KUMMER THEORY FOR p-ADIC FIELDS

FLAVIO PERISSINOTTO AND ANTONELLA PERUCCA

ABSTRACT. Let K be a p-adic field, namely a finite extension of the field of p-adic numbers $\mathbb{Q}_p$. If G is a finitely generated subgroup of $K^\times$, we describe how to compute the degrees of the Kummer extensions $K(\zeta_n, \sqrt[n]{G})/K(\zeta_n)$ for all positive integers n. Moreover, we compare a Kummer extension of number fields with the corresponding Kummer extensions of p-adic fields which arise by completion.

1. INTRODUCTION

Kummer theory is a topic of significant classical interest in number theory, and progress has recently been made for number fields, see e.g. [2, 7, 5, 1]. In this article we make detailed computations concerning Kummer theory of *p-adic fields* (namely, the finite extensions of the field of p-adic numbers $\mathbb{Q}_p$).

We fix some p-adic field K and a finitely generated subgroup G of $K^\times$. For all positive integers N, n such that $n \mid N$ we consider the Kummer extension $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$. We may compute the degrees

$$[K(\zeta_N, \sqrt[n]{G}) : K(\zeta_N)] \tag{1}$$

for a given pair n, N with a finite procedure. Given the prime factorization $n = \prod_{\ell | n} \ell^e$, by Kummer theory the above degree is the product of the degrees

$$[K(\zeta_N, \sqrt[\ell^e]{G}) : K(\zeta_N)] = \frac{[K(\zeta_{\ell^e}, \sqrt[\ell^e]{G}) : K(\zeta_{\ell^e})]}{[K(\zeta_{\ell^e}, \sqrt[\ell^e]{G}) \cap K(\zeta_N) : K(\zeta_{\ell^e})]}\,. \tag{2}$$

To compute the numerator in (2), we show more generally how to compute at once all the degrees

$$[K(\zeta_{\ell^E}, \sqrt[\ell^e]{G}) : K(\zeta_{\ell^E})] \tag{3}$$

for all positive integers $E \geqslant e$ with a finite procedure, see Section 3 (the result of the computation is an explicit formula for the degree with parameters E and e). We rely on the method for number fields, adapting it to the specificities of p-adic fields (the case $\ell = p$ requires a different definition of the divisibility parameters). We point out that, for $\ell = p$, the number of steps in our finite procedure depends on the divisibility of certain elements (so we cannot bound it if we have no bounds on the divisibility of those elements).

As for the denominator in (2), we show more generally how to compute the degree

$$[K(\zeta_n, \sqrt[n]{G}) \cap K(\zeta_N) : K(\zeta_n)]$$

for all positive integers N, n such that $n \mid N$, see Section 5. These degrees measure the *entanglement* between Kummer extensions and cyclotomic extensions, which is described explicitly in Section 4 (see Theorem 11). It turns out that we can compute the degrees in (3) for all ℓ, E, e with a finite procedure. However, as discussed before Remark 16, we can only compute (1) for all N, n with a finite procedure up to assuming that the multiplicative order of p modulo N for all N is known.

It is also a natural question to compare Kummer extensions of number fields to the corresponding Kummer extensions of p-adic fields obtained by completion (completing number fields with respect to the non-zero prime ideals of their ring of integers). In the last section we prove in particular (see Theorem 24) that there is set of primes of the number field of positive density such that the local Kummer degree is the same as the global Kummer degree.

2. PRELIMINARIES ON p-ADIC FIELDS

A very valuable introduction to the theory of p-adic fields is [8]. We fix an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, and some p-adic field $K \subseteq \bar{\mathbb{Q}}_p$. We write $[K : \mathbb{Q}_p] = ef$, where e is the ramification index and f is the degree of the maximal unramified subextension of $K/\mathbb{Q}_p$. The residue field of K is the finite field $\mathbb{F}_{p^f}$. Let $\mathcal{O}_K$ be the ring of integers of K, and let $\pi \in \mathcal{O}_K$ be a uniformizer. We call v_K the valuation on K extending the normalized valuation on $\mathbb{Q}_p$ and such that $v_K(\pi) = 1/e$.

Cyclotomic extensions of $\mathbb{Q}_p$ (see [8, Chapter IV, §4] for more details). For every positive integer n we denote by ζ_n a root of unity in $\bar{\mathbb{Q}}_p$ of order n, and by μ_n the group of roots of unity of order dividing n. We write μ_∞ for the group of all roots of unity inside $\bar{\mathbb{Q}}_p$. Remark that for every positive integer n the cyclotomic extension $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ is abelian.
Supposing $p \nmid n$, this cyclotomic extension is unramified at p and it is cyclic because its Galois group is isomorphic to the one of $\mathbb{F}_p(\zeta_n)/\mathbb{F}_p$. In particular, for every positive integer z there exists n coprime to p such that z is the degree of $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$.
For every positive integer k the cyclotomic extension $\mathbb{Q}_p(\zeta_{p^k})/\mathbb{Q}_p$ has degree $\varphi(p^k)$ and it is totally ramified at p. If $p \neq 2$, then it is cyclic, while for every $k \geqslant 2$ the Galois group of $\mathbb{Q}_2(\zeta_{2^k})/\mathbb{Q}_2$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$. Moreover, if n is coprime to p, then we have $\mathbb{Q}_p(\zeta_n) \cap \mathbb{Q}_p(\zeta_{p^k}) = \mathbb{Q}_p$. Thus for every positive integer N we know the structure of the Galois group of $\mathbb{Q}_p(\zeta_N)/\mathbb{Q}_p$. In particular, for $p \neq 2$ (respectively, $p = 2$), this group can be generated by 2 (respectively, 3) elements.
Considering the supernatural numbers p^∞ and $p_0^\infty := \prod_{\ell \text{ prime}, \ell \neq p} \ell^\infty$, the cyclotomic fields $\mathbb{Q}_p(\zeta_{p^\infty})$ and $\mathbb{Q}_p(\zeta_{p_0^\infty})$ are then linearly disjoint over $\mathbb{Q}_p$.

Roots of unity and the unit group. Define $\mu_K := \mu_\infty \cap K$ and $\tau := \#(\mu_K)$, and for any prime ℓ write $\tau_\ell := \ell^{v_\ell(\tau)}$. For every $\ell \neq p$ we have $v_\ell(\tau) = v_\ell(p^f - 1)$ hence $(p^f - 1) \mid \tau$. Moreover, $\mathbb{Q}_p(\zeta_{\tau_p}) \subseteq K$ implies that $\varphi(\tau_p) \mid e$. Notice that τ is even because $\mathbb{Z} \subseteq K$. We also define $d_p := [K(\zeta_p) : K]$, noticing that $d_p \mid (p-1)$ and that $d_p = 1$ if $p \mid \tau$. The unit group of $\mathcal{O}_K$ is the group

$$\mathcal{O}_K^\times \cong \mu_{p^f-1} \times (1 + \pi\mathcal{O}_K) \cong \mu_K \times \mathbb{Z}_p^{ef} \tag{4}$$

where $\mathbb{Z}_p^{ef}$ is an additive group and the second isomorphism is induced by the p-adic logarithm (see for example [9, Chapter 5 §4.5]). For any prime number $\ell \neq p$ we consider the projection map

$$\mathrm{Proj}_\ell : \mathcal{O}_K^\times \to \mu_{\tau_\ell}$$

induced by (4) and by the projection $\mu_K \to \mu_{\tau_\ell}$. Since $\mu_{\tau_\ell} \subseteq \mu_{p^f-1}$, for every $\alpha \in \mathcal{O}_K^\times$ the ℓ-adic valuation of the order of $\mathrm{Proj}_\ell(\alpha)$, which we call $h_\ell(\alpha)$, is the same as the ℓ-adic valuation of the order of $(\alpha \bmod \pi) \in \mathbb{F}_{p^f}^\times$. We clearly have $h_\ell(\alpha) \leqslant v_\ell(\tau)$. Notice that for almost all ℓ, and in particular if $\ell \nmid \tau$, we have $h_\ell(\alpha) = 0$.

