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 work by Kneser and Schinzel.

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 – coprime to the characteristic of K – such that $\alpha^n \in K^\times$. We fix a group G of radicals such that the index $|GK^\times : K^\times|$ is finite. We investigate the degree $[K(G) : K]$ (the extension $K(G)/K$ is separable, but in general not Galois). More precisely, we compare the above degree and index. If all K-linear relations among the radicals in G stem from multiplicative relations, then the above-mentioned degree and index will be the same. Else, we have a phenomenon that is called *entanglement* (of radicals). We denote by n the smallest positive integer such that $G^n \subseteq K^\times$ and by z the product of the odd prime divisors p of n such that $\zeta_p \notin K^\times$ and $\zeta_p \in GK^\times$. If H is a multiplicative group and m is a positive integer, we write $\mu_m(H)$ for the subgroup of H consisting of roots of unity of order dividing m. The main result of this paper is the following:

Theorem 1. *If n is odd, we have*

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

If n is even, writing $n = 2^f n'$ where f is a positive integer and n' is an odd integer, the ratio $\frac{[K(G):K]}{|GK^\times:K^\times|}$ equals

$$\frac{[K(\zeta_z) : K] \cdot 2^{-\Delta}}{|\mu_{n'}(GK^\times) \cap K(\zeta_z)^\times : \mu_{n'}(K^\times)| \cdot |\mu_{2^{f+1}}(GK^\times)(GK^\times \cap \sqrt{K^\times}) \cap K(\zeta_z)^\times : K^\times|}$$

where Δ is the non-negative integer from Definition 17.

This result allows to completely understand the K-linear relations among the radicals in $GK^\times$: 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

$$\zeta_p^{d_p}, \ldots, \zeta_p^{p-1} \in 1K + \zeta_p K + \ldots + \zeta_p^{d_p-1} K = K(\zeta_p)\,.$$

2000 *Mathematics Subject Classification.* Primary: 12J99; Secondary: 11R18.

Key words and phrases. Kneser's theorem, Kummer theory, radicals, entanglement.

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.

Beyond this phenomenon, 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 $\mu_{2^{f+1}}(GK^\times)(GK^\times \cap \sqrt{K^\times}) \cap K(\zeta_z)^\times$ provide K-linear relations between single elements of G whose square is in $K^\times$ and powers of $\zeta_{2^{f+1}z}$. Finally, as explained in Section 4, the term $2^{-\Delta}$ 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).

From the main result we deduce the following general property:

Theorem 2. *The degree* $[K(G) : K]$ *divides*

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

We conclude the paper by investigating the growth of radical extensions (see Theorems 18 and 19).

We suppose that n is coprime to the characteristic of K but this assumption is not necessary. Indeed, if $\mathrm{char}(K) = p$, the extension $K(G)/K(G^{p^{v_p(n)}})$ is purely inseparable and with degree the p-part of $|GK^\times : K|$ (see [7, Corollary 9.2, Chapter VI]). We deduce that

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

so we have reduced to the case where n is coprime to p.

We also remark that to study the K-linear relations of (finitely many) radicals we may consider the group G that they generate, so our assumption that $|GK^\times : K^\times|$ is finite is not restrictive.

Our results build on two theorems by Rybowicz (Theorems 8 and 12) which express the degree $[K(G) : K]$ also in the cases in which the famous theorem by Kneser (Theorem 4) cannot be applied. Other results that we make use of is a lemma by Schinzel about radicals to extend the base field to $K(\zeta_4)$ (Lemma 10) and Schinzel's Theorem on abelian radical extensions (Theorem 16). There is a vast literature on radical extensions however our general result seem to be new. We mention for example also [5] by Halter-Koch, [2] by Barrera Mora and Vélez, and [1] by Albu. In [8] Lenstra investigated entanglements introducing the entanglement group: this group was studied also by Palenstijn [10] and by the author with Sgobba and Tronto [11]. The entanglement has also been studied by Lenstra, Moree and Stevenhagen in [9]. Recently, the author with Chan, Pajaziti, and Perissinotto established further results on the entanglement, see [3].

Acknowledgments. We thank Daniel Gil-Munoz for discussions which also lead to a special case of the main theorem, Zeev Rudnick for a general discussion about radical extensions, and Fritz Hörmann for many 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 and coprime to the characteristic of K. We let n be a positive integer, which we suppose to be minimal, such that G^n is contained in $K^\times$ (thus, n is coprime to the characteristic of K).

For any positive integer m that is coprime to $\mathrm{char}(K)$ 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.

Remark 3. The following sequence, induced by the exponentiation by n, is exact:

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

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

$$|GK^\times : K^\times| = |G^nK^{\times n} : K^{\times n}| \cdot |\mu_n(GK^\times) : \mu_n(K^\times)|\,. \tag{2}$$

We rely on the famous result by Martin Kneser from [6]:

Theorem 4 (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 $1 \pm \zeta_4 \notin GK^\times$.

