KUMMER THEORY FOR MULTIQUADRATIC OR QUARTIC CYCLIC NUMBER FIELDS

FLAVIO PERISSINOTTO AND ANTONELLA PERUCCA

ABSTRACT. Let K be a number field which is multiquadratic or quartic cyclic. We prove several results about the Kummer extensions of K, namely concerning the intersection between the Kummer extensions and the cyclotomic extensions of K. For G a finitely generated subgroup of $K^\times$, we consider the cyclotomic-Kummer extensions $K(\zeta_{nt},\, \sqrt[n]{G})/K(\zeta_{nt})$ for all positive integers n and t, and we describe an explicit finite procedure to compute at once the degree of all these extensions.

1. INTRODUCTION

Kummer theory is a topic of significant interest in number theory, and in this paper we investigate it for a multiquadratic or quartic cyclic number field K (to ease notation we always consider quadratic number fields to be multiquadratic). Our main result concerns the degree of cyclotomic-Kummer extensions of K:

Theorem 1. *Let G be a finitely generated subgroup of $K^\times$, and let ζ_M denote a root of unity of order M. There is an explicit finite procedure to compute at once the degree*

$$\Big[K(\zeta_M,\, \sqrt[N]{G}) : K(\zeta_M)\Big] \tag{1}$$

for all positive integers N, M such that N divides M.

To achieve this theorem we fully describe the procedure mentioned in the statement, and we prove various results that classify the intersection between the Kummer extensions and the cyclotomic extensions of K. Since our results can be applied to study further number theoretical questions, we give here an overview.

1.1. **Kummer extensions and cyclotomic extensions.**

We investigate the cyclic Kummer extensions of K that are abelian over $\mathbb{Q}$ or, equivalently, that are contained in a cyclotomic extension of K (for K multiquadratic, see Sections 5–6; for K quartic cyclic, see Section 7).

In Theorem 8 we classify the intersection of $K(\zeta_{\ell^n},\, \sqrt[\ell^n]{\alpha})$ with the cyclotomic extensions of K where $\alpha \in K^\times$ and ℓ^n is any prime power.

1991 *Mathematics Subject Classification.* Primary: 11R20; Secondary: 11R18, 11Y40.

Key words and phrases. Kummer theory, Kummer extension, cyclotomic field, multiquadratic number field, quartic cyclic number field, cubic number field.

Lemma 9 and Lemma 21 (for multiquadratic and quartic cyclic number fields respectively) allow us to determine those positive integers x such that $K(\zeta_x)$ contains $\sqrt{\pm 2}$ or some given root of unity with order a power of 2.

For certain multiquadratic number fields, Lemmas 12 and 14 (see also Lemma 37 for $\mathbb{Q}(\zeta_5)$) allow us to classify all cyclic Kummer extensions of degree 4 and 8 which are contained in a cyclotomic extension of K. See also Lemma 10 to determine whether a Kummer extension is Galois over $\mathbb{Q}$.

For multiquadratic number fields, we investigate in Theorem 15 the quadratic extensions of K, more precisely which positive integers x are such that $K(\zeta_x)$ contains these extensions. In Theorems 18 and 19 we deal with the same problem for the cyclic extensions of K of degree 4 (if $\zeta_4 \in K$) and of degree 8 (if $\zeta_8 \in K$).

For quartic cyclic number fields we may check whether a quadratic extension is abelian over $\mathbb{Q}$ thanks to Lemma 22. Then in Theorems 23 and 25 we determine those positive integers x such that $K(\zeta_x)$ contains such an extension. See also Lemma 26.

Finally, Propositions 16, 17, 20 (for multiquadratic number fields) and Propositions 24, 27 (for quartic cyclic number fields) allow us to compute the positive integers x for which $K(\zeta_x)$ contains elements of the form $\zeta_{2^n}\sqrt{\beta}$, $\zeta_{2^n}\sqrt[4]{\beta}$, $\zeta_{2^n}\sqrt[8]{\beta}$ with $\beta \in K^\times$. See also Propositions 34, 36 which are related to the prime numbers 3 and 5 instead.

1.2. **The degree of Kummer extensions.** To prove Theorem 1, by [7, Section 8] we may replace G by one element $\alpha \in K^\times$ which is not a root of unity, and we consider the cyclotomic-Kummer extension

$$K(\zeta_M,\ \sqrt[N]{\alpha})/K(\zeta_M) \tag{2}$$

for all positive integers M, N such that N divides M. We clearly have

$$[K(\zeta_M,\ \sqrt[N]{\alpha}) : K(\zeta_M)] = \frac{N}{C(M,N)} \tag{3}$$

for some divisor $C(M,N)$ of N. The integer $C(M,N)$ measures the failure of maximality for the degree of the Kummer extension, and it divides a positive integer which depends only on K and α (see [11, Theorem 3.1] for a direct proof). If $N \geqslant 2$, then we consider the prime factorization $N = \prod_\ell \ell^n$, and we can write

$$C(M,N) = \prod_{\ell \mid N} C(\ell^n, \ell^n) \cdot B(M, \ell^n)\,, \tag{4}$$

where $C(\ell^n, \ell^n)$ is called the *ℓ-adic failure*, and where

$$B(M, \ell^n) := \left[K(\zeta_{\ell^n},\ \sqrt[\ell^n]{\alpha}) \cap K(\zeta_M) : K(\zeta_{\ell^n})\right]$$

is called the *ℓ-adelic failure*. By [7, Remark 17] we may compute at once all numbers $C(\ell^n, \ell^n)$ where ℓ is a prime number and $n \geqslant 1$, so we only need to provide formulas for the ℓ-adelic failure $B(M, \ell^n)$.

In [12, 7] we have described a finite procedure for the computation of the ℓ-adelic failure over $\mathbb{Q}$ and over quadratic number fields. Now we consider number fields which are either multiquadratic or quartic cyclic, and we provide an explicit finite procedure to compute the

ℓ-adelic failure $B(M,\ell^n)$ for all prime numbers ℓ, all $n \geqslant 1$, and for all $M \geqslant 1$ such that ℓ^n divides M, see Sections 8 and 9. By [11, Lemma 3.5] we have $B(M,\ell^n) = 1$ if $\zeta_\ell \notin K$. Thus for all considered number fields we investigate the 2-adelic failure; if K is multiquadratic and $\zeta_3 \in K$, then we also study the 3-adelic failure; for the quartic field $\mathbb{Q}(\zeta_5)$ we also study the 5-adelic failure.

Finally, we have the following:

Remark 2. *Theorem 1 also holds for all number fields that have no quadratic subfields (in particular, it holds for all number fields of odd degree).*

Indeed, the above discussion is still valid hence it suffices to study the 2-adelic failure, see Section 8.3.

2. Preliminaries

2.1. **Notation.**

Squarefree numbers, multiples, and divisors can be negative integers. The same holds for the *squarefree part* of a non-zero integer (i.e. the squarefree integer that multiplied by the given integer is a square) and for the *odd squarefree part* (i.e. the odd squarefree integer which multiplied by a power of 2 is the squarefree part). When we say that an integer is *minimal*, then we always mean that it is minimal w.r.t. divisibility.

If K is a number field, then we work with some algebraic closure $\bar{K}$ of K. If n is a positive integer, then μ_n denotes the group of n-th roots of unity and ζ_n denotes a fixed root of unity of order n (in general the choice does not matter, but when we write ζ_n and ζ_{nt} we sometimes choose $\zeta_n = \zeta_{nt}^t$). We also write $\mu_\infty = \cup_n \mu_n$ and, if ℓ is a prime number, $\mu_{\ell^\infty} = \cup_n \mu_{\ell^n}$. If the extension $K/\mathbb{Q}$ is abelian, then the *conductor* c_K of K is the minimal positive integer n such that $K \subseteq \mathbb{Q}(\zeta_n)$. We call *Kummer extension* of K any finite abelian extension of K of exponent n such that $\zeta_n \in K$ (in this paper Kummer extensions are usually cyclic).

If n is a non-zero integer and ℓ is a prime number, then we write $v_\ell(n)$ for the ℓ-adic valuation. If $\alpha \in K^\times$ and $\mathfrak{p}$ is a prime of K (by which we mean a non-zero prime ideal of the ring of integers of K), then $v_\mathfrak{p}(\alpha)$ is the $\mathfrak{p}$-adic valuation of the fractional ideal generated by α.

If ℓ is a prime number, then $\alpha \in K^\times$ is said to be *strongly ℓ-indivisible* if $\zeta\alpha \notin K^{\times\ell}$ for all $\zeta \in \mu_{\ell^\infty} \cap K$. Any $\alpha \in K^\times$ which is not a root of unity can be written as $\alpha = \zeta\beta^{\ell^d}$, where $\zeta \in K$ is a root of unity of order ℓ^h, $\beta \in K^\times$ is strongly ℓ-indivisible, and $d \geqslant 0$, see [10, Section 3]: we also require that $h = 0$ or $h > v_\ell(\sharp(\mu_{\ell^\infty} \cap K)) - d$, so that h and d exist unique.

2.2. **A result on quadratic extensions.**

Lemma 3. *Consider a number field Q and two finite abelian extensions K/Q and K'/Q which are linearly disjoint. A quadratic subextension of KK'/Q which is not contained in K or K' is of the form $Q(\sqrt{dd'})$ for some $d, d' \in Q$ such that $\sqrt{d} \in K \setminus Q$ and $\sqrt{d'} \in K' \setminus Q$.*

Proof. If L is a quadratic subextension of KK'/Q which is not contained in K or K', then it suffices to prove that it is contained in $L_K L_{K'}$, where $L_K \subseteq K$ and $L_{K'} \subseteq K'$ are quadratic over Q. Consider the quadratic character

$$\chi : \mathrm{Gal}(KK'/Q) \to \{\pm 1\}$$

corresponding to L: composing χ with the natural embedding

$$\mathrm{Gal}(K/Q) \hookrightarrow \mathrm{Gal}(K/Q) \times \mathrm{Gal}(K'/Q) \cong \mathrm{Gal}(KK'/Q)$$

we get a character $\chi_K : \mathrm{Gal}(K/Q) \to \{\pm 1\}$. Since $L \not\subseteq K$, the character χ_K is quadratic and corresponds to a quadratic subextension L_K/Q. We similarly define $\chi_{K'}$ and $L_{K'}$. The kernel of χ is contained in the product of the kernels of χ_K and $\chi_{K'}$, and we conclude because this product corresponds to $L_K L_{K'}$. Indeed, it is the largest subgroup of $\mathrm{Gal}(KK'/Q)$ whose restriction to $\mathrm{Gal}(K/Q)$ (respectively, $\mathrm{Gal}(K'/Q)$) is contained in the kernel of χ_K (respectively, $\chi_{K'}$). □

Remark 4. *Let F be the largest multiquadratic subextension of $\mathbb{Q}(\zeta_M)$, where $M \geqslant 3$. By Lemma 3, F is generated by the elements $\sqrt{\pm p}$, where $p \mid M$ is a prime such that $\pm p \equiv 1 \bmod 4$, and by ζ_4 (if $4 \mid M$), and by $\sqrt{2}$ (if $8 \mid M$). Moreover, if K is a multiquadratic number field, then KF is the largest multiquadratic subextension of $K(\zeta_M)$.*

Remark 5. *Let $K = \mathbb{Q}(\sqrt{d_1}, \dots \sqrt{d_r})$ for some squarefree integers $d_1, \dots, d_r$. For a non-empty subset I of $\{1, \dots, r\}$ we call d_I the squarefree part of $\prod_{i \in I} d_i$. By applying Lemma 3 the squarefree integers in $K^{\times 2}$ are the integers d_I.*

2.3. **Quartic cyclic number fields.** A quartic cyclic number field (i.e. an abelian extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}/4\mathbb{Z}$) is either a totally real or a CM field, and the quadratic subextension is totally real: for a CM quartic field embedded in $\mathbb{C}$, the quadratic subextension is the field fixed by the complex conjugation. The roots of unity contained in a quartic cyclic number field are μ_{10} for $\mathbb{Q}(\zeta_5)$, and μ_2 otherwise. In particular, for $\mathbb{Q}(\zeta_5)$ we have to study only the 2-adelic failure and the 5-adelic failure, and for the other quartic cyclic number fields only the 2-adelic failure.

Remark 6 ([4, Theorem 1 and the following lines, Theorem 3])**.** *Let D be a squarefree positive integer. A quartic cyclic number field containing $\sqrt{D}$ is of the form*

$$\mathbb{Q}\Big(\sqrt{A(D + B\sqrt{D})}\Big) = \mathbb{Q}\Big(\sqrt{A(D - B\sqrt{D})}\Big)$$

where A is an odd squarefree integer coprime to D and B is a positive integer such that $D - B^2$ is a square (the integers A and B exist unique). In particular, D and B cannot be both even, and (by the Sum of two squares theorem) D is not divisible by prime numbers congruent to 3 modulo 4. The conductor of the quartic cyclic number field is

$$\begin{cases} 8\,|A|\,D & \text{if } 2 \nmid B \\ 4\,|A|\,D & \text{if } A + B \equiv 3 \bmod 4 \\ |A|\,D & \text{if } A + B \equiv 1 \bmod 4\,. \end{cases}$$

In particular, A is the product of the odd prime numbers coprime to D that ramify in the quartic cyclic number field.

