ and $\zeta_4 \notin K$, and the parameters appearing in the formulas are explicitly computable. A natural generalization is the following:

Question 1. *Let $n_1, \dots, n_r, m$ be positive integers with $m \geqslant \max_i(n_i)$. Consider the Kummer extension*

$$K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}) \tag{1}$$

over $K(\zeta_{\ell^m})$ for all $n_1, \dots, n_r, m$. Can we express the Kummer degree for all $n_1, \dots, n_r, m$ with parametric formulas involving only a finite case distinction and finitely many computable parameters?

This question would be trivial if $r = 1$ or if we fix $n_1, \dots, n_r, m$, so if we consider only one Kummer degree (because we can reduce to the above-mentioned results).

The question is also trivial if the elements $\alpha_1, \dots, \alpha_r$ are strongly ℓ-independent in the sense of [1, Definitions 10 and 5], and we have $\ell \neq 2$ or $\zeta_4 \in K$, because in this case we simply have

$$[K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \dots, \sqrt[\ell^{n_r}]{\alpha_r}) : K(\zeta_{\ell^m})] = \ell^{\sum_{i=1}^r n_i}, \tag{2}$$

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

see Remark 11. However, the question in general does not seem to be easy. In this short note we answer Question 1 in the affirmative for rank 2:

Theorem 2. *Let K be a number field, and let ℓ be a prime number. Fix some elements α_1, α_2 of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of rank 2. Let n_1, n_2, m be positive integers with $m \geqslant \max(n_1, n_2)$. We can express the degree of the Kummer extension*

$$K(\zeta_{\ell^m}, \sqrt[\ell^{n_1}]{\alpha_1}, \sqrt[\ell^{n_2}]{\alpha_2})/K(\zeta_{\ell^m}) \tag{3}$$

for all n_1, n_2, m with parametric formulas involving only a finite case distinction and finitely many computable parameters.

The case distinction and the proof of the theorem can be found in Section 4. We have a more precise result if $\zeta_\ell \notin K$, see Section 4.3.

It is possible that the method described in this article can be used to generalize Theorem 2, however it can be expected that the case of rank 3 (or higher) requires a more involved case distinction. Notice that if finding the parametric formulas proves to be unfeasible, one could still try to argument that such formulas must exist. We leave this as a direction of future research.

For recent works about related problems see the PhD thesis of Palenstijn [2] and the following articles of the author with Sgobba and Tronto [4, 6, 7].

Acknowledgments. The author would like to thank Pietro Sgobba for a careful reading of the manuscript.

2. Preliminaries

2.1. **Notation.** From now on K is a number field and ℓ is a fixed prime number. Write μ_{K,ℓ^∞} for the group of roots of unity in $K^\times$ having order a power of ℓ. Call ω the greatest nonnegative integer such that $K^\times$ contains a primitive ℓ^ω-th root of unity. We write v_ℓ to mean the ℓ-adic valuation; for a root of unity we write ord_ℓ to mean the ℓ-adic valuation of its order. If $n \geqslant 1$, we write ζ_{ℓ^n} to mean a primitive root of unity of order ℓ^n.

We call $\alpha \in K^\times$ *strongly indivisible* if α is not an ℓ-th power in $K^\times$ times a root of unity in μ_{K,ℓ^∞}. Notice that if α is strongly indivisible, then it is also not an ℓ-th power in $K^\times$ times a root of unity in $K^\times$ (this is immediate to verify). Also notice that if $\zeta_\ell \notin K$, then strongly indivisible just means not being an ℓ-th power in $K^\times$.

If $\alpha_1, \ldots, \alpha_r$ are elements of $K^\times$, then we say that they are *strongly independent* if an element of $K^\times$ of the form $\alpha_1^{e_1} \cdots \alpha_r^{e_r}$ (where $e_1, \ldots, e_r$ are integers) is strongly indivisible unless ℓ divides all exponents e_1 to e_r. For a single element the two notions of strongly indivisible and strongly independent are the same.

