SERIE B — INFORMATIK

On Kummer Theory and the Number of Roots of Unity in Radical Extensions of $\mathbf{Q}$[◇]

Johannes Blömer[*]

B 93–14
August 1993

Abstract

Kummer theory states that if F is a field containing a primitive d-th root of unity then the subfields of a radical extension of F generated by radicals $\sqrt[d]{\rho_1}, \ldots, \sqrt[d]{\rho_k}$ over F can be described by subgroups of the group of d-th powers of elements in $F\backslash\{0\}$. Building on work of Kneser in this paper we show that the same result can be obtained if F satisfies weaker conditions. For example, it suffices that for each prime divisor p of d the field F contains primitive a p-th root of unity. This result is used to prove that an extension $\mathbf{Q}(\sqrt[d_1]{n_1}, \sqrt[d_2]{n_2}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$, $\sqrt[d_i]{n_i}$ a real radical over $\mathbf{Q}$, ζ_m a primitive m-th root of unity, contains at most $24m$ roots of unity. The bound is optimal.

[◇] This research was supported by the ESPRIT Basic Research Action No. 3075 (ALCOM II).

[*] Fachbereich Mathematik und Informatik, Freie Universität Berlin, Takustraße 9, D-14195 Berlin, Germany

1 Introduction

Kummer theory states that if F is a field of chararteristic zero containing a primitive d-th root of unity and E is a Galois extension of F with abelian Galois group of exponent d then E can be generated by a finite set of radicals $\sqrt[d]{\rho_1}, \ldots, \sqrt[d]{\rho_k}$ over F. Moreover, all subfields of the extension are in one-to-one correspondence to the subgroups of the finite group $\Gamma(G)/F^*$ where $F^* = F\backslash\{0\}$ and $\Gamma(G) = \{\gamma \prod_{i=1}^{k} \sqrt[d]{\rho_i}^{e_i} \,|\, e_i \in F^*,\, \gamma \in F^*\}$.

Building on work of Kneser [7] in the first part of this paper it will be shown that a one-to-one correspondence between subfields of a radical extension contained in $\mathbf{C}$ and subgroups of a finite group defined as $\Gamma(G)$ above holds already under much weaker conditions than required by Kummer theory.

To state precisely the conditions that are needed to obtain such a correspondence we need to describe Kneser's result. A radical extension E of F can also be defined as an extension generated by a subgroup G of E^* such that F^* has finite index in $\Gamma(G) = GF^*$. Let us call a radical extension $E = F(G)$ admissible iff (i) F^* contains for all odd primes p a primitive p-th root of unity if $\Gamma(G)$ contains such a root of unity and (ii) if $1 + \sqrt{-1} \in \Gamma(G)$ then $\sqrt{-1} \in F^*$. Kneser then showed that for admissible radical extensions the degree of E over F is exactly the index of F^* in $\Gamma(G)$.

Important admissible extension are real radical extensions, that is, extensions of $F \subset \mathbf{R}$ generated by real radicals. For this case Kneser's theorem was first proven by Siegel [11] and partial results were shown by Besicovitch [2] and Mordell [10]. If a radical extension is generated by complex radicals $\sqrt[d_i]{\rho_i}$ then Kummer theory requires that F contains a d-th primitive root of unity, where d the least common multiple of the d_i's. However, $F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$ is already admissible if F contains for each prime divisor p of d a primitive p-th root of unity.

The main result of this paper is that for each admissible radical extensions there is already a one-to-one correspondence between subfields of E and subgroups of $\Gamma(G)/F^*$. To achieve this result it is shown first that for linearly independent radicals $\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k}$ over F that generate an admissible radical extension of F any sum $\sum_{i=1}^{k} \gamma_i \sqrt[d_i]{\rho_i}$, $\gamma_i \in F\backslash\{0\}$ generates the extension $F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$. Since a radical extension has a basis consisting of radicals only, this result shows that the subfields of a radical extension correspond to subsets of the basis.

The one-to-one correspondence between subfields and subgroups as described above then follows from the fact that if $F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k}, \sqrt[d]{\rho})$ is an admissible radical extension such that $\sqrt[d]{\rho} \in F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$ then $\sqrt[d]{\rho}$ can be written as $\gamma \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i}$, $\gamma \in F$, $e_i \in \mathbf{N}$. As will be seen, this fact, too, is a consequence (better a reformulation) of Kneser's theorem.

