EXPLICIT KUMMER THEORY FOR QUADRATIC FIELDS

FRITZ HÖRMANN, ANTONELLA PERUCCA, PIETRO SGOBBA, SEBASTIANO TRONTO

ABSTRACT. Let K be a quadratic number field and let $\alpha \in K$. We present an explicit finite procedure to compute at once all Kummer degrees $[K(\zeta_m, \sqrt[n]{\alpha}) : K(\zeta_m)]$ for $n, m \geqslant 1$ with $n \mid m$, where ζ_m denotes a primitive m-th root of unity. We can also replace α by any finitely generated subgroup of $K^\times$.

1. INTRODUCTION

If K is a number field and $\alpha \in K$, then a natural question in Kummer theory is computing at once all Kummer degrees

$$\left[K(\zeta_m, \sqrt[n]{\alpha}) : K(\zeta_m)\right]$$

for $n, m \geqslant 1$ with $n \mid m$, where ζ_m denotes a primitive m-th root of unity. Equivalently, we compute the ratio

$$C(m,n) := \frac{n}{[K(\zeta_m, \sqrt[n]{\alpha}) : K(\zeta_m)]},$$

which is a positive integer dividing n that is bounded independently of m and n (see [8, Theorem 3.1] for a direct proof). If we consider the prime factorization $n = \prod_\ell \ell^e$, then we easily get the following decomposition:

$$C(m,n) = \prod_{\ell \mid n} C(\ell^e, \ell^e) \cdot B(m, \ell^e),$$

where

$$B(m,\ell^e) := \left[K(\zeta_{\ell^e}, \sqrt[\ell^e]{\alpha}) \cap K(\zeta_m) : K(\zeta_{\ell^e})\right].$$

The numbers $C(\ell^e, \ell^e)$, which we call *ℓ-adic failure*, can be computed at once for all primes ℓ and all $e \geqslant 1$, see Remark 14, so we focus on the study of the *ℓ-adelic failure* $B(m, \ell^e)$. In [9] we have described an algorithm for the computation of the ℓ-adelic failure over $\mathbb{Q}$. In this work we let K be any quadratic field: we present an explicit finite procedure which, given any quadratic number field K and any element $\alpha \in K$ (which is w.l.o.g. neither 0 nor a root of unity) computes the ℓ-adelic failure $B(m, \ell^e)$ for all m, ℓ, e such that $\ell^e \mid m$. Notice that the numbers $B(m, \ell^e)$ are 1 for $K \neq \mathbb{Q}(\zeta_3)$

2010 *Mathematics Subject Classification.* Primary: 11R11; Secondary: 11R18, 11R21, 11Y40.

Key words and phrases. Kummer theory, Kummer extension, number field, cyclotomic field, quadratic field, degree.

if $\ell \neq 2$, and for $K = \mathbb{Q}(\zeta_3)$ if $\ell \neq 2, 3$ because the ℓ-adelic failure is related to the presence of ℓ-th roots of unity in K, see [8, Lemma 3.5]. Since K is a quadratic field, the degrees of the cyclotomic extensions of K are easy to compute, so we can also compute at once the degrees of the fields $K(\zeta_m, \sqrt[n]{\alpha})$ over K (or over $\mathbb{Q}$). Moreover, we can replace α by a finitely generated subgroup G of $K^\times$, as explained in Section 8. Notice that applications of this work include problems related to the Artin primitive root conjecture because families of Kummer degrees appear in this setting, see the survey by Moree [6]. In particular, our results allow to compute explicit expressions for several densities related to the Artin primitive root conjecture.

Acknowledgments. We thank Carlo Sircana for suggesting Lemma 5 and the referee of another paper of ours for suggesting Remark 4.

2. PRELIMINARIES

2.1. **Notation.** Given two integers a, b we denote by $[a, b]$ their least common multiple, and by (a, b) their greatest common divisor. Given a non-zero integer a we write $v_2(a)$ for its 2-adic valuation. When we speak of divisors of an integer number, we consider positive and negative divisors alike. Squarefree numbers can be negative, and the same holds for the squarefree part of an integer (which is the unique squarefree integer that multiplied by the given integer is a square in $\mathbb{Z}$) and for the odd squarefree part of an integer (by which we mean the squarefree part, divided by 2 if it is even).

For an integer $n \geqslant 1$ we denote by ζ_n a primitive n-th root of unity, and by μ_n the multiplicative group of n-th roots of unity. We also make use of the following notation: if K is a number field, then $K(\zeta_\infty)$ is the compositum of all cyclotomic extensions of K, while $K(\zeta_{\ell^\infty})$ is the compositum of all fields $K(\zeta_{\ell^n})$ for $n \geqslant 1$; $\mathcal{O}_K$ is the ring of integers of K and μ_K is the group of roots of unity in K; for a prime $\mathfrak{p}$ of K and for $\alpha \in K^\times$, we denote by $v_\mathfrak{p}(\alpha)$ the $\mathfrak{p}$-adic valuation of the fractional ideal generated by α; after choosing an embedding of K in $\mathbb{C}$, we write $\overline{x}$ for the complex conjugate of an element $x \in K$. If L is a cyclic Kummer extension of K of degree m and $\zeta_m \in K$, then we call $\alpha \in K$ a *Kummer generator* for L if $L = K(\sqrt[m]{\alpha})$.

If F is a number field which is abelian over $\mathbb{Q}$, then we call the *conductor* of F the smallest positive integer n such that $F \subseteq \mathbb{Q}(\zeta_n)$: notice that we have $F \subseteq \mathbb{Q}(\zeta_n)$ if and only if n is a positive multiple of the conductor.

If K is a number field and ℓ a prime number, then we call $\alpha \in K^\times$ *strongly ℓ-indivisible* if there is no root of unity $\zeta \in K$ (whose order we may suppose to be a power of ℓ) such that $\alpha\zeta \in K^{\times\ell}$. If $\zeta_\ell \notin K$, then strongly ℓ-indivisible means not being an ℓ-th power in $K^\times$. In general, if $\alpha \in K^\times$ is not a root of unity, then we can write $\alpha = \zeta_{\ell^h} \cdot \beta^{\ell^d}$ for some $\beta \in K^\times$ which is strongly ℓ-indivisible, for some non-negative integer d, and for some root of unity ζ_{ℓ^h} in K.

2.2. **Quartic cyclic number fields.** We will make use of the following classification result for cyclic quartic extensions of $\mathbb{Q}$, which is [3, Theorem 1 and the following lines, Theorem 3]. Notice that in the following statement the condition that D is positive is no restriction because either a quartic cyclic extension is totally real or the only quadratic subfield is the field fixed by the complex conjugation, which is a totally real field.

Theorem 1. *Let D be a positive squarefree integer, and let $K = \mathbb{Q}(\sqrt{D})$. Then a quadratic extension F/K is quartic cyclic over $\mathbb{Q}$ if and only if it is of the form*

$$F = \mathbb{Q}\Big(\sqrt{A(D + B\sqrt{D})}\Big) = \mathbb{Q}\Big(\sqrt{A(D - B\sqrt{D})}\Big) \tag{1}$$

where A is an odd squarefree integer coprime to D and B is a positive integer such that $D - B^2$ is a square (in particular, we have $D \not\equiv 3 \bmod 4$). Moreover, the integers A and B satisfying the above conditions are uniquely determined. The conductor of the quartic cyclic extension is

$$\begin{array}{rl} 8|A|D & \text{if } D \equiv 2 \bmod 8, \text{ or if } D \equiv 1 \bmod 4 \text{ and } B \text{ is odd} \\ 4|A|D & \text{if } D \equiv 1 \bmod 4,\ B \text{ is even, and } A + B \equiv 3 \bmod 4 \\ |A|D & \text{if } D \equiv 1 \bmod 4,\ B \text{ is even, and } A + B \equiv 1 \bmod 4\,. \end{array}$$

2.3. **Two general results.** We will use in several occasions the following two results:

Lemma 2 ([4, Lemma C.1.7 and its proof])**.** *Let K be a number field, and let n be a positive integer such that $\zeta_n \in K$. Let $\alpha \in K^\times$ and let $\mathfrak{p}$ be a prime of K.*

(1) If $v_\mathfrak{p}(\alpha)$ is not divisible by n, then $\mathfrak{p}$ ramifies in $K(\sqrt[n]{\alpha})$.
(2) If $v_\mathfrak{p}(\alpha)$ is divisible by n and the prime number below $\mathfrak{p}$ is coprime to n, then $\mathfrak{p}$ does not ramify in $K(\sqrt[n]{\alpha})$.

