ADDENDUM TO: REDUCTIONS OF ALGEBRAIC INTEGERS

ANTONELLA PERUCCA, PIETRO SGOBBA, SEBASTIANO TRONTO

ABSTRACT. Let K be a number field, and let G be a finitely generated and torsion-free subgroup of $K^\times$. We consider Kummer extensions of G of the form $K(\zeta_{2^m}, \sqrt[2^n]{G})/K(\zeta_{2^m})$, where $n \leqslant m$. In the paper *Reductions of algebraic integers* (J. Number Theory, 2016) by Debry and Perucca, the degrees of those extensions have been evaluated in terms of divisibility parameters over $K(\zeta_4)$. We prove how properties of G over K explicitly determine the divisibility parameters over $K(\zeta_4)$. This result yields a clear computational advantage, since no field extension is required.

Aim. Let K be a number field not containing ζ_4, and let G be a finitely generated and (without loss of generality) torsion-free subgroup of $K^\times$. The aim of this note is studying the degree of Kummer extensions of G of the form

$$K(\zeta_{2^m}, \sqrt[2^n]{G})/K(\zeta_{2^m}) \qquad \text{where } n \leqslant m\,. \tag{1}$$

In [1, Theorem 18 and Lemma 19] by Debry and Perucca, such Kummer degree has been evaluated in terms of divisibility parameters for G over $K(\zeta_4)$. We show in Theorems 1 and 2 that those divisibility parameters are completely determined by properties over K, so that applying [1, Theorem 18 and Lemma 19] does not require any computation over $K(\zeta_4)$.

Notation and definitions. Let K be a number field. We denote by ζ_{2^n} a root of unity of order 2^n, and write $K_{2^n} := K(\zeta_{2^n})$ for the corresponding cyclotomic extension. We write K_{2^∞} for the compositum of all extensions K_{2^n} with $n \geqslant 1$.

An element of $K^\times$ is called *strongly* 2*-indivisible* if it is not a root of unity times a square in $K^\times$. Finitely many distinct elements of $K^\times$ are called *strongly* 2*-independent* if the product of any non-empty subset of them is strongly 2-indivisible.

We consider a finitely generated and torsion-free subgroup G of $K^\times$ and a basis $g_1, \dots, g_r$ of G. We can write

$$g_i = \zeta_i \cdot b_i^{2^{d_i}} \tag{2}$$

for some strongly 2-indivisible elements $b_1, \dots, b_r$ of $K^\times$, for some non-negative integers d_i and for some roots of unity ζ_i in K of order 2^{h_i}. We refer to b_i as the *strongly* 2*-indivisible part* of g_i. We call $g_1, \dots, g_r$ a 2*-good basis* of G if the b_i's are strongly 2-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 the h-parameters for the* 2*-divisibility* of G in K, respectively. Recall from [1, Theorem 14] that a 2-good basis of G always exists.

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

Two special elements. *From now on we suppose that K is a number field with $\zeta_4 \notin K$, and such that*

$$K \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}(\zeta_{2^s} + \zeta_{2^s}^{-1}) \tag{3}$$

holds for some $s \geqslant 2$. (Notice that otherwise the divisibility parameters do not change from K to K_4, because strongly 2-indivisible elements over K are strongly 2-indivisible also over K_4 by [2, Lemma 12].) In this case the two elements

$$\pm f := \pm(\zeta_{2^s} + \zeta_{2^s}^{-1} + 2) \tag{4}$$

are strongly 2-indivisible over K but not strongly 2-indivisible over K_4. Indeed, by [2, Lemma 9] we know that $K(\sqrt{\pm f})$ is a quadratic extension of K because its intersection with $\mathbb{Q}_{2^\infty}$ is a quadratic extension of $K \cap \mathbb{Q}_{2^\infty}$. So $\pm f$ is not a square in K, and since $\zeta_4 \notin K$ we have that $\pm f$ is strongly 2-indivisible in K. By [2, Lemma 9] we know that $K_4 \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}_{2^s}$ because this intersection is a quadratic extension of $K \cap \mathbb{Q}_{2^\infty}$ containing ζ_4. Notice that we can write

$$f = \zeta_{2^s}^{-1}(1 + \zeta_{2^s})^2\,, \tag{5}$$

so $\pm f$ is not strongly 2-indivisible in K_4. By [2, Lemma 12], up to squares in $K^\times$, only the elements $\pm f$ are strongly 2-indivisible over K but not strongly 2-indivisible over K_4.