The fact that a sum $\sum_{i=1}^{k} \gamma_i \sqrt[d_i]{\rho_i}$, $\gamma \in F\backslash\{0\}$, of linearly independent generates an admissible radical extension $F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$ is also interesting from a computational point of view. In symbolic computation exact arithmetic (especially, computing inverses) in an algebraic number field $\mathbf{Q}(\alpha)$ is done via the isomorphism $\mathbf{Q}(\alpha) \cong \mathbf{Q}[X]/(p(X))$, where $p(X)$ is the minimal polynomial of α. Hence if we want to do exact arithmetic in a radical extension of $\mathbf{Q}$ and it is known already that $\sum_{i=1}^{k} \sqrt[d_i]{q_i}$, $q_i \in \mathbf{Q}$, generates $\mathbf{Q}(\sqrt[d_1]{q_1}, \ldots, \sqrt[d_k]{q_k})$ it remains to construct the minimal polynomial for $\sum_{i=1}^{k} \sqrt[d_i]{q_i}$, say. But this can be done efficiently using a variant of the lattice basis reduction algorithm (see [6]).

As a nice application of the results on radical extensions, in the second part of this paper we prove that an extension $\mathbf{Q}(\sqrt[d_1]{q_1}, \ldots, \sqrt[d_k]{q_k}, \zeta_m)$, $q_i \in \mathbf{Q}$, and ζ_m a primitive m-th root of unity contains at most $24m$ roots of unity. It is also shown that this bound is optimal. As a corollary we obtain that only for k dividing 24 can a k-th root of unity be written as a rational combination of rational numbers, $\sqrt{-1}$, and real radicals over $\mathbf{Q}$.

2 The structure of radical extensions

Building on a result of Kneser [7] we show how to generalize certain results from *Kummer theory* (see [1]). First a few definitions. Throughout this paper let F be a subfield of $\mathbf{C}$. Denote by F^* the multiplicative group $F\backslash\{0\}$ of F. An element $\gamma \in \mathbf{C}$ is called a *radical* over F iff

$$\gamma^d \in F.$$

for some positive integer d. Although d and ρ alone do not uniquely specify a number, in this paper we will denote a radical by the familiar symbol $\sqrt[d]{\rho}$. Sometimes this symbol may in fact refer to any of the d different solutions to $X^d - \rho = 0$. On other occasions, however, statements may be correct only for a specific solution of this equation. Therefore it is always assumed that $\sqrt[d]{\rho}$ denotes a unique complex number.

Definition 2.1 *An algebraic extension E of F is called a* **radical extension** *iff it has the form $E = F(G)$, where G is a subgroup of E^* such that F^* has finite index in $\Gamma(G) = \{\gamma\beta |\, \gamma \in G,\, \beta \in F^*\}$.*

The definition simply says that $F(G)$ is generated by a finite set of radicals $\{\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k}\}$ over F. As it turns out, the formulation given above is often more convenient. However, we will also use the straightforward definition of a radical extension as $F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$.

Definition 2.2 *A radical extension $F(G)$ is called* **admissible** *if the group $\Gamma(G)$ satisfies the following conditions:*

(i) If $\Gamma(G)$ contains a p-th root of unity ζ_p, p an odd prime, then $\zeta_p \in F^*$

(ii) If $1 + \sqrt{-1} \in \Gamma(G)$ then $\sqrt{-1} \in F^*$.

Kneser has shown that for admissible radical extensions the group $\Gamma(G)$ alone determines already the degree of the extension.

Theorem 2.3 (Kneser) *If $F(G)$ is an admissible radical extension then the degree of $F(G)$ over F is the same as the index of F^* in $\Gamma(G)$.*

Our goal is to show that the subfields of the extension $F(G)$ over F are in a one-to-one correspondence to the subgroups of $\Gamma(G)/F^*$. Before we do so let us describe important classes of admissible radical extensions and derive some corollaries from Kneser's theorem that will be used in the proof of the main result of this section.

Example 2.4 *If $F(G) \subset \mathbf{R}$ then the extension is admissible.*

These extensions are admissible since the only real roots of unity are $+1$ and -1. For this class of extensions Theorem 2.3 was originally proven by Siegel [11]. Special cases were also shown by Besicovitch [2] and Mordell [10].

Example 2.5 *A radical extension $F(G) = F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ such that F contains $\sqrt{-1}$ and for all prime divisors p of $d = \prod_{i=1}^{k} d_i$ a primitive p-th root of unity is an admissible extension.*

To proof that these extensions are indeed admissible it suffices to prove property (ii) from Definition 2.2.

Assume that for p prime the group $\Gamma(G) = GF^* = \left\{\beta \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i} \,|\, e_i \in \mathbf{Z},\, \beta \in F^*\right\}$ contains a p-th root of unity ζ. Since $\zeta^p = 1 \in F$ for some k between 1 and p the k-th power of ζ must be in F. If the smallest k for which this is true is strictly less than p then F contains all p-th roots of unity. Hence, for these p the condition of Definition 2.2 is fulfilled.

