LINEAR RELATIONS AMONG RADICALS

ANTONELLA PERUCCA

In memory of Marc Rybowicz

ABSTRACT. Let K be a field, fix an algebraic closure $\overline{K}$, and let G be a subgroup of $\overline{K}^\times$. We are able to give a closed formula for the ratio between the degree $[K(G):K]$ and the index $|GK^\times : K^\times|$, provided that the latter is finite. Our formula explains all the K-linear relations among radicals, which (beyond the ones stemming from the multiplicative group $GK^\times/K^\times$) are generated by relations among roots of unity and single radicals. Our work builds on results by Rybowicz, which in turn are based on Kneser's theorem on the linear independence of radicals.

1. INTRODUCTION

We let K be a field, for which we fix an algebraic closure $\overline{K}$. We consider the *radicals* over K, by which we mean the elements $\alpha \in \overline{K}^\times$ for which there exists a positive integer n such that $\alpha^n \in K^\times$. We fix a group G of radicals such that the *index* $|GK^\times : K^\times|$ is finite and investigate the *degree* $[K(G) : K]$. (Note that the extension $K(G)/K$ is in general not Galois, but it is separable if the index is not divisible by the characteristic.) More precisely, we compare the index and the degree, keeping in mind that the former (which is usually easier to compute) will let us understand the latter. What is true in general is that

$$[K(G) : K] \leqslant |GK^\times : K^\times| \tag{1}$$

because representants for $GK^\times/K^\times$ can be taken as generators for the K-vector space $K(G)$ (and indeed the multiplicative relations that determine the index also affect the degree). Having a strict inequality in (1) is a phenomenon that is called *entanglement* of radicals. Note that the degree does not necessarily divide the index: for example, if $K = \mathbb{Q}$ and p is an odd prime number and G is generated by a root of unity of order p, then the ratio degree/index is $(p-1)/p$.

Consider the setting of Kummer theory, namely suppose that the exponent n of the group $GK^\times/K^\times$ has the following two properties: n is not divisible by the characteristic of K; $K^\times$ contains a root of unity of order n. In this case, the group $GK^\times/K^\times$ is isomorphic to $G^nK^{\times n}/K^{\times n}$ hence the core result of Kummer theory states that we have an equality in 1 (see for example [8, Chapter VI, Section 8]).

Going beyond Kummer theory, Kneser [7] has shown that we have an equality in 1 provided that the following conditions hold: n is not divisible by the characteristic of K; for every odd prime p we have $\zeta_p \in K^\times$ or $\zeta_p \notin GK^\times$; we have $\zeta_4 \in K^\times$ or $1 \pm \zeta_4 \notin GK^\times$. The second condition is motivated by our example above, while for the last condition consider $K = \mathbb{Q}$ and suppose that G is generated by $1 + \zeta_4$ (which is a fourth root of -4): the ratio degree/index equals $1/2$.

2000 *Mathematics Subject Classification.* Primary: 12J99; Secondary: 11R18.
Key words and phrases. Kneser's theorem, Kummer theory, radicals, entanglement.

For any multiplicative subgroup H of $\overline{K}^{\times}$ and for any positive integer m we call $\mu_m(H)$ the group consisting of the roots of unity of order dividing m that are contained in H. Suppose that the exponent of $GK^\times/K^\times$, which we call n, is not divisible by the characteristic of K. Rybowicz [13] (see Theorems 11 and 16) has proven that, if n is a prime power, then we have

$$\frac{[K(G):K]}{|G^nK^{\times n}:K^{\times n}|}=\delta\cdot[K(\mu_n(GK^\times)):K]$$

where $\delta\in\{1,\frac{1}{2}\}$ and where $\delta\neq 1$ can only hold if n is a power of 2. As discussed in Section 2, this result by Rybowicz builds on Kneser's theorem and also on work by Hasse and Schinzel.

There is a vast literature on radical extensions. We mention for example also [1] by Albu, [2] by Barrera Mora and Vélez, and [5] by Halter-Koch. In [9], Lenstra investigated the entanglement by introducing the entanglement group: this group was studied also by Palenstijn in his PhD thesis [11] and by the author with Sgobba and Tronto [12]. The entanglement has also been studied by Lenstra, Moree and Stevenhagen in [10]. Recently, the author with Chan, Pajaziti, and Perissinotto established further results on the entanglement, see [3].

In this paper we build on the result by Rybowicz to study the ratio

$$\frac{[K(G):K]}{|GK^\times:K^\times|}\,.$$

We are also able to remove the assumption that n is a prime power: for us the finite exponent of $GK^\times/K^\times$ can be any positive integer that is not divisible by the characteristic of K. The following remark shows that our condition on n is in fact not restrictive.

Remark 1. If $q:=\mathrm{char}(K)$ and $q\mid n$ (which implies $q\neq 0$), the extension $K(G)/K(G^{q^{v_q(n)}})$ is purely inseparable and with degree the q-part of $|GK^\times:K|$ (see [8, Corollary 9.2, Chapter VI]). We deduce that

$$\frac{[K(G):K]}{|GK^\times:K^\times|}=\frac{[K(G^{q^{v_q(n)}}):K]}{|G^{q^{v_q(n)}}K^\times:K^\times|}$$

so we have reduced to the case where n is not divisible by the characteristic of K.

The following remark shows that the entanglement that we have for a general n cannot be explained just by the entanglement that we have when n is a prime power.

Remark 2. Let $n=\prod_p p^v$, where p varies among the prime divisors of n. Defining $G_p:=G^{n/p^v}$, we have

$$|GK^\times:K^\times|=\prod_p|G_pK^\times:K^\times|\,.$$

We deduce that

$$\frac{[K(G):K]}{|GK^\times:K^\times|}\leqslant\prod_p\frac{[K(G_p):K]}{|G_pK^\times:K^\times|}$$

and that the equality holds if and only if the fields $K(G_p)$ are linearly disjoint over K. In fact, we prove (see Proposition 20, in view of Remark 1) that

$$[K(G):K]\quad\text{divides}\quad\prod_p[K(G_p):K]\,.$$

We denote by z the product of the odd prime divisors p of n such that $\zeta_p\notin K^\times$ and $\zeta_p\in GK^\times$. Moreover, we let $\sqrt{K^\times}$ be the group of all radicals over K whose square is in $K^\times$. The main result of this paper is the following.

