The intersection of cyclic Kummer extensions with cyclotomic extensions

Antonella Perucca

Abstract

We study to which extent cyclic Kummer extensions can be contained in a cyclotomic extension. Let K be a field, and consider an extension of K of the form $K(\zeta_m, \sqrt[n]{a})$ where $a \in K$, ζ_m is a root of unity, n divides m, and m is not divisible by the characteristic of K. In the case where m is a prime power, we present a formula for the degree of this extension where only few parameters occur. No such formula is possible in general if m is not a prime power. This work is based on a result by Schinzel of 1977 describing abelian radical extensions.

1 Introduction

We study to which extent cyclic Kummer extensions can be contained in a cyclotomic extension. Let K be a field, and consider an extension of K of the form $L := K(\zeta_m, \sqrt[n]{a})$ where $a \in K$, ζ_m is a root of unity, n divides m, and m is not divisible by the characteristic of K. The field L contains the cyclotomic extension $K_m := K(\zeta_m)$, and the relative extension L/K_m is the cyclic Kummer extension obtained by adjoining the n-th roots of a. The problem that we address is calculating the degree of the finite Galois extension L/K. We have to evaluate the degree of the cyclic Kummer extension L/K_m, which is a divisor of n.

The general case can be easily recovered from the special case where we assume that a has no ℓ-th roots in K for every ℓ dividing n. Then often the degree of L/K is n but in general it could be lower, and that happens when a acquires roots in K_m.

Suppose that m is the power of a prime number ℓ. The main result of this paper is showing that the phenomenon for a of acquiring ℓ-th roots in K_m is very limited.

Theorem. *Let m be the power of a prime number ℓ, and suppose that a is* strongly ℓ-indivisible *in K, by which we mean that $a\mu$ has no ℓ-th roots in K for every root of unity $\mu \in K$. If ℓ is odd then a has no ℓ-th roots in K_m, and if $\ell = 2$ then a has no 4-th roots in K_m.*

An element $a \in K^\times$ is always the power of some strongly ℓ-indivisible element times a root of unity in K, unless in the following very special case: for some roots of unity $\mu \in K$

the element $a\mu$ has ℓ^e-th roots in K for every $e \geq 1$. We neglect this case because our Kummer extension would be a cyclotomic extension, and our problem is easily solved.

We then work out a very simple formula for the degree of L/K_m for every $a \in K^\times$. Precise statements are given in theorems 11 and 14, which cover respectively the case where ℓ is odd or $i \notin K$, and the remaining case.

If m is not necessarily a prime power then it is not possible to provide an analogous formula, because a could acquire roots in K_m and this strongly depends on a. Nevertheless, if a is strongly ℓ-indivisible for every prime ℓ dividing m then a can acquire ℓ-th roots in K_m only if ζ_ℓ belongs to K. We study what can happen for a general m in theorems 16 and 17. In particular, cyclic Kummer extensions are seldom contained in a cyclotomic extension.

This work is based on a result by Schinzel of 1977 describing which extensions of the form $K(\zeta_{\ell^n}, \sqrt[\ell^n]{a})$ have abelian Galois group (cf. [7]). The results were known for the case $K = \mathbb{Q}$ (cf. [8]), and related works on radical extensions are [3],[9].

Applications

The results in this paper can be used to work out the densities arising from Artin's conjecture for primitive roots over number fields, thus generalizing Hooley's formulas which concern the field $\mathbb{Q}$. However one has to fix a number field, and the primes dividing the exponent of the torsion of $K^\times$ will require a correction factor: for $\mathbb{Q}$, the correction factor was needed only for the prime 2 (cf. [1]).

In the appendix, we use the results in this paper for another application: Let K be a number field, a an element of $K^\times$ and ℓ a prime number. We compute the density of the set of primes $\mathfrak{p}$ of K such that the reduction of a modulo $\mathfrak{p}$ is well defined and has multiplicative order coprime to ℓ. The value of this density was known only for $\mathbb{Q}$ or under the assumption that $K_{\ell^n}(\sqrt[\ell^n]{a})/K$ has degree $\phi(\ell^n)\ell^n$ for all $n \geq 1$ (cf. [5], [2]). Once a number field K is fixed, one can also write a formula for the density of $\mathfrak{p}$ for which the order of a modulo $\mathfrak{p}$ is coprime to some fixed positive integer.

Acknowledgements

It is a pleasure to thank Hendrik Lenstra for essential contributions to this paper, and Peter Jossen for many useful comments.

2 Cyclotomic extensions

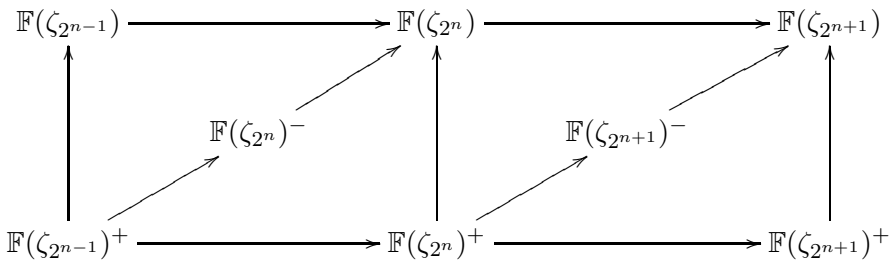
If K is a field, we fix some algebraic closure of K and work therein. For $n \geq 1$, we write ζ_n for a primitive root of unity of order n, and we denote by K_n the finite extension of K obtained by adjoining to K the n-th roots of unity. If ℓ is a prime number, we write K_{ℓ^∞} for the union of the fields K_{ℓ^n} for $n \geq 0$. In characteristic p, we write 2 for $(2 \bmod p)$. A reference for the results in this section is [10].