2.2. **Divisibility parameters.** If $\alpha \in K^\times$ is not a root of unity, we can express it as

$$\alpha = A^{\ell^d} \xi$$

for some nonnegative integer d, for some element $A \in K^\times$ which is strongly indivisible, and for some root of unity ξ in μ_{K,ℓ^∞} having order ℓ^h. We call d the *d-parameter* and h the *h-parameter*: these two nonnegative integers depend on α and K (the prime ℓ is fixed). It is not difficult to prove that the d-parameter is uniquely determined, which means that it does not depend on the chosen decomposition (see [3, Lemma 8]). Moreover, the decomposition of α can be chosen in such a way that either $h = 0$ or $h > \max(0, \omega - d)$: with these additional constraints, h is uniquely determined (see [3, Lemma 8]).

If G is a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r, then we define two sets of r parameters which we call the d-parameters and the h-parameters respectively. Let $G = \langle \alpha_1, \dots, \alpha_r \rangle$ and for each $i = 1, \dots, r$ let

$$\alpha_i = A_i^{\ell^{d_i}} \xi_i$$

for some nonnegative integer d_i, for some element $A_i \in K^\times$ which is strongly indivisible, and for some root of unity ξ_i in μ_{K,ℓ^∞} having order ℓ^{h_i}. We call $\alpha_1, \dots, \alpha_r$ a *good basis* for G if $A_1, \dots, A_r$ are strongly independent. This is equivalent to the fact that $\sum_{i=1}^r d_i$ (the sum of the d-parameters) is maximal among the possible bases of G (see [1, Section 3]). The group G always admits a good basis by [1, Theorem 14]. Every good basis has the same multiset of d-parameters (see [1, Corollary 16]), while the multiset of h-parameters is not unique. The h-parameters would become unique if we reorder the good basis of G such that the d-parameters are ordered non-decreasingly and we require the following conditions:

(1) For every $1 \leqslant i \leqslant r$ we have $h_i = 0$ or $h_i > \omega - d_i$.
(2) If $1 \leqslant i < j \leqslant r$ and $h_i, h_j > 0$ hold, then we have $h_i > h_j$ and $d_i + h_i < d_j + h_j$.
(3) If $1 \leqslant i < j \leqslant r$ and $d_i = d_j$ hold, then $h_j = 0$.

The non-uniqueness of the h-parameters for a good basis is discussed in [1, Appendix]: to gain flexibility we prefer not to impose the above conditions on the h-parameters. We call the above parameters the d-parameters and the h-parameters for G, keeping in mind that the h-parameters are not uniquely determined.

2.3. **Constructing a good basis.** Let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. Let $\alpha_1, \dots, \alpha_r$ be a basis of G with d-parameters $d_1, \dots, d_r$.

Remark 3. *As shown in* [1, Proof of Theorem 14]*, if the given basis of G is not a good basis, then there is a base change altering only one of the elements α_i's and such that the sum of the d-parameters for the new basis is greater than $\sum_{i=1}^r d_i$ (this simply amounts to the fact that the new generator has a greater d-parameter with respect to the replaced generator). We can prove that we have a good basis by showing that a base change as above does not exist.*

A good basis is explicitly computable, as explained in [1, Section 6.1].

3. Computing divisibility parameters

Let K be a number field and ℓ a fixed prime number.