3. The ℓ-adic Kummer degrees

We fix a p-adic field K and a prime number ℓ. If z is a positive integer, we say that $\alpha \in K^\times$ is *ℓ^z-divisible* if α has some ℓ^z-th root in $K^\times$ (which implies $\ell^z \mid e \cdot v_K(\alpha)$). Only the elements in $\mathcal{O}_K^\times$ can be *ℓ^∞-divisible*, namely ℓ^z-divisible for every z. By (4) we get the following:

Remark 1. The p^∞-divisible elements are the roots of unity in K of order coprime to p, namely μ_{p^f-1}. For $\ell \neq p$, the ℓ^∞-divisible elements are those $\alpha \in \mathcal{O}_K^\times$ such that $(\alpha \bmod \pi) \in \mathbb{F}_{p^f}^\times$ has order coprime to ℓ. In general, $\alpha \in \mathcal{O}_K^\times$ equals a root of unity of order $\ell^{h_\ell(\alpha)}$ times an ℓ^∞-divisible element of $K^\times$. If $\alpha \notin \mathcal{O}_K^\times$, then $v_K(\alpha) \neq 0$ and for all ℓ not dividing $e \cdot v_K(\alpha)$ we have $\alpha\zeta \notin K^{\times\ell}$ for every $\zeta \in \mu_K$.

Remark 2. By the previous remark we reduce to study elements that are p^Z-divisible for some largest non-negative integer Z. To determine Z, we can test for p^z-divisibility by increasing $z \geqslant 1$. The p-adic logarithm is explicit hence we can apply the second isomorphism in (4) to check the p^z-th divisibility of an element in $\mathcal{O}_K^\times$. Another way to check this is with Hensel's Lemma. Indeed, $\alpha \in \mathcal{O}_K^\times$ is a p^z-th power if and only if there exists $u \in \mathcal{O}_K^\times$ such that $v_K(u^{p^z} - \alpha) > 2z/e$, see [3, Theorems 9.1 and 9.3]. By expanding $u = \sum_{i \geqslant 0} u_i \pi^i$ and α as power series in π (where the coefficients are zero or roots of unity in μ_{p^f-1}) we are left to check solvability for a system with finitely many polynomial equations in $\mathbb{F}_{p^f}[(u_1 \bmod \pi), \ldots, (u_{2z} \bmod \pi)]$. Notice that the number of steps required to determine whether an element is p^z-divisibile depends on z.

We fix some finitely generated subgroup G of $K^\times$, aiming at computing the degree and the structure of the Galois group of $K(\zeta_{\ell^M}, \sqrt[\ell^m]{G})/K(\zeta_{\ell^M})$ for all positive integers $m \leqslant M$ (all at once). We define

$$D(\ell^M, \ell^m) := [K(\zeta_{\ell^M}, \sqrt[\ell^m]{G}) : K(\zeta_{\ell^M})],$$

and we notice that $D(\ell^M, \ell^m)$ is a power of ℓ.

Remark 3. There can be arbitrarily large integers n such that there are elements x in $K^\times \setminus \mu_K$ satisfying $x^{\ell^n} \in G$ and $x^{\ell^{n-1}} \notin G$ (thus [2, Lemma 12] does not hold for p-adic fields). If $\ell \neq p$, this phenomenon is due to the ℓ^∞-divisible elements that are not roots of unity. If $\ell = p$, we may consider as an example a subgroup of $\mathcal{O}_{\mathbb{Q}_p}^\times$ (thanks to (4) we may work in $\mu_{\mathbb{Q}_p} \times \mathbb{Z}_p$): if G is generated by $(1,1)$ and $(1, \sum_{i=0}^\infty a_i p^i)$, where the sequence of coefficients $a_i \in \{0, \dots, p-1\}$ is not eventually periodic, then $x := (1, \sum_{i=n}^\infty a_i p^{i-n})$ is such that $x^{p^n} \in G$ and $x^{p^{n-1}} \notin G$.

3.1. **The p-adic Kummer degree.** We define *p-divisibility parameters* for G. These parameters differ from those for number fields [2, Section 3] but they allow to extend [2, Theorem 18] (and [2, Lemma 19] if $p = 2$ and $\zeta_4 \notin K$).

If $\log : \mathcal{O}_K^\times \to \mu_K \times \mathbb{Z}_p^{ef}$ is the isomorphism in (4), we also have the isomorphism

$$\begin{aligned} \phi : K^\times &\to \mu_K \times \mathbb{Z}_p^{ef} \times \mathbb{Z} \\ x &\mapsto (\log(x\pi^{-e\cdot v_K(x)}), e \cdot v_K(x)) \,. \end{aligned}$$

By composing ϕ with projection maps we define $\phi_0 : K^\times \to \mathbb{Z}_p^{ef}$ and $\phi_1 : K^\times \to \mathbb{Z}$ and $\phi_p : K^\times \to \mu_{\tau_p}$. If $a \in \mathbb{Z}_p^{ef} \times \mathbb{Z}$ is not zero, we can define $v_p(a)$ as the minimum of the p-adic valuation of the non-zero entries of a.

Suppose that G is torsion-free and non trivial, and let $r > 0$ be its rank. In particular, $\phi_0(G) \times \phi_1(G)$ is isomorphic to G. Consider the $\mathbb{Z}_p$-module

$$\phi_0'(G) = \mathbb{Z}_p(\phi_0(G) \times \phi_1(G)) \subseteq \mathbb{Z}_p^{ef+1} \,.$$

where we identify $\mathbb{Z}_p^{ef} \times \mathbb{Z}$ with the obvious subgroup of $\mathbb{Z}_p^{ef+1}$. Recall that, given an $n \times m$ matrix A with $n \geqslant m$ over a principal ideal domain, there is an algorithm that gives two invertible matrices M_1 and M_2 such that $M_1 A M_2$ is in Smith normal form. This means that $M_1 A M_2$ is diagonal with entries $\{\alpha_i\}$ where, for some index $1 \leqslant k \leqslant m$, we have $\alpha_i = 0$ for $i > k$ and $\alpha_i \mid \alpha_{i+1}$ for $0 \leqslant i \leqslant k$. Using this algorithm, we can find a set of $\mathbb{Z}_p$-linearly independent elements $\gamma_1, \cdots, \gamma_s$ (where $s \leqslant \min(ef+1, r)$) such that $v_p(\gamma_1) \leqslant \cdots \leqslant v_p(\gamma_s)$ and moreover

$$v_p\left(\sum_{i=1}^s a_i p^{-v_p(\gamma_i)} \gamma_i\right) = 0$$

holds for all $a_i \in \{0, \cdots, p-1\}$ that are not all zero. We define the *d-parameters of p-divisibility* of G as the tuple $(d_1, \cdots, d_s)$ where $d_i := v_p(\gamma_i)$.