Let C be the positive integer such that $D = B^2 + C^2$, and notice that precisely one among the integers D, B, C is even. We define

$$\gamma = A(D + B\sqrt{D}) \qquad \text{and} \qquad \gamma' = A(D + C\sqrt{D})\,.$$

Remark 7. *Suppose that $2 \mid C$. Then we have $\mathbb{Q}(\sqrt{\gamma}, \sqrt{2}) = \mathbb{Q}(\sqrt{\gamma'}, \sqrt{2})$ because we can write*

$$2\frac{\gamma'}{\gamma} = \Big(\frac{(C-B)-\sqrt{D}}{B}\Big)^2 . \tag{5}$$

Moreover, the conductor of $\mathbb{Q}(\sqrt{\gamma})$ is $8\,|A|\,D$, so we have $\mathbb{Q}(\zeta_{|A|D}, \sqrt{\gamma}) = \mathbb{Q}(\zeta_{|A|D}, \sqrt{\pm 2})$ and hence $\sqrt{\pm\gamma'} \in \mathbb{Q}(\zeta_{|A|D})$ for one choice of the sign.

3. Intersection between cyclotomic extensions and Kummer extensions

Theorem 8. *Let K be a number field, and let ℓ be a prime number. We assume that $t \in \{1,2,3\}$, where $t = v_\ell(\sharp(\mu_{\ell^\infty} \cap K))$. Let $\alpha \in K^\times \setminus \mu_\infty$, and write $\alpha = \zeta_{\ell^h}\beta^{\ell^d}$, where $\beta \in K^\times$ is strongly ℓ-indivisible, $d \geqslant 0$, and $h = 0$ or $t - d < h \leqslant t$. For $n \geqslant 1$ we describe the field*

$$K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha}) \cap K(\mu_\infty) .$$

(1) If $1 \leqslant n \leqslant d$, then it is $K(\zeta_{\ell^{n+h}})$.

(2) If $\sqrt[\ell]{\beta} \notin K(\mu_\infty)$, then it is

$$\begin{cases} K(\zeta_{\ell^{n+2}}) & \text{if } n = d+1,\ h = 3 \\ K(\zeta_{\ell^{n+1}}) & \text{if } n = d+1,\ h = 2 \text{ or } n = d+2,\ h = 3 \\ K(\zeta_{\ell^n}) & \text{if } n \geqslant d+h . \end{cases}$$

(3) If $\sqrt[\ell]{\beta} \in K(\mu_\infty)$ and $\sqrt[\ell^2]{\beta} \notin K(\mu_\infty)$, then it is

$$\begin{cases} K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell]{\beta}) & \text{if } n = d+1 \\ K(\zeta_{\ell^{n+2}}\sqrt[\ell]{\beta}) & \text{if } n = d+2,\ h = 3 \\ K(\zeta_{\ell^{n+1}}\sqrt[\ell]{\beta}) & \text{if } n = d+2,\ h = 2 \text{ or } n = d+3,\ h = 3 \\ K(\zeta_{\ell^n}, \sqrt[\ell]{\beta}) & \text{if } n \geqslant d+1+h . \end{cases}$$

(4) If $\sqrt[\ell^2]{\beta} \in K(\mu_\infty)$ and $\sqrt[\ell^3]{\beta} \notin K(\mu_\infty)$ (which implies $t \in \{2,3\}$), then it is

$$\begin{cases} K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell]{\beta}) & \text{if } n = d+1 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell^2]{\beta}) & \text{if } n = d+2 \\ K(\zeta_{\ell^{n+2}}\sqrt[\ell^2]{\beta}) & \text{if } n = d+3,\ h = 3 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+1}}\sqrt[\ell^2]{\beta}) & \text{if } n = d+3,\ h = 2 \text{ or } n = d+4,\ h = 3 \\ K(\zeta_{\ell^n}, \sqrt[\ell^2]{\beta}) & \text{if } n \geqslant d+2+h . \end{cases}$$

(5) If $\sqrt[\ell^3]{\beta} \in K(\mu_\infty)$ (which implies $t = 3$), then it is

$$\begin{cases} K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell]{\beta}) & \text{if } n = d+1 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell^2]{\beta}) & \text{if } n = d+2 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+h}}\sqrt[\ell^3]{\beta}) & \text{if } n = d+3 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+2}}\sqrt[\ell^3]{\beta}) & \text{if } n = d+4,\ h = 3 \\ K(\zeta_{\ell^n}, \zeta_{\ell^{n+1}}\sqrt[\ell^3]{\beta}) & \text{if } n = d+4,\ h = 2 \text{ or } n = d+5,\ h = 3 \\ K(\zeta_{\ell^n}, \sqrt[\ell^3]{\beta}) & \text{if } n \geqslant d+3+h . \end{cases}$$

If $1 < r \leqslant h$, then by $\zeta_{\ell^{n+r}}$ we mean here any ℓ^{n+r-h}-th root of ζ_{ℓ^h}.

In the above formulas, the extension $K(\zeta_{\ell^n},\ \sqrt[\ell^n]{\alpha}) \cap K(\mu_\infty)/K(\zeta_{\ell^n})$ is generated by an element of the form $\zeta_{\ell^{n+x}}\sqrt[\ell]{\beta}$ only when $n+x \geqslant t+2$, of the form $\zeta_{\ell^{n+x}}\sqrt[\ell^2]{\beta}$ only when $n+x \geqslant t+3$ (and $t \in \{2,3\}$) and of the form $\zeta_{\ell^{n+x}}\sqrt[\ell^3]{\beta}$ only when $n+x \geqslant 7$ (and $t=3$).

Proof. For $t \in \{1,2\}$ we refer to [7, Theorem 12], so suppose that $t=3$. Moreover, the proof of that result also covers the case $h \leqslant 2$ and $\sqrt[\ell^3]{\beta} \notin K(\mu_\infty)$. If $n \leqslant d$, then we clearly have $K(\zeta_{\ell^n},\ \sqrt[\ell^n]{\alpha}) = K(\zeta_{\ell^{n+h}})$, so suppose that $n \geqslant d+1$. We set $L := K(\mu_\infty)$ and $K' := K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha}) \cap L$.

The case $h \leqslant 2$ and $\sqrt[\ell^3]{\beta} \in L$. If $h=0$, then a generator for $K'/K(\zeta_{\ell^n})$ is: $\sqrt[\ell]{\beta}$, if $n=d+1$; $\sqrt[\ell^2]{\beta}$, if $n=d+2$; $\sqrt[\ell^3]{\beta}$, if $n \geqslant d+3$.
If $h=1$, then we have $\sqrt[\ell^n]{\alpha} = \zeta_{\ell^{n+1}}\sqrt[\ell^x]{\beta}$ for $n=d+x$ and $x=1,2,3$, while for $n \geqslant d+4$ there is a power of $\sqrt[\ell^n]{\alpha}$ of the form $\sqrt[\ell^3]{\beta}\xi$ for some $\xi \in \mu_{\ell^n}$ which generates $K'/K(\zeta_{\ell^n})$.
If $h=2$, then $\sqrt[\ell^n]{\alpha} = \zeta_{\ell^{n+2}}\sqrt[\ell^{n-d}]{\beta}$ lies in L for $n \leqslant d+3$, its ℓ-th power lies in L for $n \leqslant d+4$, and some higher power of the form $\sqrt[\ell^3]{\beta}\xi$ for some $\xi \in \mu_{\ell^n}$ lies in L for $n \geqslant d+5$.

The case $h=3$. If $n=d+1$, then $\sqrt[\ell^n]{\alpha} = \zeta_{\ell^{n+3}}\sqrt[\ell]{\beta}$ generates $K'/K(\zeta_{\ell^n})$ if $\sqrt[\ell]{\beta} \in L$, else we have $\sqrt[\ell^n]{\alpha} \notin L$ and $K' = K(\zeta_{\ell^{n+2}})$. If $n=d+2$, then we have $\sqrt[\ell^n]{\alpha} = \zeta_{\ell^{n+3}}\sqrt[\ell^2]{\beta}$, so $K'/K(\zeta_{\ell^n})$ is generated by: $\zeta_{\ell^{n+3}}\sqrt[\ell^2]{\beta}$, if $\sqrt[\ell^2]{\beta} \in L$; its ℓ-th power, if $\sqrt[\ell]{\beta} \in L$ and $\sqrt[\ell^2]{\beta} \notin L$; its ℓ^2-th power, if $\sqrt[\ell]{\beta} \notin L$. Now suppose that $n \geqslant d+3$.
If $\sqrt[\ell]{\beta} \notin L$, then we have $K' = K(\zeta_{\ell^n})$. If $\sqrt[\ell]{\beta} \in L$ and $\sqrt[\ell^2]{\beta} \notin L$: for $n=d+3$ the ℓ^2-th power of $\sqrt[\ell^n]{\alpha}$ is in L, and some higher power is in L if $n \geqslant d+4$.
If $\sqrt[\ell^2]{\beta} \in L$ and $\sqrt[\ell^3]{\beta} \notin L$: for $n=d+3$ the ℓ-th power of $\sqrt[\ell^n]{\alpha}$ is in L; for $n=d+4$ its ℓ^2-th power; for $n \geqslant d+5$ some higher power.
If $\sqrt[\ell^3]{\beta} \in L$, then we have: for $n=d+3$ the element $\sqrt[\ell^n]{\alpha}$ lies in L; for $n=d+4$ its ℓ-th power; for $n=d+5$ its ℓ^2-th power; for $n \geqslant d+6$ some higher power. □

4. CYCLOTOMIC EXTENSIONS OF MULTIQUADRATIC NUMBER FIELDS

Let K be a multiquadratic number field.

Lemma 9. *Let $K = \mathbb{Q}(\sqrt{d_1}, \dots \sqrt{d_r})$ for some squarefree integers $d_1, \dots, d_r$. For a non-empty subset I of $\{1, \dots, r\}$ we call d_I the squarefree part of $\prod_{i \in I} d_i$. If $x \geqslant 1$, then we characterize when some elements are in $K(\zeta_x)$:*

Element in $K(\zeta_x)$	*Equivalent condition*
ζ_{2^n} *($n \geqslant 4$)*	$2^n \mid x$
ζ_8	$\zeta_4, \sqrt{2} \in K(\zeta_x)$
ζ_4	$4 \mid x$, *or* $d_I \equiv 3 \bmod 4$ *and* $d_I \mid x$ *for some* I
$\sqrt{\pm 2}$	$8 \mid x$, *or* $4 \mid x$ *and* $2 \mid d_I$ *and* $d_I \mid 2x$ *for some* I, *or* $d_I \mid 2x$ *and* $d_I \equiv \pm 2 \bmod 8$ *for some* I .

Proof. The assertion for ζ_{2^n} follows from the fact that $16 \nmid c_K$, and the assertion for ζ_8 is clear. It is straight-forward to prove that all given conditions are sufficient. We now apply Remarks 4–5.

If $\zeta_4 \in K(\zeta_x)$ and $4 \nmid x$, then there is some squarefree $m \mid x$ such that $m \equiv 1 \bmod 4$ and $-md_I \in \mathbb{Q}^{\times 2}$ hence we have $d_I = -m$ for some I.

If $\sqrt{\pm 2} \in K(\zeta_x)$ and $8 \nmid x$, then there is some odd squarefree $m \mid x$ (such that $m \equiv 1 \bmod 4$, if $2 \nmid x$) such that $\pm 2md_I \in \mathbb{Q}^{\times 2}$ hence we have $d_I = \pm 2m$ for some I. □

The following result allows us in certain cases to conclude directly that a Kummer extension of K is not contained in any cyclotomic extension of K:

Lemma 10. *If $\alpha \in K^\times$ and $0 \leqslant s \leqslant v_2(\#(\mu_{2^\infty} \cap K))$, then the following properties are equivalent:*
- *The extension $K(\sqrt[2^s]{\alpha})/\mathbb{Q}$ is Galois.*
- *For every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have $K(\sqrt[2^s]{\alpha}) = K(\sqrt[2^s]{\sigma(\alpha)})$.*
- *For every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ there is some odd integer x such that $\alpha \cdot \sigma(\alpha)^x \in K^{\times 2^s}$.*

In the last two properties we could restrict to any set of generators for $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. Up to replacing α with a root which is in $K^\times$ and choosing a smaller s, we may suppose that $[K(\sqrt[2^s]{\alpha}) : K] = 2^s$. The second and third property are equivalent by Kummer theory. The number fields $K(\sqrt[2^s]{\alpha})$ and $K(\sqrt[2^s]{\sigma(\alpha)})$ have the same degree, so the equality means that $\tilde{\sigma}(\sqrt[2^s]{\alpha}) \in K(\sqrt[2^s]{\alpha})$, where $\tilde{\sigma} : K(\sqrt[2^s]{\alpha}) \to \bar{K}$ is any field homomorphism extending σ. This shows that the first two properties are equivalent. We are left to show that the second property holds for all $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ if it holds for a set of generators. We write τ as a product of generators, and we proceed by induction on the number of factors. The assertion is clear if there is only one factor, so let $\tau = \sigma\sigma'$, where σ is a generator and the induction hypothesis holds for σ'. We know that $K(\sqrt[2^s]{\alpha}) = K(\sqrt[2^s]{\sigma'(\alpha)})$, and we conclude because $\tilde{\sigma}(\sqrt[2^s]{\alpha})$ is in this field, and $\tilde{\sigma}(\sqrt[2^s]{\sigma'(\alpha)})$ is a 2^s-th root of $\tau(\alpha)$. □

Definition 11. Let p be a prime number such that $p \equiv 1 \bmod 4$. If $p \equiv 5 \bmod 8$, then let $\beta_p \in \mathbb{Q}(\zeta_4)$ be such that $\mathbb{Q}(\zeta_4, \sqrt[4]{\beta})$ is the quartic subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$; if $p \equiv 1 \bmod 8$, then let $\beta_p \in \mathbb{Q}(\zeta_4, \sqrt{p})$ be such that $\mathbb{Q}(\zeta_4, \sqrt{p}, \sqrt[4]{\beta})$ is the subextension of degree 8 of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$. To determine these elements one can apply the procedure presented in [6, Section 4].