Proposition 3. *Let K, F be two finite extensions of a field k contained in one same field, and assume that K/k is Galois. Then there is a one-to-one correspondence between the subextensions of KF/F and the subextensions of $K/(K \cap F)$ that is given by the following bijective maps (one is the inverse of the other):*

$$\begin{array}{ll} \text{for } F \subseteq Y \subseteq KF\,, & Y \longmapsto Y \cap K\,, \\ \text{for } K \cap F \subseteq X \subseteq K\,, & X \longmapsto XF\,. \end{array}$$

In particular, we have

$$[Y : F] = [Y \cap K : K \cap F] \quad \text{and} \quad [X : K \cap F] = [XF : F]\,.$$

Proof. This is a small exercise in Galois theory which we leave to the reader. □

2.4. **Computing a single Kummer degree.** We now present a strategy to compute a single Kummer degree, which is different from the one that we develop in this paper. This allows us to compute all Kummer degrees because the results in [10] reduce the computation of all Kummer degrees to the computation of finitely many such degrees. However this strategy is more cumbersome than the one that we develop in this work.

Remark 4. *Let K be a quadratic field, and let $\alpha_1, \dots, \alpha_r$ be elements of $K^\times$. If $n_1, \dots, n_r$ are positive integers and m is a positive common multiple of them, then one can compute the degree of $K(\zeta_m, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r})$ over K. By* [2, Lemma 19.2.1] *K is a presented field, and by* [2, Lemma 19.2.2] *K has a splitting algorithm because $\mathbb{Q}$ does by* [2, Lemma 19.1.3]. *By* [2, Lemma 19.3.2] *it follows that given $f \in K[x]$ with splitting field L one can compute the Galois group of L/K as a permutation group over the roots of $f(x)$: it then suffices to apply this to*

$$f(x) = (x^m - 1) \prod_{i=1}^{r} (x^{n_i} - \alpha_i) .$$

Notice that the above strategy can be applied as soon as K is a number field presented through the minimal polynomial of a generator over $\mathbb{Q}$. A similar strategy allows us to compute the cyclotomic degree $[K(\zeta_m) : K]$, so we can also compute the degree of $K(\zeta_m, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_r]{\alpha_r})$ over $K(\zeta_m)$.

3. Quadratic subextensions inside cyclotomic fields

The following lemma is a criterion to determine whether the square root of an element of a quadratic number field lies in a cyclotomic extension of $\mathbb{Q}$.

Lemma 5. *Let K be a quadratic number field, and let $\alpha \in K^\times$. Then $K(\sqrt{\alpha})$ is contained in a cyclotomic extension of $\mathbb{Q}$ if and only if the norm $N_{K/\mathbb{Q}}(\alpha)$ is a square in K.*

Proof. The first condition means that $K(\sqrt{\alpha})/\mathbb{Q}$ is abelian, and the statement is evident if $K(\sqrt{\alpha}) = K$. Now suppose that $K(\sqrt{\alpha})/\mathbb{Q}$ has degree 4, and notice that this extension is abelian if and only if it is normal. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ containing K. Let σ be an automorphism in $\mathrm{Gal}(K|\mathbb{Q})$ and denote by $\tilde{\sigma}$ a field homomorphism from $K(\sqrt{\alpha})$ to $\overline{\mathbb{Q}}$ extending σ. If σ is the identity, then $\tilde{\sigma}(\sqrt{\alpha}) = \pm\sqrt{\alpha} \in K(\sqrt{\alpha})$. Now let σ be the non-trivial automorphism in $\mathrm{Gal}(K|\mathbb{Q})$. To prove the statement we are left to show that $\tilde{\sigma}(\sqrt{\alpha}) \in K(\sqrt{\alpha})$ if and only if $N_{K/\mathbb{Q}}(\alpha) = \alpha \cdot \sigma(\alpha)$ is a square in K. If the latter condition holds, then $K(\sqrt{\sigma(\alpha)}) = K(\sqrt{\alpha})$ and we have $\tilde{\sigma}(\sqrt{\alpha}) = \pm\sqrt{\sigma(\alpha)} \in K(\sqrt{\alpha})$. If the former condition holds, then the elements $\tilde{\sigma}(\sqrt{\alpha}) = \pm\sqrt{\sigma(\alpha)}$ and $\sqrt{\alpha}$ generate the same extension of K, which implies by Kummer theory that the product $\sigma(\alpha) \cdot \alpha$ is a square in K. □

If K is a quadratic number field, then a quadratic extension of K which is abelian over $\mathbb{Q}$ is either biquadratic or quartic cyclic. If it is biquadratic, then it is of the form $K(\sqrt{b})$ for some squarefree integer b. The conductor of $K(\sqrt{b})$ over $\mathbb{Q}$ is the least common multiple of the conductors of K and of $\mathbb{Q}(\sqrt{b})$ (in particular, there are only finitely many biquadratic fields with a given conductor). So if $K = \mathbb{Q}(\sqrt{d})$ for some squarefree integer d, then the odd part of the conductor of $K(\sqrt{b})$ is the odd part of $[b, d]$ while the 2-part of the conductor divides 8: it is 8 if and only if b or d are even, it is 1 if both b and d are congruent to 1 modulo 4 and it is 4 otherwise. We can also easily determine the integers $n \geqslant 1$ such that $K(\sqrt{b}) \subseteq K(\zeta_n)$:

Lemma 6. *Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer, and let $\alpha \in K$ be such that $K(\sqrt{\alpha})$ is biquadratic. Then there is an integer b such that $K(\sqrt{\alpha}) = K(\sqrt{b})$ (in particular b and bd are not squares in $\mathbb{Z}$). Then for $n \geqslant 1$ we have $\sqrt{\alpha} \in K(\zeta_n)$ if and only if $\sqrt{b}$ or $\sqrt{bd}$ are in $\mathbb{Q}(\zeta_n)$ (which means that n is a multiple of the conductor of $\mathbb{Q}(\sqrt{b})$ or of the conductor of $\mathbb{Q}(\sqrt{bd})$).*

Proof. The first assertion and the 'if' implication are clear, so let n be such that $\sqrt{\alpha} \in K(\zeta_n)$. We may suppose that $\sqrt{b} \notin \mathbb{Q}(\zeta_n)$ and in particular $K \not\subseteq \mathbb{Q}(\zeta_n)$. Then by Proposition 3 the intersection $K(\sqrt{b}) \cap \mathbb{Q}(\zeta_n)$ is quadratic over $\mathbb{Q}$, so it is of the form $\mathbb{Q}(\sqrt{a})$ for some squarefree integer a. One can easily check that $K(\sqrt{b})^{\times 2} \cap \mathbb{Q}^\times = \langle \mathbb{Q}^{\times 2}, a, d \rangle$. Since b is not a square in $\mathbb{Q}(\sqrt{a})$, it is not in $\langle \mathbb{Q}^{\times 2}, a \rangle$. We deduce that $\sqrt{bd}$ is in $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\zeta_n)$. □

There are only finitely many quartic cyclic number fields extensions with a given conductor, and their generators are as in Theorem 1. Recall that the 2-part of the conductor of a quartic cyclic number field divides 16.