Main results. We prove when and how the divisibility parameters change from K to K_4:

Theorem 1. *Let G be a finitely generated and torsion-free subgroup of $K^\times$. The following conditions are equivalent (where f is as in* (4)*):*

1. *the d-parameters for the 2-divisibility of G change from K to K_4;*
2. *the group G contains an element of the form $\pm(fa^2)^{2^d}$ for some $a \in K^\times$ and $d \geqslant 0$;*
3. *there is a 2-good basis of G that contains an element of the form $\pm(fa^2)^{2^d}$ for some $a \in K^\times$ and $d \geqslant 0$.*

Theorem 2. *Suppose that there is a 2-good basis $\{g_i\}$ of G over K such that*

$$g_1 = \pm(fa^2)^{2^{d_1}} \tag{6}$$

for some $a \in K^\times$ and some $d_1 \geqslant 0$. Then $\{g_i\}$ is a 2-good basis of G over K_4. The d-parameters over K_4 are those over K except for the parameter d_1 which increases by 1. The h-parameters are unchanged, except for the parameter h_1, which over K_4 becomes

$$h_1' = \begin{cases} h_1 & \text{if } d_1 \geqslant s \\ 0 & \text{if } d_1 = s-1 \text{ and } h_1 = 1 \\ 1 & \text{if } d_1 = s-1 \text{ and } h_1 = 0 \\ s - d_1 & \text{if } d_1 \leqslant s-2\,. \end{cases}$$

Example 3. Let G be the subgroup of $\mathbb{Q}^\times$ given by $\langle 1350, 75\rangle$. We are in the situation of Theorem 2 with $f = 2$. Indeed, $1350/75 = 18$ is 2 times a square, thus the divisibility parameters of G change from $\mathbb{Q}$ to $\mathbb{Q}_4$. More precisely $\{18, 75\}$ is a 2-good basis of G with parameters given by $d_1 = d_2 = h_1 = h_2 = 0$ over $\mathbb{Q}$ and by $d_1 = 1, h_1 = 2, d_2 = h_2 = 0$ over $\mathbb{Q}_4$.

We can apply Theorem 18 and Lemma 19 from [1] for $m \geqslant 2$ and $m = 1$, respectively. We obtain:

$$\left[\mathbb{Q}_{2^m}(\sqrt[2^n]{G}) : \mathbb{Q}_{2^m}\right] = \begin{cases} 4 & \text{if } m = 1, 2 \text{ and } n = 1 \\ 16 & \text{if } m = n = 2 \\ 2^{2n-1} & \text{if } m \geqslant 3 \, . \end{cases}$$

The proof of Theorem 2.

Lemma 4. *Let $b_1, \dots, b_r$ be strongly 2-independent elements of $K^\times$. Then they are strongly 2-independent over K_4 if and only if no product of the form $\prod_{i \in J} b_i$, for some subset $J \subseteq \{1, \dots, r\}$, is equal to $\pm f a^2$ for some $a \in K^\times$.*

Proof. This is clear from the definition of strongly 2-independent because the only elements of $K^\times$ that are strongly 2-indivisible over K but not over K_4 are of the form $\pm f a^2$. □

Proof of Theorem 2. Notice that there is no generator g_i other than g_1 whose strongly 2-indivisible part b_i is f times a square in $K^\times$ (otherwise the b_i's would not be strongly 2-independent over K). In particular, each b_i for $i > 1$ is strongly 2-indivisible also over K_4. Set $B_1 = (1 + \zeta_{2^s})a$, and set $B_i = b_i$ for $i > 1$. We claim that the B_i's are strongly 2-independent over K_4.

Since we can use the B_i's as strongly 2-indivisible parts of the elements g_i over K_4, it follows from this claim that the g_i's form a 2-good basis over K_4. Only the d-parameter of g_1 changes (it increases by 1) from K to K_4, and in view of (5) and (6) it is easy to check that its h-parameter changes as given in the statement.