Lemma 12. *Suppose that $\zeta_4 \in K$, and let N be a positive integer such that $\sqrt{p} \in K$ for every odd prime $p \mid N$. Any cyclic subextension of $K(\zeta_N)/K$ of degree 4 equals $K(\sqrt[4]{g})$ for some $g \in K^\times \setminus K^{\times 2}$ of the form*

$$g = \zeta_{2^e} \prod_{p \equiv 5 \bmod 8} \beta_p^{e_p} \prod_{q \equiv 1 \bmod 8} \beta_q^{e_q}$$

such that p, q are odd prime divisors of N and the integers $e \in \{0,1,2,3\}$, $e_p \in \{0,2\}$, and $e_q \in \{0,1,2\}$ satisfy the following conditions:

$e \neq 1$, *if* $\zeta_8 \in K$;
$e \neq 3$, *if* $\zeta_8 \notin K$ *or* $32 \nmid N$;
$e = 0$, *if* $8 \nmid N$ *or if* $\zeta_8 \in K$ *and* $16 \nmid N$;
$e = 3$ *or* $e_q = 1$ *for some* q.

Different choices for the exponents give rise to distinct extensions. If $x \geqslant 1$, then we have $\sqrt[4]{g} \in K(\zeta_x)$ if and only if we have $v_2(x) \geqslant e+2$ for $e \neq 0$ and $p \mid x$ for all primes $p \equiv 1 \bmod 4$ such that $e_p \neq 0$.

Proof. The given conditions on x are clearly sufficient to ensure $\sqrt[4]{g} \in K(\zeta_x)$. They are also necessary, as can be seen by adding the fourth roots of all but one of the elements ζ_{2^e} (if $e \neq 0$) and $\beta_p^{e_p}$ (if $e_p \neq 0$). This line of reasoning also shows that different choices for the exponents give rise to distinct extensions, and that $K(\sqrt[4]{g})/K$ has degree 4.

We have $\sqrt[4]{g} \in L$, where L is the field corresponding to the largest quotient of exponent 4 of $\mathrm{Gal}(K(\zeta_N)/K)$. We can factor $\mathrm{Gal}(L/K)$ as the product of the largest quotient of exponent 4 of $\mathrm{Gal}(K(\zeta_{2^{v_2(N)}})/K)$ and, for every odd prime $p \mid N$, the quotient of order 2 (respectively, 4) of $\mathrm{Gal}(K(\zeta_p)/K)$ if $p \equiv 5 \bmod 8$ (respectively, $p \equiv 1 \bmod 8$), calling L_2 and L_p the corresponding fields. Notice that the fourth roots of ζ_{2^e} (respectively, $\beta_p^{e_p}$) generate a cyclic subextension of L_2/K (respectively, L_p/K) of degree dividing 4, and of degree dividing 2 if $p \equiv 5 \mod 8$. By taking products of these roots, we get an extension of K of degree 4 unless all roots generate extensions of degree at most 2, so we may conclude with a counting argument as in the proof of [7, Theorem 11]. □

Definition 13. Let p be a prime number. If $p \equiv 5 \bmod 8$, then let $\eta_p \in \mathbb{Q}(\zeta_4)$ be such that $\mathbb{Q}(\zeta_4, \sqrt[4]{\eta_p})$ is the quartic subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$. If $p \equiv 9 \bmod 16$, then let $\eta_p \in \mathbb{Q}(\zeta_4, \sqrt{p})$ be such that $\mathbb{Q}(\zeta_4, \sqrt{p}, \sqrt[4]{\eta_p})$ is the subextension of degree 8 of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$ (alternatively, one could work with $\eta'_p \in \mathbb{Q}(\zeta_8)$ such that $\mathbb{Q}(\zeta_8, \sqrt[8]{\eta'_p})$ is the subextension of degree 8 of $\mathbb{Q}(\zeta_{8p})/\mathbb{Q}(\zeta_8)$). If $p \equiv 1 \bmod 16$, then let $\eta_p \in \mathbb{Q}(\zeta_8, \sqrt{p})$ be such that $\mathbb{Q}(\zeta_8, \sqrt{p}, \sqrt[8]{\eta_p})$ is the subextension of degree 16 of $\mathbb{Q}(\zeta_{8p})/\mathbb{Q}(\zeta_8)$. To determine these elements one can apply the procedure presented in [6, Section 4].

Lemma 14. *Suppose that $\zeta_8 \in K$, and let N be a positive integer such that $\sqrt{p} \in K$ for every odd prime $p \mid N$. Any cyclic subextension of $K(\zeta_N)/K$ of degree 8 equals $K(\sqrt[8]{g})$ for some $g \in K^\times \setminus K^{\times 2}$ of the form*

$$g = \zeta_{2^e} \prod_{p \equiv 5 \bmod 8} \eta_p^{e_p} \prod_{q \equiv 9 \bmod 16} \eta_q^{e_q} \prod_{r \equiv 1 \bmod 16} \eta_r^{e_r}$$

such that p, q, r are odd prime divisors of N and the integers $e \in \{0,1,2,3\}$, $e_p \in \{0,4\}$, $e_q \in \{0,2\}$, and $e_r \in \{0,1,2,4\}$ satisfy the following conditions:

$$\begin{aligned} &e = 0, \text{ if } 16 \nmid N;\\ &e \leqslant 1, \text{ if } 32 \nmid N;\\ &e \neq 3, \text{ if } 64 \nmid N;\\ &e = 3 \text{ or } e_r = 1 \text{ for some } r\,. \end{aligned}$$

Different choices for the exponents give rise to distinct extensions. If $x \geqslant 1$, then we have $\sqrt[8]{g} \in K(\zeta_x)$ if and only if we have $v_2(x) \geqslant e+3$ for $e \neq 0$ and $p \mid x$ for all primes $p \equiv 1 \bmod 4$ such that $e_p \neq 0$.

Proof. The proof is analogous to the one of Lemma 12 so we leave it as an exercise. □

5. Quadratic extensions of multiquadratic number fields

Let K be a multiquadratic number field, and write $K = \mathbb{Q}(\sqrt{d_1}, \dots, \sqrt{d_r})$ for some squarefree integers $d_1, \dots, d_r$ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r$. An extension of K of degree 2 is of the form $K(\sqrt{\alpha})$ for some $\alpha \in K^\times \setminus K^{\times 2}$, and we fix such an α. The extension $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian if and only if $K(\sqrt{\alpha}) \subseteq \mathbb{Q}(\mu_\infty)$, and in this case the Galois group $\mathrm{Gal}(K(\sqrt{\alpha})/\mathbb{Q})$ is isomorphic to either

$$(\mathbb{Z}/2\mathbb{Z})^{r+1} \qquad \text{or} \qquad (\mathbb{Z}/2\mathbb{Z})^{r-1} \times \mathbb{Z}/4\mathbb{Z}\,.$$

In the first case $K(\sqrt{\alpha})$ is multiquadratic and hence $K(\sqrt{\alpha}) = K(\sqrt{m})$ for some squarefree integer m (thus, $\alpha/m \in K^{\times 2}$). We can find m or conclude that no such m exists by checking finitely many possibilities because the odd prime divisors of m ramify in $K(\sqrt{\alpha})$.

In the second case we have $K(\sqrt{\alpha}) = K(\sqrt{\gamma})$ for some $\gamma \in K^\times$ such that $\mathbb{Q}(\sqrt{\gamma})$ is quartic cyclic (thus, $\alpha/\gamma \in K^{\times 2}$). We let $\gamma, \gamma', A, B, C, D$ be as in Section 2.3. We can find γ or conclude that no such γ exists by checking finitely many possibilities (since $\mathbb{Q}(\sqrt{D}) \subseteq K$, there are only finitely many possibilities for D and hence for B; the prime divisors of A ramify in $K(\sqrt{\alpha})$).

Notice that the odd primes ramifying in $K(\sqrt{\alpha})$ are those ramifying in K and those that lie below a prime of K ramifying in $K(\sqrt{\alpha})$ (these can be found with [7, Lemma 2]).

Theorem 15. *We keep the above notation, and we suppose that $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian. The minimal integers $x \geqslant 1$ such that $\sqrt{\alpha} \in K(\zeta_x)$ form a non-empty, finite, and computable set. For any $x \geqslant 1$ we have $\sqrt{\alpha} \in K(\zeta_x)$ if and only if one of the following holds:*

1. *We have $K(\sqrt{\alpha}) = K(\sqrt{m})$ and $\sqrt{m \prod_{j\in J} d_j} \in \mathbb{Q}(\zeta_x)$ for some $J \subseteq \{1, \dots, r\}$.*
2. *We have $K(\sqrt{\alpha}) = K(\sqrt{\gamma})$ and x is a multiple of*

$$\begin{cases} w8D & \text{for some } w \text{ such that } \sqrt{A} \in K(\zeta_{w8D}) \quad \text{if } 2 \mid D \\ wD & \text{for some } w \text{ such that } \sqrt{\pm A} \in K(\zeta_{wD}) \quad \text{if } 1 + B \equiv \pm 1 \bmod 4 \\ wD & \text{for some } w \text{ such that } \sqrt{\pm 2A} \in K(\zeta_{wD}) \quad \text{if } 1 + C \equiv \pm 1 \bmod 4\,. \end{cases}$$

We can take w minimal, so that it belongs to a finite computable set.

Proof. Case (1) is a consequence of Lemma 3 because we can focus on the maximal multiquadratic subextension of $\mathbb{Q}(\zeta_x)$ and because it is immediate to determine the conductor of each field $\mathbb{Q}(\sqrt{m \prod d_j})$. Now we deal with Case (2) (recall that precisely one among B, C, D is even). If $p \mid D$ is prime, then let C_p be the quartic cyclic subextension of $\mathbb{Q}(\zeta_p)$, or $\mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$ for $p = 2$; if $q \nmid D$ is an odd prime ramifying in $K(\sqrt{\alpha})$, then consider the quadratic subextension C'_q of $\mathbb{Q}(\zeta_q)$. So $K(\sqrt{\gamma})$ is contained in

$$L := \mathbb{Q}(\zeta_8) \prod_q C'_q \prod_p C_p\,.$$

We claim that $K(\sqrt{\gamma}) \not\subseteq L'$, where L' is obtained from L by replacing some C_p by a quadratic subextension. This implies that $D \mid x$, and that $16 \mid x$ if $2 \mid D$. In the three subcases of (2) the field $K(\zeta_x)$ contains $\sqrt{\gamma/A}$, $\sqrt{\pm\gamma/A}$, and $\sqrt{\pm\gamma'/A}$ respectively. So we are left to determine the minimal x such that $K(\zeta_x)$ contains $\sqrt{A}$, $\sqrt{\pm A}$ and $\sqrt{\pm 2A}$ respectively, and we conclude by Case (1).

To prove the claim, let $G := \operatorname{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^s \times (\mathbb{Z}/2\mathbb{Z})^t$ for some integers s, t. We may choose $g_1, \ldots, g_s$ which generate the cyclic factors of order 4 and are such that $g_1 g_i$ fixes $\sqrt{D}$. W.l.o.g. we have

$$G' := \operatorname{Gal}(L'/\mathbb{Q}) = G/ < g_1^2 > \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^{s-1} \times (\mathbb{Z}/2\mathbb{Z})^t \,.$$

If $\sqrt{\gamma} \in L'$, then there are subgroups $G'_2 < G'_1 < G'$ such that $G'/G'_2 \cong \mathbb{Z}/4\mathbb{Z}$ and $G'/G'_1 \cong \mathbb{Z}/2\mathbb{Z}$. This is impossible because we have $G'_1 = (\mathbb{Z}/4\mathbb{Z})^{s-1} \times (\mathbb{Z}/2\mathbb{Z})^t$ (as generators for $(\mathbb{Z}/4\mathbb{Z})^{s-1}$ we can take the class of $g_1 g_i$ for $i \neq 1$). □

Proposition 16. *If $\beta \in K^\times \setminus K^{\times 2}$ is such that $K(\sqrt{\beta})$ is multiquadratic, then the set S consisting of the squarefree integers b such that $K(\sqrt{b}) = K(\sqrt{\beta})$ is non-empty, finite, and computable. If $x \geqslant 1$, then we characterize when some elements are in $K(\zeta_x)$:*

Element in $K(\zeta_x)$	*Equivalent condition*
$\sqrt{\beta}$	$\sqrt{b} \in \mathbb{Q}(\zeta_x)$ *for some* $b \in S$
$\zeta_{2^e}\sqrt{\beta}$ *($e \geqslant 4$)*	$2^e \mid x$ *and* $b \mid x$ *for some* $b \in S$
$\zeta_8\sqrt{\beta}$	$\zeta_8 \in K(\zeta_x)$ *and* $b \mid x$ *for some odd* $b \in S$, *or* $\sqrt{2}, \sqrt{-2} \notin K$ *and* $\zeta_4 \in K(\zeta_x)$ *and* $b \mid 2x$ *for some even* $b \in S$.