Remark 4. *Let A be an element of $K^\times$ which is strongly indivisible. Then by definition for every non-zero integer X and for every $\zeta \in \mu_{K,\ell^\infty}$ the element $A^X\zeta$ has $v_\ell(X)$ as d-parameter and $\operatorname{ord}_\ell \zeta$ as h-parameter.*

Lemma 5. *Let $A_1, \dots, A_n$ be elements of $K^\times$ which are strongly independent. Then for all non-zero integers $X_1, \dots, X_n$ and for every $\zeta \in \mu_{K,\ell^\infty}$ the element $\zeta \prod_{i=1}^n A_i^{X_i}$ has d-parameter $\min_i(v_\ell(X_i))$ and h-parameter $\operatorname{ord}_\ell \zeta$.*

Proof. Call $x_i = v_\ell(X_i)$ and $m = \min_i(x_i)$. The element

$$C := \prod_{i=1}^n A_i^{X_i/\ell^m}$$

is the product of powers of strongly independent elements whose exponents are not all divisible by ℓ and hence it is strongly indivisible (by definition of strongly independent). So we can write

$$\zeta \prod_{i=1}^n A_i^{X_i} = C^{\ell^m}\zeta$$

and from the latter decomposition we can easily read off the divisibility parameters. □

Lemma 6. *Let $A_1, \dots, A_n$ be elements of $K^\times$ which are strongly independent, and let $\zeta_1, \dots, \zeta_n$ be roots of unity in μ_{K,ℓ^∞}. Then for all non-zero integers $X_1, \dots, X_n$ the elements*

$$A_1^{X_1}\zeta_1, \dots, A_n^{X_n}\zeta_n$$

form a good basis for the group that they generate. The (d,h)-parameters for this group are $(v_\ell(X_i), \operatorname{ord}_\ell \zeta_i)$ for $i = 1, \dots, n$.

Proof. Call G the group $\langle A_1^{X_1}\zeta_1, \dots, A_n^{X_n}\zeta_n\rangle$, and write $x_i = v_\ell(X_i)$. The (d,h)-parameters for the given basis are $(x_i, \operatorname{ord}_\ell \zeta_i)$ by Remark 4, so we are left to prove that we have a good basis. If not, then by Remark 3 it is possible to replace w.l.o.g. $A_1^{X_1}\zeta_1$ by

$$C := \prod_{i=1}^n A_i^{X_iE_i} \cdot \prod_{i=1}^n \zeta_i^{E_i}$$

for some integers E_i not all zero such that $G = \langle C, A_2^{X_2}\zeta_2, \dots, A_n^{X_n}\zeta_n\rangle$ and such that the d-parameter of C is greater than x_1. The first condition forces $v_\ell(E_1) = 0$ because $A_1^{X_1}$ times a root of unity belongs to G, so the d-parameter of C is at most $v_\ell(X_1E_1) = x_1$ by Lemma 5, contradiction. □

Lemma 7. *Let G be a torsion-free subgroup of $K^\times$ of rank r. Let E be an integer coprime to ℓ, and let G' be a subgroup of $K^\times$ satisfying*

$$G^E < G' < G\,.$$

Then the multisets of d-parameters for G and G' coincide.

Proof. By [1, Corollary 16] it suffices to show that the following two finite abelian groups are isomorphic for every positive integer n:

$$\frac{G}{G\cap (K^\times)^{\ell^n}} \quad \text{and} \quad \frac{G'}{G'\cap (K^\times)^{\ell^n}}\,.$$

By considering the map $G\to G^E$ which is raising to the power E one can easily deduce that

$$\frac{G}{G\cap (K^\times)^{\ell^n}} \simeq \frac{G^E}{G^E\cap (K^\times)^{\ell^n}}\,. \tag{4}$$

The claim boils down to the fact that if $x\in G$ and $a\in K^\times$ are such that $x^E=a^{\ell^n}$, then x is an ℓ^n-th power in $K^\times$, which follows from the identity $x=(a^{c_1}x^{c_2})^{\ell^n}$, where $c_1E+c_2\ell^n=1$.