Theorem 3. *Suppose that* $\mathrm{char}(K) \nmid n$. *If* n *is odd, then we have*

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = \frac{[K(\zeta_z):K]}{|\mu_n(GK^\times) \cap K(\zeta_z)^\times : \mu_n(K^\times)|}\,. \tag{2}$$

If n *is even, we write* $n = 2^f n'$ *where* f *is a positive integer and* n' *is an odd integer. Let* Δ *be the non-negative integer from Definition 22 (which concerns the radical group* $G^{n'}$ *over* $K(\zeta_z)$*). Then we have*

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = C_1 \cdot C_2$$

where

$$C_1 := \frac{[K(\zeta_z):K]}{|\mu_{n'}(GK^\times) \cap K(\zeta_z)^\times : \mu_{n'}(K^\times)|}$$

(this is (2) *for the group* G^{2^f}*) and where*

$$C_2 := \frac{1}{2^\Delta \cdot |\big(\mu_{2^{f+1}}(GK^\times) \cdot (GK^\times \cap \sqrt{K^\times})\big) \cap K(\zeta_z)^\times : K^\times|}\,.$$

As a special case of our result, suppose that n is a power of 2 (hence $n' = z = C_1 = 1$). If $f = 1$ or $\zeta_4 \notin K$, then $C_2 = 1$ and otherwise we have

$$C_2 = 2^{-\Delta} = \frac{[K(H):K]}{|HK^\times : K^\times|}$$

where H is as in Theorem 17.

From our main result we deduce the following property (which also holds in case $\mathrm{char}(K) \mid n$ provided that we exclude from z the prime factor $\mathrm{char}(K)$).

Theorem 4. *The degree* $[K(G):K]$ *divides*

$$\frac{1}{z} \cdot [K(\zeta_z):K] \cdot |GK^\times : K^\times|\,.$$

In the last section of the paper we prove a result about the (eventual maximal) growth of radical extensions, see Theorem 24. We fix a subgroup Γ of $K^\times$ and for every $N > 1$ consider the radical group R_N, which consists of all N-th roots of all elements of Γ. We show that, under suitable assumptions, there exists a positive integer N_0 (depending on Γ and K) such that

$$[K(R_N) : K(R_{\gcd(N,N_0)})] = \frac{|R_N K^\times : K^\times|}{|R_{\gcd(N,N_0)} K^\times : K^\times|}\,.$$

This relation, rewritten as

$$\frac{[K(R_N):K]}{|R_N K^\times : K^\times|} = \frac{[K(R_{\gcd(N,N_0)}):K]}{|R_{\gcd(N,N_0)} K^\times : K^\times|}\,, \tag{3}$$

shows that the ratio between the degree and the index can be understood by investigating the finitely many divisors of N_0. In view of the discussion below, (3) also shows that the K-linear relations between the radicals in R_N are generated by the multiplicative relations and by the K-linear relations between the radicals in $R_{\gcd(N,N_0)}$. Theorem 25 (which is the reformulation in our setting of [12, Theorem 1]) is similar in nature, and its formula is like (3) but with further factors.

1.1. **Linear (and polynomial) relations among radicals.** We want to describe all the polynomial relations among the radicals over K. Any polynomial relation only involves finitely many radicals $r_1, \ldots, r_m$ (for some $m \geqslant 1$) and it amounts to a non-zero polynomial $f(x_1, \ldots, x_m) \in K[x_1, \ldots, x_m]$ such that $f(r_1, \ldots, r_m) = 0$. If, beyond the constant term, the monomials in $f(x_1, \ldots, x_m)$ have degree 1, then we have a K-linear relation among $r_1, \ldots, r_m, 1$. In fact studying all the polynomial relations among all radicals amounts to study their K-linear relations. This is because any finite product of radicals is a radical (and we can assign a new variable to any monomial of f, to see f as a homogeneous polynomials of degree 1 beyond the constant term).

Consider the radical group $G := \langle r_1, \ldots, r_m \rangle$. In particular, $|GK^\times : K^\times|$ is finite. Each relation among radicals in G that is of multiplicative nature (for example, $\sqrt{6} \cdot \sqrt{10} = 2\sqrt{15}$ in $\mathbb{R}$) is explained by the group structure of $GK^\times/K^\times$. Thus, such relations are controlled by the index $|GK^\times : K^\times|$. The further polynomials relations are controlled by the degree $[K(G) : K]$ because any relation not generated by previously considered ones leads to a decrease of the degree. Our results on $[K(G) : K]/|GK^\times : K^\times|$ tell us what the degree is, so it suffices to find enough relations that provide as upper bound for the degree its actual value.

Our main result (Theorem 3) then allows to completely understand the polynomial relations among radicals. We now describe polynomial relations that (combined with the multiplicative relations) generate all polynomial relations among radicals. As discussed, we may work with a finitely generated radical group G, and we keep the notation of Theorem 3.

- For p an odd prime such that $\zeta_p \in GK^\times$ and $\zeta_p \notin K^\times$, calling $d_p = [K(\zeta_p) : K]$, we have
$$\zeta_p^{d_p}, \ldots, \zeta_p^{p-1} \in 1K + \zeta_p K + \ldots + \zeta_p^{d_p - 1} K = K(\zeta_p)\,.$$
Moreover, the fact that certain powers of $\zeta_{p^{v_p(n)}}$ of order larger than p (and contained in $GK^\times$) may be contained in $K(\zeta_p)^\times$ leads to further K-linear relations among the roots of unity.
- The elements in $\mu_{n'}(GK^\times) \cap K(\zeta_z)^\times$ are powers of $\zeta_{n'}$ and also K-linear combinations of powers of ζ_z, and equating the two expressions gives rise to a K-linear relation among roots of unity. Similarly, the elements in
$$\big(\mu_{2^{f+1}}(GK^\times) \cdot (GK^\times \cap \sqrt{K^\times})\big) \cap K(\zeta_z)^\times$$
provide K-linear relations between single elements of G whose square is in $K^\times$ and powers of $\zeta_{2^{f+1}z}$.
- As explained in Section 4, the degree loss caused by the term 2^Δ stems from K-linear relations among roots of unity of order dividing 2^{f+1}, and possibly an additional relation
$$1 + \zeta_{2^w} \in 1K + \zeta_4 K$$
where w is largest integer such that $\zeta_{2^w} + \zeta_{2^w}^{-1} \in K^\times$ (provided that such largest integer exists).

As a summary, in this paper we are able to prove the following general result.

Theorem 5. *The polynomial relations among radicals are generated by the multiplicative relations and by K-linear relations of the following type: relations among roots of unity; relations among a single radical (whose square is in $K^\times$) and roots of unity; a relation among* 1, ζ_4 *and* $1 + \zeta_{2^w}$ *for some* $w \geqslant 2$.

Acknowledgments. We thank Daniel Gil-Munoz for discussions about a special case of the main theorem, Fritz Hörmann for general discussions and feedback, Zeev Rudnick for useful references and the hint to consider also the polynomial relations, and Pieter Moree for useful comments.

2. Kneser's Theorem and Kummer theory

We let K be a field and fix an algebraic closure $\overline{K}$. We let G be a group of radicals over K such that the index $|GK^\times : K^\times|$ is finite. We let n be the smallest positive integer such that G^n is contained in $K^\times$ (thus, n is the exponent of the group $GK^\times/K^\times$ and it divides $|GK^\times : K^\times|$). In view of Remark 1 we always suppose that n is not divisible by the characteristic of K.