Lemma 1. *Let $\mathbb{F}$ be either $\mathbb{Q}$ or a prime field of odd characteristic. Let $n \geq 3$. We define the following fields:*

$$\mathbb{F}(\zeta_{2^n})^+ = \mathbb{F}\big(\zeta_{2^n} + \zeta_{2^n}^{-1}\big) = \mathbb{F}\Big(\sqrt{\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1} + 2}\Big)$$

$$\mathbb{F}(\zeta_{2^n})^- = \mathbb{F}\big(\zeta_4 \cdot (\zeta_{2^n} + \zeta_{2^n}^{-1})\big) = \mathbb{F}\Big(\sqrt{-(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1} + 2)}\Big)$$

The element ζ_4 does not belong to $\mathbb{F}(\zeta_{2^n})^+$ nor to $\mathbb{F}(\zeta_{2^n})^-$ for any n. The field $\mathbb{F}(\zeta_{2^n})^+$ (respectively, $\mathbb{F}(\zeta_{2^n})^-$) is contained in $\mathbb{F}(\zeta_{2^n})$ but not in $\mathbb{F}(\zeta_{2^m})$ for $m < n$.



The previous diagram shows all subfields of $\mathbb{F}(\zeta_{2^{n+1}})$ containing $\mathbb{F}(\zeta_{2^{n-1}})^+$. The sequences of arrows describe all fields inclusion. Each arrow corresponds to an extension of degree 2.

Note, the case of characteristic p in the previous lemma can be deduced from the case of characteristic zero by reduction modulo p.

Lemma 2. *Let ℓ be a prime number. Let K be a field of characteristic different from ℓ. The degree $[K_\ell : K]$ is a divisor of $\ell - 1$. Suppose that $K_{\ell^\infty} \neq K$ and call $t \geq 0$ the greatest integer such that $K_{\ell^t} = K$. Since $[K_{\ell^m} : K] = 1$ if $m \leq t$, we suppose $m > t$.*

(i) Let ℓ be odd, or let $t \geq 2$ if $\ell = 2$ (equivalently, $\zeta_4 \in K$). Then we have:

$$[K_{\ell^m} : K] = \begin{cases} \ell^{m-1} \cdot [K_\ell : K] & \text{if } t = 0 \\ \ell^{m-t} & \text{otherwise} \end{cases}$$

(ii) Consider the remaining case $\ell = 2$ and $t = 1$. Let $s \geq 2$ be the greatest integer such that $K_4 = K_{2^s}$, or set $s = \infty$ if no such number exists. Then we have:

$$[K_{2^m} : K] = \begin{cases} 2 & \text{if } s = \infty \text{ or if } m \leq s \\ 2^{m-s+1} & \text{if } m > s \end{cases}$$

3 Cyclic Kummer extensions

A reference for the results in this section is [6, §3 of Chapter IV]. Let K be a field, and choose an algebraic closure $\bar{K}$ of K. We denote by $K^\times$ the multiplicative group of K. Suppose that $\alpha^n = a$ for some $a \in K^\times$ and for some $n \geq 1$ not divisible by the characteristic of K, such that $\zeta_n \in K$. We then write $K(\alpha) = K(\sqrt[n]{a})$. This extension of K is obtained by adjoining one (equivalently, all) n-th roots of a. It is a Galois extension of K, being the splitting field of $X^n - a$.

Definition 3 (cyclic Kummer extension)**.** *A cyclic Kummer extension of a field K is an extension of K of the form $K(\sqrt[n]{a})$ where $a \in K^\times$, $n \geq 1$ is not divisible by the characteristic of K, and $\zeta_n \in K$.*

Such an extension is Galois, and its Galois group is cyclic of order dividing n. Kummer theory provides the following characterization:

Theorem. *Let K be a field. Let $n \geq 1$ be not divisible by the characteristic of K, and suppose that $\zeta_n \in K$. A finite Galois extension of K whose Galois group is cyclic of order dividing n is a cyclic Kummer extension.*

If L is a cyclic Kummer extension of K of degree n, we can associate to L the subgroup of $K^\times$ consisting of the elements which have some (hence all) n-th roots in L. We are associating to L a subgroup Δ of $K^\times$ satisfying the following properties: it contains $K^{\times n}$; the quotient $\Delta/K^{\times n}$ is a cyclic group of order n. The map $L \mapsto \Delta$ which sends a cyclic Kummer extension of K of degree n into a subgroup of $K^\times$ with the above properties, is bijective.

Let $a \in K^\times$, and consider the field $L = K(\sqrt[n]{a})$ which is associated to $\Delta = \langle a, K^{\times n}\rangle$. There is a canonical isomorphism

$$\Delta/K^{\times n} \simeq \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$$

such that the class of a is mapped to the character $\chi_a : \sigma \mapsto \alpha^{\sigma-1}$, where $\alpha \in \bar{K}$ is such that $\alpha^n = a$. Notice that this character does not depend on the choice of α.

The degree of L/K divides n and it is, equivalently: the order of $\Delta/K^{\times n}$; the order of the class of a in $K^\times/K^{\times n}$; the smallest d such that $\alpha^d \in K^\times$; the integer d for which n/d is the greatest divisor of n such that a has some (n/d)-th roots in K.

The field $K(\sqrt[n]{a^{n/d}}) = K(\sqrt[d]{a})$ is the unique subextension of $K(\sqrt[n]{a})$ of degree d: it is a cyclic Kummer extension of degree d. If t is coprime to n, we have $K(\sqrt[n]{a^t}) = K(\sqrt[n]{a})$.

If we consider the factorization $n = \prod p^e$ then $K(\sqrt[n]{a})$ is the composite of the extensions $K(\sqrt[p^e]{a})$, which have coprime degrees.