Proof. There is a squarefree integer m such that $K(\sqrt{\beta}) = K(\sqrt{m})$, thus S consists of the squarefree part of the integers mz, where z is a subproduct of $d_1 \cdots d_r$. The assertion on $\sqrt{\beta}$ then follows from Theorem 15 (1). Consider $b \in S$. If $8 \mid x$, then the condition $b \mid x$ is equivalent to $\sqrt{b} \in \mathbb{Q}(\zeta_x)$, and in general it is a necessary condition. If $\sqrt{2}$ and ζ_4 are in $K(\zeta_x)$, or if $\zeta_4 \in K(\zeta_x)$ and b is odd, then $b \mid x$ is sufficient for $\sqrt{b} \in K(\zeta_x)$.

The given conditions for $\zeta_{2^e}\sqrt{\beta}$ and $\zeta_8\sqrt{\beta}$ are then sufficient (for the last one, we have $\sqrt{2b} \in K(\zeta_x)$ and we conclude because $\sqrt{2}/\zeta_8 \in \mathbb{Q}(\zeta_4)$). The given condition for $\zeta_{2^e}\sqrt{\beta}$ is necessary because we must have $2^e \mid x$ (if $v_2(y) < e$, then 2^e does not divide the conductor of $K(\sqrt{\beta}, \zeta_y)$).

Now suppose that $\zeta_8\sqrt{\beta} \in K(\zeta_x)$ and hence $\zeta_4 \in K(\zeta_x)$. If $\zeta_8 \in K(\zeta_x)$, then we conclude for b odd. If b is even and $\sqrt{2}$ or $\sqrt{-2}$ are in K, then we can reduce to the case b odd and $\zeta_8 \in K(\zeta_x)$. Now suppose that $\sqrt{2}, \sqrt{-2} \notin K$. Since for all $b \in S$ we have $\sqrt{b} \in K(\zeta_{\operatorname{lcm}(8,x)})$, by Lemma 3 we deduce that $\sqrt{b} \in \mathbb{Q}(\zeta_{\operatorname{lcm}(8,x)})$ for some $b \in S$ and hence $b \mid 2x$. If b is odd, then $\sqrt{\beta}$ and hence ζ_8 would be in $K(\zeta_x)$. □

Notice that in the following result the sets S, S_4 and S_8 exist and they are non-empty, finite, and computable by Lemma 9 and Theorem 15.

Proposition 17. *If $\beta \in K^\times \setminus K^{\times 2}$ is such that $K(\sqrt{\beta})$ is contains a quartic cyclic number field, then consider the finite non-empty computable set S of minimal positive integers y such that $\sqrt{\beta} \in K(\zeta_y)$, and similarly define S_4 by requiring $\zeta_4 \in K(\zeta_y)$ and S_8 by requiring $\zeta_8 \in K(\zeta_y)$. Let y' denote the odd part of y. For any fixed $e \geqslant 3$, the integers $x \geqslant 1$ such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ are those satisfying at least one of the following conditions:*

- *$2^e \mid x$ and $y \mid x$ for some $y \in S$;*

- *if* $e = 3$, $\operatorname{lcm}(s, y) \mid x$ *for some* $s \in S_8$ *and for some* $y \in S$;
- *if* $e = 4$, $v_2(y) = 4$ *(thus,* $\zeta_8 \in K$*),* $y' \mid x$ *for some* $y \in S$;
- *if* $e = 3$ *and* $\sqrt{2}, \sqrt{-2} \notin K$, $v_2(y) = 3$, $\operatorname{lcm}(s, y') \mid x$ *for some* $s \in S_4$ *and for some* $y \in S$.

Proof. By minimality, for every $y \in S$ we have: $v_2(y) \in \{0, 2, 3, 4\}$; $v_2(y) = 4$ implies $\zeta_8 \in K$; $v_2(y) = 3$ implies $\sqrt{2}, \sqrt{-2} \notin K$; $v_2(y) = 2$ implies $\zeta_4 \notin K$.

If $x \geqslant 1$ is such that $\zeta_{2^e}\sqrt{\beta}$ (and hence also $\zeta_{2^{e-1}}$) is in $K(\zeta_x)$, then we have $\sqrt{\beta} \in K(\zeta_{\operatorname{lcm}(2^e,x)})$ and in particular $y' \mid x$ for some $y \in S$. If $\zeta_{2^e} \in K(\zeta_x)$, then we have $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ if and only if $\sqrt{\beta} \in K(\zeta_x)$ (this leads to the first two conditions in the statement). If $\zeta_{2^e} \notin K(\zeta_x)$, then we can have $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ only if $\sqrt{\beta} \notin K(\zeta_x)$. Now suppose that $\zeta_{2^e}, \sqrt{\beta} \notin K(\zeta_x)$: we claim that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ holds if and only if $\zeta_{2^{e-1}} \in K(\zeta_x)$, $y' \mid x$ for some $y \in S$, and $v_2(y) = e$ (this leads to the last two conditions in the statement).

To prove the converse implication in the claim, consider that $K(\zeta_x, \zeta_{2^e}) = K(\zeta_x, \sqrt{\beta})$ because both fields have degree 2 over $K(\zeta_x)$ and the former contains the latter, thus $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$. We now prove the direct implication, namely that $v_2(y) = e$: if $v_2(y) < e$, then we would deduce $\sqrt{\beta} \in K(\zeta_x)$; if $v_2(y) > e$ (which holds for either none or all $y \in S$), then (since $v_2(x) < e$) we would have $\sqrt{\beta} \notin K(\zeta_{\operatorname{lcm}(2^e,x)})$, contradicting $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$. □

6. Cyclic extensions of degree 4 or 8 of multiquadratic number fields

Let K be a multiquadratic number field containing ζ_4, and let $\operatorname{Gal}(K/\mathbb{Q})$ be isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some $r \geqslant 1$. If L/K is an extension which is cyclic of degree 4 and it is contained in $K(\mu_\infty)$, then $L/\mathbb{Q}$ is abelian and we have $L = K(\sqrt[4]{\alpha})$ for some $\alpha \in K^\times \setminus K^{\times 2}$. Moreover, $\operatorname{Gal}(L/\mathbb{Q})$ is isomorphic to either

$$(\mathbb{Z}/2\mathbb{Z})^r \times \mathbb{Z}/4\mathbb{Z} \qquad \text{or} \qquad (\mathbb{Z}/2\mathbb{Z})^{r-1} \times \mathbb{Z}/8\mathbb{Z}$$

because it has a cyclic subgroup of order 4 and it is not $(\mathbb{Z}/2\mathbb{Z})^{r-2} \times (\mathbb{Z}/4\mathbb{Z})^2$, as $\operatorname{Gal}(K/\mathbb{Q})$ is obtained by quotienting a cyclic subgroup of order 4. We now fix $\alpha \in K^\times \setminus K^{\times 2}$, so that $K(\sqrt[4]{\alpha})/K$ is cyclic of degree 4.

Theorem 18. *It is possible to check whether* $K(\sqrt[4]{\alpha})/\mathbb{Q}$ *is abelian, and in this case there are finitely many computable minimal integers* $x \geqslant 1$ *such that* $\sqrt[4]{\alpha} \in K(\zeta_x)$.

Proof. The extension $K(\sqrt[4]{\alpha})/\mathbb{Q}$ is abelian of exponent 4 if and only if $K(\sqrt[4]{\alpha}) = K(\sqrt{\gamma})$, where $\mathbb{Q}(\sqrt{\gamma})$ is quartic cyclic (we keep the notation of Section 2.3). If γ exists, then it belongs to a finite computable set, as seen at the beginning of Section 5 (there are only finitely many possibilities for D because $K(\sqrt{D}) = K(\sqrt{\alpha})$, and we may work with this multiquadratic number field). Those integers x as requested can be found with Theorem 15 (first we make sure that $\sqrt{D} \in K(\zeta_x)$, and then we apply the result to $K(\sqrt{D})$).

Let M be the product of all odd prime numbers ramifying in $K(\sqrt[4]{\alpha})$ (the primes of K ramifying in $K(\sqrt[4]{\alpha})$ can be found with [7, Lemma 2]). If $K(\sqrt[4]{\alpha})/\mathbb{Q}$ is abelian (and hence it has exponent dividing 8), then $\sqrt[4]{\alpha} \in K(\zeta_{32M})$ (and $\sqrt[4]{\alpha} \in K(\zeta_{16M})$ if $\zeta_8 \notin K$). To determine whether it is abelian of exponent 8, let F be the extension of K obtained by adding $\sqrt{p}$ for all odd primes $p \mid M$. It is equivalent that $F(\sqrt[4]{\alpha})/\mathbb{Q}$ is abelian of exponent 8, and this is the case if and only if $\alpha/g \in F^{\times 4}$ for some g as in Lemma 12 (notice that the set of possible g is finite and computable).

By Lemma 12 we can also determine the minimal integer $y \geqslant 1$ such that $\sqrt[4]{\alpha} \in F(\zeta_y)$. Let $y = y_0 2^v$, where y_0 is the odd part of y, and consider the largest multiquadratic subfield of $K(\zeta_{y_0})$, which we call K'. If $0 < e \leqslant 3$ is as in Lemma 12, then we have $e+2 = v \leqslant 4$ if $\zeta_8 \notin K$ and hence $\zeta_{2^e} \in K$. So we have $g \in K'$. Since $F/\mathbb{Q}$ has exponent 2 and $\sqrt[4]{\alpha/g} \in F$, we must have $\sqrt{\alpha/g} \in K'$ and hence by Proposition 16 we are able to find those finitely many minimal Y (requiring $y_0 \mid Y$) such that $\sqrt[4]{\alpha/g}$, respectively $\zeta_{2^{e+2}}\sqrt[4]{\alpha/g}$ if $e > 0$, is in $K'(\zeta_Y) = K(\zeta_Y)$. These Y are minimal with the property that $y_0 \mid Y$ and $\sqrt[4]{\alpha} \in K(\zeta_Y)$ because, writing $g = \zeta_{2^e} g_0$, we have $\sqrt[4]{g_0} \in K(\zeta_{y_0})$. □

Now we suppose that $\zeta_8 \in K$, and we study the extensions L/K which are cyclic of degree 8. We have $L = K(\sqrt[8]{\alpha})$ for some $\alpha \in K^\times \setminus K^{\times 2}$, so we fix α as such. If $K(\sqrt[8]{\alpha})/\mathbb{Q}$ is abelian, then its Galois group is isomorphic to either

$$(\mathbb{Z}/2\mathbb{Z})^r \times \mathbb{Z}/8\mathbb{Z} \qquad \text{or} \qquad (\mathbb{Z}/2\mathbb{Z})^{r-1} \times \mathbb{Z}/16\mathbb{Z}$$

because there is a cyclic subgroup of order 8, and $\mathrm{Gal}(K/\mathbb{Q})$ is a quotient by a cyclic group of order 8.

Theorem 19. *It is possible to check whether $K(\sqrt[8]{\alpha})/\mathbb{Q}$ is abelian, and in this case there are finitely many computable minimal integers $x \geqslant 1$ such that $\sqrt[8]{\alpha} \in K(\zeta_x)$.*

Proof. Let $\alpha' = \sqrt{\alpha}$. The extension $K(\sqrt[8]{\alpha})/\mathbb{Q}$ is abelian of exponent 8 only if $K(\alpha')$ is multiquadratic. In this case we have $K(\sqrt[8]{\alpha}) = K(\alpha', \sqrt[4]{\alpha'})$, so we can apply Theorem 18 to find all x such that $\sqrt[8]{\alpha} \in K(\alpha', \zeta_x)$, and then Theorem 15 (1) to select those x such that $\alpha' \in K(\zeta_x)$.

Let M, F be as in the proof of Theorem 18. The extension $K(\sqrt[8]{\alpha})/\mathbb{Q}$ is abelian only if $\sqrt[8]{\alpha} \in K(\zeta_{64M})$. It is abelian of exponent 16 if and only if the same holds for $F(\sqrt[8]{\alpha})/\mathbb{Q}$, equivalently there is some $g \in F$ as in Lemma 14 such that $\alpha/g \in F^{\times 8}$ (the set of possible g is finite and computable). By Lemma 14 we can find the minimal $y \geqslant 1$ such that $\sqrt[8]{\alpha} \in F(\zeta_y)$. Consider the largest multiquadratic subfield of $K(\zeta_y)$ or equivalently of $F(\zeta_y)$, which we call K'. As in the proof of Theorem 18, we have $g \in K'$ and $\sqrt[4]{\alpha/g} \in K'$. By Proposition 16 we may then find the finitely many minimal $Y \geqslant 1$ with $y \mid Y$ such that $\sqrt[8]{\alpha/g} \in K'(\zeta_Y) = K(\zeta_Y)$. These are the minimal $Y \geqslant 1$ such that $y \mid Y$ and $\sqrt[8]{\alpha} \in K(\zeta_Y)$ because $\sqrt[8]{g} \in K(\zeta_y)$. □

Proposition 20. *Let $\beta \in K^\times \setminus K^{\times 2}$.*

1. *Suppose that $\zeta_4 \in K$ (here we do not require $\zeta_8 \in K$) and that $K(\sqrt[4]{\beta})/\mathbb{Q}$ is abelian. Let $e \geqslant 6$, or $e = 5$ and $\zeta_8 \notin K$. We have $\zeta_{2^e}\sqrt[4]{\beta} \in K(\zeta_x)$ for some $x \geqslant 1$ if and only if $\mathrm{lcm}(2^e, y) \mid x$ for some $y \geqslant 1$ such that $\sqrt[4]{\beta} \in K(\zeta_y)$.*
2. *Suppose that $\zeta_8 \in K$ and that $K(\sqrt[8]{\beta})/\mathbb{Q}$ is abelian. Let $e \geqslant 7$. We have $\zeta_{2^e}\sqrt[8]{\beta} \in K(\zeta_x)$ for some $x \geqslant 1$ if and only if $\mathrm{lcm}(2^e, y) \mid x$ for some $y \geqslant 1$ such that $\sqrt[8]{\beta} \in K(\zeta_y)$.*

In particular, the minimal integers $x \geqslant 1$ as above are, in both cases, a finite computable set.