Our main result implies the following:

Proposition 5. *The two conditions in Kneser's theorem are necessary.*

Proof. We rely on Theorem 1. 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 $[L(G) : L] = |GL^\times : L^\times|$. We may conclude because $[K(G) : K]/[L(G) : L]$ divides 2 while $|GK^\times : K^\times|/|GL^\times : L^\times|$ is a multiple of 4 because (with the appropriate sign choice) the class of $(1 \pm \zeta_4) \in L^\times$ has order 4 in $GK^\times/K^\times$. □

Remark 6. 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 7 (Kummer theory)**.** *If $\zeta_n \in K$, the groups $\mathrm{Gal}(K(G)/K)$ and $GK^\times/K^\times$ and $G^nK^{\times n}/K^{\times n}$ are isomorphic. In particular, we have*

$$[K(G):K] = |GK^\times : K^\times| = |G^nK^{\times n} : K^{\times n}|\,. \tag{3}$$

Proof. The isomorphism between the former and latter group is one of the main results in Kummer theory (see [7, Theorem 8.1, Chapter VI]). The isomorphism between the second and the third group is a consequence of (1) 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 (3) holds (see also [12, 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 4 (in view of Remark 6) and [12, Theorem 2.3]:

Theorem 8 (Kneser - Rybowicz)**.** *We have*

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

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 9. *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 $\zeta_p \in GK^\times$, 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 8 and (2) 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 8 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 $[K(H):K] = [K(\zeta_p):K]p^{\max(m-m_0,0)}$. □

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 $1, \zeta_p, \dots, \zeta_p^{d_p}$, and all the powers ζ_p^i for $i \geqslant d_p$ are K-linear combinations of the roots of unity $1, \zeta_p, \dots, \zeta_p^{d_p-1}$. 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 generate all others for $K(G)$ (beyond those stemming from the group $GK^\times/K^\times$) because by the above result they 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. *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 4 and Remark 6). 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 set $w = \infty$ if no such largest integer exists.

The following lemma is due to Schinzel, and it also holds for $f = 1$ (see [13, Lemma 2]):

Lemma 10 (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 11. *With the notation of Lemma 10, we have* $a \notin K^{\times n}$ *if and only if* $w \geqslant f$ *or* $\mathrm{char}(K) = 0$ *and* $K \cap \mathbb{Q}(\zeta_{2^\infty})$ *is totally real.*

Proof. We have $(-1) \notin K^{\times n}$ because $\zeta_4 \notin K^\times$, 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 $\gamma = -1$. The condition $-(\xi_{2^w} + 2) = -\xi_{2^{w+1}}^2 \in K^{\times 2}$ holds in odd characteristic because for finite fields the product of two non-squares is a square (by Kummer theory, as $F(\sqrt{b}) = F(\zeta_4)$ holds if F is a finite field and $b \in F^\times \setminus F^{\times 2}$). 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 [12, Theorem 2.4], restated thanks to Lemma 11:

Theorem 12 (Rybowicz)**.** *We have*

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

where $\delta \in \{1, \frac{1}{2}\}$. *We have* $\delta = \frac{1}{2}$ *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* $\mathrm{char}(K) = 0$ *and* $K \cap \mathbb{Q}(\zeta_{2^\infty})$ *is totally real.*

Theorem 13. *Let* δ *be as in Theorem 12 and set*

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

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 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 $\zeta_n \in GK^\times$ and hence $1 + \zeta_{2^w} \in GK^\times$ and we conclude.

So 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 $(1 + \zeta_{2^w}) \in \mu_n(\overline{K}^\times) GK^\times$ 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 $\xi_{2^{w+1}} \in < 1 + \zeta_{2^w}, \zeta_n > K^{\times n}$ and we may conclude 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 3, from Theorem 12 (applied to G and to H), as $\tilde{H} := \mu_n(GK^\times) = \mu_n(HK^\times)$ we have

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

□

Lemma 14. *With the notation of Theorem 13, 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*

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

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 $p \equiv 3 \bmod 4$, w' is the 2-adic valuation of $p^2 - 1$.

Proof. If $m = 1$, then $[K(H) : K] = |HK^\times : K^\times|$ by Theorem 4 and Remark 6 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 $|HK^\times : K^\times| = |H : \mu_{2^n}(K^\times)| = 2^{m-1}$.

If $w = f$ and $-\xi_{2^{w+1}}^n \in G^n K^{\times n}$, 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 $\delta = 1$, we may conclude because we have $|HK^\times : K^\times| = 2^{m-1}$. If $\delta = 1/2$ (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 11 we know that $(1 + \zeta_{2^w})^n = \xi_{2^{w+1}}^n \notin K^{\times n}$ so there is no integer i such that $(1 + \zeta_{2^w})\zeta_n^i \in K^\times$. We deduce that

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

To conclude that $|HK^\times : K^\times| = 2^m$ we prove 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 $\zeta_{2^{w+1}} \notin K(\zeta_4)^\times$. □

Remark that $K(\zeta_4) = 1K + \zeta_4 K$. If $w > f$ or if $w = f$ and $-\xi_{2^{w+1}}^n \notin G^n K^{\times n}$, we only have entanglement if $m \geqslant 3$. Since $m \leqslant f + 1$ and $m \leqslant f$ for $w = f$, the K-linear relations for $K(G)$ (beyond those stemming from the group $GK^\times/K^\times$) are generated by those expressing

$$\zeta_{2^3}, \ldots, \zeta_{2^m} \in 1K + \zeta_4 K\,.$$

If $w = f$ and $-\xi_{2^n}^n \in G^n K^{\times n}$, 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

$$1 + \zeta_{2^w} \in 1K + \zeta_4 K\,. \tag{4}$$

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

$$\zeta_{2^3}, \ldots \zeta_{2^{m'}} \in 1K + \zeta_4 K \tag{5}$$

where m' is the largest positive integer less or equal to m such that $\zeta_{2^{m'}} \in K(\zeta_4)^\times$. If $\delta = 1/2$, the entanglement is similarly explained by (5) and (4).

