THE DEGREE OF NON-GALOIS KUMMER EXTENSIONS OF NUMBER FIELDS

ANTONELLA PERUCCA

ABSTRACT. Let K be a number field, and let $a_1, \dots, a_r$ be elements of $K^\times$ which generate a torsion-free subgroup of $K^\times$ of positive rank r. Let $\alpha_1, \dots, \alpha_r$ be ℓ^n-th roots of the given elements respectively, where ℓ is a prime number and $n > 0$. In this short note we provide explicit parametric formulas for the degree of the extension $K(\alpha_1, \dots, \alpha_r)$. This degree may depend on the choice of $\alpha_1, \dots, \alpha_r$ because we are not assuming that the ℓ^n-th roots of unity are in K.

1. INTRODUCTION

Given a number field K, we are interested in the Kummer extensions of K. More precisely, let $a_1, \dots, a_r$ be elements of $K^\times$ which generate (without loss of generality) a torsion-free subgroup of $K^\times$ of positive rank r. For every $i = 1, \dots, r$ let α_i be an ℓ^{n_i}-th root of a_i, where $n_i > 0$ and ℓ is a prime number. Then we are interested in the degree of the (not necessarily Galois) Kummer extension

$$K(\alpha_1, \dots, \alpha_r)/K\,.$$

In this short note we are able to compute this degree, which may depend on the choice of $\alpha_1, \dots, \alpha_r$ because we are not assuming that the ℓ^{n_i}-th roots of unity are in K.

Our strategy is deducing the formulas for the degree from formulas obtained by the author with Debry, Sgobba and Tronto which express the degree of the abelian Kummer extension

$$K_{\ell^n}(\alpha_1, \dots, \alpha_r)/K_{\ell^n}\,,$$

where $n = \max_i(n_i)$, and where K_{ℓ^n} denotes the extension of K obtained by adding the ℓ^n-th roots of unity. The result for rank r is based on the result for rank 1, which is described by the following two theorems, covering respectively the case ℓ odd or $K = K_4$, and the case $\ell = 2$ and $K \neq K_4$. In those statements by 'strongly indivisible' we mean an element of $K^\times$ which is not an ℓ-th power in $K^\times$ times a root of unity in K.

Theorem 1. *Let K be a number field and ℓ a prime number. If $\ell = 2$, suppose that $K = K_4$. Let $a \in K^\times$ and $n > 0$, and consider some ℓ^n-th root α of a.*

(1) Suppose that $a = b^{\ell^d}$ for some $b \in K^\times$ strongly indivisible and for some $d \geqslant 0$. If $n \leqslant d$, let ℓ^t be the order of the root of unity $\alpha/b^{\ell^{d-n}}$. Then we have $K(\alpha) = K_{\ell^t}$ and in particular

$$[K(\alpha) : K] = [K_{\ell^t} : K]\,.$$

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

If $n > d$, let β be any ℓ^{n-d}-th root of b and let ℓ^t be the order of the root of unity α/β. Then we have $K(\alpha) \supseteq K_{\ell^{\max(0,t+d-n)}}$ and

$$[K(\alpha) : K] = \ell^{n-d}[K_{\ell^{\max(0,t+d-n)}} : K] .$$

(2) Suppose that $K = K_\ell$, and let $z \geqslant 1$ be the greatest integer such that $K_{\ell^z} = K$ (for $\ell = 2$ we are assuming $z \geqslant 2$). Suppose that $a = \zeta b^{\ell^d}$ for some $b \in K^\times$ strongly indivisible, for some $d > 0$ and for some root of unity $\zeta \in K$ of order ℓ^h with $h > \max(0, z - d)$. Then we have

$$[K(\alpha) : K] = \ell^{\max(0,n+h-z)} .$$

Notice that the condition on h in the statement is motivated by [1, Proposition 31].

Theorem 2. *Let K be a number field. Suppose that $K \neq K_4$ and let $s \geqslant 2$ be the greatest integer such that $K_4 = K_{2^s}$. Let $a \in K^\times$ and $n > 0$, and consider some 2^n-th root α of a.*

(1) Suppose that $a = b^{2^d}$ for some $b \in K^\times$ strongly indivisible and for some $d \geqslant 0$. If $n \leqslant d$, let 2^t be the order of the root of unity $\alpha/b^{2^{d-n}}$. Then we have $K(\alpha) = K_{2^t}$ and in particular

$$[K(\alpha) : K] = [K_{2^t} : K] .$$

If $n > d$, let β be any 2^{n-d}-th root of b and let 2^t be the order of the root of unity α/β. Then we have $K(\alpha) \supseteq K_{2^{\max(0,t+d-n)}}$ and

$$[K(\alpha) : K] = 2^{n-d}[K_{2^{\max(0,t+d-n)}} : K] ,$$

unless we are in the special case $K(\sqrt{b}) \subseteq K_{2^{s+1}}$. In this case we have:

$$[K(\alpha) : K] = \begin{cases} 2^{n-d} & \text{if } t + d - n \leqslant 1 \text{ or } t + d - n = s \\ 2^{n-d+1} & \text{if } 1 < t + d - n < s \\ 2^{t-s+1} & \text{if } t + d - n > s . \end{cases}$$