Proof. The minimal integers y as in the statement are a non-empty finite computable set S by Theorems 18 and 19. Moreover, the condition $\operatorname{lcm}(2^e, y) \mid x$ for some $y \in S$ is clearly sufficient. To prove that it is necessary, we apply Lemma 9. For (1), since $\sqrt[4]{\beta} \in K(\zeta_{\operatorname{lcm}(2^e,x)})$, the odd part of some $y \in S$ divides x and we are left to prove $2^e \mid x$. If $e \geqslant 6$, then $\zeta_{2^{e-1}} \in K(\zeta_x)$ and hence $2^{e-1} \mid x$. Thus $y \mid x$ hence $\zeta_{2^e} \in K(\zeta_x)$ and we conclude. If $e = 5$ and $\zeta_8 \notin K$, then for every odd $z \geqslant 1$ we have $\zeta_{32}\sqrt[4]{\beta} \notin K(\zeta_{16z})$ (this field contains $\sqrt[4]{\beta}$ but not ζ_{32}) and we conclude. For (2), since $\zeta_{2^{e-1}}\sqrt[4]{\beta} \in K(\zeta_x)$ we get $2^{e-1} \mid x$ by (1), and we similarly conclude. □

7. Extensions of a quartic cyclic number field

In this section $K = \mathbb{Q}(\sqrt{\gamma})$ is a quartic cyclic number field, and we keep the notation of Section 2.3.

Lemma 21. *We characterize when some elements are in $K(\zeta_x)$, where $x \geqslant 1$:*

Element in $K(\zeta_x)$	*Equivalent condition*
ζ_{2^n} *($n \geqslant 5$)*	$2^n \mid x$
ζ_{16}	$16 \mid x$, *or* $2 \mid D$, $4AD \mid x$
ζ_8	$8 \mid x$, *or* $2 \mid D$, $2D \mid x$, *or* $2 \mid C$, $4AD \mid x$
ζ_4	$4 \mid x$, *or* $AD \mid x$, $A + B \equiv 3 \bmod 4$
$\sqrt{2}$	$\zeta_8 \in K(\zeta_x)$, *or* $2 \mid D$, $D \mid 2x$, *or* $AD \mid x$, $A + C \equiv 1 \bmod 4$
$\sqrt{-2}$	$\zeta_8 \in K(\zeta_x)$, *or* $AD \mid x$, $A + C \equiv 3 \bmod 4\,.$

Proof. We may suppose w.l.o.g. that x is odd or $4 \mid x$ (notice that in the conditions in the statement each congruence implies that D is odd). We set $\eta = 2 + \sqrt{2}$ and $\gamma_0 = \gamma/A$, and we call c_K the conductor of K. The assertion for ζ_{2^n} is clear because $32 \nmid c_K$.

The element ζ_{16}: Suppose that $\zeta_{16} \in K(\zeta_x)$ and $16 \nmid x$, which implies $16 \mid c_K$ and hence $2 \mid D$. Thus $\sqrt{\eta} \in K(\zeta_x) \setminus \mathbb{Q}(\zeta_x)$. We claim that $\sqrt{D} \in \mathbb{Q}(\zeta_x)$ or equivalently $4D \mid x$. If not, then by Lemma 3 we have $\sqrt{\eta D} \in \mathbb{Q}(\zeta_x)$ thus $(D/2) \mid x$ and $\eta \in \mathbb{Q}(\zeta_x)$, which gives $8 \mid x$ and hence $4D \mid x$, contradiction. The conductor of $\mathbb{Q}(\sqrt{\gamma_0})$ is $8D$, so both $\sqrt{\gamma}$ and $\sqrt{\gamma_0}$ generate $K(\zeta_x)$ over $\mathbb{Q}(\zeta_x)$. Thus $\sqrt{A} \in \mathbb{Q}(\zeta_x)$ and hence $A \mid x$. For the other implication: if $2 \mid D$, $4AD \mid x$, and $16 \nmid x$, then we have $\mathbb{Q}(\zeta_x) \subsetneq K(\zeta_x) \subseteq \mathbb{Q}(\zeta_x, \zeta_{16})$ so we conclude because $\zeta_8 \in \mathbb{Q}(\zeta_x)$.

The element ζ_8: Suppose that $\zeta_8 \in K(\zeta_x)$ and $8 \nmid x$, which implies $8 \mid c_K$ and hence either $2 \mid D$ or $2 \mid C$. If $\sqrt{D} \notin \mathbb{Q}(\zeta_x)$, then by Lemma 3 we have $\sqrt{2D} \in \mathbb{Q}(\zeta_x)$, which implies $2 \mid D$ and $(D/2) \mid x$. We have $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{2})$ and hence $\zeta_4 \in \mathbb{Q}(\zeta_x)$, so $2D \mid x$. Now suppose $\sqrt{D} \in \mathbb{Q}(\zeta_x)$: if D is even, then $4D \mid x$; if D is odd, then $\sqrt{2} \in K(\zeta_x)$ implies $2 \mid x$ hence $4D \mid x$. To prove $A \mid x$, or equivalently $\sqrt{A} \in \mathbb{Q}(\zeta_x)$, consider that $\sqrt{\gamma}$, $\sqrt{\gamma_0}$ are both in $K(\zeta_x) \setminus \mathbb{Q}(\zeta_x)$ because $8 \mid c_K$ and the conductor of $\mathbb{Q}(\sqrt{\gamma_0})$ is $8D$. For the other implication: if $8 \nmid x$, $2 \mid D$, and $2D \mid x$, then we have $\zeta_4 \in \mathbb{Q}(\zeta_x)$, and we also have $\sqrt{2} \in K(\zeta_x)$ because both $\sqrt{D}$ and $\sqrt{D/2}$ are in this field; if $8 \nmid x$, $2 \mid C$, and $4AD \mid x$, then $\zeta_4 \in \mathbb{Q}(\zeta_x)$ and we conclude because $K(\zeta_x)$ is contained in $\mathbb{Q}(\zeta_x, \zeta_8)$ but not in $\mathbb{Q}(\zeta_x)$.

The element ζ_4*:* Suppose that $\zeta_4 \in K(\zeta_x)$ and that x is odd, hence $4 \mid c_K$. We cannot have $8 \mid c_K$, else $K(\zeta_{|A|Dx})/\mathbb{Q}(\zeta_{|A|Dx})$ would not be cyclic as it would be generated by ζ_8. So $c_K = 4|A|D$ and hence $A+B \equiv 3 \bmod 4$, thus D is odd and hence it is congruent to $1 \bmod 4$. Since $K(\zeta_x)/\mathbb{Q}(\zeta_x)$ is cyclic and $K(\zeta_x)$ contains $\sqrt{D}$ and ζ_4, we must have $\sqrt{D} \in \mathbb{Q}(\zeta_x)$, thus $K(\zeta_x) = \mathbb{Q}(\zeta_{4x})$ and hence $AD \mid x$. For the other implication: if $4 \nmid x$ and $AD \mid x$ and $A + B \equiv 3 \bmod 4$, then we conclude because $K(\zeta_{|A|D}) \subseteq K(\zeta_x)$ is contained in $\mathbb{Q}(\zeta_{4|A|D})$ but not in $\mathbb{Q}(\zeta_{|A|D})$.

The elements $\sqrt{\pm 2}$*:* Suppose that $\sqrt{\pm 2} \in K(\zeta_x)$ and $\zeta_8 \notin K(\zeta_x)$, so $\zeta_4 \notin K(\zeta_x)$ and x is odd. Since $8 \mid c_K$, we have either $2 \mid D$ or $2 \mid C$. If $\sqrt{D} \in \mathbb{Q}(\zeta_x)$, then $2 \nmid D$ and $D \mid x$. If $\sqrt{D} \notin \mathbb{Q}(\zeta_x)$, then $\sqrt{\pm 2D} \in \mathbb{Q}(\zeta_x)$ by Lemma 3 and so the odd part of D divides x. Now we may suppose that $2 \nmid BD$ and $D \mid x$, which imply $\sqrt{D} \in \mathbb{Q}(\zeta_x)$ and hence $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{\pm 2})$. In particular, we have $A \mid x$. From Remark 7 we deduce that $\sqrt{\pm\gamma'} \in \mathbb{Q}(\zeta_x)$. With the plus sign, the conductor of $\mathbb{Q}(\sqrt{\gamma'})$ is odd, else the conductor is four times an odd number. We conclude that $A + C \equiv \pm 1 \bmod 4$. For the other implication: if $2 \mid D$ and $D \mid 2x$ (recalling that all odd prime divisors of D are congruent to $1 \bmod 4$), then $K(\zeta_x)$ contains $\sqrt{D}$ and $\sqrt{D/2}$; if $AD \mid x$ and $A + C \equiv \pm 1 \bmod 4$, then $\sqrt{\gamma} \in K(\zeta_x)$ and $\sqrt{\pm\gamma'} \in \mathbb{Q}(\zeta_{|A|D}) \subset K(\zeta_x)$, so $K(\zeta_x)$ contains $\sqrt{\pm 2}$ by Remark 7. □

Fix $\alpha \in K^\times \setminus K^{\times 2}$. If $K(\sqrt{\alpha})$ is contained in $K(\mu_\infty)$, then it is an abelian extension of $\mathbb{Q}$ of degree 8. Its Galois group over $\mathbb{Q}$ has a cyclic quotient of order 4, so it is isomorphic either to

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \text{or} \qquad \mathbb{Z}/8\mathbb{Z}\,.$$

Lemma 22. *The extension $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian if and only if it is Galois if and only if we have $\alpha \cdot \sigma(\alpha) \in K^{\times 2}$, where σ is some generator for* $\mathrm{Gal}(K/\mathbb{Q})$.

Proof. If $K(\sqrt{\alpha})/\mathbb{Q}$ is Galois, then it is abelian because its Galois group has order 8 and it has a quotient isomorphic to $\mathbb{Z}/4\mathbb{Z}$. For the second equivalence we may reason as in the proof of [7, Lemma 4], where we consider $\alpha \cdot \sigma(\alpha)$ instead of $N_{K/\mathbb{Q}}(\alpha)$. □

The extension $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian and not cyclic only if there is some squarefree integer m such that $K(\sqrt{\alpha}) = K(\sqrt{m})$ and hence $\alpha/m \in K^{\times 2}$. To determine if m exists and to find it, it suffices to check finitely many possibilities because the odd primes dividing m ramify in $K(\sqrt{\alpha})$ (these can be found with [7, Lemma 2] and by considering the conductor of K).

Theorem 23. *We keep the above notation and the one from Section 2.3. If $K(\sqrt{\alpha}) = K(\sqrt{m})$, then for $x \geqslant 1$ we have $\sqrt{\alpha} \in K(\zeta_x)$ if and only if x is a multiple of at least one of the following numbers:*

- *the conductor of $\mathbb{Q}(\sqrt{m})$;*
- *the conductor of $\mathbb{Q}(\sqrt{Dm})$;*
- *$8D$ times the conductor of $\mathbb{Q}(\sqrt{Am})$;*
- *D times the conductor of $\mathbb{Q}(\sqrt{\pm Am})$, if $A + B \equiv \pm 1 \bmod 4$;*
- *D times the conductor of $\mathbb{Q}(\sqrt{\pm 2Am})$, if $A + C \equiv \pm 1 \bmod 4$.*

Proof. Since $\mathbb{Q}(\sqrt{m})$ and $\mathbb{Q}(\sqrt{mD})$ are the quadratic subextensions of $K(\sqrt{\alpha})$ not contained in K, the first two given conditions are sufficient. The other conditions are also sufficient because $\mathbb{Q}(\zeta_x)$ respectively contains the square roots of $D + B\sqrt{D}$, $\pm(D + B\sqrt{D})$, $\pm 2(D + B\sqrt{D})$ by Remark 6 and (5), so it contains $\sqrt{A}$,$\sqrt{\pm A}$,$\sqrt{\pm 2A}$.

Now suppose that $\sqrt{\alpha} \in K(\zeta_x)$. If $K \subseteq \mathbb{Q}(\zeta_x)$ or $K \cap \mathbb{Q}(\zeta_x) = \mathbb{Q}$, then by Lemma 3 $\sqrt{m}$ or $\sqrt{Dm}$ is in $\mathbb{Q}(\zeta_x)$ and we have the first or second condition. Now suppose that $\sqrt{D} \in \mathbb{Q}(\zeta_x)$ and $K \not\subseteq \mathbb{Q}(\zeta_x)$, and in particular we have $D \mid x$, and $4D \mid x$ if $2 \mid D$.

If $A + B \equiv \pm 1 \bmod 4$, then $\sqrt{\pm(D + B\sqrt{D})} \in \mathbb{Q}(\zeta_x)$ and hence $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{\pm A})$. Thus by Lemma 3 $\sqrt{m}$ or $\sqrt{\pm Am}$ is in $\mathbb{Q}(\zeta_x)$ and we have the first or fourth condition. If $8D \mid x$, then we may reason analogously because $\sqrt{D + B\sqrt{D}} \in \mathbb{Q}(\zeta_x)$.