By considering the inclusions $G^E\hookrightarrow G'\hookrightarrow G$ we get inclusions

$$\frac{G^E}{G^E\cap (K^\times)^{\ell^n}} \hookrightarrow \frac{G'}{G'\cap (K^\times)^{\ell^n}} \hookrightarrow \frac{G}{G\cap (K^\times)^{\ell^n}}$$

and we may conclude because of the isomorphism (4). □

Remark 8. *Let G be a torsion-free subgroup of $K^\times$ of rank 2. Let E be an integer coprime to ℓ, and let G' be a subgroup of $K^\times$ satisfying*

$$G^E < G' < G\,.$$

Then for every nonnegative integer n we have an equality of Kummer extensions:

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

The proof is immediate from Kummer theory (in short: an inclusion between groups implies an inclusion of the corresponding Kummer extensions, and the Kummer extensions related to G and G^E are the same because E is coprime to ℓ).

Proposition 9. *Let A and B be elements of $K^\times$ which are strongly independent, and let ζ,ξ be roots of unity in μ_{K,ℓ^∞}. Consider non-zero integers X,Y,Z and the elements*

$$\left\{\begin{array}{rcl} b_1 &=& A^X\zeta \\ b_2 &=& A^YB^Z\xi\,. \end{array}\right.$$

Call G the group $\langle b_1,b_2\rangle$ and write x,y,z for the ℓ-adic valuation of X,Y,Z respectively.

(i) If $x\leqslant y$, then the d-parameters for G are x and z. Moreover there is a subgroup G' of $K^\times$ satisfying

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

for all nonnegative integers n and such that the (d,h)-parameters for G' are

$$(x,\mathrm{ord}_\ell\,\zeta) \quad \textit{and} \quad (z,\mathrm{ord}_\ell\,\xi')\,, \tag{5}$$

where $\xi':=\zeta^F\xi^E$ with E,F non-zero integers such that $XF+YE=0$ and E is coprime to ℓ.

(ii) If $x>y$, and $z\leqslant y$, then the (d,h)-parameters for G are

$$(x,\mathrm{ord}_\ell\,\zeta) \quad \textit{and} \quad (z,\mathrm{ord}_\ell\,\xi)\,. \tag{6}$$

(iii) If $x > y$, and $z > y$, then the d-parameters for G are $x - y + z$ and y. Moreover there is a subgroup G' of $K^\times$ satisfying

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

for all nonnegative integers n and such that the (d,h)-parameters for G' are

$$(x - y + z, \operatorname{ord}_\ell \zeta') \quad \textit{and} \quad (y, \operatorname{ord}_\ell \xi)\,, \tag{7}$$

where $\zeta' := \zeta^E \xi^F$ with E, F coprime (non-zero) integers such that $XE + YF = 0$ and E is coprime to ℓ.

Proof. Case (i): If $x \leqslant y$, then there exists an integer E coprime to ℓ and an integer F such that $XF + YE = 0$ and hence

$$\begin{cases} b_1 &= A^X \zeta \\ b_2^E b_1^F &= B^{ZE} \xi'\,. \end{cases}$$

The group $G' = \langle b_1, b_2^E b_1^F \rangle$ is contained in G and it contains G^E so we deduce from Lemma 7 that G has the same d-parameters of G'. By Lemma 6 these are x and $v_\ell(ZE) = z$, while the h-parameters are $\operatorname{ord}_\ell \zeta$ and $\operatorname{ord}_\ell \xi'$. Since $G^E < G' < G$ the Kummer extensions $K(\zeta_{\ell^n}, \sqrt[\ell^n]{G})$ and $K(\zeta_{\ell^n}, \sqrt[\ell^n]{G'})$ coincide for every n by Remark 8.

Case (ii): We claim that b_1, b_2 are a good basis for G, so that the assertion follows from Remark 4 and Lemma 5. If b_1, b_2 is not a good basis of G, then by Remark 3 we can make a base change and increase the d-parameters of the basis. Since $x > y$ we cannot increase the d-parameter of b_2 with a base change of the form

$$b_{2,new} = b_1^E b_2^F = A^{XE+YF} B^{ZF} \cdot \zeta^E \xi^F$$

where the integers E, F are not both zero. Indeed, F has to be coprime to ℓ because $b_2 \in G$. But then by Lemma 5 the divisibility parameter of $b_{2,new}$ is (since $x > y$ and F is coprime to ℓ)

$$\min(v_\ell(XE + YF), v_\ell(ZF)) = \min(v_\ell(Y), v_\ell(Z))$$

and hence it is the same as the d-parameter of b_2.