Theorem 7. *Let K be a quadratic field, and let $\alpha \in K^\times$ be such that $K(\sqrt{\alpha})$ is biquadratic or quartic cyclic. Then the odd part of the conductor of $K(\sqrt{\alpha})$ is the product of all odd primes that ramify in $K(\sqrt{\alpha})$, namely the odd primes p which divide the conductor of K or such that the primes $\mathfrak{p}$ of K over p are such that $v_\mathfrak{p}(\alpha)$ is odd.*

Proof. The odd primes that ramify in $K(\sqrt{\alpha})$ are those odd primes p which ramify in K (equivalently, they divide the conductor of K) or such that the primes $\mathfrak{p}$ of K over p ramify in $K(\sqrt{\alpha})$ (equivalently, by Lemma 2, $v_\mathfrak{p}(\alpha)$ is odd). If an odd prime ramifies in $K(\sqrt{\alpha})$ then it clearly divides the conductor of this extension. Now suppose that some odd prime p divides the conductor c of $K(\sqrt{\alpha})$, and recall that the odd part of c is squarefree because the degree of $K(\sqrt{\alpha})/K$ is 4. Then we have $K(\sqrt{\alpha}, \zeta_{c/p}) = L(\zeta_{c/p})$ for some non-trivial subextension L of $\mathbb{Q}(\zeta_p)$. Since L is ramified at p while $\mathbb{Q}(\zeta_{c/p})$ is not, we deduce that $K(\sqrt{\alpha}, \zeta_{c/p})/\mathbb{Q}(\zeta_{c/p})$ is ramified at the primes above p. This implies that p ramifies in $K(\sqrt{\alpha})$. □

Lemma 8. *Let $K = \mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a squarefree integer, and let $\alpha \in K$ be such that $K(\sqrt{\alpha})$ is quartic cyclic. Then we have $K(\sqrt{\alpha}) = \mathbb{Q}(\sqrt{\alpha})$, and we have $\sqrt{\alpha} \in K(\zeta_n)$ if and only if $\sqrt{\alpha} \in \mathbb{Q}(\zeta_n)$.*

Proof. Since $K(\sqrt{\alpha})$ is quartic cyclic, then we cannot have $\alpha \in \mathbb{Q}$ and hence $\mathbb{Q}(\sqrt{\alpha})$ contains K. The 'if' part of the second assertion is clear, so fix n such that $\sqrt{\alpha} \in K(\zeta_n)$ and suppose that $\sqrt{\alpha} \notin \mathbb{Q}(\zeta_n)$. Then $K(\zeta_n)/\mathbb{Q}(\zeta_n)$ is quadratic: we deduce that $K(\sqrt{\alpha}) \cap \mathbb{Q}(\zeta_n)$ is a quadratic field, contradicting that $K \not\subseteq \mathbb{Q}(\zeta_n)$. □

4. Cubic extensions of $\mathbb{Q}(\zeta_3)$

We determine Kummer generators for all the cubic extensions of $\mathbb{Q}(\zeta_3)$ which are contained in a cyclotomic extension of $\mathbb{Q}(\zeta_3)$. For every $n \geqslant 2$ the only cubic subextension of $\mathbb{Q}(\zeta_{3^n})/\mathbb{Q}(\zeta_3)$ is $\mathbb{Q}(\zeta_9)$, whose Kummer generator is ζ_3. Moreover, if $m = 3^n m'$, where m' is coprime to 3 and $n \geqslant 0$, then a cubic subextension of $\mathbb{Q}(\zeta_{3m})/\mathbb{Q}(\zeta_3)$ is contained in $\mathbb{Q}(\zeta_{3M})$, where M is the product of the prime divisors p of m' such that $p \not\equiv 2 \pmod 3$.

Theorem 9. *Let $M = \prod_{i=1}^{t} p_i$, where the p_i's are distinct prime numbers such that $p_i \not\equiv 2 \pmod 3$. Then $\mathbb{Q}(\zeta_{3M})/\mathbb{Q}(\zeta_3)$ has $(3^t - 1)/2$ cubic subextensions, and their Kummer generators are the elements*

$$\gamma := \prod_{\substack{i \in I \\ \emptyset \neq I \subseteq \{1,\dots,t\}}} \beta_{p_i}^{e_i}, \tag{2}$$

where $e_i \in \{1, 2\}$, and where $\beta_3 = \zeta_3$ and $\beta_{p_i} = \pi_i p_i$ is as in [5, Theorem 1] *for $p_i \equiv 1 \pmod 3$ (notice that $\prod_I \beta_{p_i}^{e_i}$ and $\prod_I \beta_{p_i}^{3-e_i}$ give the same Kummer extension). The positive integers m such that $\sqrt[3]{\gamma} \in \mathbb{Q}(\zeta_{3m})$ are the positive multiples of $\prod_I p_i$.*

Proof. Notice that the third roots of two elements α_1, α_2 in $\mathbb{Q}(\zeta_3)^\times$ generate the same extension of $\mathbb{Q}(\zeta_3)$ if and only if $\alpha_1 \cdot \alpha_2^2$ or $\alpha_1 \cdot \alpha_2$ is a cube in $\mathbb{Q}(\zeta_3)$.

If γ is as in (2), then $\sqrt[3]{\gamma}$ generates a cubic extension of $\mathbb{Q}(\zeta_3)$ inside $\mathbb{Q}(\zeta_{3M})$ by [5, Theorem 1]. Indeed, ζ_3 and ζ_3^2 are not cubes in $\mathbb{Q}(\zeta_3)$, whereas for $p_i \neq 3$, the prime ideals appearing in the factorization of the fractional ideal (β_{p_i}) all lie above p_i, and the element β_{p_i} is not a cube (as it generates a non-trivial Kummer extension of $\mathbb{Q}(\zeta_3)$).

We have thus proven that there are $(3^t-1)/2$ distinct cubic subextensions of $\mathbb{Q}(\zeta_{3M})/\mathbb{Q}(\zeta_3)$ generated by the elements (2). We now show that $\mathbb{Q}(\zeta_{3M})/\mathbb{Q}(\zeta_3)$ has exactly $(3^t-1)/2$ cubic subextensions. The Galois group G of $\mathbb{Q}(\zeta_{3M})/\mathbb{Q}(\zeta_3)$ is the product of t cyclic groups of order divisible by 3. The quotient map to a quotient of order 3 factors through $G/G^3 \simeq (\mathbb{F}_3)^t$, which is an $\mathbb{F}_3$-vector space. Then the kernels of the surjective

maps $(\mathbb{F}_3)^t \to \mathbb{F}_3$ are the vector subspaces of codimension 1, and hence by orthogonality w.r.t. the standard scalar product (after having fixed a basis) they correspond to the subspaces of dimension 1 of $(\mathbb{F}_3)^t$, which are $(3^t-1)/2$.

Let $m_0 := \prod_I p_i$. Replacing M with m_0, by the first part of the statement we have $\sqrt[3]{\gamma} \in \mathbb{Q}(\zeta_{3m_0})$. Now suppose that $\sqrt[3]{\gamma} \in \mathbb{Q}(\zeta_{3m})$: we have to prove that $p_i \mid m$ for every $i \in I$. If $p_i \neq 3$, then p_i ramifies in $\mathbb{Q}(\zeta_3, \sqrt[3]{\gamma})$ by Lemma 2 and we conclude. If $3 \mid m_0$, then we have $\mathbb{Q}(\zeta_{3(m_0/3)}, \sqrt[3]{\gamma}) = \mathbb{Q}(\zeta_{3(m_0/3)}, \sqrt[3]{\zeta_3}) = \mathbb{Q}(\zeta_{3m_0})$. Thus $\zeta_9 \in \mathbb{Q}(\zeta_{3m})$ and $3 \mid m$. □

5. Quadratic and quartic cyclic extensions of $\mathbb{Q}(\zeta_4)$

We determine Kummer generators for all the quadratic and quartic cyclic extensions of $\mathbb{Q}(\zeta_4)$ which are contained in a cyclotomic extension of $\mathbb{Q}(\zeta_4)$.

The integer 2 is a Kummer generator for the quadratic extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}(\zeta_4)$, which is the only quadratic extension of $\mathbb{Q}(\zeta_4)$ inside $\mathbb{Q}(\zeta_{2^\infty})$. Moreover, if p is an odd prime, then p is a Kummer generator for the quadratic extension of $\mathbb{Q}(\zeta_4)$ inside $\mathbb{Q}(\zeta_{4p})$.

Any quadratic extension of $\mathbb{Q}(\zeta_4)$ inside $\mathbb{Q}(\zeta_\infty)$ is biquadratic: the 2-part of its conductor is either 4 or 8 while the odd part of its conductor is squarefree.