(2) Suppose that $a = -b^{2^d}$ for some $b \in K^\times$ strongly indivisible and for some $d > 0$. If $n \leqslant d$, then $K(\alpha) = K_{2^{n+1}}$ and in particular

$$[K(\alpha) : K] = 2^{1+\max(0,n+1-s)} .$$

If $n > d$, then let β be any 2^{n-d}-th root of b. We then have $K(\alpha) \supseteq K_{2^{d+1}}$ and we also have

$$[K(\alpha) : K] = 2^{n-d+1+\max(d+1-s,0)} ,$$

unless the condition $K(\sqrt{b}) \subseteq K_{2^{s+1}}$ holds. In this case we have

$$[K(\alpha) : K] = 2^{n-d+\epsilon+\max(d+1-s,0)} ,$$

where $\epsilon \in \{0, 1\}$ and $\epsilon = 0$ if and only if $d = s - 1$.

Notice that by [2, Lemma 8] the cases treated in the above two results cover every possibility. The generalization to higher rank of the above results are Theorems 10 and 11 respectively, which again cover all cases by the theory developed in [1, 3] (see also Remark 9).

2. THE RESULTS FOR RANK 1

In this section we are going to prove the results stated in the Introduction. We let K be a number field and ℓ a prime number. Recall that $b \in K^\times$ is *strongly indivisible* if it is not an ℓ-th power in $K^\times$ times a root of unity in K (whose order we may suppose to be a power of ℓ). We denote by K_{ℓ^n} the extension of K obtained by adding the ℓ^n-th roots of unity, and by K_{ℓ^∞} the union of K_{ℓ^n} for $n \geqslant 0$. We also denote by ζ_{2^s} a root of unity of order 2^s. Notice that we have

$$\zeta_{2^s} + \zeta_{2^s}^{-1} + 2 = \zeta_{2^s}^{-1}(1 + \zeta_{2^s})^2 \tag{1}$$

Lemma 3. *Let $b \in K^\times$ be strongly indivisible in K, and let $n > 0$. Then for any $m \geqslant 0$ the element b is also strongly indivisible in K_{ℓ^m} and for every ℓ^n-th root β of b we have*

$$[K_{\ell^m}(\beta) : K_{\ell^m}] = \ell^n\,,$$

unless all the following conditions hold: $\ell = 2$, $K \neq K_4$, and for some $s \geqslant 2$ we have

$$K \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}(\zeta_{2^s} + \zeta_{2^s}^{-1})$$

$$\pm b/(\zeta_{2^s} + \zeta_{2^s}^{-1} + 2) \in (K^\times)^2\,.$$

In this case $\sqrt{b}$ is not in $K_4 = K_{2^s}$ but it generates $K_{2^{s+1}}$ over K_4, and it is strongly indivisible over K_{2^m} for every $m \geqslant s+1$. Moreover, in this case we have

$$[K_{2^m}(\beta) : K_{2^m}] = \begin{cases} 2^n & \text{if } m < s+1, \\ 2^{n-1} & \text{if } m \geqslant s+1. \end{cases}$$

Proof. Notice that if F is a number field, $a \in F^\times$, and $x > 0$, then the equality $[F_{\ell^\infty}(\sqrt[\ell^x]{a}) : F_{\ell^\infty}] = \ell^x$ implies that a is strongly indivisible in F. Then the assertions about the strong indivisibility follow from the assertions on the degree.

The assertion on the degree, apart from the special case, can be found in [2, Theorems 11.1 and 13.1] (where we set $d = 0$) for $m \geqslant n$, and this implies the assertion for $m < n$. Now consider the special case, and suppose first that $m \geqslant s+1$. Since $\sqrt{b} \in K_{2^{s+1}}$ by [2, Theorem 13.1], then the degree of $[K_{2^m}(\beta) : K_{2^m}]$ is at most 2^{n-1}. This degree is then exactly 2^{n-1} because [2, Theorem 13.1] implies that $[K_{2^\infty}(\beta) : K_{2^\infty}] = 2^{n-1}$. If $m < s+1$, then $K_{2^m} \subseteq K_4$ and hence $[K_{2^m}(\beta^{2^{n-1}}) : K_{2^m}] = 2$. We also have that $[K_{2^m}(\beta) : K_{2^m}(\beta^{2^{n-1}})] = 2^{n-1}$ because $K_{2^m}(\beta^{2^{n-1}}) \subseteq K_{2^\infty}$ and $[K_{2^\infty}(\beta) : K_{2^\infty}] = 2^{n-1}$ as above. □

We now prove Theorem 1, which covers the case ℓ odd or $K = K_4$:

Proof of Theorem 1. Proof of (1): If $n \leqslant d$, then $K(\alpha) = K(\alpha/b^{\ell^{d-n}})$ because $b^{\ell^{d-n}} \in K$, and hence the assertion is clear. Now suppose that $n > d$. For any choice of β we have $[K(\beta) : K] = \ell^{n-d}$ by Lemma 3. This explains the assertion for the case $t \leqslant n-d$. If $t > n-d$, let $\alpha/\beta = \xi$. Then α is an ℓ^{n-d}-th root of $b\xi^{\ell^{n-d}}$ and hence $K(\alpha)$ contains $K_{\ell^{t-n+d}}$. Over this field the element b and hence $b\xi^{\ell^{n-d}}$ is strongly indivisible by Lemma 3, so we may deduce the formula

$$[K(\alpha) : K] = \ell^{n-d}[K_{\ell^{t-n+d}} : K]\,.$$

Proof of (2): If $n \leqslant d$, then $\alpha = b^{\ell^{d-n}}\xi$, where ξ is a root of unity of order ℓ^{h+n}, so we have

$$[K(\alpha) : K] = [K_{\ell^{h+n}} : K] = \ell^{\max(0,h+n-z)}\,.$$

If $n > d$, then (independently of the choice of α) the element $\alpha^{\ell^{n-d}}/b$ is a root of unity of order ℓ^{h+d}. This means that $K(\alpha)$ contains $K_{\ell^{h+d}}$. Since b and hence $\alpha^{\ell^{n-d}}$ is strongly indivisible in $K_{\ell^{h+d}}$ by Lemma 3, we deduce that

$$[K(\alpha) : K] = \ell^{n-d}[K_{\ell^{h+d}} : K]\,.$$

Since $[K_{\ell^{h+d}} : K] = \ell^{h+d-z}$ (as $h > z - d$), we find that $[K(\alpha) : K] = \ell^{n+h-z}$. □

We now prove Theorem 2, which covers the remaining case:

Proof of Theorem 2. Proof of (1): If $n \leqslant d$ we may reason as in Theorem 1. Now suppose that $n > d$ and that we are not in the special case. We may again reason as in Theorem 1. Indeed, for any choice of β we have $[K(\beta) : K] = 2^{n-d}$ by Lemma 3. This explains the assertion for the case $t \leqslant n - d$. If $t > n - d$, let $\alpha/\beta = \xi$. Then α is a 2^{n-d}-th root of $b\xi^{2^{n-d}}$ and hence $K(\alpha)$ contains $K_{2^{t-n+d}}$. Over this field the element $b\xi^{2^{n-d}}$ is strongly indivisible by Lemma 3, so we may deduce the formula

$$[K(\alpha) : K] = 2^{n-d}[K_{2^{t-n+d}} : K]\,.$$

Now suppose that $n > d$ and that we are in the special case. Let $\alpha/\beta = \xi$. We compute

$$[K(\alpha) : K] = [K(\beta\xi) : K((\beta\xi)^{2^{n-d-1}})][K((\beta\xi)^{2^{n-d-1}}) : K]\,.$$

Notice that $K((\beta\xi)^{2^{n-d-1}})$ is contained in K_{2^∞}. Then the first degree is 2^{n-d-1} because $[K_{2^\infty}(\beta) : K_{2^\infty}] = 2^{n-d-1}$ by Lemma 3. Studying the second degree amounts to studying the degree of $K(\xi^{2^{n-d-1}}\sqrt{b})$ over K. If $t \leqslant n - d$, then we have

$$[K((\beta\xi)^{2^{n-d-1}}) : K] = [K(\sqrt{b}) : K] = 2\,.$$

If $t = n - d + 1$, then $\xi^{2^{n-d-1}}$ has order 4. Since the quadratic extensions $K(\sqrt{b})$ and K_4 are linearly disjoint, we have again that $[K((\beta\xi)^{2^{n-d-1}}) : K] = 2$. If $t \geqslant n - d + 2$, then the field $K(\xi^{2^{n-d-1}}\sqrt{b})$ contains $\xi^{2^{n-d}}$ and hence it contains K_4, so it is the same as $K_4(\zeta\xi^{2^{n-d-1}})$, where ζ is any primitive root of unity of order 2^{s+1} (notice that ζ^2/b is a square in K_4 by (1)). We may easily conclude.

Proof of (2): If $n \leqslant d$, then $[K(\alpha) : K] = [K_{2^{n+1}} : K]$ and hence the assertion follows. Now suppose that $n > d$. Let $\alpha/\beta = \xi$, where ξ is a root of unity of order 2^{n+1}. The extension $K(\beta\xi)$ contains $b\xi^{2^{n-d}}$ and hence $K_{2^{d+1}}$. Suppose that we are not in the special case. Then the extension $K(\beta\xi)$ over $K_{2^{d+1}}$ has maximal degree 2^{n-d} because $[K_{2^\infty}(\beta) : K_{2^\infty}] = 2^{n-d}$ by Lemma 3. So we have

$$[K(\alpha) : K] = 2^{n-d}[K_{2^{d+1}} : K] = 2^{n-d+1+\max(d+1-s,0)}\,.$$

Now suppose that we are in the special case, which corresponds to the special case of Lemma 3. We study the degree of $K_{2^{d+1}}(\xi^{2^{n-d-1}}\sqrt{b})$ over $K_{2^{d+1}}$. If $d \geqslant s$, then $\sqrt{b} \in K_{2^{d+1}}$ and the above extension is quadratic. If $d \leqslant s - 2$, then $\xi^{2^{n-d-1}} \in K_{2^{d+1}}$ and hence the above extension is quadratic. If $d = s - 1$, let ζ be a root of unity of order 2^{s+1} such that