Lemma 4. *Let K be a field. Let $n \geq 1$ be not divisible by the characteristic of K, and suppose that $\zeta_n \in K$. If $a, b \in K^\times$ are such that $K(\sqrt[n]{a}) = K(\sqrt[n]{b})$ then $a = b^t\gamma^n$ for some $\gamma \in K^\times$ and for some t coprime to n.*

Proof. Since $\langle a, K^{\times n}\rangle = \langle b, K^{\times n}\rangle$, we have $a = b^t\gamma^n$ for some integer t and for some $\gamma \in K^\times$. Since the classes of a and b in $K^\times/K^{\times n}$ have the same order then t is coprime to n. □

Lemma 5. *Let K be a field. Let $n \geq 1$ be not divisible by the characteristic of K, and suppose that $\zeta_n \in K$. If $a, b \in K^\times$ are such that the fields $K(\sqrt[n]{a})$ and $K(\sqrt[n]{b})$ are either linearly disjoint over K, or if for every $\ell \mid n$ the ℓ-adic valuation of their degrees over K are different, then we have*

$$\big[K(\sqrt[n]{ab}) : K\big] = \operatorname{lcm}\big([K(\sqrt[n]{a}) : K], [K(\sqrt[n]{b}) : K]\big)$$

Proof. It suffices to compare the order of the characters χ_a, χ_b, χ_{ab}. □

Lemma 6. *Let K be a field. Let ℓ be a prime number not dividing the characteristic of K. Let $n \geq 0$, and suppose that $\zeta_{\ell^n} \in K$. If $a \in K^\times$ then either $K(\sqrt[\ell^n]{a}) = K$ or there is some smallest $h \geq 1$ such that $K(\sqrt[\ell^h]{a}) \neq K$ and we have*

$$[K(\sqrt[\ell^n]{a}) : K] = \ell^{n-h+1}$$

Proof. By assumption, $\chi_{a^{\ell^{(n-h-1)}}}$ is the trivial character while $\chi_{a^{\ell^{(n-h)}}}$ is non-trivial. We deduce that the second has order ℓ hence χ_a has order ℓ^{n-h+1}. □

The key ingredient for this paper is the following result of Schinzel:

Theorem 7 ([7, theorem 2])**.** *Let K be a field, and let $n \geq 1$ be not divisible by the characteristic of K. Let $a \in K^\times$. The extension $K_n(\sqrt[n]{a})/K$ is abelian if and only if $a^m = \gamma^n$ for some $\gamma \in K^\times$ and for some divisor m of n such that $\zeta_m \in K$.*

Proof of Schinzel's theorem by Stevenhagen and by Wójcik ([4], [11]). First suppose that $a^m = \gamma^n$ with γ and m as in the statement. Then $K_n(\sqrt[n]{a})$ is contained in the compositum of the fields $K(\sqrt[m]{\gamma})$ and K_n. By definition of m the first field is a cyclic Kummer extension of K, while the second field is a cyclotomic extension of K. They are both abelian extensions of K therefore their compositum, and in particular $K_n(\sqrt[n]{a})$, is an abelian extension of K. For the other implication, let $G = \operatorname{Gal}(K_n(\sqrt[n]{a})/K)$ and suppose that G is abelian. Fix some n-th root α of a in $K_n(\sqrt[n]{a})$. For each $\sigma \in G$, one has $\zeta_\sigma := \sigma(\alpha)/\alpha \in \langle\zeta_n\rangle$, and $\sigma(\zeta_n) = \zeta_n^{c(\sigma)}$ for some $c(\sigma) \in \mathbb{Z}$. For any σ, $\tau \in G$ one has

$$\tau(\alpha^{c(\sigma)})/\alpha^{c(\sigma)} = \zeta_\tau^{c(\sigma)} = \sigma\big(\tau(\alpha)/\alpha\big) = \tau\sigma(\alpha)/\sigma(\alpha)$$

hence $\alpha^{c(\sigma)}/\sigma(\alpha)$ is fixed by all τ so it belongs to K, and taking the n-th power one sees that $a^{c(\sigma)-1} \in K^{\times n}$. Let m denote the gcd of n and all numbers $c(\sigma) - 1$ for σ varying in G. Then $a^m \in K^{\times n}$. Since $m \mid n$ and $m \mid c(\sigma) - 1$ for every $\sigma \in G$, we have $\sigma(\zeta_m)/\zeta_m = 1$ for every $\sigma \in G$ hence $\zeta_m \in K$. □

We end this section by explaining a convenient way of writing the elements of $K^\times$:

Definition 8. *Let K be a field, and let ℓ be a prime number different from the characteristic of K. Let $a \in K^\times$. We say that a is* strongly ℓ-indivisible *in K if $a\mu$ has no ℓ-th roots in K, for every root of unity $\mu \in K$ of order a power of ℓ.*

Note, the roots of unity in K are not strongly ℓ-indivisible. If a has ℓ^n-th roots of unity in K for every $n \geq 1$ then we say that a is ℓ^∞-divisible in K. If $a\mu$ is ℓ^∞-divisible in K for some root of unity $\mu \in K$ then we may replace a by μ^{-1} and our problem is easily solved by lemma 2. In the remaining cases, we can express a as the power of a strongly ℓ-indivisible element times a root of unity in K:

Lemma 9. *Let K be a field, and let ℓ be a prime number different from the characteristic of K. Then one of the following holds:*

(i) we have $a = b^{\ell^d}$ for some $d \geq 0$ and for some $b \in K^\times$ strongly ℓ-indivisible

(ii) (supposing that $K_{\ell^\infty} \neq K$, let $t \geq 0$ be maximal such that $K_{\ell^t} = K$) we have $a = b^{\ell^d}\mu$ for some $d > 0$, for some $b \in K^\times$ strongly ℓ-indivisible and for some root of unity μ in K of order ℓ^r with $r > \max(0, t - d)$

(iii) $a\mu$ is ℓ^∞-divisible in K for some root of unity $\mu \in K$

Proof. Suppose that there exists $d \geq 0$ is maximal such that we can write $a = b^{\ell^d}\mu$ for some $d \geq 0$, for some $b \in K^\times$ and for some root of unity μ in K of order ℓ^r with $r \geq 0$. Then b is strongly ℓ-indivisible by maximality of d. If $0 \neq r \leq t - d$, we may replace b so to get $\mu = 1$. Now suppose that there is no such maximal d. If $K = K_{\ell^\infty}$ this means that a is ℓ^∞-divisible in K. If $K \neq K_{\ell^\infty}$, since the number of roots of unity in K of order a power of ℓ is finite we have an infinite sequence of integers h such that $a = b_h^{\ell^h}\mu$ for some $b_h \in K^\times$ and for some fixed $\mu \in K^\times$ of order ℓ^r with $r \geq 0$. Then $a\mu^{-1}$ is ℓ^∞-divisible in K. □

Note, in the lemma the integers d and r do not depend of the choice of b and μ because b is strongly ℓ-indivisible. Moreover, we are in case (iii) if and only if $K_{\ell^\infty}(\sqrt[\ell^\infty]{a}) = K_{\ell^\infty}$, so in particular when a is a root of unity.