Proposition 10. *Given a squarefree integer $M \geqslant 2$, the divisors of M greater than 1 are Kummer generators for the quadratic extensions of $\mathbb{Q}(\zeta_4)$ inside $\mathbb{Q}(\zeta_{4M})$. Moreover, if m is such a divisor, then the positive integers n such that $\sqrt{m} \in \mathbb{Q}(\zeta_{4n})$ are the positive multiples of m.*

Proof. The last assertion follows from the fact that the conductor of $\mathbb{Q}(\sqrt{m})$ is $|m|$ or $|4m|$ if m is odd, and $|8m|$ otherwise. This also proves that square roots of distinct divisors of M greater than 1 generate distinct quadratic extensions of $\mathbb{Q}(\zeta_4)$. So if t is the number of prime factors of M, then we have found $2^t - 1$ quadratic subextensions of $\mathbb{Q}(\zeta_{4M})/\mathbb{Q}(\zeta_4)$. We conclude by proving that there are at most $2^t - 1$ quadratic subextensions: the Galois group of such an extension is a quotient of order 2 of $\mathrm{Gal}(\mathbb{Q}(\zeta_{4M})|\mathbb{Q}(\zeta_4))$, and such a quotient factors through $(\mathbb{Z}/2\mathbb{Z})^t$. □

Now we study the subfields of $\mathbb{Q}(\zeta_\infty)$ which are quartic cyclic over $\mathbb{Q}(\zeta_4)$. The only such field contained in $\mathbb{Q}(\zeta_{2^\infty})$ is $\mathbb{Q}(\zeta_{16})$, and a Kummer generator for it is ζ_4. Moreover, any such field is contained in $\mathbb{Q}(\zeta_{16M})$ for some odd squarefree integer M.

Theorem 11. *Let $M > 1$ be an odd squarefree integer, and consider the following two sets of prime numbers:*

$$S_1 = \{p \mid M : p \equiv 1 \pmod 4\} \qquad S_3 = \{p \mid M : p \equiv 3 \pmod 4\}.$$

The extension $\mathbb{Q}(\zeta_{16M})/\mathbb{Q}(\zeta_4)$ has $(2\cdot 4^{\sharp S_1}-2^{\sharp S_1})2^{\sharp S_3}$ quartic cyclic subextensions. Kummer generators for these extensions are the elements

$$\gamma := \zeta_4^{x_2}\cdot\prod_{p\in S_1}\gamma_p^{x_p}\cdot\prod_{p\in S_3}p^{y_p} \tag{3}$$

for some choice of $x_2, x_p \in \{0,1,2,3\}$ and $y_p\in\{0,2\}$ such that x_2, x_p are not all even, and where γ_p is as in [5, Theorem 2] *(notice that γ^3 is, up to a fourth power, again of the form* (3) *and it generates the same Kummer extension as γ). The positive integers n such that $\sqrt[4]{\gamma}\in\mathbb{Q}(\zeta_{4n})$ are the positive multiples of*

$$\mathrm{ord}(\zeta_4^{x_2})\cdot\prod_{p\in S_1:x_p\neq 0}p\cdot\prod_{p\in S_3:y_p\neq 0}p\,, \tag{4}$$

where ord *denotes the order of a root of unity.*

Proof. Notice that we have $\sqrt[4]{\gamma}\in\mathbb{Q}(\zeta_{4n})$ where n is as in (4) because $\sqrt[4]{\gamma_p}$ for $p\in S_1$ such that $x_p\neq 0$ and $\sqrt{p}$ for $p\in S_3$ such that $y_p\neq 0$ are contained in this field. To conclude the proof of the last assertion we first make sure (with a ramification argument as in the proof of Theorem 9) that the odd part of (4) divides n, then it is clear that the fourth root of $\zeta_4^{x_2}$ lies in $\mathbb{Q}(\zeta_{4n})$ if and only if n is a positive multiple of the order of $\zeta_4^{x_2}$.

We have $(4^{\sharp S_1+1}-2^{\sharp S_1+1})2^{\sharp S_3}$ elements as in (3) where the exponents x_2 and x_p for $p\in S_1$ are not all even. These elements are all distinct modulo fourth powers in $\mathbb{Q}(\zeta_4)$, and for each of them there is exactly another one (which coincides with its cube modulo fourth powers) which generates the same quartic extension. Therefore we find $(2\cdot 4^{\sharp S_1}-2^{\sharp S_1})2^{\sharp S_3}$ quartic cyclic extensions. We claim that this is the number of quartic cyclic subextensions of $\mathbb{Q}(\zeta_{16M})/\mathbb{Q}(\zeta_4)$, which is the same as the number of cyclic quotients of order 4 of the greatest subgroup G of $\mathrm{Gal}(\mathbb{Q}(\zeta_{16M})|\mathbb{Q}(\zeta_4))$ of exponent 4, which is $G=(\mathbb{Z}/4\mathbb{Z})^{\sharp S_1+1}\times(\mathbb{Z}/2\mathbb{Z})^{\sharp S_3}$. Since G is a finite abelian group, it is isomorphic to its Pontryagin dual $\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$. Cyclic subgroups of G of order 4 correspond to cyclic quotients of order 4 of the dual but, because of the isomorphism, they are in bijection with the cyclic quotients of order 4 of G. The number of cyclic subgroups of order 4 can be computed as the number of elements of G of order dividing 4 minus the number of elements of order at most 2 divided by 2, which gives the desired formula. □

6. Intersection of cyclotomic-Kummer extensions with $K(\zeta_\infty)$

Let ℓ be a prime number. To study the ℓ-adelic failure we will apply the following result. First recall that any element $\alpha\in K^\times$ which is not a root of unity can be written as $\alpha=\zeta\beta^{\ell^d}$ where ζ is a root of unity of order ℓ^h, β is strongly ℓ-indivisible in K, and $d\geqslant 0$. Moreover, setting $t:=v_\ell(\sharp\mu_K)$, by [1, Sect. 7.1] we may suppose that $h=0$ or $t\geqslant h>t-d$, and in this case the parameters d,h are unique.

Theorem 12. *Let ℓ be a prime number and let K be a number field such that $t := v_\ell(\sharp\mu_K) \in \{1,2\}$. Let $\alpha \in K^\times$ be not a root of unity, and write $\alpha = \zeta_{\ell^h}\beta^{\ell^d}$ where $\beta \in K$ is strongly ℓ-indivisible, $d \geqslant 0$, and $h = 0$ or $t - d < h \leqslant t$. Let $n \geqslant 1$. We have*

$$K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha}) \cap K(\zeta_\infty) = K(\zeta_{\ell^{n+h}}) \qquad \text{for } 1 \leqslant n \leqslant d\,.$$

If $\sqrt[\ell]{\beta} \notin K(\zeta_\infty)$, then we have:

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

If $\sqrt[\ell]{\beta} \in K(\zeta_\infty)$ and $\sqrt[\ell^2]{\beta} \notin K(\zeta_\infty)$, then we have:

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

If $\sqrt[\ell^2]{\beta} \in K(\zeta_\infty)$ and $\sqrt[\ell^3]{\beta} \notin K(\zeta_\infty)$ (which happens only if $t = 2$), then we have:

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

Proof. Let $K' = K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha}) \cap K(\zeta_\infty)$ and $L = K(\zeta_{\ell^n})$. All the fields in the statement are contained in K', so we only need to prove the reverse inclusions. The field K' is a finite abelian extension of L contained in $L(\sqrt[\ell^n]{\alpha})$ of exponent dividing ℓ^n and hence by Kummer theory it is of the form $L(\sqrt[\ell^n]{\gamma})$ for some $\gamma \in \langle \alpha, L^{\times \ell^n} \rangle$. Therefore it is sufficient to determine under which conditions $L(\sqrt[\ell^n]{\alpha^{\ell^e}}) \subseteq K(\zeta_\infty)$, where $e \geqslant 0$. Let t be as in the statement and notice that by Schinzel's theorem on abelian radical extensions [8, Theorem 3.3] the element $\sqrt[\ell^{t+1}]{\beta}$ is never contained in $K(\zeta_\infty)$.

First of all, with $\alpha = \zeta_{\ell^h}\beta^{\ell^d}$ and d, h as in the statement, if $n \leqslant d$, then $\sqrt[\ell^n]{\alpha}$ equals $\zeta_{\ell^{n+h}}$ times an element of K. From now on suppose that $n \geqslant d+1$.