So suppose that p is the smallest integer k such that ζ^k is in F. Now for any element γ in $\Gamma(G)$ its d-th power lies in F. Moreover, we claim that for each γ in $\Gamma(G)$ the smallest integer k such that γ^k is in F divides d. The fact that $F(G) = F(\sqrt[d_1]{\rho_1}, \sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$ is admissible follows from this claim.

To prove the claim let k be the smallest integer such that $\gamma^k \in F$ for $\gamma \in \Gamma(G)$. Assume k does not divide d. Then d can be written as $d = kl + r$, with $0 < r < k$. Since $\gamma^d \in F$ and $\gamma^{kl} \in F$ it follows $\gamma^r \in F$, contradicting the minimality of k. This proves the claim.

The next result is a simple but important corollary to Kneser's theorem.

Corollary 2.6 *Let $F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$ be an admissible extension of F. If a sum $S = \sum_{i=1}^{k} \kappa_i \sqrt[d_i]{\rho_i}$ is zero for $\kappa_i \in F$ not all zero then different radicals $\sqrt[d_i]{\rho_i}$, $\sqrt[d_j]{\rho_j}$ exist such that*

$$\sqrt[d_i]{\rho_i} = \kappa \sqrt[d_j]{\rho_j}$$

for some $\kappa \in F$.

In other words, the radicals $\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k}$ are linearly independent over F if any two of them are linearly independent.

Proof: Again let $\Gamma(G)$ denote the group $\left\{\beta \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i} \,|\, e_i \in \mathbf{Z},\, \beta \in F^*\right\}$.

We claim that if for every pair of different radicals $\sqrt[d_i]{\rho_i}$, $\sqrt[d_j]{\rho_j}$

$$\sqrt[d_i]{\rho_i} / \sqrt[d_j]{\rho_j} \notin F,$$

then the set $\{\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k}\}$ can be extended to a basis of $F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ over F. It follows from Kneser's theorem that a complete system of representatives for the factor group $\Gamma(G)/F^*$ is a basis for the extension E. Hence we only need to show that $\{\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k}\}$ can be extended to a complete system of representatives of the factor group $\Gamma(G)/F^*$.

To prove this let R be a complete system of representatives. Not all radicals $\sqrt[d_i]{\rho_i}$ need to be an element of R. However, the condition $\sqrt[d_i]{\rho_i} / \sqrt[d_j]{\rho_j} \notin F$ implies that any radical $\sqrt[d_i]{\rho_i}$ is a multiple of a *different* element s_i in R. Replacing each r_i by $\sqrt[d_i]{\rho_i}$ still yields a complete system of representatives for $\Gamma(G)/F^*$. The claim and hence the corollary follows. $\square$

As mentioned in the previous proof, Kneser's theorem implies that the minimal polynomial of a radical $\sqrt[d]{\rho}$ over F that generates an admissible extension of F has the form $X^k - \sqrt[d]{\rho}k$, where $\sqrt[d]{\rho}^k \in F$. More general, if $F(G)$ is an admissible extension then the minimal polynomial of any element in $\Gamma(G)$ has the form $X^k - \gamma$ for $k \in \mathbf{N}$, $\gamma \in F$.

Now consider an admissible extension $F(G)$ and a subgroup H of G. $F(H)$ is an admissible extension of F and $F(G)$ is an admissible extension of $F(H)$. We want to determine the form of the minimal polynomials of elements in G (or equivalently $\Gamma(G)$) over $F(H)$. From Kneser's theorem follows directly that these polynomials have the form $X^k - \gamma$, where k is a positive integer and γ is a linear combination of elements in $\Gamma(H)$ with coefficients in F. However, it can be shown that γ is an element of $\Gamma(H)$ itself. It suffices to prove the following result.

Corollary 2.7 *Let $F(G)$ be an admissible radical extension of F. Assume that H is a subgroup of G. Then the degree of E over $F(H)$ is the index of $\Gamma(H)$ in $\Gamma(G)$.*

Proof: The degree $[F(G) : F(H)]$ of the extension $F(G)$ over $F(H)$ is the same as the degree $[F(G) : F]$ of $F(G)$ over F divided by the degree $[F(H) : F]$ of $F(H)$ over F.

From Kneser's theorem we know that $[F(G) : F]$ and $[F(H) : F]$ are the indices of F^* in $\Gamma(G)$ and $\Gamma(H)$, respectively. Let us denote these indices by $[\Gamma(G) : F^*]$ and $[\Gamma(H) : F^*]$.