Remark 10. *We will assume $K_{\ell^\infty}(\sqrt[\ell^\infty]{a}) \neq K_{\ell^\infty}$ in what follows because otherwise our problem is easily solved by lemma 2.*

4 The degree of Kummer extensions: the case ℓ odd or $\zeta_4 \in K$

In this section, ℓ is a prime number and K is a field of characteristic different from ℓ. If $\ell = 2$, we suppose that $\zeta_4 \in K$. Let t be the greatest positive integer such that $K_{\ell^t} = K$, or $t = \infty$ if no such number exists (if $\ell = 2$, we have by assumption $t \geq 2$).

Theorem 11. *Let $a \in K^\times$ satisfy $K_{\ell^\infty}(\sqrt[\ell^\infty]{a}) \neq K_{\ell^\infty}$. Let $m \geq n > 0$ and without loss of generality suppose $m \geq t$. If a is strongly ℓ-indivisible we have*

$$[K_{\ell^m}(\sqrt[\ell^n]{a}) : K_{\ell^m}] = \ell^n$$

and more generally if $a = b^{\ell^d}$ for some $b \in K^\times$ strongly ℓ-indivisible and for some $d \geq 0$ we have

$$[K_{\ell^m}(\sqrt[\ell^n]{a}) : K_{\ell^m}] = \max(1, \ell^{n-d}) .$$

In the remaining case, we have $t \neq \infty$ and we can write $a = b^{\ell^d}\mu$ for some $b \in K^\times$ strongly ℓ-indivisible, for some $d > 0$, and for some root of unity $\mu \in K$ of order ℓ^r with $r > \max(0, t-d)$. Then we have

$$[K_{\ell^m}(\sqrt[\ell^n]{a}) : K_{\ell^m}] = \max(1, \ell^{n-d}, \ell^{n+r-m}) .$$

Note, if $\zeta_\ell \notin K$ and $K_{\ell^\infty}(\sqrt[\ell^\infty]{a}) \neq K_{\ell^\infty}$ then a is the power of a strongly ℓ-indivisible element.

Lemma 12. *If a is strongly ℓ-indivisible then the field $K_\ell(\sqrt[\ell]{a})$ is not contained in K_{ℓ^∞}.*

Proof. Suppose that $K_\ell(\sqrt[\ell]{a})$ is contained in K_{ℓ^h} for some $h \geq 0$ so in particular that it is an abelian extension of K. If $K_\ell \neq K$ then by theorem 7 we deduce $a = \gamma^\ell$ for some $\gamma \in K$, contradicting the assumption on a. If $K_\ell = K$, since $K \neq K(\sqrt[\ell]{a}) \subseteq K_{\ell^h}$, we must have $K(\sqrt[\ell]{a}) = K_{\ell^{t+1}}$. Thus $K(\sqrt[\ell]{a}) = K(\sqrt[\ell]{\zeta_{\ell^t}})$ and so by lemma 4 we have $a = \gamma^\ell \zeta_{\ell^t}$. Since $\zeta_{\ell^t} \in K$, this contradicts the assumption on a. □

Proof of theorem 11. Case 1: Suppose that $a = b^{\ell^d}$ for some $d \geq 0$ and for some $b \in K^\times$ strongly ℓ-indivisible. We have shown in lemma 12 that $[K_{\ell^m}(\sqrt[\ell]{b}) : K_{\ell^m}] = \ell$ so by lemma 6 we have $[K_{\ell^m}(\sqrt[\ell^{n-d}]{b}) : K_{\ell^m}] = \ell^{n-d}$. We conclude because $K_{\ell^m}(\sqrt[\ell^n]{a}) = K_{\ell^m}(\sqrt[\ell^{n-d}]{b})$ if $d \leq n$ and $K_{\ell^m}(\sqrt[\ell^n]{a}) = K_{\ell^m}$ if $d \geq n$.

Case 2: Suppose that $t \neq \infty$, $a = b^{\ell^d}\mu$ for some $d \geq 0$, for some $b \in K^\times$ strongly ℓ-indivisible and for some root of unity μ in K of order ℓ^r such that $r > \max(0, t-d)$. Call $\gamma = a\mu^{-1} = b^{\ell^d}$. We have just shown that the extensions $K_{\ell^m}(\sqrt[\ell^n]{\gamma})$ and $K_{\ell^m}(\sqrt[\ell^n]{\mu})$ are linearly disjoint over K_{ℓ^m}. So by lemma 5 the degree of $K_{\ell^m}(\sqrt[\ell^n]{a})$ over K_{ℓ^m} is the least common multiple of the degrees of $K_{\ell^m}(\sqrt[\ell^n]{\gamma})$ and of $K_{\ell^m}(\sqrt[\ell^n]{\mu})$. The degree of $K_{\ell^m}(\sqrt[\ell^n]{\gamma})$ over K_{ℓ^m} was evaluated above as $\max(1, \ell^{n-d})$. The degree of $K_{\ell^m}(\sqrt[\ell^n]{\mu})$ over K_{ℓ^m} is $\max(1, \ell^{n+r-m})$ by lemma 2. □

5 The degree of Kummer extensions: the case $\ell = 2$ and $\zeta_4 \notin K$

In this section, K is a field of odd characteristic such that $\zeta_4 \notin K$. Let s be the greatest integer such that $K_4 = K_{2^s}$, or $s = \infty$ if no such number exists.