If $2 \mid D$ (thus $4D \mid x$) and $8D \nmid x$, then we have $K(\zeta_x) = \mathbb{Q}\big(\zeta_x, \sqrt{A(2+\sqrt{2})}\big)$ because $\sqrt{2+\sqrt{2}}$ and $\sqrt{D + B\sqrt{D}}$ generate the same extension over $\mathbb{Q}(\zeta_{4D})$. By Lemma 3 and since $\sqrt{2} \in \mathbb{Q}(\zeta_x)$ all quadratic subextensions of $K(\zeta_x)$ are contained in $\mathbb{Q}\big(\zeta_x\big)$, so we have the first condition.

If $A + C \equiv \pm 1 \bmod 4$, then we have $\sqrt{\pm 2(D + B\sqrt{D})} \in \mathbb{Q}(\zeta_x)$ by (5). So $K(\zeta_x) = \mathbb{Q}(\zeta_x, \sqrt{\pm 2A})$ and hence $\sqrt{m}$ or $\sqrt{\pm 2Am}$ is in $\mathbb{Q}(\zeta_x)$ and we conclude. □

Proposition 24. *Let $\beta \in K^\times$ be such that $K(\sqrt{\beta})/\mathbb{Q}$ is abelian and not cyclic, and let $e \geqslant 3$. An integer $x \geqslant 1$ such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ is the multiple of at least one of the following numbers:*
- $\operatorname{lcm}(2^e, y)$*, for $e \geqslant 5$, where y is such that $\sqrt{\beta} \in K(\zeta_y)$;*
- $\operatorname{lcm}(w, y)$*, if $e = 4$, where w is such that $\zeta_{2^e} \in K(\zeta_w)$ and y is such that $\sqrt{\beta} \in K(\zeta_y)$;*
- $\operatorname{lcm}(4, z)$*, if $e = 3$, where z is such that $\sqrt{2\beta} \in K(\zeta_z)$;*
- $\operatorname{lcm}(AD, z)$*, if $e = 3$ and $A + B \equiv 3 \bmod 4$, where z is such that $\sqrt{2\beta} \in K(\zeta_z)$.*

The minimal integers x form a non-empty finite computable set.

Proof. We can find all minimal w, y, z by applying Lemmas 21 and Theorem 23.

Write $K(\sqrt{\beta}) = K(\sqrt{m})$ for some squarefree integer m as seen before Theorem 23. So we need to describe those x such that $\zeta_{2^e}\sqrt{m} \in K(\zeta_x)$. Notice that $\zeta_{2^e}\sqrt{m} \in K(\zeta_x)$ implies $\zeta_{2^{e-1}} \in K(\zeta_x)$.

For $e \geqslant 4$ (considering Lemma 21 for $e \geqslant 5$) it suffices to prove that both ζ_{2^e} and $\sqrt{m}$ are in $K(\zeta_x)$. This is the case because, if $K(\zeta_x, \sqrt{m})$ and $K(\zeta_x, \zeta_{2^e})$ are non-trivial over $K(\zeta_x)$, then they cannot be equal as the former field has more quadratic subextensions than the latter by Lemma 3.

If $e = 3$, then $\zeta_4 \in K(\zeta_x)$ and hence $\sqrt{2\beta} \in K(\zeta_x)$ so we conclude by Lemma 21. □

Theorem 25. *Let c_K be the conductor of K (call c'_K its odd part and v_K its 2-adic valuation). Let $\mathcal{P}$ be a prime of K over 2. If $K(\sqrt{\alpha})/\mathbb{Q}$ is cyclic of degree 8, then there exists unique a minimal integer $x \geqslant 1$ such that $\sqrt{\alpha} \in K(\zeta_x)$. The odd part of x is a multiple of c'_K and it is the product of all odd primes whose primes of K above them ramify in $K(\sqrt{\alpha})$. Moreover,*

$v_2(x)$ *is given by*

$$\begin{cases} 5 & \textit{if } v_K = 4 \\ 4 & \textit{if } v_K = 3 \\ 3 & \textit{if } v_K = 2 \textit{ and } \mathcal{P} \textit{ ramifies in } K(\sqrt{\alpha}), \textit{ or } v_K = 0 \textit{ and } \mathcal{P} \textit{ ramifies in } K(\sqrt{\alpha}),\ K(\sqrt{-\alpha}) \\ 2 & \textit{if } v_K = 0 \textit{ and } \mathcal{P} \textit{ does not ramify in } K(\sqrt{-\alpha}) \\ 0 & \textit{if } v_K = 0, 2 \textit{ and } \mathcal{P} \textit{ does not ramify in } K(\sqrt{\alpha})\,. \end{cases}$$

Proof. Let x be minimal such that $\sqrt{\alpha} \in K(\zeta_x)$: its odd part x' is squarefree, $1 \neq v_2(x) \leqslant 5$, all prime divisors of x ramify in $K(\sqrt{\alpha})$. Recall that the primes ramifying in K are those dividing c_K, and notice that, if $p \nmid c_K$ is a prime ramifying in $K(\sqrt{\alpha})$, then $p \mid x$.

To show $c'_K \mid x'$ it suffices to prove $c'_K \mid y$, where $y \geqslant 1$ is such that $\sqrt{\alpha} \in K(\zeta_4, \zeta_y)$. Notice that $K(\zeta_4, \sqrt{\alpha})/\mathbb{Q}(\sqrt{D}, \zeta_4)$ is a cyclic Kummer extension of degree 4 with intermediate extension $K(\zeta_4)$. Thus the extension $K(\zeta_4, \zeta_y)/\mathbb{Q}(\sqrt{D}, \zeta_4, \zeta_y)$ is trivial as it has degree at most 2 and hence the base field contains $K(\zeta_4)$. We deduce that A and the odd part of D divide y because if $p \mid AD$ is an odd prime, then $\mathbb{Q}(\zeta_{16|A|D/p}) \neq K(\zeta_{16|A|D/p}) \subseteq \mathbb{Q}(\zeta_{16|A|D})$. We may reason analogously to prove that $v_K \leqslant v_2(x)$ holds if $v_K \geqslant 3$.

Since $K(\sqrt{\alpha}, \zeta_{c_K})/\mathbb{Q}(\zeta_{c_K})$ has degree at most 2, we have $v_2(x) \leqslant \max(3, v_K + 1)$.

If $v_K = 3, 4$, then we know $v_2(x) \in \{v_K, v_K + 1\}$, so we conclude by the minimality of x because $K(\zeta_{2^{v_K} x'}) = K(\zeta_{2^{v_K - 1} x'})$.

If $v_K = 2$, then $K(\sqrt{\alpha}, \zeta_{x'})$ is either $\mathbb{Q}(\zeta_{4x'})$ or $\mathbb{Q}(\zeta_{8x'})$. In the latter case $\mathcal{P}$ ramifies in $K(\sqrt{\alpha})$, while in the former case it does not because $K(\sqrt{\alpha}, \zeta_{x'}) = K(\zeta_{x'})$.

If $v_K = 0$, then 2 does not ramify in K: if $\mathcal{P}$ does not ramify in $K(\sqrt{\alpha})$, then $v_2(x) = 0$; else $v_2(x) \in \{2, 3\}$, and it equals 2 if and only if $\mathcal{P}$ does not ramify in $K(\sqrt{-\alpha})$.

Notice that there is an explicit finite procedure to check whether the primes of K lying over 2 ramify in $K(\sqrt{\alpha})$, see [1, Algorithm 6.2.9]. □

Lemma 26. *If A has some prime divisor which is congruent to* $3 \bmod 4$*, then $K(\sqrt{\alpha})/\mathbb{Q}$ is not cyclic.*

If $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian, then it is cyclic if and only if all prime ideals of K above the odd prime divisors of AD ramify in $K(\sqrt{\alpha})$ (we can apply [7, Lemma 2] *to check this condition).*

Proof. If $K(\sqrt{\alpha})/\mathbb{Q}$ is cyclic, then $\sqrt{\alpha} \notin K(\zeta_4)$ and we have $\sqrt{\alpha} \in K(\zeta_{16|A|Dw})$ for some odd squarefree integer $w \geqslant 1$ coprime to AD. So $K(\zeta_4, \sqrt{\alpha})/\mathbb{Q}(\sqrt{D}, \zeta_4)$ is cyclic of degree 4 and $K \not\subseteq \mathbb{Q}(\sqrt{D}, \zeta_4, \zeta_x)$ if $A \nmid x$. Thus, if $p \mid A$ is prime, then

$$K(\zeta_{16|A|Dw/p}, \sqrt{\alpha})/\mathbb{Q}(\zeta_{16|A|Dw/p})$$

is a subextension of $\mathbb{Q}(\zeta_{16|A|Dw})/\mathbb{Q}(\zeta_{16|A|Dw/p})$ of degree 4, which implies $p \equiv 1 \bmod 4$.

In the second assertion, the prime divisors of AD divide the conductor of K hence the ramification condition is necessary by Theorem 25. It is also sufficient because if $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian and not cyclic, then by Theorem 23 (the first two cases) there is some $x \geqslant 1$ such that $\sqrt{\alpha} \in K(\zeta_x)$ and $D \nmid 2x$. □

Proposition 27. *Let $\beta \in K^\times$ be such that $K(\sqrt{\beta})/\mathbb{Q}$ is cyclic of degree 8, and let $e \geqslant 3$. Let y vary in the set of integers such that $\sqrt{\beta} \in K(\zeta_y)$, and denote by y' the odd part of y. Those integers $x \geqslant 1$ such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ are the multiples of at least one of the following numbers:*
- $\operatorname{lcm}(2^e, y)$*;*
- $4y'$*, if $e = v_2(y) = 5$;*
- $\operatorname{lcm}(w, y')$*, if $e = v_2(y) = 4$ or if $e = 3$ and $v_2(y) < 3$, where w is such that $\zeta_8 \in K(\zeta_w)$;*
- $\operatorname{lcm}(z, y')$*, if $e = v_2(y) = 3$, where z is such that $\zeta_4 \in K(\zeta_z)$.*

The minimal x are a non-empty finite computable set.

Proof. We can find all minimal w and z with Lemma 21 and y with Theorem 25. If $x \geqslant 1$ is such that $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$, then we have $\zeta_{2^{e-1}} \in K(\zeta_x)$ and $\sqrt{\beta} \in K(\zeta_{\operatorname{lcm}(2^e,x)})$, and in particular $y' \mid x$ for some y.

Unless ζ_{2^e} and $\sqrt{\beta}$ are both in $K(\zeta_x)$, we have $\zeta_{2^e} \notin K(\zeta_x)$ and $\sqrt{\beta} \notin K(\zeta_x)$ so, as in the proof of Proposition 17, $\zeta_{2^e}\sqrt{\beta} \in K(\zeta_x)$ holds if and only if $\zeta_{2^{e-1}} \in K(\zeta_x)$, $y' \mid x$ for some y as above, and $v_2(y) = e$.

Suppose that ζ_{2^e} and $\sqrt{\beta}$ are both in $K(\zeta_x)$. If $e > 3$ or if $e = 3$ and $v_2(y) \geqslant 3$, then the first condition is necessary and sufficient. Now let $e = 3$ and $v_2(y) < 3$. Then the third condition is sufficient because $K(\zeta_{\operatorname{lcm}(w,y')}) = K(\zeta_{\operatorname{lcm}(w,4y')})$ and it is necessary because $\zeta_8 \in K(\zeta_x)$.

Now suppose that neither ζ_{2^e} nor $\sqrt{\beta}$ are in $K(\zeta_x)$, and let $e = v_2(y)$ and $y' \mid x$. We only have to ensure $\zeta_{2^{e-1}} \in K(\zeta_x)$. If $e = 3$ or $e = 4$, then clearly the last condition or respectively the third condition applies. Finally let $e = v_2(y) = 5$, which implies $2 \mid D$ and that (recalling from Theorem 25 that $AD \mid 2y$) we have $K(\zeta_{4y'}) = \mathbb{Q}(\zeta_{4y'}, \sqrt{\delta}) = \mathbb{Q}(\zeta_{16y'})$, where $\delta = 2 + \sqrt{2}$, while clearly $\zeta_{16} \notin K(\zeta_{y'})$. □

8. The 2-adelic failure

8.1. **The 2-adelic failure for quartic cyclic number fields.** Let K be a quartic cyclic number field and let $n, M \geqslant 1$ be such that $2^n \mid M$. W.l.o.g. let $\alpha \in K^\times$ be not a root of unity. We write $F = K(\zeta_{2^n}, \sqrt[2^n]{\alpha}) \cap K(\mu_\infty)$ and we compute the 2-adelic failure

$$B(M, 2^n) = [F \cap K(\zeta_M) : K(\zeta_{2^n})]\,.$$

We can write $\alpha = \pm\beta^{2^d}$, where $d \geqslant 0$ and $\beta \in K^\times$ is strongly 2-indivisible. By Theorem 8 we can determine F, and we have

$$B(M, 2^n) = \begin{cases} 2 & \text{if } F = K(\zeta_{2^{n+1}}) \text{ and } \zeta_{2^{n+1}} \in K(\zeta_M), \\ & \text{or if } F = K(\zeta_{2^n}, \sqrt{\beta}) \text{ and } \sqrt{\beta} \in K(\zeta_M), \\ & \text{or if } n \geqslant 2,\ F = K(\zeta_{2^{n+1}}\sqrt{\beta}), \text{ and } \zeta_{2^{n+1}}\sqrt{\beta} \in K(\zeta_M) \\ 1 & \text{otherwise} \end{cases}$$

so we may conclude by applying the results of Section 7 to determine whether the given elements are in $K(\zeta_M)$.