Assume that $\alpha = \beta^{\ell^d}$. If $\sqrt[\ell]{\beta} \notin K(\zeta_\infty)$, then $K' = L$. If $\sqrt[\ell]{\beta} \in K(\zeta_\infty)$ and $\sqrt[\ell^2]{\beta} \notin K(\zeta_\infty)$, then $\sqrt[\ell]{\beta}$ generates K' over L. If $\sqrt[\ell^2]{\beta} \in K(\zeta_\infty)$, then $\sqrt[\ell]{\beta}$ generates K' over L for $n = d+1$, and $\sqrt[\ell^2]{\beta}$ generates K' over L for $n \geqslant d+2$.

Next suppose that $\alpha = \zeta_\ell\beta^{\ell^d}$. If $\sqrt[\ell]{\beta} \notin K(\zeta_\infty)$, then $K' = L$. If $\sqrt[\ell]{\beta} \in K(\zeta_\infty)$, then for $n = d+1$ we have that $\sqrt[\ell^n]{\alpha} = \zeta_{\ell^{n+1}}\sqrt[\ell]{\beta}$ lies in $K(\zeta_\infty)$, while for $n \geqslant d+2$ and $\sqrt[\ell^2]{\beta} \notin K(\zeta_\infty)$ there is a power of $\sqrt[\ell^n]{\alpha}$ which equals $\sqrt[\ell]{\beta}$ times an element of μ_{ℓ^n} and which generates K' over L. If $\sqrt[\ell^2]{\beta} \in K(\zeta_\infty)$, then we have that K' is generated over L by $\zeta_{\ell^{n+1}}\sqrt[\ell^2]{\beta}$ for $n = d+2$, whereas for $n \geqslant d+3$ there is a power of $\sqrt[\ell^n]{\alpha}$ which equals $\sqrt[\ell^2]{\beta}$ times an element of μ_{ℓ^n} and which generates K' over L.

We now deal with the case $\alpha = \zeta_{\ell^2}\beta^{\ell^d}$ ($t = 2$). If $n = d + 1$, then $\sqrt[\ell^n]{\alpha} = \zeta_{\ell^{n+2}}\sqrt[\ell]{\beta}$, which generates K' over L if $\sqrt[\ell]{\beta} \in K(\zeta_\infty)$, else its ℓ-th power still lies in $K(\zeta_\infty)$. Let $n \geqslant d + 2$. If $\sqrt[\ell]{\beta} \notin K(\zeta_\infty)$, then $K' = L$. If $\sqrt[\ell]{\beta} \in K(\zeta_\infty)$ and $\sqrt[\ell^2]{\beta} \notin K(\zeta_\infty)$, then $\sqrt[\ell^n]{\alpha} = \zeta_{\ell^{n+2}}\sqrt[\ell^{n-d}]{\beta}$ has its ℓ-th power in $K(\zeta_\infty)$ for $n = d+2$, and some higher power equal to $\sqrt[\ell]{\beta}$ in $K(\zeta_\infty)$ for $n \geqslant d + 3$. If $\sqrt[\ell^2]{\beta} \in K(\zeta_\infty)$, then $\sqrt[\ell^n]{\alpha}$ lies in $K(\zeta_\infty)$ for $n = d + 2$, it has its ℓ-th power in $K(\zeta_\infty)$ for $n = d + 3$, and some higher power equal to $\sqrt[\ell^2]{\beta}$ in $K(\zeta_\infty)$ for $n \geqslant d + 4$. □

Remark 13. *In the cases of Theorem 12 notice that* $K(\zeta_{\ell^n}, \sqrt[\ell^n]{\alpha}) \cap K(\zeta_\infty)/K(\zeta_{\ell^n})$ *has as generator an element of the form* $\zeta_{\ell^{n+x}}\sqrt[\ell]{\beta}$ *only when* $n + x \geqslant t + 2$*, and of the form* $\zeta_{\ell^{n+x}}\sqrt[\ell^2]{\beta}$ *only when* $n + x \geqslant 5$ *(and* $t = 2$*).*

7. The procedure to compute the Kummer degrees

Let K be a quadratic number field, and let $\alpha \in K$ be an element which is w.l.o.g. neither 0 nor a root of unity. Let $M, N \geqslant 1$ with $N \mid M$ and write $n = v_\ell(N)$, where ℓ is a fixed prime number. As mentioned in the Introduction, the ratio

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

can be decomposed in terms of the ℓ-adic failure $C(\ell^n, \ell^n)$ and the ℓ-adelic failure

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

where ℓ runs through the prime divisors of N.

Remark 14. *The numbers* $C(\ell^n, \ell^n)$ *can be computed for* all *primes* ℓ *and* all $n \geqslant 1$ *by the explicit formulas in* [7, Section 3]*, and they are equal to* 1 *for almost all* ℓ *(see for instance* [8, Lemma 3.2]*). In particular, the computation of the* ℓ*-adic failure depends on the* ℓ*-divisibility of the considered element. Therefore we need to check if* α *is an* ℓ*-th power in* K*, up to a root of unity in* K*. Notice that, for* K *and* α *fixed, the finitely many prime numbers* ℓ *for which* $C(\ell^n, \ell^n)$ *might be greater than* 1 *can be determined effectively (see* [8, Section 2]*).*

We are left to compute the ℓ-adelic failure $B(M, \ell^n)$, for all M and n, where $\ell^n \mid M$, which equals 1 for all but finitely many primes ℓ (cf. [8, Lemma 3.5]). In particular, we have $B(M, \ell^n) = 1$ if $\zeta_\ell \notin K$.

7.1. **The 2-adelic failure for the quadratic fields different from $\mathbb{Q}(\zeta_4)$.** Let K be a quadratic field different from $\mathbb{Q}(\zeta_4)$. The only roots of unity in K of order a power of 2 are ± 1. Studying the 2-adelic failure for α in K amounts to computing all degrees

$$[K(\zeta_{2^n}, \sqrt[2^n]{\alpha}) \cap K(\zeta_M) : K(\zeta_{2^n})] \tag{5}$$

where $n, M \geqslant 1$ and $v_2(M) \geqslant n$, and where without loss of generality $v_2(M) \neq 1$. We may assume that $\alpha = \pm\beta^{2^d}$ with $\beta \in K$ strongly 2-indivisible. By Theorem

12 (applied with $\ell = 2$, $t = 1$) and Propositions 15 and 16 we may suppose that α is strongly 2-indivisible. Then by Schinzel's Theorem [8, Theorem 3.3] we have $\sqrt[4]{\alpha} \notin \mathbb{Q}(\zeta_\infty)$ hence (5) is either 1 or 2. We are left to check whether $\sqrt{\alpha} \in \mathbb{Q}(\zeta_\infty)$ by making use of Lemma 5, and if so we may find all the positive integers M such that $K(\sqrt{\alpha}) \subseteq K(\zeta_M)$ by Lemmas 6 and 8. Notice that in the following statement the condition that d is positive is necessary to ensure that K is contained in a quartic cyclic number field:

Proposition 15. *Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a positive and squarefree integer. Let $\beta \in K$ be a strongly 2-indivisible element such that $K(\sqrt{\beta}) \subseteq \mathbb{Q}(\zeta_\infty)$ is quartic cyclic over $\mathbb{Q}$. Let N be the conductor of $K(\sqrt{\beta})$. For $x \geqslant 3$ the integers $M \geqslant 1$ such that $\zeta_{2^x}\sqrt{\beta} \in K(\zeta_M)$ are the positive multiples of $[2^x, N]$ and the following integers: if $d \equiv 1 \bmod 4$ and $x = 3$ and $8 \mid N$, the positive multiples of $N/2$; if $d \equiv 2 \bmod 8$ and $x = 4$, the positive multiples of $N/4$.*

Proof. We clearly have $\zeta_{2^x}\sqrt{\beta} \in K(\zeta_M)$ if $[2^x, N]$ divides M. Call n the odd part of N.