5. The general case

Let n be a positive integer coprime to 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 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 $G_p^{n_p} \in K^\times$. Since n_p is a prime power, we may apply the results in the previous sections to study G_p.

Remark 15. We clearly have

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

where p varies among the prime divisors of n, and the same holds if we replace K by a finite extension. We also have

$$[K(G) : K(\zeta_z)] = \prod_p [K(\zeta_z, G_p) : K(\zeta_z)]$$

because by Corollary 9 (for p odd), by Theorem 4 (for $p = 2$ and $\zeta_4 \in K^\times$ or $4 \nmid n$) and by Theorem 13 and Lemma 14 (in the remaining case) the factors on the right hand side are a power of p and hence the fields $K(\zeta_z, G_p)$, whose compositum is $K(G)$, are linearly disjoint over $K(\zeta_z)$.

The following result is [13, Theorem 2]:

Theorem 16 (Schinzel's theorem on abelian radical extensions)**.** *Let $n \geqslant 1$ be not divisible by $\mathrm{char}(K)$. If $a \in K^\times$, the extension $K(\zeta_n, \sqrt[n]{a})/K$ is abelian if and only if $a^m = b^n$ holds for some $b \in K^\times$ and for some $m \mid n$ such that $\zeta_m \in K$.*

Proof of Theorem 1 if n is odd. By Remark 15 we can write

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

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 16).

By Theorem 4 (in view of Remark 6) 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

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

□

Definition 17. We set $\Delta = 0$ if $\zeta_4 \in K^\times$ or $4 \nmid n$. In the remaining case, we let H' be the group H from Theorem 13 and Lemma 14 for $G^{n'}$ over $K(\zeta_z)$ and set

$$2^{-\Delta} := \frac{[K(\zeta_z, H') : K(\zeta_z)]}{|H'K(\zeta_z)^\times : K(\zeta_z)^\times|}\,. \tag{6}$$

Proof of Theorem 1 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 1 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

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

As $K(\zeta_z)/K$ is abelian, by Theorem 16 we have

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

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 13 and (6) (or of Theorem 4 if $\zeta_4 \in K^\times$ or $4 \nmid n$). □

Proof of Theorem 2. Equivalently, we prove that $[K(\zeta_z, G) : K(\zeta_z)]$ divides $\frac{1}{z} \cdot |GK^\times : K^\times|$. Letting p be a prime number, by Remark 15 we have

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

and

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

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 9. If $p \neq 2$ and $p \nmid z$, or if $p = 2$ and $\zeta_4 \in K^\times$ or $4 \nmid n$ we have

$$[K(\zeta_z, G_p) : K(\zeta_z)] = |G_pK(\zeta_z)^\times : K(\zeta_z)^\times|$$

by Theorem 4 (in view of Remark 6) and this index divides $|G_pK^\times : K^\times|$. For $p = 2$, $\zeta_4 \notin K^\times$ and $4 \mid n$ the degree $[K(\zeta_z, G_2) : K(\zeta_z)]$ divides $|G_2K(\zeta_z)^\times : K(\zeta_z)^\times|$ by Theorem 13 and (6). □

We set $\mu_\infty = \cup_{m \geqslant 1} \mu_m$. We conclude by proving a result that shows the eventual maximal growth of certain radical extensions:

Theorem 18. *For every positive integer N let R_N be a subgroup of $\overline{K}^\times$ such that the index $|R_NK^\times : K^\times|$ 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 $\zeta_p \in R_NK^\times$ 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

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

Proof. Let N_0 be a number that is divisible by $4z$ and with the property that for every N the group $\mu_N(R_NK^\times) \cap K(\zeta_z)^\times$ 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 $\mu_N(R_NK^\times) \cap K(\zeta_z)^\times$. Moreover, if p is any prime number, we have $\mu_{p^{v_p(N)}}(R_NK^\times) = \mu_{p^{v_p(N)}}(R_{p^{v_p(N)}}K^\times)$. Combining these two observations we obtain

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

If N is odd, we may conclude by Theorem 1. 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

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

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 1 because, considering Definition 17, 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 [11, Theorem 1]:

Theorem 19. *Let K be a number field, fix a finitely generated subgroup Γ of $K^\times$ and for every positive integer N let $R_N = \sqrt[N]{\Gamma}$. 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 14 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 1, 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 18. □

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

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

[8] 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`.

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

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

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

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

[13] 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.