We are left to prove the claim. Suppose that the B_i's are not strongly 2-independent over K_4, and consider a non-empty set $J \subseteq \{1, \dots, r\}$ such that we can write

$$\zeta \cdot \alpha^2 = \prod_{i \in J} B_i$$

where ζ is a root of unity in K_4 and $\alpha \in K_4^\times$. This is impossible if $1 \notin J$ because $b_2, \dots, b_r$ are strongly 2-independent also over K_4 by Lemma 4. So by (5) we can write $\zeta' \cdot \alpha^4 = f \cdot b^2$ where ζ' is a root of unity in K_4 and $b \in K^\times$. This gives a contradiction because $f \cdot b^2$ cannot have a fourth root in K_{2^∞} (see for instance [2, Proof of Lemma 12]).

□

The proof of Theorem 1.

Proposition 5. *Let G be a finitely generated and torsion-free subgroup of $K^\times$ of rank r. The following conditions are equivalent (where f is as in (4)):*

1. *the group G contains an element of the form $\pm(fa^2)^{2^d}$ for some $a \in K^\times$ and $d \geqslant 0$;*
2. *there is a 2-good basis $\{g_i\}$ of G and some subset $J \subseteq \{1, \dots, r\}$ such that $\prod_{i \in J} b_i = \pm f a^2$ for some $a \in K^\times$;*
3. *for every 2-good basis $\{g_i\}$ of G there is some subset $J \subseteq \{1, \dots, r\}$ such that $\prod_{i \in J} b_i = \pm f a^2$ for some $a \in K^\times$;*
4. *the d-parameters for the 2-divisibility of G change from K to K_4.*

Proof. The implication (3) $\Rightarrow$ (2) is obvious, and to prove (2) $\Rightarrow$ (1) it suffices to raise $\pm fa^2$ to the power 2^d, where d is the maximum of the d-parameters of the g_i with $i \in J$. Now we prove (1) $\Rightarrow$ (3). Expressing the element in (1) in terms of the generators of a 2-good basis, we can write

$$(fa^2)^{2^d} = \pm \prod_i b_i^{z_i \cdot 2^{d_i}}$$

for some integers z_i. Since the b_i's are strongly 2-independent, we have that $2^d \mid 2^{d_i} z_i$ for all i. Hence there are some integers $y_i \in \{0, 1\}$ such that $\prod_i b_i^{y_i} = \pm f\alpha^2$ for some $\alpha \in K^\times$ (recall that $\zeta_4 \notin K$).

The equivalence (3) $\Leftrightarrow$ (4) is clear by Lemma 4 because the b_i's are not strongly 2-independent over K_4 if and only if the sum of the d-parameters increases from K to K_4. $\square$

Proposition 6. *Let G be a finitely generated and torsion-free subgroup of $K^\times$. Suppose that G contains an element of the form $\pm(fa^2)^{2^d}$ for some $a \in K^\times$, and for some $d \geqslant 0$. Then G has a 2-good basis containing an element of the same form.*

Proof. By Proposition 5 we know that there is a 2-good basis $g_1, \dots, g_r$ of G such that the strongly 2-indivisible parts b_i satisfy $\prod_{i \in J} b_i = \pm fa^2$ for some $a \in K^\times$ and for some nonempty subset $J \subseteq \{1, \dots, r\}$. Let d_j be the largest divisibility parameter of the g_i's for $i \in J$. Then we have

$$(fa^2)^{2^{d_j}} = \pm g_j \cdot \prod_{i \in J, i \neq j} g_i^{2^{d_j - d_i}}.$$

In particular, we may replace the generator g_j by $\pm(fa^2)^{2^{d_j}}$. The d-parameter of this generator does not change, so the obtained basis is again a 2-good basis. $\square$

Notice that the above proof is constructive in that it provides an explicit way of constructing a 2-good basis of G containing an element of the form $\pm(fa^2)^{2^d}$ where f is as in (4), $a \in K^\times$, and $d \geqslant 0$.

Proof of Theorem 1. The equivalence (1) $\Leftrightarrow$ (2) is proven in Proposition 5 and the equivalence (2) $\Leftrightarrow$ (3) in Proposition 6. $\square$

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.

Mathematics Research Unit, University of Luxembourg, 6 av. de la Fonte, 4364 Esch-sur-Alzette, Luxembourg

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