If $d \equiv 1 \bmod 4$ and $8 \mid N$ (in this case $v_2(N) = 3$ by Theorem 1), then $\sqrt{\beta}$ and ζ_8 both generate the quadratic extension $\mathbb{Q}(\zeta_{8n})/\mathbb{Q}(\zeta_{4n})$ hence $\zeta_8\sqrt{\beta} \in K(\zeta_{N/2})$. If $d \equiv 2 \bmod 8$, then $v_2(N) = 4$ (again by Theorem 1) and $K(\zeta_{4n}) = \mathbb{Q}(\zeta_{8n})$: since ζ_{16} and $\sqrt{\beta}$ both generate the quadratic extension $\mathbb{Q}(\zeta_{16n})/\mathbb{Q}(\zeta_{8n})$ we deduce that $\zeta_{16}\sqrt{\beta} \in K(\zeta_{4n})$.

Now let M be an integer such that $\zeta_{2^x}\sqrt{\beta} \in K(\zeta_M)$, and notice that by Lemma 8 we have $n \mid M$ because $\sqrt{\beta} \in K(\zeta_{16M})$. Moreover, we must have $\zeta_{2^{x-1}} \in K(\zeta_M)$.

If $x \geqslant 5$, then we obtain that $2^{x-1} \mid M$. However, $\zeta_{2^x}\sqrt{\beta}$ is not contained in $K(\zeta_{2^{x-1}ny}) = \mathbb{Q}(\zeta_{2^{x-1}ny})$ where $y \geqslant 1$ is any odd integer, as this field contains $\sqrt{\beta}$ but not ζ_{2^x}: we deduce that $2^x n \mid M$. The same holds if $d \equiv 1 \bmod 4$ and either $x = 4$ or $x = 3$ and $8 \nmid N$. If $d \equiv 1 \bmod 4$ and $x = 3$ and $v_2(N) = 3$, then $\zeta_4 \in K(\zeta_M)$ implies that $4 \mid M$ hence $(N/2) \mid M$.

Now suppose that $d \equiv 2 \bmod 8$ and hence $v_2(N) = 4$. The element $\zeta_8\sqrt{\beta}$ is not contained in $K(\zeta_{8ny}) = \mathbb{Q}(\zeta_{8ny})$ where $y \geqslant 1$ is any odd integer, as this field contains ζ_8 but not $\sqrt{\beta}$: we deduce that $N \mid M$ for $x = 3$ (in particular $8 \mid M$). Finally, let $x = 4$. We have $(d/2) \equiv 1 \bmod 4$ and from $n \mid M$ we deduce $(d/2) \mid M$. Thus $K(\zeta_M) \subseteq \mathbb{Q}(\sqrt{2}, \zeta_M)$ and we must have $4 \mid M$, else we would not have $\zeta_8 \in K(\zeta_M)$. □

Proposition 16. *Let $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a squarefree integer. Let $\beta \in K$ be strongly 2-indivisible and such that $K(\sqrt{\beta})$ is biquadratic over $\mathbb{Q}$. Let m be a squarefree integer (which we assume to be odd if d is even) such that $K(\sqrt{\beta}) = K(\sqrt{m})$, and set m' to be the squarefree part of md.*

(1) For $x \geqslant 4$ the integers $M \geqslant 1$ such that $\zeta_{2^x}\sqrt{\beta} \in K(\zeta_M)$ are the positive multiples of $[2^x, m]$ or of $[2^x, m']$.
(2) The integers $M \geqslant 1$ such that $\zeta_8\sqrt{\beta} \in K(\zeta_M)$ are those such that:
$8m$ or $8m'$ divide M, if m and d are odd;
$2m$ or $2m'$ divide M, if m is even and $d \equiv 1 \bmod 4$;
$2m$ or $2m'$ or $[m, m']/2$ divide M, if m is even and $d \equiv 3 \bmod 4$;
$8m$ or $2m'$ divide M, if m is odd and d is even.

Proof. Call s the absolute value of $[m, m']$. By assumption we have $K(\sqrt{\beta}) = K(\sqrt{m}) = K(\sqrt{m'})$. Thus for $x \geqslant 3$, if $[2^x, m]$ or $[2^x, m']$ divide M, then $\zeta_{2^x}\sqrt{\beta} \in K(\zeta_M)$. If m is even and d is odd, then suppose that $2m$ or $2m'$ divide M: we have $\zeta_8\sqrt{\beta} \in K(\zeta_M)$ because $\zeta_8\sqrt{m} \in \mathbb{Q}(\zeta_{2|m|})$ and $\zeta_8\sqrt{m'} \in \mathbb{Q}(\zeta_{2|m'|})$ as $\zeta_8\sqrt{2} = 1 + \zeta_4$ and m, m' are even. If m is even and $d \equiv 3 \bmod 4$, then $\zeta_8\sqrt{\beta} \in K(\zeta_{s/2})$ because this field equals $K(\zeta_{2|m|})$. If m is odd and d is even, then m' is even: supposing that $2m'$ divides M, then $4 \mid M$: we then have $\zeta_8 \in K(\zeta_M)$ and $\sqrt{\beta} \in K(\zeta_M)$ hence $\zeta_8\sqrt{\beta} \in K(\zeta_M)$.

Now let M be an integer such that $\zeta_{2^x}\sqrt{\beta} \in K(\zeta_M)$. Since $\sqrt{\beta} \in K(\zeta_{[2^x,M]})$, by Lemma 6 we obtain that $m \mid 2M$ or $m' \mid 2M$ (as m and m' are squarefree).

If $x \geqslant 4$, then we cannot have that $\zeta_{2^x}\sqrt{\beta}$ is contained in $K(\zeta_{[2^{x-1},s]y}) \subseteq \mathbb{Q}(\zeta_{2^{x-1}}, \zeta_{4sy})$ where $y \geqslant 1$ is any odd integer, as the latter field contains $\sqrt{\beta}$ but not ζ_{2^x}. Hence we must have $2^x \mid M$. This concludes the proof of (1).

If m and d are odd, then $\zeta_8\sqrt{\beta}$ is not contained in $K(\zeta_4, \zeta_{sy}) \subseteq \mathbb{Q}(\zeta_{4sy})$, where $y \geqslant 1$ is any odd integer, as the latter field contains $\sqrt{\beta}$ but not ζ_8: thus we must have $8 \mid M$ and we conclude.

If m is even and $d \equiv 1 \bmod 4$, then $\zeta_8\sqrt{\beta}$ is not contained in $K(\zeta_{sy})$ where $y \geqslant 1$ is any odd integer because this field is contained in $\mathbb{Q}(\sqrt{2}, \zeta_{sy})$ or $\mathbb{Q}(\sqrt{-2}, \zeta_{sy})$ so it does not contain ζ_4: thus $4 \mid M$ and we deduce that $2m \mid M$ or $2m' \mid M$.

Now suppose that m is even and $d \equiv 3 \bmod 4$. If $v_2(M) \geqslant 2$, then $2m$ or $2m'$ divides M. If $v_2(M) \leqslant 1$ (w.l.o.g. $v_2(M) = 0$), then $\zeta_4 \in K(\zeta_M)$ implies by Lemma 6 that $\sqrt{-d} \in \mathbb{Q}(\zeta_M)$ and hence $d \mid M$. Thus the odd part of both m and m' divides M, giving $(s/2) \mid M$.