Now we prove that we cannot increase the d-parameter of b_1 with a base change of the form

$$b_{1,new} = b_1^E b_2^F = A^{XE+YF} B^{ZF} \cdot \zeta^E \xi^F$$

where the integers E, F are not both zero. The integer E must be coprime to ℓ in order to have a base change. Let us consider the d-parameter for $b_{1,new}$. In view of Lemma 5, we should have $v_\ell(ZF) > x$. Moreover, in order to have

$$v_\ell(XE + YF) > x = v_\ell(X) = v_\ell(XE)$$

we should have $v_\ell(F) = x - y$. So we have $v_\ell(ZF) = z + x - y \leqslant x$, contradiction.

Case (iii): We can find an integer E coprime to ℓ and an integer F such that $EX + YF = 0$ so we can write

$$\begin{cases} b_1^E b_2^F &= B^{ZF} \cdot \zeta^E \xi^F \\ b_2 &= A^Y B^Z \xi\,. \end{cases}$$

In particular, we must have $v_\ell(F) = x - y > 0$. By Case (ii), the d-parameters for the group $G' = \langle b_1^E b_2^F, b_2 \rangle$ are $v_\ell(ZF) = x - y + z$ and y while the h-parameters are $\operatorname{ord}_\ell \zeta^E \xi^F$ and

$\mathrm{ord}_\ell\,\xi$. But the divisibility parameters of G' and G are the same by Lemma 7, so we conclude by Remark 8. □

4. Computing Kummer degrees

Let K be a number field and ℓ a prime number. Fix elements α_1 and α_2 of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of rank 2. Let n_1,n_2 be non-negative integers, and set $n := \max(n_1, n_2)$. Let m be an integer such that $m \geqslant n$. The Kummer extension

$$K(\zeta_{\ell^m},\ \sqrt[\ell^{n_1}]{\alpha_1},\ \sqrt[\ell^{n_2}]{\alpha_2})/K(\zeta_{\ell^m}) \tag{8}$$

is the same as the Kummer extension

$$K\Big(\zeta_{\ell^m},\ \sqrt[\ell^n]{(\alpha_1)^{\ell^{n-n_1}}},\ \sqrt[\ell^n]{(\alpha_2)^{\ell^{n-n_2}}}\Big)/K(\zeta_{\ell^m})\,.$$

Setting $G(n_1,n_2) := \langle (\alpha_1)^{\ell^{n-n_1}}, (\alpha_2)^{\ell^{n-n_2}}\rangle$, this Kummer extension can be written as

$$K\big(\zeta_{\ell^m},\ \sqrt[\ell^n]{G(n_1,n_2)}\big)/K(\zeta_{\ell^m})\,.$$

Convention. *For the remaining of the section (with the exception of Section 4.4), we suppose that $\ell \neq 2$ or that $\zeta_4 \in K$.*

Remark 10. *By* [1, Theorem 18]*, calling $d_i := d_i(n_1,n_2)$ and $h_i := h_i(n_1,n_2)$ for $i = 1,2$ the (d,h)-parameters of $G(n_1,n_2)$, the degree of* (8) *is a power of ℓ with exponent*

$$\max(h_1+\min(n,d_1)-m, h_2+\min(n,d_2)-m, 0)+\max(n-d_1,0)+\max(n-d_2,0) \tag{9}$$

so we are left to evaluate the (d,h)-parameters of $G(n_1,n_2)$.

Notice that if $h_1 = h_2 = 0$ then the above formula simplifies to

$$\max(n-d_1,0)+\max(n-d_2,0)$$

(and this generalises straight-forwardly to higher rank).