Example 28. Let $K = \mathbb{Q}(\sqrt{3(5+2\sqrt{5})})$, and let $\alpha = 21$ or $\alpha = -21^4$. Consider all $n, M \geqslant 1$ such that $2^n \mid M$, and recall that $B(M, 2^n) \in \{1, 2\}$.
If $\alpha = 21$, then $B(M, 2^n) = 2$ if and only if $2^n \cdot 21 \mid M$ or $2^{\max(2,n)} \cdot 35 \mid M$.
If $\alpha = -21^4$, then $B(M, 2^n) = 2$ if and only if we are in the following cases: $n \leqslant 2$ and $2^{n+1} \mid M$; $n = 3$ and $16 \cdot 21 \mid M$ or $16 \cdot 35 \mid M$; $n \geqslant 4$ and $2^n \cdot 21 \mid M$ or $2^n \cdot 35 \mid M$.

Indeed, Theorem 8 gives $K(\zeta_{2^n}, \sqrt[2^n]{21}) \cap K(\mu_\infty) = K(\zeta_{2^n}, \sqrt{21})$ and

$$K(\zeta_{2^n}, \sqrt[2^n]{-21^4}) \cap K(\mu_\infty) = \begin{cases} K(\zeta_{2^{n+1}}) & \text{if } n \leqslant 2 \\ K(\zeta_{2^{n+1}}\sqrt{21}) & \text{if } n = 3 \\ K(\zeta_{2^n}, \sqrt{21}) & \text{if } n \geqslant 4\,. \end{cases}$$

Moreover, by Lemma 21 for $n \geqslant 2$ we have $\zeta_{2^n} \in K(\zeta_M)$ if and only if $2^n \mid M$; by Theorem 23 we have $\sqrt{21} \in K(\zeta_M)$ if and only if $21 \mid M$ or $4 \cdot 35 \mid M$; by Proposition 24 for $n \geqslant 3$ we have $\zeta_{2^n}\sqrt{21} \in K(\zeta_M)$ if and only if $2^n \cdot 21 \mid M$ or $2^n \cdot 35 \mid M$ (by Theorem 23 we have $\sqrt{42} \in K(\zeta_M)$ if and only if $8 \cdot 21 \mid M$ or $8 \cdot 35 \mid M$).

Example 29. Let $K = \mathbb{Q}(\sqrt{\gamma})$, where $\gamma = 5(17 + \sqrt{17})$, so the conductor of K is $8 \cdot 85$. Let $\alpha = -\beta^8$, where $\beta = 12\sqrt{\gamma} + 78\gamma + 7\gamma\sqrt{\gamma}$. Consider all $n, M \geqslant 1$ such that $2^n \mid M$, and recall that $B(M, 2^n) \in \{1, 2\}$. We prove that $B(M, 2^n) = 2$ if and only if we are in the following cases: $n = 2$, and $8 \mid M$ or $4 \cdot 85 \mid M$; $n = 3$ and $16 \mid M$; $n = 4$ and $32 \cdot 85 \mid M$; $n \geqslant 5$ and $2^n \cdot 85 \mid M$.

With [14] we can check that $\beta \in K^\times$ is strongly 2-indivisible, and that $\beta \cdot \sigma(\beta) \in K^{\times 2}$, where σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$. By Lemma 22 $K(\sqrt{\beta})/\mathbb{Q}$ is then abelian, so Theorem 8 gives

$$K(\zeta_{2^n}, \sqrt[2^n]{\alpha}) \cap K(\mu_\infty) = \begin{cases} K(\zeta_{2^{n+1}}) & \text{if } n \leqslant 3 \\ K(\zeta_{2^{n+1}}\sqrt{\beta}) & \text{if } n = 4 \\ K(\zeta_{2^n}, \sqrt{\beta}) & \text{if } n \geqslant 5\,. \end{cases}$$

By [14], working with the ring of integers of K, the prime ideals dividing (β) with an odd exponent lie over $2, 5, 17$. Then by Lemma 26 the Galois group of $K(\sqrt{\beta})/\mathbb{Q}$ is $\mathbb{Z}/8\mathbb{Z}$ and hence by applying Theorem 25 we have $\sqrt{\beta} \in K(\zeta_x)$ if and only if $16 \cdot 85 \mid x$.

By Lemma 21 for $n \neq 1, 3$ we have $\zeta_{2^n} \in K(\zeta_x)$ if and only if $2^n \mid x$, while $\zeta_8 \in K(\zeta_x)$ if and only if $8 \mid x$ or $4 \cdot 85 \mid x$. By Proposition 27 we have $\zeta_{2^n}\sqrt{\beta} \in K(\zeta_x)$ if and only if $n \geqslant 5$ and $2^n \cdot 85 \mid x$, or $n = 4$ and $4 \cdot 85 \mid x$, or $n = 3$ and $16 \cdot 85 \mid x$.

8.2. **The 2-adelic failure for multiquadratic number fields.** Let K be a multiquadratic number field and let $n, M \geqslant 1$ be such that $2^n \mid M$. W.l.o.g. let $\alpha \in K^\times$ be not a root of unity. We write $F = K(\zeta_{2^n}, \sqrt[2^n]{\alpha}) \cap K(\mu_\infty)$ and we compute the 2-adelic failure

$$B(M, 2^n) = [F \cap K(\zeta_M) : K(\zeta_{2^n})]\,.$$

We can write $\alpha = \zeta_{2^h}\beta^{2^d}$, where $\zeta_{2^h} \in K$ (thus $h \leqslant 3$), $d \geqslant 0$, and $\beta \in K^\times$ is strongly 2-indivisible. We can find F by applying Theorem 8, and then we can find the degrees $B(M, 2^n)$ by applying the results in Sections 5–6 to the generator of F over $K(\zeta_{2^n})$ indicated by Theorem 8 (and to the generators of the subextensions of F over $K(\zeta_{2^n})$, which are 2-powers of the given generator).

Example 30. Let $K=\mathbb{Q}(\zeta_4,\sqrt{5},\sqrt{21})$ and $\alpha=\zeta_4\beta^8$, where $\beta=3(5+2\sqrt{5})\in K^\times$ is strongly 2-indivisible. We prove that for all $n,M\geqslant 1$ such that $2^n\mid M$ we have

$$B(M,2^n)=\begin{cases}4 & \text{if } n=2,3 \text{ and } 2^{n+2}\mid M \text{, or}\\ & \text{if } n=4 \text{ and } 2^6\cdot 15\mid M \text{ or } 2^6\cdot 35\mid M\\ 2 & \text{if } n=1 \text{ and } 2^3\mid M\text{, or}\\ & \text{if } n=2,3 \text{ and } v_2(M)=n+1\text{, or}\\ & \text{if } n=4 \text{ and } 2^5\mid M,\ 2^6\cdot 15\nmid M,\ 2^6\cdot 35\nmid M\text{, or}\\ & \text{if } n=5 \text{ and } 2^6\cdot 15\mid M \text{ or } 2^6\cdot 35\mid M\text{, or}\\ & \text{if } n\geqslant 6 \text{ and } 2^n\cdot 15\mid M \text{ or } 2^n\cdot 35\mid M\\ 1 & \text{otherwise}\,.\end{cases}$$

Since $\mathbb{Q}(\sqrt{\beta})$ is quartic cyclic, the Galois group of $K(\sqrt{\beta})/\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2\times\mathbb{Z}/4\mathbb{Z}$. We have $\sqrt[4]{\beta}\notin K(\mu_\infty)=\mathbb{Q}(\sqrt{\beta},\mu_\infty)$ by Lemma 22 because $\sqrt{\beta\cdot 3(5-2\sqrt{5})}=3\sqrt{5}\notin\mathbb{Q}(\sqrt{\beta})^{\times 2}$. By Theorem 15 we have $\sqrt{\beta}\in K(\zeta_M)$ if and only if $15\mid M$ or $35\mid M$.

For $N\geqslant 3$, $\zeta_{2^N}\in K(\zeta_M)$ implies $2^N\mid M$ by Lemma 9, so by Proposition 17 we have $\zeta_{2^N}\sqrt{\beta}\in K(\zeta_M)$ if and only if $2^N\cdot 15\mid M$ or $2^N\cdot 35\mid M$. We may conclude because Theorem 8 gives

$$K(\zeta_{2^n},\sqrt[2^n]{\alpha})\cap K(\mu_\infty)=\begin{cases}K(\zeta_{2^{n+2}}) & \text{if } n\leqslant 3\\ K(\zeta_{2^6}\sqrt{\beta}) & \text{if } n=4,5\\ K(\zeta_{2^n},\sqrt{\beta}) & \text{if } n\geqslant 6\,.\end{cases}$$

Example 31. Let $K=\mathbb{Q}(\zeta_4,\sqrt{17})$ and let $\alpha=8(13\sqrt{17}+51)(4\zeta_4-1)$. With [14] we can check that $K(\sqrt[4]{\alpha})$ is the subextension of degree 8 of $\mathbb{Q}(\zeta_{4\cdot 17})/\mathbb{Q}(\zeta_4)$, and then by Lemma 12 that $K(\sqrt[4]{\alpha})\subseteq K(\zeta_M)$ holds if and only if $17\mid M$. Since $K(\sqrt{\alpha})$ is the quartic subextension of $\mathbb{Q}(\zeta_{4\cdot 17})/\mathbb{Q}(\zeta_4)$, we also have that $\sqrt{\alpha}\in K(\zeta_M)$ holds if and only if $17\mid M$. We can apply Theorem 8 to get, for $n\geqslant 1$ and $2^n\mid M$:

$$B(M,2^n)=\begin{cases}4 & \text{if } n\geqslant 2 \text{ and } 17\mid M\\ 2 & \text{if } n=1 \text{ and } 17\mid M\\ 1 & \text{otherwise}\,.\end{cases}$$

8.3. **Number fields without quadratic subfields.**

Let K be a number field without quadratic subfields, i.e. such that the maximal subextension of K which is Galois over $\mathbb{Q}$ has odd degree. In particular $K\cap\mathbb{Q}(\mu_\infty)$ has odd degree, and $K\cap\mu_\infty=\{\pm1\}$. So for K we only need to study the 2-adelic failure: if $\alpha\in K^\times\setminus\{\pm1\}$, then we write $F=K(\zeta_{2^n},\ \sqrt[2^n]{\alpha})\cap K(\mu_\infty)$ and we compute the 2-adelic failure

$$B(M,2^n)=[F\cap K(\zeta_M):K(\zeta_{2^n})]$$

for all $M,n\geqslant 1$ such that $2^n\mid M$. We can write $\alpha=\pm\beta^{2^d}$ where $d\geqslant 0$ and $\beta\in K^\times$ is such that $\pm\beta\notin K^{\times 2}$. Notice that $\sqrt[4]{\beta}\notin K(\mu_\infty)$ by Schinzel's Theorem on abelian radical extensions (see [15, Theorem 2]). We can apply Theorem 8 to compute F, and we have

$$B(M,2^n)=\begin{cases} 2 & \text{if } F=K(\zeta_{2^{n+1}}) \text{ and } \zeta_{2^{n+1}}\in K(\zeta_M),\\ & \text{or if } F=K(\zeta_{2^n},\sqrt{\beta}) \text{ and } \sqrt{\beta}\in K(\zeta_M),\\ & \text{or if } n\geqslant 2,\, F=K(\zeta_{2^{n+1}}\sqrt{\beta}), \text{ and } \zeta_{2^{n+1}}\sqrt{\beta}\in K(\zeta_M)\\ 1 & \text{otherwise}\,. \end{cases}.$$

To determine whether the given elements are in $K(\zeta_M)$, we can apply the following Proposition.