Finally suppose that m is odd and d is even. Notice that $\zeta_8\sqrt{\beta}$ is not contained in $K(\zeta_{sy})$, where y is any odd integer, because this field does not contain ζ_4. Thus $4 \mid M$. If the odd part of m' divides M we deduce that $2m' \mid M$. If m divides M, then we have $\sqrt{\beta} \in K(\zeta_M)$, hence $\zeta_8 \in K(\zeta_M)$. We conclude because, if $8m \nmid M$, then $M = 4my$ for some odd integer y hence $m' \mid 2my$: indeed, we can have $\sqrt{2} \in K(\zeta_{4my})$ only if $d/2$ divides my by Lemma 6. □

Example 17. Let $K = \mathbb{Q}(\sqrt{5})$ and $\alpha = \frac{15+5\sqrt{5}}{2} = \left(-\frac{5+\sqrt{5}}{2}\right)^2$. As can easily be seen by expressing the sine and cosine of $\frac{2\pi}{5}$ in terms of $\sqrt{5}$, we have $K(\sqrt{-\frac{5+\sqrt{5}}{2}}) = \mathbb{Q}(\zeta_5)$. This implies

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

7.2. **The 2-adelic failure for $\mathbb{Q}(\zeta_4)$.** If $\alpha \in \mathbb{Q}(\zeta_4)$, then we want to compute its 2-adelic failure, namely the degrees

$$[\mathbb{Q}(\zeta_4, \sqrt{\alpha}) \cap \mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_4)] \tag{6}$$

for $M \geqslant 1$ and $4 \mid M$, and the degrees

$$[\mathbb{Q}(\zeta_{2^n}, \sqrt[2^n]{\alpha}) \cap \mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_{2^n})] \tag{7}$$

for $n \geqslant 2$ and $M \geqslant 1$ with $v_2(M) \geqslant n$. We may assume that $\alpha = \zeta\beta^{2^d}$, where $\zeta \in \mu_4$ and $\beta \in \mathbb{Q}(\zeta_4)$ is strongly 2-indivisible. By Theorem 12 (applied with $\ell = 2$, $t = 2$) and by Proposition 18 we may reduce to the case where α is strongly 2-indivisible. Then the above degrees divide 4 because by Schinzel's Theorem [8, Theorem 3.3] we have $\sqrt[8]{\alpha} \notin \mathbb{Q}(\zeta_\infty)$.

Notice that in Proposition 18 (2) if $x = 3$, then the conductor of $\mathbb{Q}(\zeta_4, \zeta_8\sqrt[4]{\beta})$ is simply the conductor of $\mathbb{Q}(\zeta_4, \sqrt[4]{-\beta})$ (and $-\beta$ is again strongly 2-indivisible).

Proposition 18. *Let $\beta \in \mathbb{Q}(\zeta_4)$ be strongly 2-indivisible.*

1. *If $\sqrt{\beta} \in \mathbb{Q}(\zeta_\infty)$, let N be the conductor of $\mathbb{Q}(\zeta_4, \sqrt{\beta})$. For $x \geqslant 3$ the conductor of $\mathbb{Q}(\zeta_4, \zeta_{2^x}\sqrt{\beta})$ is $[2^x, N]$, unless $x = v_2(N) = 3$, in which case it is $N/2$.*
2. *If $\sqrt[4]{\beta} \in \mathbb{Q}(\zeta_\infty)$, let N be the conductor of $\mathbb{Q}(\zeta_4, \sqrt[4]{\beta})$. For $x \geqslant 4$ the conductor of $\mathbb{Q}(\zeta_4, \zeta_{2^x}\sqrt[4]{\beta})$ is $[2^x, N]$, unless $x = v_2(N) = 4$: in this case one of the conductors of $\mathbb{Q}(\zeta_4, \sqrt[4]{\beta\zeta_{16}^4}) = \mathbb{Q}(\zeta_4, \zeta_{16}\sqrt[4]{\beta})$ and $\mathbb{Q}(\zeta_4, \sqrt[4]{\beta\zeta_{16}^{12}})$ is not divisible by 8 while the other is, and the conductor of first field is $N/4$ or $N/2$ accordingly.*

Proof. (1): By Proposition 10 we have $\beta = mk^2$, where m is a positive squarefree integer and $k \in \mathbb{Q}(\zeta_4)$, so that $N = 4m$. If M is the conductor of $\mathbb{Q}(\zeta_{2^x}\sqrt{\beta})$, then $\zeta_{2^{x-1}} \in \mathbb{Q}(\zeta_M)$ hence $2^{x-1} \mid M$. Moreover, M divides $[2^x, N]$ and N divides $[2^x, M]$. If m is odd we deduce that $N \mid M$ and hence $\zeta_{2^x} \in \mathbb{Q}(\zeta_M)$, which gives also $2^x \mid M$. If $x \geqslant 4$, then $8 \mid M$: since $16 \nmid N$ we deduce that $N \mid M$ and may reason as above. If m is even and $x = 3$, then the odd part of m divides M and $4 \mid M$, thus $(N/2) \mid M$. Finally we have $\zeta_8\sqrt{\beta} \in \mathbb{Q}(\zeta_{N/2})$ because $\zeta_8\sqrt{2} \in \mathbb{Q}(\zeta_4)$.

(2): By Theorem 11 we have $N = 2^eN'$ where $e \in \{2, 3, 4\}$ and N' is odd and squarefree. Then M divides $[2^x, N] = 2^xN'$ and $2^{x-2} \mid M$. Moreover, we have

$N' \mid M$ because N divides $[2^x, M]$. If $x \geqslant 5$, then we have $2^{x-1} \mid M$ because 2^{x-1} divides the conductor of $\mathbb{Q}(\zeta_{2^{x-1}}\sqrt{\beta})$ by part (1): thus $N \mid M$, hence $\zeta_{2^x} \in \mathbb{Q}(\zeta_M)$ and we conclude that $2^x \mid M$.

By Theorem 11 there is a unique root of unity $\zeta \in \mu_4$ such that $\sqrt[4]{\beta\zeta} \in \mathbb{Q}(\zeta_{4N'})$. If ζ has order 1 or 2 (which holds whenever $v_2(N) \leqslant 3$), then $\zeta_{16}\sqrt[4]{\beta}$ does not lie in $\mathbb{Q}(\zeta_{8N'})$ hence $M = 16N'$. If $v_2(N) = 4$, then ζ has order 4: from $\zeta = \zeta_{16}^4$ we deduce $\zeta_{16}\sqrt[4]{\beta} \in \mathbb{Q}(\zeta_{4N'})$ and from $\zeta = \zeta_{16}^{12}$ we deduce $\zeta_8\zeta_{16}\sqrt[4]{\beta} \in \mathbb{Q}(\zeta_{4N'})$ hence one of the conductors of the fields in the statement will be $4N'$ and the other will be $8N'$. □

Making use of Lemma 5 we can determine whether $\sqrt{\alpha} \in \mathbb{Q}(\zeta_\infty)$ and, in this case, we may determine the smallest positive integer n such that $\sqrt{\alpha} \in \mathbb{Q}(\zeta_{4n})$. Indeed, by Theorem 7 we can find the odd part m of n. Then to find n we only need to check whether α/m or $\alpha/2m$ is a square in $\mathbb{Q}(\zeta_4)$, see Proposition 10.

Secondly, we check whether $\sqrt[4]{\alpha} \in \mathbb{Q}(\zeta_\infty)$ and if so we find the smallest positive integer N such that $\sqrt[4]{\beta} \in \mathbb{Q}(\zeta_{4N})$. Such an integer N exists if and only if α admits, up to fourth powers in $\mathbb{Q}(\zeta_4)$, a decomposition of the form (3). Since $\mathbb{Q}(\zeta_4)$ has class number 1 and its group of units is μ_4, we may factor α as a product of prime elements and a root of unity using its factorization in prime ideals (we may assume without loss of generality that α is integral). We may then check if this factorization is of the desired form, and if so Theorem 11 gives us such a minimal N.

Example 19. If $\alpha = 13(12\zeta_4+5)$, then $\alpha \in \mathbb{Q}(\zeta_4)$ is strongly 2-indivisible and we have $N_{\mathbb{Q}(\zeta_4)/\mathbb{Q}}(\alpha) = 169^2$. By Lemma 5 we deduce $\sqrt{\alpha} \in \mathbb{Q}(\zeta_\infty)$. Since $\alpha/13 = (2\zeta_4+3)^2$ we have $\sqrt{\alpha} \in \mathbb{Q}(\zeta_{4\cdot 13})$. By [5, Theorem 2] we know that α is a Kummer generator for the quartic subextension of $\mathbb{Q}(\zeta_{4\cdot 13})/\mathbb{Q}(\zeta_4)$. Then for $n \geqslant 2$ and $M \geqslant 1$ the degree

$$[\mathbb{Q}(\zeta_{2^n},\ \sqrt[2^n]{\alpha}) \cap \mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_{2^n})]$$

is 4 if $13 \mid M$ and it is 1 otherwise, while for $M \geqslant 1$ the degree

$$[\mathbb{Q}(\zeta_4, \sqrt{\alpha}) \cap \mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_4)]$$

is 2 if $13 \mid M$ and it is 1 otherwise.