We observe that, for the purposes of this paper, it would be not restrictive to suppose that G is finitely generated. Indeed, it is possible to replace G by any set of representatives of the group $G/(G \cap K^\times) \simeq GK^\times/K^\times$, which is assumed to be finite (as this change does not affect neither the index nor the degree under consideration).

For any positive integer m that is not divisible by $\mathrm{char}(K)$ we fix some root of unity ζ_m in $\overline{K}^\times$ of order m (with a coherent choice, namely that if m, M are positive integers such that $m \mid M$ then we have $\zeta_M^{M/m} = \zeta_m$). If H is a subgroup of $\overline{K}^\times$ and m is a positive integer, we write $\mu_m(H)$ for the group of roots of unity in H whose order divides m. We let φ denote Euler's totient function.

Remark 6. The following sequence, induced by the exponentiation by n, is exact:

$$1 \to \mu_n(GK^\times)K^\times/K^\times \to GK^\times/K^\times \to G^nK^{\times n}/K^{\times n} \to 1\,. \tag{4}$$

Indeed, if $(ga)^n = b^n$ for some $g \in G$ and for some $a, b \in K^\times$, then $g^n \in K^{\times n}$ and hence $g \in \mu_n(GK^\times)K^\times$. Moreover, the following sequence is exact

$$1 \to \mu_n(K^\times) \to \mu_n(GK^\times) \to \mu_n(GK^\times)K^\times/K^\times \to 1$$

because we have $\mu_n(K^\times) = \mu_n(GK^\times) \cap K^\times$. We deduce that

$$|GK^\times : K^\times| = |G^nK^{\times n} : K^{\times n}| \cdot |\mu_n(GK^\times) : \mu_n(K^\times)|\,. \tag{5}$$

We rely on the famous result by Martin Kneser from [7]:

Theorem 7 (Kneser's theorem)**.** *We have*

$$[K(G) : K] = |GK^\times : K^\times|$$

if the following two conditions hold: for every odd prime p we have $\zeta_p \in K^\times$ or $\zeta_p \notin GK^\times$; we have $\zeta_4 \in K^\times$ or $1 \pm \zeta_4 \notin GK^\times$.

We observe that for every $m > 1$ and for every $\alpha \in K^\times$ the radical group $\langle \zeta_m \alpha \rangle$ contains a root of unity different from 1 if and only if $\alpha \neq \zeta_m^{-1}$ is a root of unity. Unless K has positive characteristic q and it is algebraic over $\mathbb{F}_q$, there is $\alpha \in K^\times$ that is not a root of unity. Thus, even if $\zeta_m \notin K^\times$ and $G \cap \mu_m(\overline{K}^\times) = \{1\}$, it is possible that $GK^\times$ contains μ_m.

Kneser's result covers all cases for which $[K(G) : K] = |GK^\times : K^\times|$ holds. Indeed, in [15, Chapter 2, Theorem 20] Schinzel proved the following:

Proposition 8 (Schinzel)**.** *The two conditions in Kneser's theorem are necessary.*

Proof (alternative proof based on Theorem 3). If $z > 1$, then $[K(\zeta_z) : K] \leqslant \varphi(z)$ while $|\mu_{n'}(GK^\times) \cap K(\zeta_z)^\times : K^\times|$ is divisible by z hence there is some prime $p \mid z$ such that the p-adic valuation of $[K(G) : K]/|GK^\times : K^\times|$ is non-zero. Now suppose that $z = 1$ but that the second condition in Kneser's theorem does not hold: we prove that the 2-adic valuation of $[K(G) : K]/|GK^\times : K^\times|$ is non-zero. To study this 2-adic valuation, we may replace G by $G^{n'}$ (hence n becomes 2^f). Then by Kneser's theorem over $L = K(\zeta_4)$ we have $[L(G) : L] = |GL^\times : L^\times|$. The claim holds because $[K(G) : K]/[L(G) : L]$ divides 2 while $|GK^\times : K^\times|/|GL^\times : L^\times|$ is a multiple of 4, as (with the appropriate sign choice) the class of $(1 \pm \zeta_4) \in L^\times$ has order 4 in $GK^\times/K^\times$. □

Remark 9. If $\zeta_p \in GK^\times$ and $\zeta_p \notin K^\times$, then we have $p \mid n$. If (for a sign choice) $1 \pm \zeta_4 \in GK^\times$ and $\zeta_4 \notin K^\times$, then $4 \mid n$ because $(1 \pm \zeta_4)^2 = \pm 2\zeta_4$ and $(1 \pm \zeta_4)^4 = -4$ hence the order of $1 \pm \zeta_4$ in $GK^\times/K^\times$ is 4.

By the above remark, the two conditions in Kneser's theorem are satisfied if $\zeta_n \in K$. In this case, the extension $K(G)/K$ is a *Kummer extension* and its Galois group is abelian of exponent dividing n:

Theorem 10 (Kummer theory)**.** *If $\zeta_n \in K$, the groups $\mathrm{Gal}(K(G)/K)$ and $GK^\times/K^\times$ and $G^n K^{\times n}/K^{\times n}$ are isomorphic. In particular, we have*

$$[K(G) : K] = |GK^\times : K^\times| = |G^n K^{\times n} : K^{\times n}|\,. \tag{6}$$

Proof. The isomorphism between the former and latter group is one of the main results in Kummer theory (see [8, Theorem 8.1, Chapter VI]). The isomorphism between the second and the third group is a consequence of (4) because $\mu_n(GK^\times) = \mu_n(K^\times) = \langle \zeta_n \rangle$. □

If K and G consist of real numbers, then $\mu_n(GK^\times) = \mu_n(K^\times) = \{\pm 1\}$ and the two conditions in Kneser's theorem are satisfied. Hence, (6) holds (see also [13, Theorem 2.2]).

3. THE CASE WHERE n IS AN ODD PRIME POWER

We suppose that n is the power of an odd prime number p (thus, the characteristic of K is different from p). We rely on the following result, which combines Theorem 7 (in view of Remark 9) and [13, Theorem 2.3]. To be precise, [13, Theorem 2.3] is stated for characteristic zero (there is a remark in the paper that most results should extend to separable extensions in positive characteristic) however the proof goes through also in positive characteristic: this can easily be checked as the proof is self-contained up to Kneser's theorem.

Theorem 11 (Kneser - Rybowicz)**.** *We have*

$$\frac{[K(G) : K]}{|G^n K^{\times n} : K^{\times n}|} = [K(\mu_n(GK^\times)) : K]\,.$$

Moreover, if $\zeta_p \notin GK^\times$ or $\zeta_p \in K^\times$, then we have

$$[K(G) : K] = |GK^\times : K^\times|\,.$$

We deduce that, if $\zeta_p \notin GK^\times$ or $\zeta_p \in K^\times$, then the degree $[K(G) : K]$ is a power of p while in the remaining case it is a power of p times $[K(\zeta_p) : K]$.