$\zeta/\sqrt{b} \in K_4$. Then the root of unity $\zeta\xi^{2^{n-d-1}}$ is the product of two primitive roots of unity of order $s+1 = d+2$ and hence it has order at most s: we deduce that the above extension is trivial. Finally, the degree of $K(\beta\xi)$ over $K(\xi^{2^{n-d-1}}\sqrt{b}) \subseteq K_{2^\infty}$ is maximal i.e. equal to 2^{n-d-1} because $[K_{2^\infty}(\beta) : K_{2^\infty}] = 2^{n-d-1}$ by Lemma 3. So we have

$$[K(\alpha) : K] = 2^{n-d-1+\epsilon}[K_{2^{d+1}} : K] = 2^{n-d+\epsilon+\max(d+1-s,0)}\,.$$

□

Example 4. Let $K = \mathbb{Q}$ and $\ell = 3$. Then the third roots of 8 are 2, $2\zeta_3$ and $2\zeta_3^2$, where ζ_3 is a root of unity of order 3. The degrees over $\mathbb{Q}$ of these elements are 1, 2, and 2, respectively.

Example 5. Let $K = \mathbb{Q}$ and $\ell = 2$. Then the fourth roots of -9 are of the form $\alpha = \xi\sqrt{3}$, where ξ is a root of unity of order 8. The degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 4 by Theorem 2 (we have $n = s = 2$, $b = 3$ and $d = 1$, i.e. we apply the second case of the theorem, with $n > d$ and $\sqrt{b} \notin \mathbb{Q}_8$ obtaining degree $2^{n-d+1+\max(d+1-s,0)} = 2^2$). One can also see that $\alpha^2 = 3\zeta$, where ζ is a root of unity of order 4. So $\mathbb{Q}(\alpha)$ contains $\mathbb{Q}_4$. Then $\mathbb{Q}(\alpha)$ is quadratic over $\mathbb{Q}_4$.

Example 6. Let $K = \mathbb{Q}$ and $\ell = 2$. Recall that $\sqrt{2} \in \mathbb{Q}_8$.
• The fourth roots of 4 are of the form $\alpha = \xi\sqrt{2}$, where ξ is a root of unity of order dividing 4. The degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 2 by Theorem 2 or by direct inspection.
• The eighth roots of 16 are of the form $\alpha = \xi\sqrt{2}$, where ξ is a root of unity of order dividing 8. By Theorem 2 (or by the above example) the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 2 if the order of ξ divides 4. If the order of ξ equals 8, then α^2 generates $\mathbb{Q}_4$ hence $\mathbb{Q}(\alpha)$ contains $\mathbb{Q}_4$. The degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$, if the order of ξ equals 8, is then 2. Indeed, $\xi\sqrt{2} = 1 + \xi^2$ is contained in $\mathbb{Q}_4$. This is also what follows from Theorem 2.
• The sixteenth roots of 256 are of the form $\alpha = \xi\sqrt{2}$, where ξ is a root of unity of order dividing 16. If the order of ξ divides 8, then the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 2 as shown above, while if the order of ξ is 16, then the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 8 by Theorem 2. Indeed, in the latter case $\mathbb{Q}(\alpha)$ contains $\mathbb{Q}(\alpha^2) = \mathbb{Q}_8$ and hence it equals $\mathbb{Q}_{16}$.
• The eighth roots of -16 are of the form $\alpha = \xi\sqrt{2}$, where ξ is a root of unity of order 16. By Theorem 2 the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 8. Indeed $\mathbb{Q}(\alpha^2) = \mathbb{Q}_8 \ni \sqrt{2}$ and hence $\mathbb{Q}(\alpha) = \mathbb{Q}_{16}$.
• The fourth roots of -4 are of the form $\alpha = \xi\sqrt{2}$, where ξ is a root of unity of order 8. This is the case in Theorem 2 in which ϵ is 0. Indeed, the field $\mathbb{Q}(\alpha)$ is $\mathbb{Q}_4$, so the degree of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is 2.

Example 7. Let $K = \mathbb{Q}(\sqrt{2})$ and $\ell = 2$. Then the eighth roots of $(2+\sqrt{2})^4$ are of the form $\alpha = \xi\sqrt{2+\sqrt{2}}$, where ξ is a root of unity of order dividing 8. The extension $K(\alpha)/K$ is quadratic if the order of ξ divides 4. If the order of ξ is 8, then $K(\alpha)$ contains $K(\alpha^2) = \mathbb{Q}_8$ and it is a quadratic extension of $\mathbb{Q}_8$. We deduce that the degree of $K(\alpha)$ over K is 4. This is also what follows from Theorem 2.