Lemma 13. *Let $a \in K^\times$ be strongly 2-indivisible. Then $K(\sqrt[4]{a}) \not\subseteq K_{2^\infty}$ and we have $K(\sqrt{a}) \subseteq K_{2^\infty}$ if and only if*

$$\begin{aligned} K \cap \mathbb{F}_{2^\infty} &= \mathbb{F}(\zeta_{2^s} + \zeta_{2^s}^{-1}) \\ a &= \pm(\zeta_{2^s} + \zeta_{2^s}^{-1} + 2) \cdot \eta^2 \end{aligned} \tag{1}$$

where $\mathbb{F}$ is the prime field, $\eta \in K$ and $s \geq 2$ is an integer. In this case, we have $K(\sqrt{a}) \subseteq K_{2^m}$ if and only if $m \geq s+1$.

Proof. Suppose that $K(\sqrt[4]{a}) \subseteq K_{2^\infty}$. Then $K(\sqrt[4]{a})$ would be an abelian extension of K so by theorem 7 we find that $a^2 = \gamma^4$ for some $\gamma \in K$. This implies $a = \pm\gamma^2$ so it contradicts the assumption on a.

Note, $K(\sqrt{a})$ does not contain ζ_4 because otherwise $K(\sqrt{a}) = K(\sqrt{-1})$ hence by lemma 4 we would have $a = -\gamma^2$ for some $\gamma \in K$, contradicting the assumption on a. Also $K(\sqrt{a}) \neq K$, again because a is strongly 2-indivisible.

Suppose that $K(\sqrt{a}) \subseteq K_{2^\infty}$. Since $[K(\sqrt{a}) : K] = 2$ and $\zeta_4 \notin K(\sqrt{a})$, by lemma 1 we must have $K \cap \mathbb{F}_{2^\infty} = \mathbb{F}(\zeta_{2^s} + \zeta_{2^s}^{-1})$ for some $s \geq 2$ (we cannot have $s = \infty$). We then deduce from lemma 1 that

$$K(\sqrt{a}) = K\left(\sqrt{\pm(\zeta_{2^s} + \zeta_{2^s}^{-1} + 2)}\right).$$

By lemma 4, it follows that $a = \pm(\zeta_{2^s} + \zeta_{2^s}^{-1} + 2) \cdot \eta^2$ for some $\eta \in K$. It is clear that if a satisfies condition (1) then $K(\sqrt{a}) \subseteq K_{2^\infty}$. By lemma 1, we conclude that in this case $K(\sqrt{a}) \subseteq K_{2^{s+1}}$ and $K(\sqrt{a}) \not\subseteq K_{2^s}$. □

Theorem 14. *Let $a \in K^\times$ satisfy $K_{2^\infty}(\sqrt[2^\infty]{a}) \neq K_{2^\infty}$. Let n, m be such that $m \geq n > 0$.*

(i) If $a = b^{2^d}$ for some $d \geq 0$ and some $b \in K^\times$ which is strongly 2-indivisible then we have:

$$[K_{2^m}(\sqrt[2^n]{a}) : K_{2^m}] = \begin{cases} 1 & \text{if } n \leq d \\ 2^{n-d-1} & \text{if } n > d \text{ and } K(\sqrt{b}) \subseteq K_{2^\infty},\ m \geq s+1 \\ 2^{n-d} & \text{otherwise} \end{cases}$$

(ii) If $a = -b^{2^d}$ for some $d > 0$ and for some $b \in K^\times$ which is strongly 2-indivisible, let $h \geq 0$ be such that $2^h = [K_{2^m}(\sqrt[2^n]{-a}) : K_{2^m}]$. Then we have:

$$[K_{2^m}(\sqrt[2^n]{a}) : K_{2^m}] = \begin{cases} 2 & \text{if } m = 1 \text{ or if } h = 0,\ s \neq \infty \text{ and } m = n \geq s \\ 1 & \text{if } h = 1,\ K(\sqrt{b}) \subseteq K_{2^\infty} \text{ and } m = n = s = d+1 \\ 2^h & \text{otherwise} \end{cases}$$

Recall from lemma 13 that $K(\sqrt{b}) \subseteq K_{2^\infty}$ if and only if

$$\begin{array}{ll} K \cap \mathbb{F}_{2^\infty} = \mathbb{F}(\zeta_{2^s} + \zeta_{2^s}^{-1}) & \textit{for some } s \geq 2 \\ b = \pm(\zeta_{2^s} + \zeta_{2^s}^{-1} + 2) \cdot \eta^2 & \textit{for some } \eta \in K \end{array}$$

where $\mathbb{F}$ is the prime field.

Proof. By combining lemma 6 and lemma 13 we have

$$[K_{2^m}(\sqrt[2^n]{b}) : K_{2^m}] = \begin{cases} 2^{n-1} & \text{if } K(\sqrt{b}) \subseteq K_{2^\infty} \text{ and } m \geq s+1 \\ 2^n & \text{otherwise} \end{cases}$$

The formulas for the case $a = b^{2^d}$ follow at once because $K_{2^m}(\sqrt[2^n]{a}) = K_{2^m}(\sqrt[2^{n-d}]{b})$ if $n > d$ and $K_{2^m}(\sqrt[2^n]{a}) = K_{2^m}$ if $n \leq d$.

Let us now consider the case $a = -b^{2^d}$, where $d > 0$. If $m = 1$ then $n = 1$ and so the degree of $K_2(\sqrt{a}) = K_4$ over $K_2 = K$ is 2.

From now on, let $m \geq 2$. Let 2^h be the degree of $K_{2^m}(\sqrt[2^n]{-a})$ over K_{2^m}, which can be evaluated by the previous case. Since $m \geq n$ and $m \geq 2$, we have

$$[K_{2^m}(\sqrt[2^n]{-1}) : K_{2^m}] = \begin{cases} 2 & \text{if } s \neq \infty \text{ and } n = m \geq s \\ 1 & \text{otherwise} \end{cases}$$

Thus, unless $s \neq \infty$ and $n = m \geq s$, we have $K_{2^m}(\sqrt[2^n]{a}) = K_{2^m}(\sqrt[2^n]{-a})$ and the requested degree is 2^h.