The factor group $\Gamma(H)/F^*$ is a subgroup of the factor group $\Gamma(G)/F^*$. Moreover by one of the isomorphism theorems for groups (see [4]) the factor group $\Gamma(G)/\Gamma(H)$ is isomorphic to the factor group of $\Gamma(H)/F^*$ in $\Gamma(G)/F^*$. Hence

$$[F(G) : F(H)] = \frac{[F(G) : F^*]}{[F(H) : F^*]} = \frac{[\Gamma(G) : F^*]}{[\Gamma(H) : F^*]}$$

is the index of $\Gamma(H)$ in $\Gamma(G)$. □

The lemma states for example that the only real radicals contained in a real radical extension $F(G)$ are the obvious ones, they are exactly the elements of $\Gamma(G)$.

Before we can prove the one-to-one correspondence between subfields of a radical extension $F(G)$ and subgroups of $\Gamma(G)/F^*$ one more technical lemma has to be shown.

Lemma 2.8 *Let F be a field and ζ a root of unity. If $\sqrt[d]{\rho}$ is a radical over F such that $F(\sqrt[d]{\rho})$ is an admissible radical extension of F and is contained in $F(\zeta)$ then the minimal polynomial of $\sqrt[d]{\rho}$ over F has the form $X^l - \sqrt[d]{\rho}^l$, where l is an integer such that l divides d and $F(\zeta)$ contains a primitive l-th root of unity.*

Proof: The extension $F(\zeta) : F$ is a Galois extension with abelian Galois group (see [5]). Hence all its subfields, and in particular $F(\sqrt[d]{\rho})$, must be Galois extensions of F.

By Kneser's theorem the minimal polynomial of $\sqrt[d]{\rho}$ over F has the form $X^l - \sqrt[d]{\rho}^l$, where l is the smallest integer such that $\sqrt[d]{\rho}^l \in F$. As in the discussion of the second class of admissible extension it can be shown that l divides d.

Since $F(\sqrt[d]{\rho})$ is Galois it must contain all roots of $X^l - \sqrt[d]{\rho}^l$. But then it contains a primitive l-th root of unity, too. This proves the lemma. □

We are ready to prove the main result of this section.

Theorem 2.9 *Let $F(G) = F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ be an admissible radical extensions of F. The subfields of $F(G)$ are in one-to-one correspondence to the subgroups of the finite group $\Gamma(G)/F^*$, where $\Gamma(G) = GF^* = \left\{\beta \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i} \,|\, e_i \in \mathbf{Z},\ \beta \in F^*\right\}$.*

If the radicals $\sqrt[d_i]{\rho_i}$ are linearly independent over F then any sum of the form $\sum_{i=1}^{k} \kappa_i \sqrt[d_i]{\rho_i}$ with non-zero coefficients $\kappa_i \in F$ is a primitive element for $F(G)$.

Proof: Denote by n_{i+1} the degree of $F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_{i+1}]{\rho_{i+1}})$ over $F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_i]{\rho_i})$. Then the set

$$B = \left\{ \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i},\ 0 \leq e_1 < n_1, 0 \leq e_2 < n_2, \ldots, 0 \leq e_k < n_k \right\}$$

is a basis of $F(G)$ over F. This basis will be called the standard basis of the extension. By definition, B consists of linearly independent radicals over F.

Moreover, due to Corollary 2.7 there is a one-to-one correspondence between the elements in B and the elements in $\Gamma(G)/F^*$.

Hence it remains to show that each subfield of E can be generated by a subset of the standard basis. By the Primitive Element Theorem each subfield can be generated by a single element γ. We claim that $F(\gamma)$ is the field generated by those elements in B that occur with non-zero coefficient in the representation of γ as a linear combination of elements in the standard basis. By what has been said before the theorem follows from the claim.

Hence it remains to prove: *Let $F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ be an admissible radical extension over F. If the radicals $\sqrt[d_i]{\rho_i}$ are linearly independent over F then any sum of the form $\sum_{i=1}^{k} \kappa_i \sqrt[d_i]{\rho_i}$, $\kappa_i \in F$, $\kappa_i \neq 0$, generates the extension $F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$.*

To prove the claim denote by d the least common multiple of the integers d_i. Let ζ_d be a d-th primitive root of unity.