Remark 11. *If α_1 and α_2 are strongly independent, then by Lemma 6 we simply have $d_1 = n - n_1$ and $d_2 = n - n_2$, while h_1, h_2 may be taken to be zero, so the ℓ-adic valuation of the Kummer degree* (8) *is simply*

$$n_1 + n_2\,.$$

This remark can be easily generalized to higher rank thus it is possible to prove (2) *by applying* [1, Theorem 18] *under the assumption that $\ell \neq 2$ or that $\zeta_4 \in K$.*

By considering a good basis for the group $\langle \alpha_1, \alpha_2\rangle$ we can find two strongly independent elements A, B of $K^\times$ and roots of unity $\eta, \theta \in \mu_{K,\ell^\infty}$ and integers E_1, E_2, F_1, F_2 such that we have

$$\left\{\begin{array}{lcl} \alpha_1 &=& A^{E_1}B^{F_1}\eta \\ \alpha_2 &=& A^{E_2}B^{F_2}\theta\,. \end{array}\right. \tag{10}$$

Notice that $A, B, \eta, \theta, E_1, E_2, F_1, F_2$ are independent of n_1, n_2 and explicitly computable. Write e_1, e_2, f_1, f_2 for the ℓ-adic valuation of E_1, E_2, F_1, F_2 respectively (if such numbers are non-zero).

4.1. **Special cases in which there are some zero exponents in** (10)**.** We now treat the case where some of the exponents in (10) are zero. Notice that there can be at most two zeros and that if there are two zeros, then we either have $E_2 = F_1 = 0$ or $E_1 = F_2 = 0$. We first suppose that there are two zeros and apply Lemma 6:

• *If $E_2 = F_1 = 0$, then the (d,h)-parameters for $G(n_1, n_2)$ are*

$$(n - n_1 + e_1, \operatorname{ord}_\ell \eta^{\ell^{n-n_1}}) \quad \textit{and} \quad (n - n_2 + f_2, \operatorname{ord}_\ell \theta^{\ell^{n-n_2}}) .$$

By plugging these values in (9) we get the ℓ-adic valuation of the Kummer degree (8). If $E_1 = F_2 = 0$, we clearly have the analogous result.

Now we suppose that there is exactly one zero exponent and apply Proposition 9 (the integers E, F are as in Proposition 9 according to the case we are considering).

• *If $F_1 = 0$, then to compute the Kummer degree* (8) *with* (9) *we can take as (d,h)-parameters:*

(i) If $n_2 - n_1 \leqslant e_2 - e_1$:

$$(n - n_1 + e_1, \operatorname{ord}_\ell \eta^{\ell^{n-n_1}}) \quad \textit{and} \quad (n - n_2 + f_2, \operatorname{ord}_\ell \eta^{F\ell^{n-n_1}} \theta^{E\ell^{n-n_2}}) .$$

(ii) If $n_2 - n_1 > e_2 - e_1$ and $f_2 \leqslant e_2$:

$$(n - n_1 + e_1, \operatorname{ord}_\ell \eta^{\ell^{n-n_1}}) \quad \textit{and} \quad (n - n_2 + f_2, \operatorname{ord}_\ell \theta^{\ell^{n-n_2}}) .$$

(iii) If $n_2 - n_1 > e_2 - e_1$ and $f_2 > e_2$:

$$(n - n_1 + e_1 - e_2 + f_2, \operatorname{ord}_\ell \eta^{E\ell^{n-n_1}} \theta^{F\ell^{n-n_2}}) \quad \textit{and} \quad (n - n_2 + e_2, \operatorname{ord}_\ell \theta^{\ell^{n-n_2}}) .$$

If $E_1 = 0$, or if $E_2 = 0$, or if $F_2 = 0$ we have the analogous case distinction and result with respect to the case $F_1 = 0$ (it suffices to swap α_1 and α_2, or swap A and B, or both).