Let $\mathcal{B} := \{b_1, \dots, b_r\}$ be a basis of G. We consider the matrix $M \in \mathrm{GL}_r(\mathbb{Z}_p)$ that maps $\phi'_0(\mathcal{B})$ to the vectors $\gamma_1, \cdots, \gamma_s, 0, \cdots, 0$ and the matrix $M' \in \mathrm{GL}_r(\mathbb{Z}/\tau_p\mathbb{Z})$ such that $M \equiv M' \bmod \tau_p$. For all $i = 1, \dots, r$ we define $h_i \in \mathbb{Z}_{\geqslant 0}$ as the p-adic valuation of the order of the i-th entry of

$$M' \begin{pmatrix} \phi_p(b_1) \\ \vdots \\ \phi_p(b_r) \end{pmatrix} .$$

Theorem 4. *If G is torsion-free with positive rank r, then for any positive integer n there exists a basis $g_1, \cdots, g_r$ of G such that*

$$g_i = A_i^{p^{d_i}} \xi_i \quad \textit{for } 1 \leqslant i \leqslant s \qquad \textit{and} \quad g_i \in \xi_i K^{\times p^n} \quad \textit{for } s < i \leqslant r$$

where $\xi_i \in \mu_K$ has order p^{h_i} and $A_i \in K^\times$ and the A_i's are strongly p-independent.

Proof. We let $\mathcal{B}$ and M be as above, and we suppose without loss of generality that $n \geqslant \max(d_s, v_p(\tau))$. Since M is invertible, we may choose $M' \in \mathrm{GL}_r(\mathbb{Z})$ such that $(M' \bmod p^n) = (M \bmod p^n)$. We let M' act on $(\mathbb{Z} \times \mathbb{Z}_p^{ef})^r$ and set $g'_i := M'(\phi'_0(b_i))$. Then $g'_1, \dots, g'_r$ is a basis of $\phi'_0(G)$ that satisfies $v_p(g'_i) = d_i$ for $i \leqslant s$ and $v_p(g'_i) \geqslant n$ otherwise. Moreover, we have

$$v_p\left(\sum_{i=1}^{s} a_i p^{-d_i} g'_i\right) = 0$$

for all $a_i \in \{0, \cdots, p-1\}$ that are not all zero. Thanks to this property, the elements $A_i := \phi^{-1}((1, p^{-d_i} g'_i))$ for $1 \leqslant i \leqslant s$ are strongly p-independent in $K^\times$. We also have $\phi^{-1}((1, g'_i)) \in K^{\times p^n}$ for $s < i \leqslant r$.

Since $G \cap \mu_K = \{1\}$ there exists unique a basis $\mathcal{B}' = \{g_1, \cdots, g_r\}$ of G such that $\phi'_0(\mathcal{B}') = M'\phi'_0(\mathcal{B})$. The basis $\mathcal{B}'$ is as requested because we have $\phi(g_i) = (\zeta_i, g'_i)$ for some root of unity ζ_i whose τ_p-part ξ_i has order p^{h_i}, as $n \geqslant v_p(\tau_p)$. □

Corollary 5. *With the above notation, suppose w.l.o.g. that $M \geqslant v_p(\tau)$ and (applying Theorem 4 with $n = m$) call $H := \langle g_1, \dots, g_s \rangle$. Let $h := \max(h_{s+1}, \cdots, h_r)$, setting $h = 0$ if $r = s$. Then we have*

$$K(\zeta_{p^M}, \sqrt[p^m]{G}) = K(\zeta_{p^{\max(M, m+h)}}, \sqrt[p^m]{H}).$$

In particular, we have

$$D(p^M, p^m) = p^{\max(M, m+h) - M} [K(\zeta_{p^{\max(M,m+h)}}, \sqrt[p^m]{H}) : K(\zeta_{p^{\max(M,m+h)}})] .$$

Proof. For $i = s+1, \cdots, r$ we have $K(\zeta_{p^M}, \sqrt[p^m]{g_i}) = K(\zeta_{p^M}, \zeta_{p^{m+h_i}})$ and the statement follows. □

Remark 6. The given basis of H satisfies the assumptions of [2, Theorem 14], therefore, to compute the Kummer degree

$$[K(\zeta_{p^N}, \sqrt[p^n]{H}) : K(\zeta_{p^N})]$$

for any positive integers $n \leqslant N$ we may apply [2, Theorem 18] (and [2, Lemma 19] if $p = 2$ and $\zeta_4 \notin K$) to H with parameters of p-divisibility $(d_1, \cdots, d_s; h_1, \cdots, h_s)$. By inspecting those degree formulas, for all integers $n \leqslant N$ large enough we have

$$D(p^N, p^n) = D(p^n, p^n) \qquad \text{and} \qquad D(p^{n+1}, p^{n+1}) = p^s D(p^n, p^n)$$

and therefore we only need to compute finitely many degrees to determine $D(p^M, p^m)$ for all positive integers $m \leqslant M$.

Example 7. Consider the subgroup of $\mathbb{Q}_p^\times$ generated by g_1, g_2, where $\phi(g_1) = (1, 1, 0)$ and $\phi(g_2) = (1, \sum_{i=0}^{\infty} a_i p^i, 0)$, the sequence of coefficients $a_i \in \{0, \ldots, p-1\}$ being not eventually periodic. Then we have $H = \langle g_1 \rangle$, $d_1 = 0$ and $h_1 = h_2 = 0$. Then for every $M \geqslant m \geqslant 1$ we have $D(p^M, p^m) = p^m$.

3.2. **The ℓ-adic Kummer degree for $\ell \neq p$.** We fix some prime $\ell \neq p$. We define $d_\ell(G)$ as follows: if $G \subseteq \mathcal{O}_K^\times$, then $d_\ell(G) = \infty$; if $G \nsubseteq \mathcal{O}_K^\times$, then $d_\ell(G)$ is the minimum of $v_\ell(e \cdot v_K(\alpha))$ by varying $\alpha \in G \setminus \mathcal{O}_K^\times$.

Firstly, we reduce to the case where 1 is the only element of G that is ℓ^∞-divisible. Denote by H the subgroup of $K^\times$ consisting of the ℓ^∞-divisible elements, and consider the subgroup GH/H of $K^\times/H$. Any class in GH/H is represented by an element of $K^\times$ of the form $\zeta\pi^D$ for some root of unity $\zeta \in \mu_K$ whose order is a power of ℓ and some non-negative integer D. Call G_ℓ the group consisting of these representatives, which is a finitely generated subgroup of $K^\times$ such that $G_\ell \cap H = \{1\}$. Moreover, remark that $K(\zeta_{\ell^n}, \sqrt[\ell^n]{G}) = K(\zeta_{\ell^n}, \sqrt[\ell^n]{G_\ell})$ and $d_\ell(G) = d_\ell(G_\ell)$.