Now we treat the remaining case: we have $s \neq \infty$, $n = m \geq s$, $K_{2^n}(\sqrt[2^n]{-1}) = K_{2^{n+1}}$ and $[K_{2^{n+1}} : K_{2^n}] = 2$. If $h = 0$, the requested degree is 2 because $K_{2^n}(\sqrt[2^n]{a}) = K_{2^n}(\sqrt[2^n]{-1})$. If $h > 1$, the requested degree is 2^h by lemma 5.

We are left with $h = 1$, and so the fields $K_{2^n}(\sqrt[2^n]{-a})$ and $K_{2^n}(\sqrt[2^n]{-1})$ have both degree 2 over K_{2^n}. If the two fields are different then they are linearly disjoint and the requested degree is 2 by lemma 5. If the two fields are equal then a is a 2^n-th power in K_{2^n} by lemma 4 hence the requested degree is 1. We now prove that the two fields coincide if and only if $K(\sqrt{b}) \subseteq K_{2^\infty}$ and $n = s = d + 1$. These conditions are sufficient because (14) holds. We now prove that they are necessary. Since $h = 1$, we must have $n > d$ and in particular $K(\sqrt{b}) \subseteq K_{2^\infty}$. We are supposing that $K_{2^n}(\sqrt[2^{n-d}]{b}) = K_{2^{n+1}}$ so by lemma 13 we have $n - d < 2$. Thus $n = d + 1$. We have $K_{2^n}(\sqrt{b}) = K_{2^{n+1}} \not\subseteq K_{2^n}$ so from lemma 13 we deduce that $n < s + 1$ hence $n = s$. □

6 The general case

Let K be a field. In this section, we are concerned with studying the degree of a cyclic Kummer extension of the form $K_m(\sqrt[n]{a})/K_m$, where $a \in K^\times$ and where $m, n \geq 1$ are

such that $n \mid m$ and m is coprime to the characteristic of K. Suppose that a is strongly ℓ-indivisible for every ℓ dividing n. Then in the generic case we have $[K_m(\sqrt[n]{a}) : K_m] = n$, nevertheless this degree could also be any divisor d of n. We can reduce to the case where n is a prime power:

Lemma 15. *Suppose that for every prime divisor ℓ of n we can find $a_\ell \in K^\times$ which is strongly ℓ-indivisible and such that $[K_m(\sqrt[\ell^{v_\ell(n)}]{a_\ell}) : K_m] = \ell^{v_\ell(d)}$. Then there is $a \in K^\times$ which is strongly ℓ-indivisible for every prime ℓ dividing n, and such that $[K_m(\sqrt[\ell^n]{a}) : K_m] = d$.*

Proof. Write $a'_\ell := a_\ell^{n/\ell^{v_\ell(n)}}$ and $a := \prod a'_\ell$. We have $[K_m(\sqrt[n]{a'_\ell}) : K_m] = \ell^{v_\ell(d)}$ for every ℓ. Note that $a \in K^\times$ and is strongly ℓ-indivisible for any prime number ℓ dividing n, so it suffices to apply lemma 5. □

We may then restrict to studying cyclic Kummer extensions of prime power degree.

Theorem 16. *Let K be a field. Let $m \geq 1$ be not divisible by the characteristic of K. Let ℓ be a prime divisor of m, and let $n \geq 1$ satisfy $\ell^n \mid m$. Suppose that for some $a \in K^\times$ which is strongly ℓ-indivisible we have*

$$[K_m(\sqrt[\ell^n]{a}) : K_m] = \ell^{n-d}$$

for some $0 < d \leq n$. Then $\zeta_{\ell^d} \in K$. Moreover there is some odd prime $q \neq \ell$ dividing m such that $\ell^d \mid [K_q : K]$, unless $\ell = 2$, $d = 1$ and $K(\sqrt{a}) \subseteq K_{2^{v_2(m)}}$.

Note, Lemma 6 implies that $[K_m(\sqrt[\ell^n]{a}) : K_m] = \ell^{n-d}$ is equivalent to $K_m(\sqrt[\ell^d]{a}) = K_m$ and either $d = n$ or $K_m(\sqrt[\ell^{d+1}]{a}) \neq K_m$.

Proof. We first show that $\zeta_{\ell^d} \in K$. Since $K_m(\sqrt[\ell^d]{a}) = K_m$, in particular $K_{\ell^d}(\sqrt[\ell^d]{a})$ is an abelian extension of K. Theorem 7 implies that $a^{\ell^e} = \gamma^{\ell^d}$ for some $\gamma \in K^\times$, and for some $e \geq 0$ such that $\zeta_{\ell^e} \in K$. Since a is strongly ℓ-indivisible, we have $d \leq e$ hence $\zeta_{\ell^d} \in K$.

Let $m' := \ell^{v_\ell(m)} \cdot \prod q$ where the product is taken over the odd primes $q \neq \ell$ dividing m such that $q \equiv 1 (\mathrm{mod}\, \ell)$. Then $K_m(\sqrt[\ell^d]{a}) = K_m$ if and only if $K_{m'}(\sqrt[\ell^d]{a}) = K_{m'}$ because $K_m/K_{m'}$ has degree coprime to ℓ. Note, the Galois group of $K_{m'}/K$ is the product of the Galois groups of $K_{\ell^{v_\ell(m)}}/K$ and of the extensions K_q/K.