Corollary 12. *If* $H := \mu_n(GK^\times)$*, then we have*

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = \frac{[K(H):K]}{|HK^\times : K^\times|}\,.$$

If $\zeta_p \notin K^\times$ *and* $\zeta_p \in GK^\times$*, then we have* $H = \langle \zeta_{p^m} \rangle$ *for some positive integer* m*. Let* m_0 *be the largest positive integer such that* $\zeta_{p^{m_0}} \in K(\zeta_p)^\times$ *(or* ∞*, if no such largest integer exists). Then we have*

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = \begin{cases} 1 & \text{if } \zeta_p \in K^\times \text{ or } \zeta_p \notin GK^\times \\ [K(\zeta_p):K]\cdot p^{-\min(m_0,m)} & \text{otherwise}\,. \end{cases}$$

Proof. Combining Theorem 11 and (5) we get

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = \frac{[K(\mu_n(GK^\times)):K]}{|\mu_n(GK^\times):\mu_n(K^\times)|}\,.$$

From $H \cap K^\times = \mu_n(K^\times)$ we deduce that $|H : \mu_n(K^\times)| = |HK^\times : K^\times|$. By Theorem 11 we are left to deal with the case $\zeta_p \notin K^\times$ and $\zeta_p \in GK^\times$. We may conclude because $|H : \mu_n(K^\times)| = p^m$ while $[K(H):K] = [K(\zeta_p):K]\cdot p^{\max(m-m_0,0)}$. □

Remark 13. We observe that we may have $m_0 = \infty$ even if $\zeta_p \notin K$. For example, let F be a prime field with a characteristic that is not p. The extension $F(\zeta_{p^\infty})/F$ has a Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$. We may then take as K the subfield that is fixed by the subgroup of order 2 of the Galois group (ζ_p is not fixed but $\zeta_{p^t} + \zeta_{p^t}^{-1}$ is fixed for any $t \geqslant 1$). The requested properties are preserved if we enlarge K without changing $K \cap F(\zeta_{p^\infty})$.

As explained in Section 1.1, we can make use of Corollary 12 to determine K-linear relations among radicals that, together with the multiplicative relations, generate all the K-linear relations. If n is an odd prime power, all entanglement stems from K-linear relations among roots of unity. The K-linear relation

$$1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0$$

has to be counted only if $\zeta_p \notin K^\times$, and it is only relevant if $\zeta_p \in GK^\times$. If $d_p := [K(\zeta_p):K]$, the minimal polynomial of ζ_p gives a K-linear relation among $1, \zeta_p, \ldots, \zeta_p^{d_p}$, and all the powers ζ_p^i for $i \geqslant d_p$ are K-linear combinations of the roots of unity $1, \zeta_p, \ldots, \zeta_p^{d_p-1}$. We also have

$$(\zeta_{p^m})^{p^{j+\max(m-m_0,0)}} \in 1K + \zeta_p K + \cdots + \zeta_p^{d_p-1}K \qquad \text{for} \quad j \geqslant 0$$

because any element in $K(\zeta_p)$ is of this form. These K-linear relations already explain the degree of $K(G)/K$.

4. The case where n is a power of 2

Let $n = 2^f$ for some positive integer f (so we assume that $\mathrm{char}(K) \neq 2$). *We suppose that* $f \geqslant 2$ *and* $\zeta_4 \notin K^\times$ (else, we already know that $[K(G):K] = |GK^\times : K^\times|$ by Theorem 7 and Remark 9). For every positive integer t we write $\xi_{2^t} = \zeta_{2^t} + \zeta_{2^t}^{-1}$. Moreover, we let w be the largest integer such that $\xi_{2^w} \in K^\times$, or we set $w = \infty$ if no such largest integer exists.

The following lemma is due to Hasse [6, Satz 2], and it also holds for $f = 1$ (see [14, Lemma 2] by Schinzel).

Lemma 14 (Hasse and Schinzel)**.** *The kernel of the map*

$$K^\times/K^{\times n} \to K^\times K(\zeta_4)^{\times n}/K(\zeta_4)^{\times n}$$

induced by the inclusion is generated by the class of the following element:

$$a = \begin{cases} -1 & \text{if } w > f \\ -\xi_{2^{w+1}}^n & \text{if } w = f \\ \xi_{2^{w+1}}^n & \text{if } w < f\,. \end{cases}$$

Notice that $\xi_{2^{w+1}}^n = (\xi_{2^w} + 2)^{\frac{n}{2}}$. Since $\xi_{2^w} \in K^\times$, we always have $a^2 \in K^{\times n}$. However, the class of a modulo $K^{\times n}$ may have order 1 or 2.

Lemma 15. *With the notation of Lemma 14, we have $a \notin K^{\times n}$ if and only if $w \geqslant f$ or $\operatorname{char}(K) = 0$ and $K \cap \mathbb{Q}(\zeta_{2^\infty})$ is totally real.*

Proof. We can easily settle the case $w > f$ because $(-1) \notin K^{\times n}$ as $\zeta_4 \notin K^\times$. So now suppose that $w \leqslant f$. The condition $a \in K^{\times n}$ means that $(\xi_{2^w} + 2)\gamma \in K^{\times 2}$, where γ is a root of unity of order dividing $n/2$ for $w < f$ and of order n for $w = f$. Since $\gamma \in K^\times$, we must have $\gamma \in \{\pm 1\}$. We cannot have $\gamma = 1$ because $\xi_{2^{w+1}} \notin K$, so now suppose that $\gamma = -1$.

We observe that for a finite field F of odd characteristic and such that $\zeta_4 \notin F$ the product of two non-squares is a square (by Kummer theory, as $F(\sqrt{b}) = F(\zeta_4)$ holds if $b \in F^\times \setminus F^{\times 2}$). We deduce that $-(\xi_{2^w} + 2) = (-1) \cdot (\xi_{2^{w+1}}^2) \in K^{\times 2}$ in odd characteristic.

In characteristic 0, the square roots of $-(\xi_{2^w} + 2)$ are in $\mathbb{Q}(\zeta_{2^\infty})$ and not totally real. They cannot be in $K^\times$ if $K \cap \mathbb{Q}(\zeta_{2^\infty})$ is totally real. In the remaining case, ζ_4 and $\xi_{2^{w+1}}$ generate the same quadratic extension of $K \cap \mathbb{Q}(\zeta_{2^\infty})$ hence of K, so by Kummer theory $-(\xi_{2^w} + 2)$ is a square in $K^\times$. □

We rely on the following result, which is [13, Theorem 2.4], restated thanks to Lemma 15. Similarly to Theorem 11, the original result is stated in characteristic zero, but the proof also goes through in positive characteristic.

Theorem 16 (Rybowicz)**.** *We have*

$$\frac{[K(G):K]}{|G^n K^{\times n} : K^{\times n}|} = \delta_G \cdot [K(\mu_n(GK^\times)) : K]$$

where $\delta_G \in \{1, \frac{1}{2}\}$. Let a be as in Lemma 14. We have $\delta_G = \frac{1}{2}$ if and only if $a \in G^n K^{\times n}$ and, in the case $w < f$, additionally $1 + \zeta_{2^w} \in GK^\times$ and $\operatorname{char}(K) = 0$ and $K \cap \mathbb{Q}(\zeta_{2^\infty})$ is totally real.