3. THE RESULTS FOR HIGHER RANK

Let K be a number field, and let ℓ be a prime number. We call $a_1, \dots, a_r \in K^\times$ *strongly independent* if $a_1^{x_1} \cdots a_r^{x_r}$ is strongly indivisible whenever $x_1, \dots, x_r$ are integers not all divisible by ℓ.

Lemma 8. *Let $I = \{1, \dots, r\}$. For every $i \in I$, let n_i be a non-negative integer. Let $b_1, \dots, b_r \in K^\times$ be strongly independent, and consider for every $i \in I$ an ℓ^{n_i}-th root β_i of b_i. Then we have*

$$[K_{\ell^m}(\beta_i : i \in I) : K_{\ell^m}] = \ell^{\sum_i n_i}$$

for every $m \geqslant 0$ if ℓ is odd, or if no product of the β_i is as in the special case of Lemma 3. If $\ell = 2$, $K \neq K_4$ and $n_1 > 0$ and

$$K \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}(\zeta_{2^s} + \zeta_{2^s}^{-1})$$

$$\pm b_1/(\zeta_{2^s} + \zeta_{2^s}^{-1} + 2) \in (K^\times)^2$$

we have

$$[K_{2^m}(\beta_i : i \in I) : K_{2^m}] = \begin{cases} 2^{\sum_i n_i} & \text{if } m < s+1, \\ 2^{(\sum_i n_i)-1} & \text{if } m \geqslant s+1. \end{cases},$$

and also

$$[K_{2^m}(\beta_i : i \in I) : K_{2^m}(\sqrt{b_1})] = 2^{(\sum_i n_i)-1}$$

for every $m \geqslant 0$. Moreover, $\sqrt{b_1}, b_2, \dots, b_r$ are strongly independent over K_{2^∞}.

Proof. Unless we are in the special case, the elements $b_1, \dots, b_r$ are again strongly independent over K_4 as a consequence of Lemma 3. So we may conclude by [1, Theorem 18]. For the second assertion, we need to consider the special case of Lemma 3 for the element b_1. By [3, Theorem 2] applied to the group generated by $b_1, \dots, b_r$ (and by the first part of the statement which ensures – in view of [1, Theorem 18] – that strongly independent elements stay strongly independent while passing from K_4 to $K_{2^{s+1}}$) we deduce that $\beta_1^{2^{n_1-1}}, b_2, \dots, b_r$ are strongly independent over $K_{2^{s+1}}$ and hence over K_{2^∞} by Lemma 3. So we are left to check that $K_{2^m}(\sqrt{b_1})$ is either a trivial or a quadratic extension of K_{2^m} according to whether $m \geqslant s+1$ or not. □

Let G be a finitely generated and torsion-free subgroup of $K^\times$ of positive rank r. If $a_1, \dots, a_r$ is a basis of G, we can write

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

for some strongly 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 call $a_1, \dots, a_r$ a *good basis* of G if $b_1, \dots, b_r$ are strongly independent or, equivalently, if the sum $\sum_i d_i$ is maximal among the possible bases of G, see [1, Section 3.1]. In this case we call d_i and h_i the *d-parameters and h-parameters for the 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 [1, Appendix]). Recall from [1, Theorem 14] that a good basis of G always exists, and from [1, Section 6.1] that a good basis and the parameters for the divisibility are computable.

Remark 9. *Let $a_1, \dots, a_r$ be elements of $K^\times$ which generate (without loss of generality) a torsion-free subgroup of $K^\times$ of positive rank r. For every $i = 1, \dots, r$ let α_i be an ℓ^{n_i}-th root of a_i, where $n_i \geqslant 0$ and ℓ is a prime number. Then, letting $n = \max(n_i)$, we may consider α_i to be an ℓ^n-th root of $a_i^{\ell^{n-n_i}}$. In particular, up to replacing the a_i's, we may assume that all n are equal.*

Next consider the group generated by the a_i's, and an ℓ-good basis $g_1, \dots, g_r$ of this group. By considering the base-change from the a_i's to the g_i's (with the iterative procedure described in [1, Proof of Theorem 14]*) we can explicitly determine ℓ^n-th roots γ_i's of the g_i's such that*

$$\mathbb{Q}(\alpha_1, \dots, \alpha_r) = \mathbb{Q}(\gamma_1, \dots, \gamma_r)\,.$$

So we may reduce to the case where $a_1, \dots, a_r$ are a good basis for the group that they generate. In particular, we may suppose that

$$a_i = \zeta_i b_i^{\ell^{d_i}}$$

where ζ_i is a root of unity in K of order a power of ℓ and the elements $b_1, \dots, b_r \in K^\times$ are strongly independent.