Suppose that $K_{\ell^{v_\ell(m)}}(\sqrt[\ell^d]{a})/K_{\ell^{v_\ell(m)}}$ has degree ℓ^d. Then $K_{m'}/K_{\ell^{v_\ell(m)}}$ contains a cyclic subextension of degree ℓ^d hence the Galois group of some extension K_q/K has exponent divisible by ℓ^d. Since a is strongly ℓ-indivisible, theorems 11 and 14 imply that in the remaining case we have $\ell = 2$, and $d = 1$ because $\zeta_{2^d} \in K$. In particular $K_{\ell^{v_\ell(m)}}(\sqrt[\ell^d]{a})/K_{\ell^{v_\ell(m)}}$ has degree 1. □

We now argument that the degree of $K_m(\sqrt[\ell^n]{a})/K_m$ could take as value any possibile divisor of ℓ^n, even if we require a to be strongly ℓ-indivisible:

Theorem 17. *Let K be a field. Let ℓ be a prime different from the characteristic of K, and suppose that $K^\times/K^{\times\ell}$ is infinite. Let $m \geq 1$ be not divisible by the characteristic of K. If $n \geq 1$ is such that $\ell^n \mid m$, and $d \geq 0$ is either zero or we have $d \leq n$, $\zeta_{\ell^d} \in K$ and $\ell^d \mid [K_q : K]$ for some odd prime $q \neq \ell$ dividing m, then there is some $a \in K^\times$ which is strongly ℓ-indivisible and such that*

$$[K_m(\sqrt[\ell^n]{a}) : K_m] = \ell^{n-d}\,.$$

Proof. Let $b \in K^\times$ be such that $\sqrt[\ell]{b}$ is not contained in K_m: such an element exists because K_m contains only finitely many subextensions of degree ℓ while $K^\times/K^{\times\ell}$ is infinite. Suppose that $d \geq 1$. By assumption, there is a cyclic Kummer extension C of K of degree ℓ^d contained in K_q. Let $a \in K^\times$ be such that $C = K(\sqrt[\ell^d]{a})$. In particular, the degree $\delta := [K_m(\sqrt[\ell^n]{a}) : K_m]$ divides ℓ^{n-d}. If $\delta \neq \ell^{n-d}$ it suffices to replace a by ab^{ℓ^d}, so that $K_m(\sqrt[\ell^d]{a}) = C$ but $K_m(\sqrt[\ell^{d+1}]{a}) \not\subseteq K_m$. Then a is strongly ℓ-indivisible: if $a = \gamma^\ell\mu$ for some $\gamma \in K^\times$ and $\mu \in K$ then $\sqrt[\ell]{a}$ belongs to K_{ℓ^∞} but since it is not in K (cf. lemma 6) then it cannot be in K_q, contradiction. Now let $d = 0$. We have $[K_m(\sqrt[\ell^n]{b}) : K_m] = \ell^n$ by lemma 6. It is left to show that b is strongly ℓ-indivisible. If $K = K_{\ell^\infty}$ or if $\zeta_\ell \notin K$ this is equivalent to the condition that b has no ℓ-th roots in K, so it is true by the choice of b. Otherwise, if $t \geq 1$ is the greatest integer such that $K = K_{\ell^t}$ then it suffices to choose b such that $\sqrt[\ell]{b}$ is not contained in $K_{m\ell^{t+1}}$. □

Appendix: The density of sets of primes related to the reductions of an algebraic number

Let K be a number field, and let $a \in K^\times$. Let ℓ be a prime number. In this section we are concerned with computing the density of the set of primes $\mathfrak{p}$ of K such that the multiplicative order of the reduction of a modulo $\mathfrak{p}$ has a prescribed ℓ-adic valuation, namely

$$\mathrm{dens}(a, n) = \mathrm{dens}\{\mathfrak{p} : \mathrm{ord}_\ell(a \bmod \mathfrak{p}) = n\}$$

for some $n \geq 0$. We tacitly assume that $(a \bmod \mathfrak{p})$ is well-defined, so we exclude the finitely many primes $\mathfrak{p}$ such that $v_\mathfrak{p}(a) < 0$. These values are known if $K = \mathbb{Q}$ (cf. [5]) or under the assumption that $K_{\ell^n}(\sqrt[\ell^n]{a})/K$ has degree $\phi(\ell^n)\ell^n$ for all $n \geq 1$ (cf. [2]): notice that in this last case a is strongly ℓ-indivisible. Recall that the density exists, and that it is a natural density (cf. [2]). Suppose that a is not a root of unity, because otherwise the the density is trivially either 0 or 1.

The results in this paper suffice to calculate the density, because of the following well-known formula:

Lemma 18.

$$\mathrm{dens}(a, 0) = \sum_{i \geq 0} [K_{\ell^i}(\sqrt[\ell^i]{a}) : K]^{-1} - [K_{\ell^{i+1}}(\sqrt[\ell^i]{a}) : K]^{-1}$$

Proof. Recall that only finitely many primes of K ramify in $K_{\ell^i}(\sqrt[\ell^i]{a})$ for some $i \geq 0$ (it is a consequence of the fact that, for a number field, for almost all primes the reduction is injective on the roots of unity of order a power of ℓ contained in the field). Let $\mathfrak{p}$ be a prime of K which does not ramify in any of these extensions, and suppose that $(a \bmod \mathfrak{p})$ has order coprime to ℓ, or equivalently that it has some ℓ^n-th root in the residue field $k_\mathfrak{p}$ for every $n \geq 1$. Let $i \geq 0$ be the greatest integer such that the residue field $k_\mathfrak{p}$ contains the ℓ^i-th roots of unity. Then $\mathfrak{p}$ belongs to the following set of primes of K: the primes which split completely in $K_{\ell^i}(\sqrt[\ell^i]{a})$ but not in $K_{\ell^{i+1}}(\sqrt[\ell^i]{a})$. Note, for different i we obtain disjoint sets. Conversely, for such a prime $\mathfrak{p}$ and if i is defined as above, $(a \bmod \mathfrak{p})$ has order coprime to ℓ because there are no elements in $k_\mathfrak{p}^*$ of order ℓ^{i+1}. We conclude by applying the Chebotarev Density Theorem: the sum converges because the density of the i-th set goes to zero for i going to infinity. □

The following remark can be used to reduce the calculation of $\mathrm{dens}(a, n)$ to the case where $n = 0$.