Secondly, we may suppose without loss of generality that G_ℓ is torsion-free. Indeed, suppose that the torsion group of G_ℓ is generated by ζ_{ℓ^h} for some $h > 0$ and write $G_\ell = \langle \zeta_{\ell^h} \rangle \times G'_\ell$ for some torsion-free subgroup G'_ℓ of G_ℓ. Then we have

$$K(\zeta_{\ell^M}, \sqrt[\ell^m]{G_\ell}) = K(\zeta_{\max(\ell^M, \ell^{h+m})}, \sqrt[\ell^m]{G'_\ell}) \,.$$

Since the unit group consists of products of roots of unity and ℓ^∞-divisible elements, we may now suppose w.l.o.g. that $G_\ell \cap \mathcal{O}_K^\times = \{1\}$. As we may clearly suppose that G_ℓ is non-trivial, we have reduced to the case where G_ℓ is cyclic, being generated by an element $\beta \notin \mathcal{O}_K^\times$ such that $v_\ell(e \cdot v_K(\beta)) = d_\ell(G)$. We can formally apply to $G_\ell = \langle \beta \rangle$ the theory presented in [2, Section 3], where the ℓ-divisibility parameters of G_ℓ are those of β, namely $(d_\ell(G), h_\ell(\beta))$, where $\ell^{h_\ell(\beta)}$ is the order of a root of unity ζ such that $\beta\zeta$ is a power of exponent $\ell^{d_\ell(G)}$. Supposing w.l.o.g. that $M \geqslant \max(m, v_\ell(\tau))$, [2, Theorem 18] gives

$$v_\ell\big(D(\ell^M, \ell^m)\big) = \max(0, h_\ell(\beta) - \delta + m - M) + \delta$$

where $\delta = \max(0, m - d_\ell(G))$.

Remark 8. Suppose that $G_\ell = \langle \beta \rangle$ is as above. We have $d_\ell(G) = 0$ for almost all primes and we have $h_\ell(\beta) = 0$ if $\tau_\ell = 0$. Therefore, for all but finitely many primes $\ell \neq p$ we have $D(\ell^M, \ell^m) = \ell^m$ for every $m \leqslant M$. In general, for $\ell \neq p$ and for all $n \leqslant N$ large enough (in particular, if $n \geqslant h_\ell(\beta) + d_\ell(G)$) we have

$$D(\ell^N, \ell^n) = D(\ell^n, \ell^n) \qquad \text{and} \qquad D(\ell^{n+1}, \ell^{n+1}) = \ell D(\ell^n, \ell^n)\,.$$

Therefore we only need to compute finitely many degrees to know $D(\ell^M, \ell^m)$ for all primes $\ell \neq p$ and for all positive integers $m \leqslant M$.

Example 9. For the group $G = \langle 35, 98 \rangle$ inside $\mathbb{Q}_7^\times$ we have $D(2,2) = 2$ and $D(3,3) = 9$ because $G_2 = \langle -7 \rangle$ and $G_3 = \langle \zeta_3, 7 \rangle$.

4. KUMMER EXTENSIONS INSIDE CYCLOTOMIC EXTENSIONS

We consider a p-adic field K and work within an algebraic closure $\bar{\mathbb{Q}}_p$ containing K. The largest Kummer extension of K is the largest abelian extension of exponent τ, namely $K_{\text{Kum}} := K(\sqrt[\tau]{a} : a \in K^\times)$. We study the *entanglement field*

$$K_{\text{Ent}} := K_{\text{Kum}} \cap K(\mu_\infty)\,.$$

We also define

$$K_{\text{Ent},p} := K_{\text{Kum}} \cap K(\mu_{p^\infty}) \qquad K_{\text{Ent},p_0} := K_{\text{Kum}} \cap K(\mu_{p_0^\infty})\,.$$

Lemma 10. *Suppose that $\zeta_{\ell^z} \in K$ for some prime ℓ and for some $z \geqslant 1$. Let $K(\beta)/K$ be a cyclic extension of degree ℓ^z, and let σ be a generator of its Galois group. Then $\alpha := \sum_{i=1}^{\ell^z} \zeta_{\ell^z}^i \sigma^i(\beta)$ is such that $K(\alpha) = K(\beta)$ and $\alpha^{\ell^z} \in K^\times$.*

Proof. We have $\alpha^{\ell^z} = \prod_i \zeta_{\ell^z}^{-i} \alpha = \prod_i \sigma^i(\alpha) \in K$, we have $\alpha \neq 0$ because the $\sigma^i(\beta)$'s are K-independent, and we have $K(\alpha) = K(\beta)$ because the $\sigma^i(\alpha)$'s are distinct. □

We remark that $\tau/\tau_p = p^f - 1$ and hence $\tau = p^f - 1$ if $p \nmid \tau$.

Theorem 11. *The extension K_{Ent}/K is finite and abelian of exponent τ. Moreover, we have*

$$K_{\text{Ent}} = K_{\text{Ent},p_0} K_{\text{Ent},p} \qquad \textit{and} \qquad K_{\text{Ent},p_0} \cap K_{\text{Ent},p} = K\,.$$

The extension $K_{\text{Ent},p_0}/K$ is cyclic of degree τ, and we have $K_{\text{Ent},p_0} = K(\zeta_{(p^{f\tau}-1)})$. We can write $K_{\text{Ent},p_0} = K(\gamma_0)$ such that $\gamma_0^\tau \in K^\times$, setting

$$\gamma_0 := \begin{cases} \zeta_{\tau^2} & \textit{if } p \nmid \tau \\ \alpha \zeta_{\tau^2/\tau_p} & \textit{if } p \mid \tau\,, \end{cases}$$

where, letting q be a prime such that $v_p(\operatorname{ord}(p \bmod q)) \geqslant 2v_p(\tau) + v_p(f)$, the element α is as in Lemma 10 for the cyclic subextension of $K(\zeta_q)/K$ of degree τ_p.

Letting $r \geqslant 3$ be the greatest integer such that $(\zeta_{2^r} + \zeta_{2^r}^{-1})^2 \in K$, we have

$$K_{\mathrm{Ent},p} = \begin{cases} K(\zeta_p) = K(\sqrt[p-1]{-p}) & \textit{if } p \neq 2 \textit{ and } p \nmid \tau \\ K(\zeta_{2^r}) = K(\zeta_4, \zeta_{2^r} + \zeta_{2^r}^{-1}) & \textit{if } p = 2 \textit{ and } 4 \nmid \tau \\ K(\zeta_{\tau_p^2}) & \textit{otherwise} \end{cases}$$

$$\textit{and} \quad \mathrm{Gal}(K_{\mathrm{Ent},p}/K) \simeq \begin{cases} \mathbb{Z}/d_p\mathbb{Z} & \textit{if } p \neq 2 \textit{ and } p \nmid \tau \\ (\mathbb{Z}/2\mathbb{Z})^2 & \textit{if } p = 2 \textit{ and } 4 \nmid \tau \\ \mathbb{Z}/\tau_p\mathbb{Z} & \textit{otherwise}\,. \end{cases}$$

Proof. Since $K_{\mathrm{Ent},p_0}/K$ is unramified while $K_{\mathrm{Ent},p}/K$ is totally ramified, we have $K_{\mathrm{Ent},p_0} \cap K_{\mathrm{Ent},p} = K$. Clearly we have $K_{\mathrm{Ent},p_0}K_{\mathrm{Ent},p} \subseteq K_{\mathrm{Ent}}$, while the other inclusion follows from the fact that $K(\mu_\infty) = K(\zeta_{p_0^\infty}, \zeta_{p^\infty})$ and that K_{Ent,p_0}, $K_{\mathrm{Ent},p}$ are the largest Kummer subextensions of $K(\zeta_{p_0^\infty})/K$ and $K(\zeta_{p^\infty})/K$ respectively. Indeed, it suffices to show that any cyclic Kummer subextension of K_{Ent} is contained in $K_{\mathrm{Ent},p_0}K_{\mathrm{Ent},p}$, which can be done by working within a finite cyclotomic extension and decomposing the radical generating the Kummer extension.