If $\ell = 2$ and $K \neq K_4$, then by [3, Proposition 5] *we may choose the 2-good basis such that (without loss of generality) b_1 is as in the special case of Lemma 3, or such that no product of the b_i's is as in the special case of Lemma 3.*

The following result covers the case ℓ odd or $K = K_4$:

Theorem 10. *Let ℓ be odd, or $K = K_4$. Let $I = \{1, \dots, r\}$. Let $a_1, \dots, a_r$ be elements of $K^\times$ such that*

$$a_i = \zeta_i b_i^{\ell^{d_i}}$$

for every $i \in I$, where $d_i \geqslant 0$, where ζ_i is a root of unity in K of order ℓ^{h_i} for some $h_i \geqslant 0$, and where the elements $b_1, \dots, b_r \in K^\times$ are strongly independent. Let α_i be an ℓ^n-th root of a_i for some $n > 0$. We partition the index set I into four subsets I_1, I_2, I_3, I_4.

• Let I_1 consist of those indexes i such that $n \leqslant d_i$ and $h_i = 0$. Let ℓ^{t_i} be the order of the root of unity $\alpha_i / b_i^{\ell^{d_i - n}}$.
• Let I_2 consist of those indexes i such that $n > d_i$ and $h_i = 0$. Let β_i be any ℓ^{n-d_i}-th root of b_i and let ℓ^{t_i} be the order of the root of unity α_i / β_i.
• Let I_3 consist of those indexes i such that $n \leqslant d_i$ and $h_i > 0$.
• Let I_4 consist of those indexes i such that $n > d_i$ and $h_i > 0$.
Then we have

$$[K(\alpha_i : i \in I) : K] = [K_{\ell^x} : K]\ell^y$$

where

$$x = \max\left(0, \max_{I_1}(t_i), \max_{I_2}(t_i + d_i - n), \max_{I_3}(h_i + n), \max_{I_4}(h_i + d_i)\right)$$

and

$$y = \sum_{i \in I_2 \cup I_4} n - d_i\,.$$

Proof. If suffices to consider Theorem 1 and its proof. One first shows that K_{ℓ^x} is contained in $K(\alpha_i : i \in I)$. The only point which requires some attention with respect to the case of rank 1 is the following: since $b_1, \dots, b_r$ are strongly independent, then the degree over K_{ℓ^∞} of $K_{\ell^\infty}(\beta_i : i \in I_2 \cup I_4)$, where β_i is any ℓ^{n-d_i}-th root of b_i, equals ℓ^y by Lemma 8. It follows that the same holds for the analogous degree over K_{ℓ^x}. □

The following result covers the case $\ell = 2$ and $K \neq K_4$:

Theorem 11. *Let $\ell = 2$ and $K \neq K_4$, and let $s \geqslant 2$ be the greatest integer such that $K_4 = K_{2^s}$. Let $I = \{1, \dots, r\}$. Let $a_1, \dots, a_r$ be elements of $K^\times$ such that for every $i \in I$ we have*

$$a_i = (-1)^{h_i} b_i^{\ell^{d_i}}$$

where $d_i \geqslant 0$, $h_i \in \{0, 1\}$ and the elements $b_1, \dots, b_r \in K^\times$ are strongly independent. Let α_i be a 2^n-th root of a_i for some $n > 0$.

(1) Suppose that no product of the b_i's is as in the special case of Lemma 3, or that (without loss of generality) b_1 is as such but $n \leqslant d_1$. We partition the index set I into four subsets I_1, I_2, I_3, I_4.
• Let I_1 consist of those indexes i such that $n \leqslant d_i$ and $h_i = 0$. Let 2^{t_i} be the order of $\alpha_i / b_i^{2^{d_i - n}}$.
• Let I_2 consist of those indexes i such that $n > d_i$ and $h_i = 0$. Let β_i be any 2^{n-d_i}-th root of b_i and let 2^{t_i} be the order of α_i / β_i.
• Let I_3 consist of those indexes i such that $n \leqslant d_i$ and $h_i = 1$.
• Let I_4 consist of those indexes i such that $n > d_i$ and $h_i = 1$.
Then we have

$$[K(\alpha_i : i \in I) : K] = [K_{2^x} : K] 2^y$$

where

$$x = \max\left(0, \max_{I_1}(t_i), \max_{I_2}(t_i + d_i - n), \max_{I_3}(n+1), \max_{I_4}(d_i + 1)\right)$$

and

$$y = \sum_{i \in I_2 \cup I_4} n - d_i \,.$$

(2) Suppose (without loss of generality) that b_1 is as in the special case of Lemma 3, and that $n > d_1$. Let β_1 be any 2^{n-d_1}-th root of b_1, and write $\xi = \alpha_1 / \beta_1$. Let t be the order of ξ. We partition the index set $I \setminus \{1\}$ into four subsets I_1, I_2, I_3, I_4 as above. Then we have

$$[K(\alpha_i : i \in I) : K] = [K_{2^x} : K] 2^y$$

where the notations are as follows.
• If $h_1 = 0$, then

$$x = \max\left(0, \max_{I_1}(t_i), \max_{I_2}(t_i + d_i - n), \max_{I_3}(n+1), \max_{I_4}(d_i + 1)\right)$$