4.2. **The generic case in which there are no zero exponents in** (10)**.** Setting $N_1 := \ell^{n-n_1}$ and $N_2 := \ell^{n-n_2}$, we can write

$$\begin{cases} \alpha_1^{N_1} &= A^{E_1 N_1} B^{F_1 N_1} \eta^{N_1} \\ \alpha_2^{N_2} &= A^{E_2 N_2} B^{F_2 N_2} \theta^{N_2} . \end{cases}$$

Suppose that $v_\ell(F_1 N_1) \geqslant v_\ell(F_2 N_2)$. Then there are integers W_1, R_1 coprime to ℓ (which are independent of n_1, n_2 and explicitly computable) such that we have

$$F_1 N_1 W_1 + F_2 N_2 R_1 \ell^{(f_1+n-n_1)-(f_2+n-n_2)} = 0$$

so we get

$$\begin{cases} \alpha_1^{N_1 W_1} \alpha_2^{N_2 R_1 \ell^{(f_1-n_1)-(f_2-n_2)}} &= A^{E_1 N_1 W_1 + E_2 N_2 R_1 \ell^{(f_1-n_1)-(f_2-n_2)}} \nu \\ \alpha_2^{N_2} &= A^{E_2 N_2} B^{F_2 N_2} \theta^{N_2} , \end{cases}$$

where

$$\nu := (\eta^{W_1} \theta^{R_1 \ell^{f_1 - f_2}})^{\ell^{n-n_1}} .$$

Notice that ν depends on n_1 and n_2 only through $n_2 - n_1$ (because $n - n_1$ equals $n_2 - n_1$ or 0), and (since ν is the power of a computable root of unity) we can determine ν with a finite

case distinction and ν is explicitly computable in each of the finitely many cases. The above system can be rewritten as

$$\left\{ \begin{array}{rcl} \alpha_1^{N_1W_1}\alpha_2^{N_2R_1\ell^{(f_1-n_1)-(f_2-n_2)}} & = & A^{S_1N_1}\nu \\ \alpha_2^{N_2} & = & A^{E_2N_2}B^{F_2N_2}\theta^{N_2}\,, \end{array} \right. \tag{11}$$

where

$$S_1 := E_1W_1 + E_2R_1\ell^{f_1-f_2}\,.$$

Notice that the non-zero rational number S_1 is independent of n_1 and n_2 and explicitly computable, and write $s_1 := v_\ell(S_1)$. Since W_1 is coprime to ℓ, by Remark 8 the group $G(n_1,n_2)$ has the same Kummer extensions as the group generated by the two elements in (11). Then we apply Proposition 9 to the latter group and get the following result:

• *If $E_1,E_2,F_1,F_2\neq 0$ and $v_\ell(F_1N_1)\geqslant v_\ell(F_2N_2)$, then to compute the Kummer degree of* (8) *with* (9) *we can take as (d,h)-parameters (where E and F are as in Proposition 9 according to the case distinction):*

(i) If $n_2-n_1\leqslant e_2-s_1$:

$$(n-n_1+s_1,\mathrm{ord}_\ell\,\nu)\quad\textit{and}\quad(n-n_2+f_2,\mathrm{ord}_\ell\,\nu^F\theta^{\ell^{n-n_2}E})\,.$$

(ii) If $n_2-n_1>e_2-s_1$ and $f_2\leqslant e_2$:

$$(n-n_1+s_1,\mathrm{ord}_\ell\,\nu)\quad\textit{and}\quad(n-n_2+f_2,\mathrm{ord}_\ell\,\theta^{\ell^{n-n_2}})\,.$$

(iii) If $n_2-n_1>e_2-s_1$ and $f_2>e_2$:

$$(n-n_1+s_1-e_2+f_2,\mathrm{ord}_\ell\,\nu^E\theta^{\ell^{n-n_2}F})\quad\textit{and}\quad(n-n_2+e_2,\mathrm{ord}_\ell\,\theta^{\ell^{n-n_2}})\,.$$

Notice that the roots of unity in the formulas depend on n_1 and n_2, but only through a finite case distinction, so that all parameters that we will appear in formula (9) are explicitly computable.