The remaining assertions are easy to prove. First of all, $K_{\mathrm{Ent},p_0} = K(\zeta_{(p^{f\tau}-1)})$ and $K_{\mathrm{Ent},p_0}/K$ is cyclic of degree τ (this is the unique unramified extension of K of degree τ). It is clear that $\gamma_0^\tau \in K^\times$ and $K_{\mathrm{Ent},p_0} = K(\gamma_0)$ if $p \nmid \tau$, while the same assertions hold by Lemma 10 if $p \mid \tau$ (notice that the choice of q does not matter).

If $2 \neq p \nmid \tau$, the largest extension of K of degree dividing τ inside $K(\zeta_{p^\infty})$ is $K(\zeta_p)$, as $(p-1) \mid \tau$ and the only subextension of $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$ of degree coprime to p is $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p$. Similarly, the cases $p = 2$ and $p \mid \tau$ arise from the structure of the extension $\mathbb{Q}_p(\zeta_{p^\infty})/\mathbb{Q}_p$. Finally, recalling e.g. from [4, §5.6] that $(\zeta_p - 1)^{p-1} = -p$, we have $K(\zeta_p) = K(\sqrt[p-1]{-p})$. □

Remark 12. Define

$$\gamma := \begin{cases} \sqrt[p-1]{-p} & \text{if } p \neq 2 \text{ and } p \nmid \tau \\ \zeta_{2^r} + \zeta_{2^r}^{-1} & \text{if } p = 2 \text{ and } 4 \nmid \tau \\ \zeta_{\tau_p^2} & \text{otherwise}\,. \end{cases}$$

According to this case distinction, γ^{d_p}, γ^2, or γ^{τ_p} belongs to $K^\times$. We have $K_{\mathrm{Ent}} = K(R_K)$ where $R_K := \langle \gamma_0, \gamma \rangle$ or, if $p = 2$ and $4 \nmid \tau$, $R_K := \langle \zeta_4, \gamma_0, \gamma \rangle$. Notice that the quotient $R_K K^\times / K^\times$ is finite.

Example 13. For $p \neq 2$ we have $\mathrm{Gal}(\mathbb{Q}_{p\ \mathrm{Ent}}/\mathbb{Q}_p) \simeq (\mathbb{Z}/(p-1)\mathbb{Z})^2$ and hence

$$\mathbb{Q}_{p\ \mathrm{Ent}} = \mathbb{Q}_p(\zeta_{p(p^{p-1}-1)}) = \mathbb{Q}_p(\sqrt[p-1]{\zeta_{p-1}}, \sqrt[p-1]{-p}) = \mathbb{Q}_p(\sqrt[p-1]{z_p}, \sqrt[p-1]{-p})$$

for any $z_p \in \mathbb{Z}_p^\times$ whose residue in $\mathbb{F}_p^\times$ has order $p-1$, e.g. $z_3 = -1$ and $z_5 = 2$.

5. Computing the entanglement

Let K be a p-adic field, and fix a finitely generated subgroup G of $K^\times$. The aim of this section is computing the degrees

$$B(N,n) := [K(\zeta_n, \sqrt[n]{G}) \cap K(\zeta_N) : K(\zeta_n)]$$

adapting the method for number fields, for which we refer to [7, 5].

Theorem 14. *For all positive integers n, N such that n divides N we have*

$$K(\zeta_n, \sqrt[n]{G}) \cap K(\zeta_N) = K(\zeta_n, H_{N,n}) \tag{5}$$

for some computable group $H_{N,n}$ (generated over $K^\times$ by at most two elements and possibly ζ_4) such that

$$H_{N,n}^{\gcd(n,\tau)} \subseteq K^\times \subseteq H_{N,n} \subseteq K^\times_{\mathrm{Ent}} \cap K(\zeta_N)^\times \,.$$

Moreover, if R_K is as in Remark 12 and S denotes the finite set of the subgroups of $R_K K^\times$ containing $K^\times$, then $H_{N,n}$ belongs to S, and we may take

$$H_{N,n} := H_n \cap K(\zeta_N) \qquad \textit{where} \qquad H_n := \sqrt[n]{GK^{\times n}} \cap K^\times_{\mathrm{Ent}} \,.$$

Proof. We have $H_n^{\gcd(n,\tau)} \subseteq K^\times$ (recall that K_{Ent}/K has exponent τ) and

$$K(\zeta_n, \sqrt[n]{G}) \cap K(\zeta_\infty) = K(\zeta_n, H_n) \,.$$

Then (5) holds for $H_{N,n} := H_n \cap K(\zeta_N)$. Notice that H_n is the largest $M \in S$ satisfying $M \subseteq \sqrt[n]{GK^{\times n}}$. We finish the proof by observing that this condition is equivalent to $M^\tau \subseteq \sqrt[n]{G^\tau K^{\times \tau}}$ and it can be computed because R_K and G are finitely generated. □

Remark 15. Let t be the largest integer such that $K(\zeta_p) = K(\zeta_{p^t})$ if $p \neq 2$ and $K(\zeta_4) = K(\zeta_{2^t})$ if $p = 2$. We can write

$$\#\mu_{K(\zeta_N)\cap K_{\mathrm{Ent}}} = \begin{cases} p^{2v_p(\tau)-a}(p^{f\tau/b}-1) & \text{if } p \neq 2, p \mid \tau \text{ or } p = 2, 4 \mid \tau \\ p^t(p^{f\tau/b}-1) & \text{if } p \neq 2, p \nmid \tau, p \mid N \text{ or } p = 2, 4 \nmid \tau, 4 \mid N \\ p^{f\tau/b}-1 & \text{if } p \neq 2, p \nmid \tau, p \nmid N \text{ or } p = 2, 4 \nmid \tau, 4 \nmid N \end{cases}$$

where $0 \leqslant a \leqslant v_p(\tau)$ depends on N only through $v_p(N)$ and $b \mid \tau$ depends on N only through the multiplicative order of p modulo $\gcd(N, p_0^\infty)$. Then we have $H_{N,n} = H_n \cap M'K^\times$, where $M' \subseteq R_K$ is, with the above case distinction: $\langle \gamma_0^b, \gamma^{p^a} \rangle$; $\langle \gamma_0^b, \gamma \rangle$ if $p \neq 2$ and $\langle \zeta_4, \gamma_0^b, \gamma \rangle$ if $p = 2$; $\langle \gamma_0^b \rangle$.

We remark that the group H_n can be computed with a finite procedure for all $n \geqslant 1$. Indeed, for every $n \mid m$ the group H_n is a subgroup of H_m. Also notice that the ℓ-part of $H_n/K^\times$ is $H_{\ell^{v_\ell(n)}}/K^\times$ and it is trivial if $\ell \nmid \tau$. For every $\ell \mid \tau$ there is some integer B_ℓ such that $H_{\ell^{B_\ell}}$ contains H_{ℓ^v} for every $v \geqslant 1$ (this integer B_ℓ can easily be computed in terms of the ℓ-divisibility parameters of G). Consequently, $H_n = H_{\gcd(n,B)}$ where $B = \prod_{\ell \mid \tau} \ell^{B_\ell}$.