Theorem 17. *Let δ_G be as in Theorem 16 and set*

$$H = \begin{cases} \mu_{2n}(GK^\times) & \text{if } w > f \\ \mu_n(GK^\times) & \text{if } w = f \text{ and } -\xi_{2^{w+1}}^n \notin G^n K^{\times n} \\ \langle 1 + \zeta_{2^w}, \zeta_n \rangle & \text{if } w = f \text{ and } -\xi_{2^{w+1}}^n \in G^n K^{\times n} \\ \mu_n(GK^\times) & \text{if } w < f \text{ and } \delta_G = 1 \\ \langle 1 + \zeta_{2^w} \rangle \mu_n(GK^\times) & \text{if } w < f \text{ and } \delta_G = 1/2\,. \end{cases}$$

Then H is a subgroup of $GK^\times$ and we have

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = \frac{[K(H):K]}{|HK^\times : K^\times|}\,.$$

Proof. For $w = f$, we first prove the claim that $H = \langle 1 + \zeta_{2^w}, \zeta_n \rangle \cap GK^\times$. Observe that $\zeta_{2^{w+1}}\xi_{2^{w+1}} = 1+\zeta_{2^w}$. If $-\xi_{2^{w+1}}^n \notin G^n K^{\times n}$, there is no integer i such that $(1+\zeta_{2^w})\zeta_n^i \in GK^\times$ and hence $\langle 1 + \zeta_{2^w}, \zeta_n \rangle \cap GK^\times = \mu_n(GK^\times)$. Else, fix i such that $(1 + \zeta_{2^w})\zeta_n^i \in GK^\times$. Considering that $\xi_{2^{w+1}}^2 \in K^\times$, we deduce that $\zeta_n \in GK^\times$ hence $1 + \zeta_{2^w} \in GK^\times$ and the claim is proven.

Note that in all cases H is a subgroup of $GK^\times$ such that $\mu_n(HK^\times) = \mu_n(GK^\times)$. We now prove that $\delta_G = \delta_H$. If $w > f$, this is because $-1 \in G^n K^{\times n}$ is equivalent to $\zeta_{2n} \in GK^\times$. If $w = f$, this is because $-\xi_{2^{w+1}}^n \in G^n K^{\times n}$ is equivalent to $(1+\zeta_{2^w}) \in \mu_n(\overline{K}^\times)\cdot GK^\times$ and we have $H = \langle 1+\zeta_{2^w}, \zeta_n\rangle \cap GK^\times$. If $w < f$, we observe that $\delta_G = 1$ implies $\delta_H = 1$, so suppose that $\delta_G = \frac{1}{2}$. We clearly have $1 + \zeta_{2^w} \in HK^\times$, so we are left to prove that $\xi_{2^{w+1}}^n \in H^n K^{\times n}$. This is equivalent to $\xi_{2^{w+1}} \in \langle 1 + \zeta_{2^w}, \zeta_n \rangle K^{\times n}$, which holds because $\xi_{2^{w+1}} = \zeta_{2^{w+1}}^{-1}(1 + \zeta_{2^w})$ and $\zeta_{2^{w+1}}$ is a power of ζ_n.

In view of Remark 6, from Theorem 16 (applied to G and to H), as $\tilde{H} := \mu_n(GK^\times) = \mu_n(HK^\times)$ and $\delta_G = \delta_H$, we have

$$\frac{[K(G) : K]}{|GK^\times : K^\times|} = \delta_G \cdot \frac{[K(\tilde{H}) : K]}{|\tilde{H} : \mu_n(K^\times)|} = \frac{[K(H) : K]}{|HK^\times : K^\times|}\,.$$

□

Example 18. All five cases in Theorem 17 do occur. For the first case we may choose $K = \mathbb{Q}(\xi_{2^w})$ with $w \geqslant 3$ and $G = \langle \sqrt[n]{5} \rangle$ with $2 \leqslant f < w$. Now let $K = \mathbb{Q}$ (thus, $w = 2$). In the second and third case we have $n = 4$ and the condition to check is whether $-4 \in G^4\mathbb{Q}^{\times 4}$. So for the second (respectively, third) case we may take G to be $\langle \sqrt[4]{5} \rangle$ (respectively, $\langle \zeta_8\sqrt{2} \rangle$). Finally, let $n = 8$ hence $a = 16$. For the fourth case we may take $G = \langle \sqrt[8]{5} \rangle$ as $16 \notin \langle 5 \rangle \mathbb{Q}^{\times 8}$. For the fifth case we may take $G = \langle \zeta_8\sqrt{2} \rangle$ as $16 \in \langle 16 \rangle \mathbb{Q}^{\times 8}$ and $1 + \zeta_4 = \zeta_8\sqrt{2}$.

Lemma 19. *With the notation of Theorem 17, we let m be the largest positive integer such that $\zeta_{2^m} \in H$. If $m = 1$ then we have $\frac{[K(H):K]}{|HK^\times:K^\times|} = 1$, while if $m \geqslant 2$ then we have*

$$\frac{[K(H) : K]}{|HK^\times : K^\times|} = \begin{cases} 2^{2-m} & \text{if } w > f \text{ or if } w = f \text{ and } -\xi_{2^{w+1}}^n \notin G^n K^{\times n} \\ 2^{1-f} & \text{if } w = f \text{ and } -\xi_{2^{w+1}}^n \in G^n K^{\times n} \\ 2^{2-\min(w',m)} & \text{if } w < f,\ \delta_G = 1 \\ 2^{1-\min(w',m)} & \text{if } w < f,\ \delta_G = 1/2 \end{cases}$$

where, if w is finite, w' is the largest positive integer such that $\zeta_{2^{w'}} \in K(\zeta_4)^\times$. In the last case we have $m = \max(w, \overline{m})$, where $\overline{m}$ is the largest integer such that $\zeta_{2^{\overline{m}}} \in \mu_n(GK^\times)$.

We observe the following: in characteristic 0, we have $w' = w$ or $w' = w + 1$ and the latter case holds if and only if $\mathrm{char}(K) = 0$ and $K \cap \mathbb{Q}(\zeta_{2^\infty})$ is not totally real; in odd characteristic p (thus $p \equiv 3 \bmod 4$ because $\zeta_4 \notin K$), w' is the 2-adic valuation of $p^2 - 1$.

Proof. If $m = 1$, then $[K(H) : K] = |HK^\times : K^\times|$ by Theorem 7 and Remark 9 so suppose that $m \geqslant 2$.

We remark that $m \leqslant w$ if $w > f$ (because $m \leqslant f + 1$) or if $w = f$ and $-\xi_{2^{w+1}}^n \notin G^n K^{\times n}$. In these cases, we have $[K(H) : K] = 2$ and $|HK^\times : K^\times| = |H : \mu_{2n}(K^\times)| = 2^{m-1}$.