If $E_1,E_2,F_1,F_2\neq 0$ and $v_\ell(F_1N_1)<v_\ell(F_2N_2)$ one has the analogous result by swapping α_1 and α_2.

We have considered all cases, and in particular have proven Theorem 2 under the assumption that $\ell\neq 2$ or $\zeta_4\in K$.

4.3. **Formulas for the case $\zeta_\ell\notin K$.** Now suppose that $\zeta_\ell\notin K$. With this assumption all h-parameters are zero and the formulas simplify.

Remark 12. *Suppose that $\zeta_\ell\notin K$. Recall that e_1, e_2, f_1, f_2, s_1 are integers independent from n_1 and n_2 and explicitly computable. Up to swapping α_1, α_2 or A, B or both, the ℓ-adic valuation of the Kummer degree of* (3) *is given by one of the following expressions (according to the above case-distinction):*

$$\begin{gathered} \max(n_1-e_1,0)+\max(n_2-f_2,0) \\ \max(n_1-e_1+e_2-f_2,0)+\max(n_2-e_2,0) \\ \max(n_1-s_1,0)+\max(n_2-f_2,0) \\ \max(n_1-s_1+e_2-f_2,0)+\max(n_2-e_2,0)\,. \end{gathered}$$

4.4. **The case $\ell = 2$ and $\zeta_4 \notin K$.** Now suppose that we are in the case $\ell = 2$ and $\zeta_4 \notin K$. The Kummer extension

$$K(\zeta_{2^m},\ \sqrt[2^{n_1}]{\alpha_1},\ \sqrt[2^{n_2}]{\alpha_2})/K(\zeta_{2^m}) \tag{12}$$

can be seen as a Kummer extension over the base field $K(\zeta_4)$ as soon as $n_1 \geqslant 2$ or $n_2 \geqslant 2$ or $m \geqslant 2$. If this holds, we can reduce to the previous case in which ζ_4 belongs to the base field by simply extending K to $K(\zeta_4)$ (notice that by the results in [5] the divisibility parameters over $K(\zeta_4)$ can be deduced from the divisibility parameters over K). We are left to compute the degrees of the following extensions:

$$K(\ \sqrt[2^{n_1}]{\alpha_1},\ \sqrt[2^{n_2}]{\alpha_2})/K$$

where n_1 and n_2 are in $\{0, 1\}$. If $n_1 = 0$ or $n_2 = 0$ then this is trivial because we have at most to see if an element of $K^\times$ is a square or not (the above degree can only be 1 or 2 in this special case). Now we are left to compute the degree of

$$K(\sqrt{\alpha_1}, \sqrt{\alpha_2})/K\ .$$

By Kummer theory we only need to check whether α_1 or α_2 or $\alpha_1\alpha_2$ are squares in $K^\times$. In this way we can determine whether this degree is 1, 2, or 4.

We have now dealt with the missing case $\ell = 2$ and $\zeta_4 \notin K$, and in particular we have proven Theorem 2.

REFERENCES

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

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

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

[4] PERUCCA, A. - SGOBBA, P., *Kummer theory for number fields and the reductions of algebraic numbers*, Int. J. Number Theory, **15** (2019), 1617–1633.

[5] 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.

[6] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Explicit Kummer theory for the rationals*, submitted for publication, preprint available on ORBilu `https://orbilu.uni.lu/handle/10993/39282`.

[7] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Kummer theory for number fields via entanglement groups*, submitted for publication, preprint available on ORBilu `https://orbilu.uni.lu/handle/10993/40831`.

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

Email address: `antonella.perucca@uni.lu`