Fixing n, the group $H_{N,n} \cap K(\zeta_{p^\infty})$ is determined by $v_p(N)$, and

$$H_{N,n} \cap K(\zeta_{p^\infty}) = H_{pN,n} \cap K(\zeta_{p^\infty})$$

holds if $v_p(N) \geqslant 2v_p(\tau)$. Moreover, the group $H_{N,n} \cap K(\zeta_{p_0^\infty})$ depends on N only through the multiplicative order of p modulo $N' := \gcd(N, p_0^\infty)$. Indeed, this group is determined by $\mu_{K(\zeta_{N'})} \cap H_n$ (because $K(\zeta_{N'})/K$ corresponds to an extension of finite fields), and we recall that $\mu_{K(\zeta_{N'})}$ is isomorphic to the multiplicative group of $\mathbb{F}_{p^f}(\zeta_{N'})$, whose order only depends on p^f and the multiplicative order of p modulo N'. This leads to a finite but not explicit case distinction. If one accepts it, then we have shown that $H_{N,n}$ can be determined for all N, n at once and hence all degrees $B(N, \ell^m)$ for all integers m and N such that $\ell^m \mid N$ can be computed at once. Therefore (accepting the above case distinction), thanks to the considerations in Remark 8, the degrees of the Kummer extensions $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ can be determined for all $n \mid N$ at once with an explicit finite procedure.

Remark 16. We can compute at once the groups $H_{N,n}$ for all N, n that are powers of one fixed prime number ℓ. It suffices to compute H_{ℓ^z} (see the proof of Theorem 14) for every z, namely determining the largest subgroup $M \in S$ such that $M^\tau \subseteq \sqrt[\ell^z]{G^\tau} K^{\times\tau}$. Notice that

$$M^\tau \subseteq (\sqrt[\ell^z]{G^\tau} \cap K^\times) K^{\times\tau}$$

and that we can replace G by G_ℓ as done in Section 3.2. Then we easily conclude because $\sqrt[\ell^z]{G_\ell^\tau} \cap K^\times$ is finitely generated and can be computed for all z (it does not depend on z provided that z is sufficiently large).

Example 17. We continue Example 9, showing that $[\mathbb{Q}_7(\zeta_{18}, \sqrt[6]{G}) : \mathbb{Q}_7(\zeta_{18})] = 6$ by computing $B(18,2) = 1$ and $B(18,3) = 3$. Notice that $[\mathbb{Q}_7(\zeta_{18}) : \mathbb{Q}_7] = 3$ hence $B(18,2) = 1$ and $B(18,3) \in \{1,3\}$. To conclude, observe that $\zeta_{18} \in \mathbb{Q}_7(\sqrt[3]{G})$ because $7^6 \cdot 10^2 \in G$ and $\mathrm{ord}(10^2 \bmod 7) = 3$, thus the residue field of $\mathbb{Q}_7(\sqrt[3]{G})$ contains the 18-th roots of unity.

Example 18. For the group $\langle -1 \rangle \subseteq \mathbb{Q}_3^\times$ and for any positive integers $Z \geqslant z$, clearly $B(2^Z, 2^z)$ is 2 if $Z = z$, and it is 1 otherwise. As $R_{\mathbb{Q}_3} = \langle \zeta_4, \sqrt{-3} \rangle$, we have $H_{2^z} = \langle \zeta_4 \rangle \mathbb{Q}_3^\times$. Thus for $2^z \mid N$ we have $H_{N,2^z} \in \{H_{2^z}, \mathbb{Q}_3^\times\}$ and it is H_{2^z} if and only if $\zeta_4 \in \mathbb{Q}_3(\zeta_N)$, i.e. $4 \mid (3^{\mathrm{ord}(3 \bmod N)} - 1)$ or, equivalently, $2 \mid \mathrm{ord}(3 \bmod N)$.

We conclude by considering the structure of the Galois group of the Kummer extensions:

Remark 19. Fix some positive integers N, n such that $n \mid N$. Considering the prime decomposition of $n = \prod \ell^e$, observe that

$$\operatorname{Gal}(K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)) = \prod_{\ell \mid n} \operatorname{Gal}\left(\frac{K(\zeta_{\ell^e}, \sqrt[\ell^e]{G})}{K(\zeta_{\ell^e}, \sqrt[\ell^e]{G}) \cap K(\zeta_N)} \right) . \tag{6}$$

By Theorem 14 we have

$$K' := K(\zeta_{\ell^e}, \sqrt[\ell^e]{G}) \cap K(\zeta_N) = K(\zeta_{\ell^e}, H_{N,\ell^e}).$$

The size of the cyclic components of the factor in (6) corresponding to the prime $\ell = p$ can be then computed with the method described in [1, Theorem 6] with parameters of p-divisibility

$$(\infty, d_1, \cdots, d_s; h, h_1, \cdots, h_s)$$

with $h = \max(h_{s+1}, \cdots, h_r)$, where the h_i and d_i are as in Theorem 4 applied to the group G over the field K'. Consider now the factors in (6) for primes $\ell \neq p$. If $G \subseteq \mathcal{O}_{K'}^\times$, then each factor is cyclic as it corresponds to a cyclotomic extension. If $G \nsubseteq \mathcal{O}_{K'}^\times$, then each factor can be reduced to the product of at most two cyclic groups, again applying [1, Theorem 6] with parameters of ℓ-divisibility

$$(\infty, d_\ell(G); h, h_\ell(\beta))$$

defined in Section 3.2 for the group G and over the field K'. Notice that $h = h_\ell(\beta) = 0$ if $\ell \nmid \#(\mu_{K'})$ and $d_\ell(G) = 0$ for almost all primes as seen in Remark 8. Therefore there are only finitely many primes $\ell \neq p$ for which the factor is not cyclic of order ℓ^e.

Notice that, if we accept the case distinction to compute H_{N,ℓ^e} for all N and e at once, we can also compute the group structure of the Galois group of the Kummer extension $K(\zeta_N, \sqrt[n]{G})/K(\zeta_N)$ for all N and n at once.

6. Completions of Kummer extensions of number fields

In this section k is a number field and $\alpha \in k^\times$ is not a root of unity. If $\wp$ is a nonzero prime ideal of the ring of integers $\mathcal{O}_k$ over the rational prime p, we write $k_\wp$ for the corresponding completion of k and we identify k with a subfield of $k_\wp$. If ℓ is a prime number and $M \geqslant m$ are positive integers, we consider the Kummer extension of number fields

$$k(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha})/k(\zeta_{\ell^M})$$

and the corresponding Kummer extension of p-adic fields

$$k_\wp(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha})/k_\wp(\zeta_{\ell^M}) .$$

Let $\ell \neq p$. For almost all primes $\wp$ we have $v_\wp(\alpha) = 0$, and in this case the above extension of local fields is a cyclotomic extension, uniquely determined by $h_{\ell,\wp}(\alpha)$, namely the ℓ-adic valuation of the order of $(\alpha \bmod \wp)$. For a fixed $\wp$, we have $h_{\ell,\wp}(\alpha) = 0$ for almost all primes ℓ (as α is ℓ^∞-divisible if $\ell \nmid N(\wp) - 1 = p^f - 1$). If we fix ℓ instead, a prime $\wp$ is such that $h_{\ell,\wp}(\alpha) > 0$ if and only if ℓ divides the order of $(\alpha \bmod \wp)$ in $(\mathcal{O}_k/\wp)^\times$. There are infinitely many such $\wp$, even a set with positive density [6].