and

$$y = \Big(\sum_{i \in \{1\} \cup I_2 \cup I_4} n - d_i \Big) - 1 + \epsilon$$

$$\epsilon = \begin{cases} 1 & \text{if } t+d_1-n \leqslant 1 \text{ and } x \leqslant s \\ 0 & \text{if } t+d_1-n \leqslant 1 \text{ and } x \geqslant s+1 \\ 2 & \text{if } 1 < t+d_1-n < s \text{ and } x \leqslant 1 \\ 1 & \text{if } 1 < t+d_1-n < s \text{ and } 2 \leqslant x \leqslant s \\ 0 & \text{if } 1 < t+d_1-n < s \text{ and } x \geqslant s+1 \\ 1 & \text{if } t+d_1-n = s \text{ and } x \leqslant 1 \\ 0 & \text{if } t+d_1-n = s \text{ and } x \geqslant 2 \\ t+d_1-n+2-s & \text{if } t+d_1-n > s \text{ and } x \leqslant 1 \\ t+d_1-n+1-s & \text{if } t+d_1-n > s \text{ and } 2 \leqslant x \leqslant s \\ \max(t+d_1-n+1-x,0) & \text{if } t+d_1-n > s \text{ and } x \geqslant s+1 \end{cases}$$

• *If* $h_1 = 1$*, then*

$$x = \max\left(d_1+1, \max_{I_1}(t_i), \max_{I_2}(t_i+d_i-n), \max_{I_3}(n+1), \max_{I_4}(d_i+1)\right)$$

and

$$y = \Big(\sum_{i\in\{1\}\cup I_2\cup I_4} n-d_i\Big) - 1 + \epsilon$$

where $\epsilon \in \{0,1\}$ *and* ϵ *equals* 0 *if and only if* $x \geqslant \max(d_1+2, s+1)$ *or* $d_1 = s-1$.

Proof. For the first part, it suffices to consider Theorem 2 and its proof. One first shows that K_{2^x} is contained in $K(\alpha_i : i \in I)$. The only point which requires some attention with respect to the case of rank 1 is the following: since $b_1, \ldots, b_r$ are strongly independent, then the degree over K_{2^∞} of $K_{2^\infty}(\beta_i : i \in I_2 \cup I_4)$, where β_i is any 2^{n-d_i}-th root of b_i, equals 2^y by Lemma 8.

For the second part we have to take care of the fact that the extension generated by α_1 behaves differently.

If $h_1 = 0$, notice that $K(\alpha_2, \ldots, \alpha_r) \cap K_{2^\infty}$ is K_{2^x}. Then we consider $K(\alpha_1)$ by investigating the proof of Theorem 2. Notice that $K(\sqrt{b_1})$ is contained in K_{2^x} if $x \geqslant s+1$ and K_4 is contained in K_{2^x} if $x \geqslant 2$. The degree of $K_{2^x}((\beta_1\xi)^{2^{n-d_1-1}})$ over K_{2^x} is 2^ϵ, while the degree of $K(\alpha_1, \ldots, \alpha_r)$ over $K_{2^x}((\beta_1\xi)^{2^{n-d_1-1}})$ is 2 raised to the power $\big(\sum_{i\in\{1\}\cup I_2\cup I_4} n-d_i\big) - 1$ by Lemma 8 because the elements $\beta_1^{2^{n-d_1-1}}$ and b_i for $i \in I_2 \cup I_4$ are strongly independent over K_{2^∞}, so the same holds for $\alpha_1^{2^{n-d_1-1}} = (\beta_1\xi)^{2^{n-d_1-1}}$ and $\alpha_i^{2^{n-d_i}}$ for $i \in I_2 \cup I_4$.

If $h_1 = 1$, notice that $K(\beta_1)$ contains $K_{2^{d_1+1}}$. Then let $K' = K_{2^{d_1+1}}(\beta_2, \ldots, \beta_r) \cap K_{2^\infty}$. If K_4 is contained in K', then the extension $K'(\beta_1^{2^{n_1-d_1-1}})$ equals $K'_{2^{s+1}}$ by Lemma 3. Else $\beta_1^{2^{n_1-d_1-1}}$ is just an element in K_{2^∞} which generates a quadratic extension of K' which does not change the greatest X such that $K_{2^X} \subseteq K(\alpha_i : i \in I)$. Finally the degree of $K(\alpha_i : i \in I)$ over $K_{2^X}((\beta_1)^{2^{n_1-d_1-1}})$ equals 2^y with $y = (\sum_{i\in\{1\}\cup I_2\cup I_4} n-d_i) - 1$ by Lemma 8. □

Example 12. Let $K = \mathbb{Q}(\zeta_3)$, where ζ_3 is a third root of unity, and let $\ell = 3$. Consider third roots α_1 and α_2 of the elements $a_1 = 5$ and $a_2 = 8\zeta_3$. The field $K(\alpha_1, \alpha_2)$ has degree 9 over K because $K(\alpha_1)$ and $K(\alpha_2)$ have each degree 3 over K and are linearly disjoint extensions. With the notation of Theorem 10, we have $d_1 = h_1 = 0$ and $d_2 = h_2 = 1$. So the sets I_1 and

I_4 are empty. We then have $x = \max(t_1 - 1, 2) = 2$. Indeed, the field $K(\alpha_2)$ contains $\mathbb{Q}_9$. We also have $y = 1$, thus the degree of $K(\alpha_1, \alpha_2)$ over $\mathbb{Q}_9$ equals 3 and hence the degree over K equals 9.