7.3. **The 3-adelic failure for $\mathbb{Q}(\zeta_3)$.** If $\alpha \in \mathbb{Q}(\zeta_3)$, then we want to compute its 3-adelic failure, namely all degrees

$$[\mathbb{Q}(\zeta_{3^n},\ \sqrt[3^n]{\alpha}) \cap \mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_{3^n})] \tag{8}$$

for all $n, M \geqslant 1$ with $v_3(M) \geqslant n$. We may assume that $\alpha = \zeta\beta^{3^d}$, where $\zeta \in \mu_3$ and $\beta \in \mathbb{Q}(\zeta_3)$ is strongly 3-indivisible. By Theorem 12 (applied with $\ell = 3$, $t = 1$) and by Proposition 20 we may reduce to the case where α is strongly 3-indivisible.

Proposition 20. *Let $\beta \in \mathbb{Q}(\zeta_3)$ be strongly 3-indivisible. Suppose that $\sqrt[3]{\beta} \in \mathbb{Q}(\zeta_\infty)$, and let N be the conductor of $\mathbb{Q}(\zeta_3, \sqrt[3]{\beta})$. Then for $x \geqslant 3$ the conductor of $\mathbb{Q}(\zeta_3, \zeta_{3^x}\sqrt[3]{\beta})$ is $[3^x, N]$.*

Proof. If M is the conductor of $\mathbb{Q}(\zeta_3, \zeta_{3^x}\sqrt[3]{\beta})$, then $\mathbb{Q}(\zeta_M)$ is contained in $\mathbb{Q}(\zeta_{3^x}, \zeta_N)$ and contains $\mathbb{Q}(\zeta_{3^{x-1}})$. Thus M divides $[3^x, N]$ and $9 \mid M$. As remarked before Theorem 9 we have $v_3(N) \leqslant 2$, so we deduce $N \mid M$. Thus $\zeta_{3^x} \in \mathbb{Q}(\zeta_M)$, so that $3^x \mid M$ and we may conclude. □

Supposing that α is strongly 3-indivisible, by Schinzel's Theorem [8, Theorem 3.3] we have $\sqrt[9]{\alpha} \notin \mathbb{Q}(\zeta_\infty)$, hence (8) is either 1 or 3. So we are left to check if $\sqrt[3]{\alpha} \in \mathbb{Q}(\zeta_\infty)$ and if so find the smallest positive integer m such that $\sqrt[3]{\alpha} \in \mathbb{Q}(\zeta_{3m})$. Such an integer m exists if and only if α admits, up to cubes in $\mathbb{Q}(\zeta_3)$, a decomposition of the form (2). Since $\mathbb{Q}(\zeta_3)$ has class number 1 and its group of units is μ_6, we may factor α as a product of prime elements and a root of unity using its factorization in prime ideals (we may assume without loss of generality that α is integral). We may then check if this factorization is of the desired form, and if so Theorem 9 gives us the minimal m we need.

Example 21. If $\alpha = \frac{21\sqrt{-3}-7}{2}$, then α is a Kummer generator for the cubic subextension of $\mathbb{Q}(\zeta_{21})/\mathbb{Q}(\zeta_3)$, see [5, Theorem 1]. In particular, 7 is the smallest positive integer m such that $\sqrt[3]{\alpha} \in \mathbb{Q}(\zeta_{3m})$. So for $n \geqslant 1$ and $3^n \mid M$ we have

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

8. The case of finite rank

Let K be a number field, and let G be a subgroup of $K^\times$ of positive finite rank r. We explain how to compute the Kummer degrees $[K(\zeta_m, \sqrt[n]{G}) : K(\zeta_m)]$ for all $n, m \geqslant 1$ with $n \mid m$, provided that we can compute those degrees if the rank of G is 1, and that we can compute the degrees of the cyclotomic extensions of K. We may suppose that G is torsion-free:

Remark 22. *If G is not torsion-free, write $G = \langle\zeta\rangle \times G'$, where G' is torsion-free and where ζ is a root of unity of order $t > 1$. Then we have*

$$[K(\zeta_m, \sqrt[n]{G}) : K(\zeta_m)] = [K(\zeta_{[m,nt]}, \sqrt[n]{G'}) : K(\zeta_{[m,nt]})] \cdot [K(\zeta_{[m,nt]}) : K(\zeta_m)]\,.$$

Notice that it suffices to compute

$$C(m,n) := \frac{n^r}{[K(\zeta_m, \sqrt[n]{G}) : K(\zeta_m)]}$$

and that we have the decomposition

$$C(m,n) = \prod_{\ell \mid n} C(\ell^e, \ell^e) \cdot B(m, \ell^e)\,,$$

where ℓ runs through the prime factors of n and $e = v_\ell(n)$, and where we call $C(\ell^e, \ell^e)$ the ℓ-adic failure and

$$B(m, \ell^e) := \left[K(\zeta_{\ell^e}, \sqrt[\ell^e]{G}) \cap K(\zeta_m) : K(\zeta_{\ell^e})\right] \tag{9}$$

the ℓ-adelic failure. The ℓ-adic failure can be computed by the explicit formulas of [1, Theorem 18 and Lemma 19] and it is 1 for almost all ℓ by [8, Lemma 3.2] (and this set of primes is computable).

We now focus on the ℓ-adelic failure. By [8, Lemma 3.5] the integers $B(m, \ell^e)$ are 1 if $\zeta_\ell \notin K$ and, if $s := v_\ell(\sharp \mu_K)$, then we have $B(m, \ell^e) \mid \ell^{sr}$. Now consider some ℓ for which the ℓ-adelic failure might be non-trivial. By [10, Theorem 5.3] there are computable integers m_0 and e_0, which only depend on K, G and ℓ, such that

$$B(m, \ell^e) = B((m, m_0), (\ell^e, \ell^{e_0}))\,, \tag{10}$$

so we may suppose that $m \mid m_0$ and $e \leqslant e_0$. As an aside remark, notice that the integer e_0 as chosen in [10, Proof of Theorem 5.3] satisfies the equality of fields

$$K\big(\zeta_{\ell^E}, \sqrt[\ell^e]{G}\big) \cap K(\zeta_\infty) = K\big(\zeta_{\ell^E}, \sqrt[\ell^{e_0}]{G}\big) \cap K(\zeta_\infty)$$

for all $E \geqslant e \geqslant e_0$, see [10, Lemma 3.3]. Now fix $e \leqslant e_0$, and suppose that for each of the finitely many representants α of G modulo ℓ^e-th powers we can determine the integers x such that

$$K\big(\zeta_{\ell^e}, \sqrt[\ell^e]{\alpha}\big) \cap K(\zeta_\infty) \subseteq K(\zeta_x)\,.$$

Then for all $m \mid m_0$ and all $e \leqslant e_0$ with $\ell^e \mid m$ we can write

$$K\big(\zeta_{\ell^e}, \sqrt[\ell^e]{G}\big) \cap K(\zeta_m) = K\big(\zeta_{\ell^e}, \sqrt[\ell^e]{H}\big),$$

where H is a computable subgroup of G containing G^{ℓ^e} (which depends on ℓ, e, m). We are left to compute the degree of the extension $K\big(\zeta_{\ell^e}, \sqrt[\ell^e]{H}\big)/K\big(\zeta_{\ell^e}\big)$, which can be done with the results of [1].

REFERENCES

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

[2] FRIED, M. D. - JARDEN, M. *Field arithmetic*, Third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge, A Series of Modern Surveys in Mathematics, **11**, Springer-Verlag, Berlin, 2008.

[3] 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.

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

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

[6] MOREE, P., *Artin's primitive root conjecture – a survey*, Integers **12** (2012), no. 6, 1305–1416.

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

[8] 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.
[9] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *Explicit Kummer theory for the rational numbers*, Int. J. Number Theory, **16** (2020), no. 10 , 2213–2231.
[10] PERUCCA, A. - SGOBBA, P. - TRONTO, S., *The degree of Kummer extensions of number fields*, to appear in Int. J. Number Theory, DOI: https://doi.org/10.1142/S1793042121500263.

MATHEMATISCHES INSTITUT, ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG, ERNST-ZERMELO-STRASSE 1, D-79104 FREIBURG, GERMANY

Email address: fritz.hoermann@math.uni-freiburg.de

DEPARTMENT OF MATHEMATICS, 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