Remark 19. *For every $n \geq 1$ we have*

$$\mathrm{dens}(a, n) = \mathrm{dens}(a^{\ell^n}, 0) - \mathrm{dens}(a^{\ell^{n-1}}, 0)\,.$$

For $\ell = 2$, we have $\mathrm{dens}(a, 0) = \mathrm{dens}(-a, 1)$ and $\mathrm{dens}(a, n) = \mathrm{dens}(-a, n)$ if $n \geq 2$.

Proof. The first assertion is immediate from the definition. For the others, notice that $(-1 \bmod p)$ is the only element of order 2 in $(\mathbb{Z}/\mathbb{Z}p)^*$, for every odd prime number p. □

The density if ℓ is odd or $i \in K$

Let ℓ be a prime number. Let K be a number field. Let $a \in K^\times$ be not a root of unity.

1. Suppose that $K_\ell \neq K$ (hence ℓ is odd). Write $a = b^{\ell^d}$ for some $d \geq 0$ and for some $b \in K$ which is strongly ℓ-indivisible. Then we have:

$$\mathrm{dens}(a, 0) = 1 - [K_\ell : K]^{-1} \cdot \frac{\ell}{\ell + 1} \cdot \ell^{-d}$$

2. Suppose that $K_\ell = K$ and, if $\ell = 2$, suppose that $i \in K$. Let $t > 0$ be the greatest positive integer such that $K_{\ell^t} = K$.

   (i) Let $a = b^{\ell^d}$ for some $d \geq 0$ and for some $b \in K$ which is strongly ℓ-indivisible. Then we have:

$$\mathrm{dens}(a, 0) = \begin{cases} \frac{\ell}{\ell+1} \cdot \ell^{-t} \cdot \ell^d & \text{if } d < t \\ 1 - \frac{\ell+2}{\ell(\ell+1)} \cdot \ell^t \cdot \ell^{-d} & \text{if } d \geq t \end{cases}$$

(ii) Let $a = b^{\ell^d}\mu$ for some $d \geq 0$, for some $b \in K$ which is strongly ℓ-indivisible, for some root of unity $\mu \in K$ of order ℓ^r such that $r > \max(0, t-d)$. Then we have:

$$\mathrm{dens}(a, 0) = \ell^{-r} - \frac{1}{\ell+1} \cdot \ell^{-2r-d+t}$$

The density if $\ell = 2$ and $i \notin K$

Let K be a number field such that $i \notin K$. Let $a \in K^\times$ be not a root of unity.

1. Let $a = b^{2^d}$ for some $d \geq 0$ and for some $b \in K$ which is strongly 2-indivisible. Then we have:

$$\mathrm{dens}(a, 0) = \begin{cases} 1 - \frac{2}{3} \cdot 2^{-d} & \text{if } K(\sqrt{b}) \not\subseteq K_{2^\infty} \\ 1 - \frac{2}{3} \cdot 2^{-d} - \frac{2}{3} \cdot 2^{-2s+d} & \text{if } K(\sqrt{b}) \subseteq K_{2^\infty} \text{ and } d < s \\ 1 - \frac{1}{3} \cdot 2^{-d} & \text{if } K(\sqrt{b}) \subseteq K_{2^\infty} \text{ and } d \geq s \end{cases}$$

2. Let $a = -b^{2^d}$ for some $d \geq 0$ and for some $b \in K$ which is strongly 2-indivisible. Then we have:

$$\mathrm{dens}(a, 0) = \begin{cases} \frac{1}{3} \cdot 2^{-d} & \text{if } K(\sqrt{b}) \not\subseteq K_{2^\infty} \\ \frac{1}{3} \cdot 2^{-d} - \frac{2}{3} \cdot 2^{-2s+d} & \text{if } K(\sqrt{b}) \subseteq K_{2^\infty} \text{ and } d < s-1 \\ \frac{4}{3} \cdot 2^{-s} & \text{if } K(\sqrt{b}) \subseteq K_{2^\infty} \text{ and } d = s-1 \\ \frac{1}{6} \cdot 2^{-d} & \text{if } K(\sqrt{b}) \subseteq K_{2^\infty} \text{ and } d \geq s \end{cases}$$

Recall from lemma 13 that $K(\sqrt{b}) \subseteq K_{2^\infty}$ if and only if

$$\begin{array}{ll} K \cap \mathbb{Q}_{2^\infty} = \mathbb{Q}(\zeta_{2^s} + \zeta_{2^s}^{-1}) & \text{for some } s \geq 2 \\ b = \pm(\zeta_{2^s} + \zeta_{2^s}^{-1} + 2) \cdot \eta^2 & \text{for some } \eta \in K \end{array}$$

References

[1] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[2] R. Jones and J. Rouse, *Iterated endomorphisms of abelian algebraic groups.*, Proc. Lond. Math. Soc. **100** (2010), no. 3, 763–794.

[3] F. Halter-Koch, *Eine Galoiskorrespondenz für Radikalerweiterungen*, J. Algebra **63** (1980), no. 2, 318–330.

[4] H. W. Jr. Lenstra, *Commentary on H: Divisibility and congruences.* Andrzej Schinzel, Selected papers, European Mathematical Society, Zürich, 2007, vol. II, 901–902.

[5] P. Moree, *On primes p for which d divides* ord(g), Funct. Approx. Comment. Math. **33** (2005), 85–95.

[6] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften 322, Springer-Verlag, Berlin, 1999.

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

[8] E. T. Jacobson and W. Y. Vélez, *The Galois group of a radical extension of the rationals*, Manuscripta Math. **67** (1990), no. 3, 271–284.

[9] F. Barrera-Mora and W. Y. Vélez, *Some results on radical extensions*, J. Algebra **162** (1993), no. 2, 295–301.

[10] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics 83, Springer-Verlag, New York, 1997.

[11] J. Wójcik, *Criterion for a field to be abelian*, Colloq. Math. **68** (1995), no. 2, 187–191.