If $w = f$ and $-\xi^n_{2^{w+1}} \in G^n K^{\times n}$, then $K(H) = K(\zeta_4)$. We conclude because $(1+\zeta_{2^w})^2 = \zeta_{2^w}(2+\xi_{2^w})$ and ζ_{2^w} are in the same class modulo $K^\times$ and hence

$$|HK^\times : K^\times| = 2|\langle\zeta_n\rangle K^\times : K^\times| = n\,.$$

Finally suppose that $w < f$. Since $1+\zeta_{2^w} \in K(\zeta_4)^\times$, we have

$$[K(H) : K] = 2^{1+\max(m-w',0)}\,.$$

If $\delta_G = 1$, we may conclude because we have $|HK^\times : K^\times| = 2^{m-1}$. If $\delta_G = 1/2$ (in particular, $\mathrm{char}(K) = 0$ and $K \cap \mathbb{Q}(\zeta_{2^\infty})$ is totally real), recall that $(1+\zeta_{2^w})^2 \in \zeta_{2^w}K^\times \setminus K^\times$. By Lemma 15 we know that $(1+\zeta_{2^w})^n = \xi^n_{2^{w+1}} \notin K^{\times n}$ so there is no integer i such that $(1+\zeta_{2^w})\zeta_n^i \in K^\times$. We deduce that

$$|HK^\times : K^\times| = 2|\langle\zeta_{2^w}\rangle\mu_n(GK^\times)K^\times : K^\times|\,.$$

We are left to show that $|HK^\times : K^\times| = 2^m$ and we do so by proving that $m = \max(w, \overline{m})$. For $\overline{m} \geqslant w$, H is contained in $K(\zeta_{2^{\overline{m}}})^\times$ and we conclude because this group does not contain $\zeta_{2^{\overline{m}+1}}$. For $\overline{m} < w$, H is contained in $K(\zeta_4)^\times$ and we conclude because $\zeta_{2^{w+1}} \notin K(\zeta_4)^\times$. □

We make use of Theorem 17 and Lemma 19 (as described in Section 1.1) to find K-linear relations among radicals which, together with the multiplicative relations, generate all K-linear relations (in case n is a power of 2). Remark that $K(\zeta_4) = 1K + \zeta_4 K$.

- If $w > f$ or if $w = f$ and $-\xi^n_{2^{w+1}} \notin G^n K^{\times n}$, we only have entanglement if $m \geqslant 3$. Since $m \leqslant f+1$ and $m \leqslant f$ for $w = f$, it suffices to consider the K-linear relations expressing
$$\zeta_{2^3}, \dots, \zeta_{2^m} \in 1K + \zeta_4 K\,.$$
- If $w = f$ and $-\xi^n_{2n} \in G^n K^{\times n}$, there is also an additional entanglement (as there is the loss of a factor 2 in the degree $[K(G) : K]$) which is due to $1+\zeta_{2^w} \in GK^\times \cap K(\zeta_4)^\times$, and it is expressed by the K-linear relation

(7) $$1 + \zeta_{2^w} \in 1K + \zeta_4 K\,.$$

- Finally, suppose that $w < f$. If $\delta_G = 1$, then the entanglement is similarly due to

(8) $$\zeta_{2^3}, \dots \zeta_{2^{m'}} \in 1K + \zeta_4 K$$

where m' is the largest positive integer less or equal to m such that $\zeta_{2^{m'}} \in K(\zeta_4)^\times$. If $\delta_G = 1/2$, the entanglement is similarly explained by (8) and (7).

5. The general case

Let n be a positive integer that is not divisible by the characteristic of K. If $n = 1$, then we have

$$[K(G) : K] = |GK^\times : K^\times| = 1$$

so we suppose that $n \geqslant 2$ and write $n = \prod_p p^{v_p}$ for the prime factorization of n, where p varies among the prime divisors of n. Let z be the product of the odd primes p such that $\zeta_p \notin K^\times$ and $\zeta_p \in GK^\times$. We observe that $\zeta_z \in K(G)$. We set $n_p := p^{v_p}$ and $G_p = G^{n/n_p}$. In this way, n_p is the smallest positive integer such that $G_p^{n_p} \subseteq K^\times$. Since n_p is a prime power, we may apply the results in the previous sections to study G_p. Note that we have

(9) $$|GK^\times : K^\times| = \prod_p |G_p K^\times : K^\times|$$

and the same holds if we replace K by a finite extension.

Proposition 20. *We have*

$$[K(G):K(\zeta_z)] = \prod_p [K(\zeta_z, G_p):K(\zeta_z)] \tag{10}$$

and

$$[K(G):K] \quad \textit{divides} \quad \prod_p [K(G_p):K]\,.$$

Proof. To prove (10) we show that the fields $K(\zeta_z, G_p)$, whose compositum is $K(G)$, are linearly disjoint over $K(\zeta_z)$. It suffices to prove that the degree $[K(\zeta_z, G_p):K(\zeta_z)]$ is a power of p. This holds by Corollary 12 (for p odd), by Theorem 7 (for $p=2$ and $\zeta_4 \in K^\times$ or $4 \nmid n$) and by Theorem 17 and Lemma 19 (in the remaining case).

The second assertion follows from (10). Indeed, consider that the Galois extension $K(\zeta_z)/K$ is the compositum of its Galois subextensions $K(\zeta_p)/K$ hence

$$[K(\zeta_z):K] \quad \text{divides} \quad \prod_p [K(\zeta_p):K]\,.$$

Moreover, since $K(\zeta_z)/K(\zeta_p)$ is Galois and applying [8, Theorem 1.12, Chapter VI],

$$[K(\zeta_z, G_p):K(\zeta_z)] \quad \text{divides} \quad [K(\zeta_p, G_p):K(\zeta_p)]\,.$$

□

The following result is [14, Theorem 2]:

Theorem 21 (Schinzel's theorem on abelian radical extensions)**.** *Let $n \geqslant 1$ be not divisible by* $\mathrm{char}(K)$*. If $\alpha \in K^\times$, the extension $K(\zeta_n, \sqrt[n]{\alpha})/K$ is abelian if and only if $\alpha^m = \beta^n$ holds for some $\beta \in K^\times$ and for some $m \mid n$ such that $\zeta_m \in K$.*

Proof of Theorem 3 if n is odd. By (9) and (10) we can write

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = [K(\zeta_z):K] \cdot \prod_{p\mid n} \frac{[K(\zeta_z, G_p):K(\zeta_z)]}{|G_pK^\times : K^\times|}\,.$$

We have $G_pK^\times \cap K(\zeta_z)^\times \subseteq \mu_{p^{v_p}}(G_pK^\times)$ because $\zeta_p \notin K^\times$ and the extension $K(\zeta_z)/K$ is abelian (we apply Theorem 21).