Example 13. Let $K = \mathbb{Q}$ and $\ell = 2$, and consider fourth roots α_1 and α_2 of the elements $a_1 = 5$ and $a_2 = -9$. Then, with the notation of Theorem 11, we have $d_1 = h_1 = 0$ and $d_2 = h_2 = 1$. So we get $I_1 = I_3 = \emptyset$ and $x = \max(t_1 - 2, 2) = 2$ and $y = 3$. So the field $\mathbb{Q}(\alpha_1, \alpha_2)$ contains $\mathbb{Q}_4$ and it has degree 8 over this field, making a total of degree 16 over $\mathbb{Q}$. This makes sense because $\mathbb{Q}(\alpha_1)$ and $\mathbb{Q}(\alpha_2)$ have each degree 4 over $\mathbb{Q}$ and they are linearly disjoint. If we now replace a_1 by -25 we similarly get that $\mathbb{Q}(\alpha_1, \alpha_2)$ contains $\mathbb{Q}_4$, but now the degree over this field is 4. So the total degree over $\mathbb{Q}$ is 8. Indeed, the fields $\mathbb{Q}(\alpha_1)$ and $\mathbb{Q}(\alpha_2)$ have each degree 4 over $\mathbb{Q}$ but they are not linearly disjoint, their intersection being $\mathbb{Q}_4$.

Example 14. Let $K = \mathbb{Q}$ and $\ell = 2$, and consider the eighth roots α_1 and α_2 of the elements $a_1 = 4$ and $a_2 = 81$. Then, with the notation of Theorem 11, we have $d_1 = 1$, $h_1 = 0$ (and the element 2 is as in the special case of Lemma 3), and $d_2 = 2$, $h_2 = 0$. We have $I_1 = I_3 = I_4 = \emptyset$ and $I_2 = \{2\}$, so that $x = \max(0, t_2 - 1)$, where 2^{t_2} is the order of $\alpha_2/\sqrt{3}$. Let 2^t be the order of $\alpha_1/\sqrt{2}$. We then have $\epsilon = 1$ because $t + d_1 - n \leqslant 1$ and $x \leqslant s$. If $x \leqslant 1$, then $[K_{2^x} : K] = 1$, while if $x = 2$, then $[K_{2^x} : K] = 2$. We have $y = 3$, so the degree of $\mathbb{Q}(\alpha_1, \alpha_2)$ over $\mathbb{Q}$ is either 8 or 16. Indeed, $\mathbb{Q}(\alpha_2)$ can be either $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}_4(\sqrt{3})$ while $\mathbb{Q}(\alpha_1)$ is a quadratic extension of $\mathbb{Q}(\sqrt{\pm 2})$ which does not contain $\mathbb{Q}_4$.

Example 15. Let $K = \mathbb{Q}$ and $\ell = 2$, and consider the eighth roots α_1 and α_2 of the elements $a_1 = -4$ and $a_2 = 81$. Then, with the notation of Theorem 11, we have $d_1 = h_1 = 1$ (and the element 2 is as in the special case of Lemma 3), and $d_2 = 2$, $h_2 = 0$. We have $I_1 = I_3 = I_4 = \emptyset$ and $I_2 = \{2\}$, so that $x = \max(2, t_2 - 1) = 2$, where 2^{t_2} is the order of $\alpha_2/\sqrt{3}$. We have $d_1 = s - 1$ and hence $\epsilon = 0$. So the field $\mathbb{Q}(\alpha_1, \alpha_2)$ contains $\mathbb{Q}_4$ and its degree over $\mathbb{Q}_4$ is 4 by Theorem 11. Indeed, $\mathbb{Q}(\alpha_1)$ is $\mathbb{Q}_8$ and hence its degree over $\mathbb{Q}$ is 4. Moreover, the field extension $\mathbb{Q}_4(\alpha_2)/\mathbb{Q}_4$ is generated by $\zeta\sqrt{3}$ for some root of unity ζ of order dividing 8, and hence it is quadratic over $\mathbb{Q}(\alpha_1)$. So we have indeed found that the degree of $\mathbb{Q}(\alpha_1, \alpha_2)$ over $\mathbb{Q}$ is 8.

Acknowledgements. The author would like to thank Pietro Sgobba for reading the manuscript and making useful comments.

REFERENCES

[1] DEBRY, C. - PERUCCA, A., *Reductions of algebraic integers*, J. Number Theory **167** (2016), 259–283.
[2] PERUCCA, A., *The order of the reductions of an algebraic integer*, J. Number Theory, **148** (2015), 121–136.
[3] 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.

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

Email address: antonella.perucca@uni.lu