Proposition 32. *There is a finite procedure to determine whether $\sqrt{\beta}\in K(\mu_\infty)$. In this case there exists unique a minimal integer $x\geqslant 1$ such that $\sqrt{\beta}\in K(\zeta_x)$. Moreover, if $e\geqslant 3$, then there exists unique a minimal integer $y_e\geqslant 1$ such that $\zeta_{2^e}\sqrt{\beta}\in K(\zeta_{y_e})$. We have $y_e=\operatorname{lcm}(2^e,x)$ unless $e=v_2(x)=3$, where we have $y_e=x/2$. We can determine x (and hence y_e) with a finite procedure.*

Proof. We have $\sqrt{\beta}\in K(\mu_\infty)$ if and only if there is some squarefree integer m (it is unique) such that $K(\sqrt{\beta})=K(\sqrt{m})$, which means $\beta m\in K^{\times 2}$. In this case, since $K\cap\mathbb{Q}(\mu_\infty)$ has odd degree over $\mathbb{Q}$, we have that x is the conductor of $\mathbb{Q}(\sqrt{m})$, and y_e is the conductor of $\mathbb{Q}(\zeta_{2^e}\sqrt{m})$. To check if m exists and, if so, to determine it, it suffices to find a finite set to which m belongs: an odd prime divisors of m is such that there is some prime $\mathfrak{p}$ of K above it which ramifies in $K(\sqrt{\beta})$, so the $\mathfrak{p}$-adic valuation of the fractional ideal (β) is odd (see [7, Lemma 2]). □

Example 33. Consider the number field $K=\mathbb{Q}(T)$, where T is a root of $X^4+8X+12$. By [2, Remark 4.16] K has no quadratic subfields because the Galois group of $K/\mathbb{Q}$ is isomorphic to A_4. Let $\alpha=2T+3=-(T^2/2)^2$, so with the above notation we have $\beta=T^2/2$ and $d=1$. Since $K(\sqrt{\beta})=K(\sqrt{2})$, we have $\sqrt{\beta}\in K(\zeta_x)$ if and only if $8\mid x$. By Theorem 8 (where $t=1$ and $h=1$) and by Proposition 32 we deduce that for $n,M\geqslant 1$ and $2^n\mid M$ we have

$$B(M,2^n)=\begin{cases} 2 & \text{if } n=1 \text{ and } 4\mid M\\ 1 & \text{otherwise}\,. \end{cases}$$

9. The ℓ-adelic failure for ℓ odd

9.1. The 3-adelic falilure for multiquadratic number fields containing ζ_3.

Let K be a multiquadratic number field containing ζ_3, and let $n,M\geqslant 1$ be such that $3^n\mid M$. If $\alpha\in K^\times$, then we set $F=K(\zeta_{3^n},\sqrt[3^n]{\alpha})\cap K(\mu_\infty)$ and we compute the 3-adelic failure

$$B(M,3^n)=[F\cap K(\zeta_M):K(\zeta_{3^n})]\,.$$

This computation is evident if α is a root of unity, so we exclude this case and we write $\alpha=\beta^{3^d}$ with $d\geqslant 0$ or $\alpha=\zeta_3\beta^{3^d}$ with $d\geqslant 1$, where $\beta\in K^\times$ is strongly 3-indivisible. We can apply

Theorem 8 to compute F, and we have

$$B(M,3^n)=\begin{cases}3 & \text{if } F=K(\zeta_{3^{n+1}}) \text{ and } 3^{n+1}\mid M,\\ & \text{or if } F=K(\zeta_{3^n},\sqrt[3]{\beta}) \text{ and } \sqrt[3]{\beta}\in K(\zeta_M),\\ & \text{or if } n\geqslant 2,\ F=K(\zeta_{3^{n+1}}\sqrt[3]{\beta}), \text{ and } \zeta_{3^{n+1}}\sqrt[3]{\beta}\in K(\zeta_M)\\ 1 & \text{otherwise}\,.\end{cases}$$

To determine whether the given elements are in $K(\zeta_M)$ we can apply the following result:

Proposition 34. *We can check whether $K(\sqrt[3]{\beta})/\mathbb{Q}$ is abelian. In this case, if $e\geqslant 0$, then there is precisely one minimal integer $x\geqslant 1$ such that $\zeta_{3^e}\sqrt[3]{\beta}\in K(\zeta_x)$, and x is computable. If $e\geqslant 3$, then $x=\operatorname{lcm}(3^e,y)$, where y is the minimal integer such that $\sqrt[3]{\beta}\in K(\zeta_y)$.*

Proof. Since $K(\sqrt[3]{\beta})/K$ has degree 3, we have $K(\sqrt[3]{\beta})=KL$ for some number field L such that $L/\mathbb{Q}(\zeta_3)$ is an extension of degree 3. Moreover, we have

$$K(\sqrt[3]{\beta})\subseteq K(\zeta_x)\quad\Leftrightarrow\quad L\subseteq\mathbb{Q}(\zeta_3,\zeta_x)\,.$$

Thus to check if $K(\sqrt[3]{\beta})/\mathbb{Q}$ is abelian it suffices to check whether $\beta/g\in K^{\times 3}$ for some g as in [7, Theorem 9], where we take M to be the product of 3 and all primes congruent to 1 modulo 3 that ramify in $K(\sqrt[3]{\beta})$ (which can be found with [7, Lemma 2]). The same result provides the minimal $y\geqslant 1$ such that $\sqrt[3]{g}$, or equivalently $\sqrt[3]{\beta}$, is in $K(\zeta_y)$.

For $e=1$ we may reduce to the case $e=0$ because $\zeta_3\in K$, and the same holds for $e=2$ because we may replace β with $\zeta_3\beta$. Finally, if $e\geqslant 3$ and $\zeta_{3^e}\sqrt[3]{\beta}\in K(\zeta_x)$, then we need $3^e\mid x$. Else $K(\zeta_x,\zeta_{3^e})=K(\zeta_x,\sqrt[3]{\beta})$ would be impossible because the latter field does not contain ζ_{3^e}. □

Example 35. Let K be a multiquadratic number field containing ζ_3. Then $\alpha=\frac{21\sqrt{-3}-7}{2}$ is such that $\sqrt[3]{\alpha}$ generates the cubic subextension of $\mathbb{Q}(\zeta_{21})/\mathbb{Q}(\zeta_3)$. Thus 7 is the minimal integer $z\geqslant 1$ such that $\sqrt[3]{\alpha}\in\mathbb{Q}(\zeta_{3z})$. For $n\geqslant 1$ and $3^n\mid M$ we have:

$$[K(\zeta_{3^n},\sqrt[3^n]{\alpha})\cap K(\zeta_M):K(\zeta_{3^n})]=\begin{cases}3 & \text{if } 7\mid M\\ 1 & \text{otherwise}\,.\end{cases}$$

9.2. **The 5-adelic failure for $\mathbb{Q}(\zeta_5)$.** Let $K=\mathbb{Q}(\zeta_5)$, and let $n,M\geqslant 1$ with $5^n\mid M$. If $\alpha\in K^\times$, then we set $F=K(\zeta_{5^n},\sqrt[5^n]{\alpha})\cap K(\mu_\infty)$ and we compute the 5-adelic failure

$$B(M,5^n)=[F\cap K(\zeta_M):K(\zeta_{5^n})]\,.$$

We proceed as in the previous subsection: w.l.o.g. α is not a root of unity, and we associate to it some $\beta\in K^\times$ which is strongly 5-indivisible. We can apply Theorem 8 to compute F, and we have

$$B(M,5^n)=\begin{cases}5 & \text{if } F=K(\zeta_{5^{n+1}}) \text{ and } 5^{n+1}\mid M,\\ & \text{or if } F=K(\zeta_{5^n},\sqrt[5]{\beta}) \text{ and } \sqrt[5]{\beta}\in K(\zeta_M),\\ & \text{or if } n\geqslant 2,\ F=K(\zeta_{5^{n+1}}\sqrt[5]{\beta}), \text{ and } \zeta_{5^{n+1}}\sqrt[5]{\beta}\in K(\zeta_M)\\ 1 & \text{otherwise}\,.\end{cases}$$

To determine whether the given elements are in $K(\zeta_M)$ we can apply the following result:

Proposition 36. *We can check whether $K(\sqrt[5]{\beta})/\mathbb{Q}$ is abelian. In this case, if $e \geqslant 0$, then there is precisely one minimal $x \geqslant 1$ such that $\zeta_{5^e}\sqrt[5]{\beta} \in K(\zeta_x)$, and x is computable. If $e \geqslant 3$, then $x = \operatorname{lcm}(5^e, y)$, where y is the minimal integer such that $\sqrt[5]{\beta} \in K(\zeta_y)$.*

Proof. The statement is analogous to Proposition 34, thus we can prove analogously the last assertion and we may reduce to the case $e = 0$. So let $e = 0$. Since x is minimal, then we have $x \mid 25t$, where t is either 1 or it is a squarefree product of prime numbers congruent to 1 modulo 5, and we may take t to be the product of the prime numbers $p \neq 5$ ramifying in $K(\sqrt[5]{\alpha})$. We may find these p with [7, Lemma 2], and having $p \not\equiv 0, 1 \bmod 5$ for some p ramifying in $K(\sqrt[5]{\beta})$ already implies that $K(\sqrt[5]{\beta})/\mathbb{Q}$ is not abelian. Then to check if $K(\sqrt[5]{\beta})/\mathbb{Q}$ is abelian it suffices to check whether $\beta/g \in K^{\times 5}$ for some g as in Lemma 37 (where $N = 5t$). We conclude because we know the minimal integer x such that $\sqrt[5]{g} \in K(\zeta_x)$. □

Lemma 37. *Let $N = \prod_{i=1}^{r} p_i$, where the p_i's are distinct prime numbers such that $p_i = 5$ or $p_i \equiv 1 \pmod 5$. Set $\beta_5 = \zeta_5$, and for $p_i \neq 5$ let $\beta_{p_i} \in K^\times$ be such that $K(\sqrt[5]{\beta_i})$ is the subextension of $K(\zeta_{p_i})/K$ of degree 5 (to find β_i see* [6, Section 4]*).*

The extension $\mathbb{Q}(\zeta_{5N})/K$ has $(5^r - 1)/4$ subextensions of degree 5. They are of the form $K(\sqrt[5]{g})$, where

$$g = \prod_{\emptyset \neq I \subseteq \{1,\dots,r\}} \beta_{p_i}^{e_i}\,, \qquad e_i \in \{1,2,3,4\}\,.$$

Moreover, for every $x \geqslant 1$ we have $K(\sqrt[5]{g}) \subseteq \mathbb{Q}(\zeta_{5x})$ if and only if $p_i \mid x$ for every $i \in I$.

Proof. The field $K(\sqrt[5]{g})$ is contained in $\mathbb{Q}(\zeta_{5x})$ if $p_i \mid x$ for every $i \in I$ by definition of the β_i's. Conversely, if $K(\sqrt[5]{g}) \subseteq \mathbb{Q}(\zeta_{5x})$, then $p_i \mid x$ because $\sqrt[5]{\beta_i} \in \mathbb{Q}(\zeta_{5x})$. In particular, $K(\sqrt[5]{g})/K$ has degree 5.

There are $5^r - 1$ elements g as in the statement, and they generate $(5^r - 1)/4$ distinct extensions (because $K(\sqrt[5]{g_1}) = K(\sqrt[5]{g_2})$ holds if and only if $g_1 \cdot g_2^e \in K^{\times 5}$ for some $e \in \{1,2,3,4\}$).

We conclude by proving that $\mathbb{Q}(\zeta_{5N})/K$ has $(5^r - 1)/4$ subextensions of degree 5. Its Galois group G is such that $G/G^5 \simeq (\mathbb{F}_5)^r$. Thus counting the kernels of the surjective group homomorphisms $G \to \mathbb{F}_5$ amounts to counting the kernels of the surjective linear maps $(\mathbb{F}_5)^r \to \mathbb{F}_5$. These are precisely the vector subspaces of $(\mathbb{F}_5)^r$ of codimension 1: by orthogonality w.r.t. the standard scalar product (after having fixed a basis) they correspond to the vector subspaces of dimension 1 and we conclude. □

Example 38. Let $K = \mathbb{Q}(\zeta_5)$ and let $\alpha = \zeta_5\beta^5$, where $\beta = 11(15\zeta_5^3 + 35\zeta_5^2 + 25\zeta_5 + 41)$. We can check with [14] that $\sqrt[5]{\beta}$ generates the subextension of $\mathbb{Q}(\zeta_{55})/\mathbb{Q}(\zeta_5)$ of degree 5. Thus 11 is the minimal integer $z \geqslant 1$ such that $\sqrt[5]{\beta} \in \mathbb{Q}(\zeta_{5z})$. We then have, for $n \geqslant 1$ and $5^n \mid M$:

$$[K(\zeta_{5^n}, \sqrt[5^n]{\alpha}) \cap K(\zeta_M) : K(\zeta_{5^n})] = \begin{cases} 5 & \text{if } n = 1 \text{ and } 5^2 \mid M, \text{ or} \\ & \text{if } n = 2 \text{ and } 5^3 \cdot 11 \mid M, \text{ or} \\ & \text{if } n \geqslant 3 \text{ and } 11 \mid M \\ 1 & \text{otherwise}\,. \end{cases}$$

ACKNOWLEDGEMENTS

Supported by the Luxembourg National Research Fund PRIDE17/1224660/GPS. A CC BY or equivalent licence is applied to the AAM/VoR arising from this submission, in accordance with the grant's open access conditions. All authors are very grateful to Fritz Hörmann, Pietro Sgobba, and Sebastiano Tronto, who assisted with the preparation of the paper.

REFERENCES

[1] COHEN H.: *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, **138**, Springer-Verlag, Berlin Heidelberg, 1993.

[2] CONRAD, K.: *Galois groups as permutation groups*, Lecture notes, available at `https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf`.

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

[4] HARDY, K. - HUDSON, R. H. - RICHMAN, D. - WILLIAMS, K. S. - HOLTZ, N. M. *Calculation of the class numbers of imaginary cyclic quartic fields.* Math. Comp. **49** (1987), no. 180, 615–620.

[5] HINDRY, M. - SILVERMAN, J. H.: *Diophantine geometry - An introduction*, Graduate Texts in Mathematics, **201**, Springer-Verlag, New York, 2000.

[6] HÖRMANN, F. - PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Explicit Kummer generators for cyclotomic extensions*, submitted for publication, available online at `http://hdl.handle.net/10993/46428`.

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

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

[9] MASLEY, J. M.: *Class numbers of real cyclic number fields with small conductor*, Compositio Math. **37** (1978), no. 3, 297–319.

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

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

[12] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Explicit Kummer theory for the rational numbers*, Int. J. Number Theory, **16** (2020), no. 10, 2213–2231.

[13] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *The degree of Kummer extensions of number fields*, Int. J. Number Theory, **17** (2021), no. 5, 1091–1110.

[14] THE SAGE DEVELOPERS, *SageMath, the Sage Mathematics Software System (Version 9.2)*, `https://www.sagemath.org`, 2021.

[15] SCHINZEL, A., *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), no. 3, 245–274. Addendum, ibid. **36** (1980),101–104. See also Andrzej Schinzel Selecta Vol.II, European Mathematical Society, Zürich, 2007, 939–970.

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

Email address: `flavio.perissinotto@uni.lu, antonella.perucca@uni.lu`