Remark 20. Let $\mathrm{Cl}(k)$ be the class group of k and h_k the class number. Let h, d be the ℓ-divisibility parameters of α, meaning that $\alpha = \zeta_{\ell^h}\beta^{\ell^d}$, where $\beta \in k^\times$ and d is maximal (we refer the reader to [2]). If $\ell \nmid h_k$, there exists a prime $\wp$ of k such that $\gcd(v_\wp(\beta), \ell) = 1$, else d would not be maximal. Consequently, the parameter $d_\wp$ of ℓ-divisibility of β in $k_\wp$ is the same as the one in k. In general, supposing that $v_\wp(\beta) \neq 0$, consider the order of $[\wp]$ in $\mathrm{Cl}(k)$ and denote by n its ℓ-adic valuation: the parameter $d_\wp$ can be any integer between d and $d + n$.

Example 21. Let $k = \mathbb{Q}(\sqrt{-5})$ and $\ell = 2$. Since $h_k = 2$, we could have $d_\wp = d + 1$. This happens for $\alpha = 2 - \sqrt{-5}$ and $\wp = (3, \sqrt{-5} + 1)$, noticing that $d = 0$ and $(\alpha) = (3, \sqrt{-5} + 1)^2$.

If ℓ is odd (respectively, $\ell = 2$) we define t as the largest integer for which $k(\zeta_\ell) = k(\zeta_{\ell^t})$ (respectively, $k(\zeta_4) = k(\zeta_{2^t})$) and, for a non-zero prime ideal $\wp$ of $\mathcal{O}_k$, we call $t_\wp$ the largest integer for which $k_\wp(\zeta_\ell) = k_\wp(\zeta_{\ell^{t_\wp}})$ (respectively, $k_\wp(\zeta_4) = k_\wp(\zeta_{2^{t_\wp}})$).

Theorem 22. *We keep the above notation, and suppose that $\ell \nmid h_k$. Consider the set P of non-zero prime ideals $\mathfrak{a} \subseteq \mathcal{O}_k$ for which $v_\ell(v_\mathfrak{a}(\alpha)) = d$. Fix some positive integers $m \leqslant M$ such that $M \geqslant \min_P t_\mathfrak{a}$. If the extension*

$$k(\zeta_{\ell^M},\ \sqrt[\ell^m]{\alpha})/k(\zeta_{\ell^M})$$

is not a cyclotomic extension, there exists $\wp \in P$ such that the corresponding extension

$$k_\wp(\zeta_{\ell^M},\ \sqrt[\ell^m]{\alpha})/k_\wp(\zeta_{\ell^M})$$

has the same degree and it is also not a cyclotomic extension.

Proof. Let $A := [k(\zeta_{\ell^M},\ \sqrt[\ell^m]{\alpha}) : k(\zeta_{\ell^M})]$, which is a power of ℓ. Since the given extension is not cyclotomic, we must have $d < m$. Since $M \geqslant t$, by [2, Theorem 18] we get

$$v_\ell(A) = \begin{cases} m - (M - h) & \text{if } d \geqslant M - h \\ m - d & \text{if } d < M - h\,. \end{cases}$$

Consider a prime $\wp \in P$ for which $t_\wp$ is minimal, so $M \geqslant t_\wp$ (we have $P \neq \emptyset$ by Remark 20). The ℓ-divisibility parameters of α in $k_\wp$ are $h_\wp$ and d. We show that $A_\wp := [k_\wp(\zeta_{\ell^M},\ \sqrt[\ell^m]{\alpha}) : k_\wp(\zeta_{\ell^M})]$ equals A by applying [2, Theorem 18] also to compute $A_\wp$. If $h_\wp = h$, then $A = A_\wp$ as all the parameters in the formula are the same. Else, we claim that $d \leqslant M - h_\wp$ and we conclude because $v_\ell(A_\wp) = m - d = v_\ell(A)$. To prove the claim, we show that $d \leqslant t_\wp - h_\wp$ in case $h_\wp > h$ (respectively, $d \leqslant t_\wp - h$ in case $h_\wp < h$). For $h_\wp > h$, the claim holds because $\beta^{\ell^d}/\zeta \bmod \wp$ has oder coprime to ℓ for some root of unity ζ of order $\ell^{h_\wp}$ (since $h_\wp > 0$, we conclude by considering the order of $(\beta \bmod \wp)$, whose ℓ-adic valuation is at most $t_\wp$). For $h_\wp < h$ the claim holds because $\beta^{\ell^d}/\zeta_{\ell^h}^{-1}\zeta$ has order coprime to ℓ for some root of unity ζ of order $\ell^{h_\wp}$, and again the order of $(\beta \bmod \wp)$ has ℓ-adic valuation at most $\ell^{t_\wp}$. □

Theorem 23. *Fix a prime number ℓ and positive integers $m \leqslant M$. There is a set of primes $\wp$ of k of positive density such that*

$$[k(\zeta_{\ell^M},\, \sqrt[\ell^m]{\alpha}) : k(\zeta_{\ell^M})] = [k_\wp(\zeta_{\ell^M},\, \sqrt[\ell^m]{\alpha}) : k_\wp(\zeta_{\ell^M})]\,.$$

Proof. Set $\ell^{D_\ell} := [k(\zeta_{\ell^M},\, \sqrt[\ell^m]{\alpha}) : k(\zeta_{\ell^M})]$. The degree of the local extension at $\wp$ divides ℓ^{D_ℓ}. So the statement is clear if $D_\ell = 0$, and we suppose that $D_\ell \geqslant 1$.

If $\ell = 2$, we suppose that $\zeta_4 \in k$ or that $M > 1$. Then, without loss of generality, we may assume that $M \geqslant t$. Consider the primes $\wp$ of k such that $v_\wp(\alpha) = 0$ and remark that $h_\wp$ is the ℓ-adic valuation of the order of $(\alpha \bmod \wp)$. The conditions $t_\wp \geqslant M$ and $h_\wp = t_\wp - (m - D_\ell)$ imply that $k_\wp(\zeta_{\ell^M},\, \sqrt[\ell^m]{\alpha})/k_\wp(\zeta_{\ell^M})$ is cyclotomic of degree ℓ^{D_ℓ}. By the Chebotarev density theorem and the density results in [6] the primes satisfying $t_\wp = M$ and $h_\wp = t_\wp - (m - D_\ell)$ admit the density

$$\frac{1}{[k(\zeta_{\ell^M}) : k]} - \frac{1}{[k(\zeta_{\ell^{M+1}}) : k]} - \frac{1}{[k(\zeta_{\ell^M}, \sqrt[\ell^m]{\alpha^{\ell^{D_\ell - 1}}}) : k]} + \frac{1}{[k(\zeta_{\ell^{M+1}}, \sqrt[\ell^m]{\alpha^{\ell^{D_\ell - 1}}}) : k]}\,.$$

This density is positive because $\zeta_{\ell^{M+1}} \notin k(\zeta_{\ell^M})$ (as $M \geqslant t$) and $\alpha^{\ell^{D_\ell}} \notin k(\zeta_{\ell^M})$ (as $D_\ell \geqslant 1$).