By Theorem 7 (in view of Remark 9) we then have

$$[K(\zeta_z, G_p):K(\zeta_z)] = |G_pK(\zeta_z)^\times : K(\zeta_z)^\times| = \frac{|G_pK^\times : K^\times|}{|\mu_{p^{v_p}}(G_pK^\times)\cap K(\zeta_z)^\times : \mu_{p^{v_p}}(K^\times)|}\,.$$

We may then conclude remarking that

$$|\mu_n(GK^\times)\cap K(\zeta_z)^\times : \mu_n(K^\times)| = \prod_{p\mid n} |\mu_{p^{v_p}}(G_pK^\times)\cap K(\zeta_z)^\times : \mu_{p^{v_p}}(K^\times)|\,.$$

□

Definition 22. We set $\Delta = 0$ if $\zeta_4 \in K^\times$ or $4 \nmid n$. Otherwise, we let H' be the group H from Theorem 17 and Lemma 19 for the radical group $G^{n'}$ over $K(\zeta_z)$ and set

$$2^{-\Delta} := \frac{[K(\zeta_z, H'):K(\zeta_z)]}{|H'K(\zeta_z)^\times : K(\zeta_z)^\times|}\,. \tag{11}$$

Proof of Theorem 3 if n is even. Call $G_P = \prod_{p|n, p\neq 2} G_p$. Remarking that $\zeta_z \in G_P$, we can write

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = [K(\zeta_z):K]\cdot \frac{[K(G_P):K(\zeta_z)]}{|G_PK^\times : K^\times|}\cdot \frac{[K(\zeta_z, G_2):K(\zeta_z)]}{|G_2K^\times : K^\times|}\,.$$

By the odd case of Theorem 3 we have

$$\frac{[K(G_P):K]}{|G_PK^\times : K^\times|} = \frac{[K(\zeta_z):K]}{|\mu_{n/n_2}(G_PK^\times)\cap K(\zeta_z)^\times : \mu_{n/n_2}(K^\times)|}\,.$$

Since $\mu_{n/n_2}(GK^\times) = \mu_{n/n_2}(G_PK^\times)$ and $\mu_{2n_2}(GK^\times) = \mu_{2n_2}(G_2K^\times)$ and $GK^\times \cap \sqrt{K^\times} = G_2K^\times \cap \sqrt{K^\times}$ we are left to prove that

$$\frac{[K(\zeta_z, G_2):K(\zeta_z)]}{|G_2K^\times : K^\times|} = \frac{2^{-\Delta}}{|\big(\mu_{2n_2}(G_2K^\times)\cdot(G_2K^\times\cap\sqrt{K^\times})\big)\cap K(\zeta_z)^\times : K^\times|}\,.$$

As $K(\zeta_z)/K$ is abelian, by Theorem 21 we have

$$G_2K^\times \cap K(\zeta_z)^\times = \big(\mu_{2n_2}(G_2K^\times)\cdot(G_2K^\times\cap\sqrt{K^\times})\big)\cap K(\zeta_z)^\times$$

so it suffices to show that

$$\frac{[K(\zeta_z, G_2):K(\zeta_z)]}{|G_2K(\zeta_z)^\times : K(\zeta_z)^\times|} = 2^{-\Delta}\,,$$

which is a consequence of Theorem 17 and (11) (or of Theorem 7 if $\zeta_4\in K^\times$ or $4\nmid n$). □

Example 23. We recover Theorem 3 for $K = \mathbb{Q}(\sqrt{5})$ and $G = \langle \zeta_n, \sqrt[n]{g}\rangle$, where $n > 1$ and $g = 2\sqrt{5}(1-\sqrt{5})$. As shown in [12, Example 42], we have $[K(G):K] = n\varphi(n)/d$ (where $d = 4$ if $10 \mid n$ and $d = 2$ if $\gcd(10, n) = 5$ and $d = 1$ otherwise). We have $|GK^\times : K^\times| = n^2$. Let p vary among the prime divisors of n. If n is odd, then we have

$$[K(\zeta_z):K] = \frac{1}{d}\prod_p (p-1) = \frac{\varphi(n)z}{nd}$$

and $\mu_n(GK^\times)\cap K(\zeta_z)^\times = \mu_z(\overline{K}^\times)$ while $\mu_n(K^\times) = \{1\}$ hence

$$\frac{[K(G):K]}{|GK^\times : K^\times|} = \frac{\varphi(n)}{nd} = \frac{[K(\zeta_z):K]}{|\mu_n(GK^\times)\cap K(\zeta_z)^\times : \mu_n(K^\times)|}\,.$$

If n is even, then we have

$$\big(\mu_{2^{f+1}}(GK^\times)\cdot(GK^\times\cap\sqrt{K^\times})\big)\cap K(\zeta_z)^\times = \begin{cases}\{\pm 1\} & \text{if } 5\nmid n\\ \langle\sqrt{g}\rangle K^\times & \text{otherwise}\,.\end{cases}$$

We may then recover the formula of Theorem 3 because $\Delta = 0$ (as $H' = \mu_{2^f}(\overline{K}^\times)$ for $f \geqslant 2$).

Proof of Theorem 4. Equivalently, we prove that $[K(G):K(\zeta_z)]$ divides $\frac{1}{z}\cdot|GK^\times : K^\times|$. Recall from (10) that

$$[K(G):K(\zeta_z)] = \prod_{p|n}[K(\zeta_z, G_p):K(\zeta_z)]$$

and write

$$\frac{1}{z}\cdot|GK^\times : K^\times| = \left(\prod_{p|z}\frac{1}{p}\cdot|G_pK^\times : K^\times|\right)\left(\prod_{p|n, p\nmid z}|G_pK^\times : K^\times|\right)\,.$$

For $p \mid z$ the degree $[K(\zeta_z, G_p) : K(\zeta_z)]$ divides $\frac{1}{p} \cdot |GK^\times : K^\times|$ by Corollary 12. If $p \neq 2$ and $p \nmid z$, or if $p = 2$ and $\zeta_4 \in K^\times$ or $4 \nmid n$ we have

$$[K(\zeta_z, G_p) : K(\zeta_z)] = |G_p K(\zeta_z)^\times : K(\zeta_z)^\times| \tag{12}$$

by Theorem 7 (in view of Remark 9) and the index in (12) divides $|G_p K^\times : K^\times|$. For $p = 2$, $\zeta_4 \notin K^\times$ and $4 \mid n$ the degree $[K(\zeta_z, G_2) : K(\zeta_z)]$ divides $|G_2 K(\zeta_z)^\times : K(\zeta_z)^\times|$ by Theorem 17 and (11). □

We set $\mu_\infty = \cup_{m \geqslant 1} \mu_m$. We conclude by proving two results on the growth of certain radical extensions.