We are left with the case $\ell = 2$, $\zeta_4 \notin k$ and $M = 1$ hence $m = D_\ell = 1$. We may similarly consider the primes $\wp$ of k for which $4 \nmid \#\mu_{k_\wp}$and $\sqrt{\alpha} \notin k_\wp$, which have density at least $1/4$. □

Now consider a more general Kummer extension $k(\zeta_N,\, \sqrt[n]{\alpha})/k(\zeta_N)$ where n and N are positive integers such that $n \mid N$. We generalize Theorem 23:

Theorem 24. *Let n, N be positive integers such that $n \mid N$. There is a set of primes $\wp$ of k of positive density such that*

$$[k(\zeta_N,\, \sqrt[n]{\alpha}) : k(\zeta_N)] = [k_\wp(\zeta_N,\, \sqrt[n]{\alpha}) : k_\wp(\zeta_N)]\,.$$

Proof. Let T be the greatest integer for which $k(\zeta_N) = k(\zeta_T)$. Up to replacing N, we may assume that $N = T$. For a prime $\wp$ of k, consider the prime factorization $n = \prod \ell^{m_\ell}$ and observe that

$$[k_\wp(\zeta_N,\, \sqrt[n]{\alpha}) : k_\wp(\zeta_N)] = \prod_{\ell \mid n} \frac{[k_\wp(\zeta_{\ell^{m_\ell}},\, \sqrt[\ell^{m_\ell}]{\alpha}) : k_\wp(\zeta_{\ell^{m_\ell}})]}{[k_\wp(\zeta_{\ell^{m_\ell}},\, \sqrt[\ell^{m_\ell}]{\alpha}) \cap k_\wp(\zeta_N) : k_\wp(\zeta_{\ell^{m_\ell}})]}\,. \tag{7}$$

Suppose that $\wp$ is such that $N \mid \#\mu_{k_\wp}$ and $\ell^{v_\ell(N)+1} \nmid \#\mu_{k_\wp}$ for every $\ell \mid N$. For such $\wp$ the denominators in (7) are 1 because we have $k_\wp(\zeta_{\ell^{m_\ell}}) = k_\wp(\zeta_N)$. We additionally require that, for every $\ell \mid N$, the ℓ-adic local Kummer extension has degree

$$\ell^{D_\ell} := [k(\zeta_N,\, \sqrt[\ell^{m_\ell}]{\alpha}) : k(\zeta_N)].$$

If $D_\ell = 0$, this condition holds because the degree of the local extension divides ℓ^{D_ℓ}. If $D_\ell > 0$ and if we exclude the finitely many primes $\wp$ for which $v_\wp(\alpha) \neq 0$, the above condition means that the order of $(\alpha \bmod \wp)$ has ℓ-adic valuation $v_\ell(N) - (m_\ell - D_\ell)$, because the extension $k_\wp(\zeta_N,\, \sqrt[\ell^{m_\ell}]{\alpha})/k_\wp(\zeta_N)$ is cyclotomic.

We conclude by proving that there is a set of primes $\wp$ of positive density such that the following holds: we have $N \mid \#\mu_{k_\wp}$; for every $\ell \mid N$, we have $\ell^{v_\ell(N)+1} \nmid \#\mu_{k_\wp}$; if $D_\ell > 0$, the order of $(\alpha \bmod \wp)$ has ℓ-adic valuation $v_\ell(N) - (m_\ell - D_\ell)$. We may restrict to the positive density of primes $\wp$ that split completely in $k(\zeta_N,\, \sqrt[E]{\alpha})$, where

$$E := \prod_{\ell : D_\ell > 0} (m_\ell - D_\ell)\,.$$

We are left to select those primes that, for every ℓ, satisfy the following condition: they do not split in $k(\zeta_{N\ell},\, \sqrt[E]{\alpha})$ and, if $D_\ell > 0$, they do not split in $k(\zeta_N, \sqrt[E\ell]{\alpha})$. Notice that these two fields have degree ℓ over $k(\zeta_N,\, \sqrt[E]{\alpha})$. Indeed, by the definition of D_ℓ, for every ℓ such that $D_\ell \geqslant 1$ we have that $\sqrt[\ell^{m_\ell - D_\ell}]{\alpha} \in k(\zeta_N)$ but $\sqrt[\ell^{m_\ell - D_\ell + 1}]{\alpha} \notin k(\zeta_N)$. In particular, the conditions for different primes ℓ involve field extensions that are linearly disjoint. So we are left to check that the density of primes $\wp$ satisfying the condition for one single ℓ is positive. This holds because not splitting in any of the two given extensions of degree ℓ gives density $1 - \frac{1}{\ell}$ if the two fields are the same and density $(1 - \frac{1}{\ell})(1 - \frac{1}{\ell})$ if the two fields are different hence linearly disjoint. □

Remark 25. For any number field extension $L(\gamma)/L$ and for any prime $\wp$ of L, we have $[L(\gamma) : L] \geqslant [L_\wp(\gamma) : L_\wp]$. Then Theorem 24 implies

$$[k(\zeta_N,\, \sqrt[n]{\alpha}) : k(\zeta_N)] = \min_{\substack{\wp \subseteq \mathcal{O}_k \\ \wp \text{ prime}}} [k_\wp(\zeta_N,\, \sqrt[n]{\alpha}) : k_\wp(\zeta_N)].$$

Example 26. Remark 25 does not hold for a subgroup G of $k^\times$ in place of α. For $k = \mathbb{Q}$ and $G = \langle 2, 5 \rangle$, the Kummer extension $\mathbb{Q}(\zeta_9,\, \sqrt[3]{G})/\mathbb{Q}(\zeta_9)$ has degree 9, while for every prime p the extension $\mathbb{Q}_p(\zeta_9,\, \sqrt[3]{G})/\mathbb{Q}_p(\zeta_9)$ has degree strictly less than 9: the degree is at most 3 for $p \neq 3$ and it is 1 for $p = 3$. (For $p = 3$ notice that 2 and 5 are cubes in $\mathbb{Q}_3$. For $p \neq 3$ we can use the results of Section 3.2, considering G_ℓ for $\ell = 3$. Indeed, if $p \notin \{2, 3, 5\}$ then G_3 is a subgroup of $\mu_{\mathbb{Q}_p}$ hence it is cyclic, while if $p = 2, 5$ the group G_3 is torsion free and hence it is cyclic.)

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. The authors thank Fritz Hörmann and Peter Stevenhagen for helpful discussions.

References

[1] Advocaat, B. - Chan, C.W. - Pajaziti, A. - Perissinotto, F. - Perucca, A.: *Galois groups of Kummer extensions of number fields*, to appear in the Publ. Math. Besançon.

[2] Debry, C. - Perucca, A.: *Reductions of algebraic integers*, J. Number Theory, **167** (2016), 259–283.

[3] Conrad, K. *Hensel's Lemma*, unpublished lecture notes, `https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`.

[4] Gouvêa, F. Q., *p-adic Numbers: An Introduction (second edition)*, Universitext, Springer-Verlag, Berlin Heidelberg, 1997.

[5] Perissinotto, F. - Perucca, A. *Kummer theory for multiquadratic or quartic cyclic number fields*, Unif. Distrib. Theory, **17** (2022), no. 2, 165–194.

[6] Perucca, A.: *The order of reduction of an algebraic integer*, J. Number Theory, **148** (2015), 121–136.

[7] Perucca, A. - Sgobba, P. - Tronto, S., *Explicit Kummer theory for the rational numbers*, Int. J. Number Theory, **16** (2020), no. 10, 2213–2231.

[8] Serre, J.-P., *Local Fields*, Graduate Texts in Mathematics, **67**, Springer-Verlag, New York, 1979.

[9] Robert, A. M., *A Course in p-adic Analysis*, Graduate Texts in Mathematics, **198**, Springer-Verlag, New York, 2000.

[10] Schinzel, A., *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), no. 3, 245–274.