Theorem 24. *For every positive integer N let R_N be a subgroup of $\overline{K}^\times$ such that the index $|R_N K^\times : K^\times|$ divides N^c for some constant c, $R_1 \in K^\times$ and such that $R_N^M = R_{N/M}$ holds for every $M \mid N$. Suppose that there are only finitely many primes p such that $\zeta_p \notin K^\times$ and $\zeta_p \in R_N K^\times$ for some N, and call z their product. Moreover, suppose that*

$$|\mu_\infty(K(\zeta_{4z})^\times) : \mu_\infty(K^\times)|$$

is finite. Then there exists a positive integer N_0 such that

$$\frac{[K(R_N) : K]}{|R_N K^\times : K^\times|} = \frac{[K(R_{\gcd(N,N_0)}) : K]}{|R_{\gcd(N,N_0)} K^\times : K^\times|} .$$

Proof. Let N_0 be a number that is divisible by $4z$ and with the property that for every N the group $\mu_N(R_N K^\times) \cap K(\zeta_z)^\times$ is a subgroup of $\mu_{N_0}(R_{N_0} K^\times)$. Thus removing from N the prime factors coprime to N_0 does not affect $\mu_N(R_N K^\times) \cap K(\zeta_z)^\times$. Moreover, if p is any prime number, we have $\mu_{p^{v_p(N)}}(R_N K^\times) = \mu_{p^{v_p(N)}}(R_{p^{v_p(N)}} K^\times)$. Combining these two observations we obtain

$$\mu_N(R_N K^\times) \cap K(\zeta_z)^\times = \mu_{\gcd(N,N_0)}(R_{\gcd(N,N_0)} K^\times) \cap K(\zeta_z)^\times .$$

If N is odd, we may conclude by Theorem 3. So suppose that N is even. Since $R_N \cap \sqrt{K^\times} = R_{2^{v_2(N)}} \cap \sqrt{K^\times}$ and because of the bound on $|R_N K^\times : K^\times|$ we may define N_0 (such that $v_2(N_0)$ is large enough) so that $R_N K^\times \cap \sqrt{K^\times} = R_{\gcd(N,N_0)} K^\times \cap \sqrt{K^\times}$. Similarly, we may define N_0 such that the group

$$\left(\mu_{2^{v_2(N)+1}}(R_N K^\times) \cdot (R_N K^\times \cap \sqrt{K^\times})\right) \cap K(\zeta_z)^\times$$

does not change by replacing N by $\gcd(N, N_0)$ (because the squares of its elements are in $\mu_{2^{v_2(N)}}(R_N K^\times) \cap K(\zeta_z)^\times$ which stabilizes when $v_2(N)$ is large enough). We may then conclude by Theorem 3 because, considering Definition 22, we may define N_0 such that $v_2(N_0) > w'$ (or we have $w' = \infty$) and such that $1 + \zeta_{2^{w'}}$ is contained in $R_{2^{v_2(N_0)}}$ if it is contained in R_{2^v} for some positive integer v. □

The following result is the reformulation in our setting of [12, Theorem 1]:

Theorem 25. *Let K be a number field, fix a finitely generated subgroup Γ of $K^\times$ and for every positive integer N let R_N consist of all N-th roots of all elements of Γ. Then there exists a positive integer N_0 such that*

$$\frac{[K(R_N) : K]}{|R_N K^\times : K^\times|} = \frac{[K(R_{\gcd(N,N_0)}) : K]}{|R_{\gcd(N,N_0)} K^\times : K^\times|} \cdot \prod_{p \mid N, p \nmid N_0, \zeta_p \notin K^\times} \frac{p-1}{p} .$$

Proof. There is an odd squarefree integer Z such that for all primes $p \nmid Z$ we have $[K(\zeta_p) : K] = p-1$. Additionally, we can choose Z such that for any $N \geqslant 1$ the extensions $K(R_{p^{v_p(N)}}, \zeta_Z)/K(\zeta_Z)$ are linearly disjoint for every prime number p. Thus for any odd squarefree integer Z' that is a multiple of Z and for every positive integer N we have

$$\mu_{2^{v_2(N)+1}}(R_N K^\times)(R_N K^\times \cap \sqrt{K^\times}) \cap K(\zeta_{Z'})^\times \subseteq R_{2^{v_2(N)}} K^\times \cap K(\zeta_{Z'})^\times \subseteq K(\zeta_Z)^\times .$$

By Lemma 19 we may choose the 2-adic valuation of N_0 to be large enough such that

$$\frac{[K(R_{2^{v_2(N)}}, \zeta_Z) : K(\zeta_Z)]}{|R_{2^{v_2(N)}} K(\zeta_Z)^\times : K^\times|} = \frac{[K(R_{2^{\min(v_2(N), v_2(N_0))}}, \zeta_Z) : K(\zeta_Z)]}{|R_{2^{\min(v_2(N), v_2(N_0))}} K(\zeta_Z)^\times : K^\times|} .$$

Then, following the proof of Theorem 3, we are left to control those N which divide a power of Z, and for them we can find a suitable N_0 following the proof of Theorem 24. □

REFERENCES

[1] ALBU, T., *Cogalois theory*, Pure and Applied Mathematics 252, Marcel Dekker, New York, 2003.

[2] BARRERA MORA, F. AND VÉLEZ, W. Y. *Some results on radical extensions*, J. Algebra **162** (1993) no. 2, 295–301.

[3] CHAN, C.W., PAJAZITI, A., PERUCCA, A. AND PERISSINOTTO, F. *The entanglement of radicals*, arXiv preprint `https://arxiv.org/abs/2508.19211`.

[4] HALTER-KOCH, F., *Eine Galoiskorrespondenz für Radikalerweiterungen (A Galois correspondence for radical extensions)*, J.Algebra **63** (1980), 318–330.

[5] HALTER-KOCH, F., *Über Radikalerweiterungen (On radical extensions)*, Acta Arith. **36** (1980), 43–58.

[6] HASSE, H. *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*, J. Reine Angew. Math. **188** (1950), 40–64.

[7] KNESER, M., *Lineare Abhängigkeit von Wurzeln (Linear dependence of roots)*, Acta Arith. **26** (1975), 307–308.

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

[9] LENSTRA, H. W. JR., *Entangled radicals*, Colloquium Lectures, AMS 112th Annual Meeting, San Antonio, January 12–15, 2006, available at `https://www.math.leidenuniv.nl/~hwl/papers/rad.pdf`.

[10] LENSTRA, H. W. JR., MOREE, P. AND STEVENHAGEN, P., *Character sums for primitive root densities.* Math. Proc. Cambridge Philos. Soc. **157** (2014), no. 3, 489–511.

[11] PALENSTIJN, W. J., *Radicals in arithmetic*, PhD thesis, University of Leiden (2014), available at `https://openaccess.leidenuniv.nl/handle/1887/25833`.

[12] PERUCCA, A., SGOBBA, P. AND TRONTO, S., *Kummer theory for number fields via entanglement groups*, Manuscripta Math., **169** (2022), no. 1-2, 251–270.

[13] RYBOWICZ, M., *On the normalization of numbers and functions defined by radicals*, J. Symbolic Comput., **35** (2003), 651–672.

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

[15] SCHINZEL, A., *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and Its Applications, Encycl. Math. Appl. 77, Cambridge University Press, 2000.