By the previous lemma if

$$\frac{\kappa_j \sqrt[d_j]{\rho_j}}{\kappa_i \sqrt[d_i]{\rho_i}} \in F(\zeta_d)$$

for two different indices $i, j \leq k$ then the ratio must be an l-th root of an element in F such that F contains a primitive l-th root of unity. Hence after an appropriate renumbering of the radicals $\sqrt[d_i]{\rho_i}$ the sum $\sum_{i=1}^{k} \kappa_i \sqrt[d_i]{\rho_i}$ can be written as

$$\sum_{i=1}^{k'} \kappa_i \left(1 + \mu_{i,1} + \cdots + \mu_{i,h_i}\right) \sqrt[d_i]{\rho_i},$$

where $\mu_{i,j}$ is the $l_{i,j}$-th root of an element in F such that F contains a primitive $l_{i,j}$-th root of unity.

Moreover, $F(\zeta_d, \sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_i]{\rho_{k'}})$ is an admissible radical extension of $F(\zeta)$ (see Example 2.5). By Corollary 2.7 the radicals $\sqrt[d_i]{\rho_i}$, $i = 1, 2, \ldots, k'$, are linearly independent over $F(\zeta_d)$.

The elements in a set $\{1, \mu_{i,1}, \ldots, \mu_{i,h_i}\}$, $i = 1, 2, \ldots, k'$, are also linearly independent over F. Otherwise the radicals $\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k}$ would be linearly dependent over F.

Next observe that $F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ is the same field as the field generated by the elements in

$$H = \bigcup_{i=1}^{k'} \{\sqrt[d_i]{\rho_i}, \mu_{i,1}, \ldots, \mu_{i,h_i}\}.$$

We now use the Primitive Element Theorem in the following form (see for example [9]): *Let E be an algebraic extension of F. $\gamma \in E$ generates E if for any two embeddings σ and τ of E into the complex numbers $\sigma(\gamma) \neq \tau(\gamma)$.*

Any embedding of $F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ maps $\sqrt[d_i]{\rho_i}$ onto $\zeta_i \sqrt[d_i]{\rho_i}$ for some d_i-th root of unity ζ_i and likewise $\mu_{i,j}$ is mapped $\zeta_{i,j}\mu_{i,j}$, where $\zeta_{i,j}$ is a $l_{i,j}$-th root of unity. Furthermore different embeddings map at least one element in H onto different complex numbers.

Hence, using the above formulation of the Primitive Element Theorem it suffices to show that

$$\sum_{i=1}^{k'} \zeta_i \kappa_i \left(1 + \zeta_{i,1}\mu_{i,1} + \cdots + \zeta_{i,h_i}\mu_{i,h_i}\right) \sqrt[d_i]{\rho_i} \neq$$

$$\sum_{i=1}^{k'} \zeta'_i \kappa_i \left(1 + \zeta'_{i,1}\mu_{i,1} + \cdots + \zeta'_{i,h_i}\mu_{i,h_i}\right) \sqrt[d_i]{\rho_i},$$

where $\zeta_i, \zeta'_i, \zeta_{i,j}, \zeta'_{i,j}$ are as before and for at least one index i $\zeta_i \neq \zeta'_i$ or $\zeta_{i,j} \neq \zeta'_{i,j}$ for some j.

Observe that in both sums the coefficients are elements of $F(\zeta_d)$. Therefore if the two sums are equal then a linear relation over $F(\zeta_d)$ between the radicals $\sqrt[d_i]{\rho_i}$, $i = 1, \ldots k'$, exists. By construction these radicals are linearly independent over $F(\zeta_d)$ and hence the two sums are equal if and only if all coefficients in their difference are zero. We will show that this is impossible.

Let i be such that $\zeta_i \neq \zeta'_i$ or $\zeta_{i,j} \neq \zeta'_{i,j}$ for some j. $\kappa_i \neq 0$ by assumption. Hence

$$\zeta_i \left(1 + \zeta_{i,1}\mu_{i,1} + \cdots + \zeta_{i,h_i}\mu_{i,h_i}\right) - \zeta'_i \left(1 + \zeta'_{i,1}\mu_{i,1} + \cdots + \zeta'_{i,h_i}\mu_{i,h_i}\right) = 0.$$

We must show that this is impossible. For the sake of simplicity we drop the index i. $\zeta \neq 0$, hence

$$\zeta \left(1 + \zeta_1\mu_1 + \cdots + \zeta_h\mu_h\right) - \zeta' \left(1 + \zeta'_1\mu_1 + \cdots + \zeta'_h\mu_h\right) = 0$$

implies

$$\left(1 + \zeta_1\mu_1 + \cdots + \zeta_h\mu_h\right) = \frac{\zeta'}{\zeta} \left(1 + \zeta'_1\mu_1 + \cdots + \zeta'_h\mu_h\right).$$

First assume that the ratio is not an element of F. Consider for both sides the trace with respect to the extension $F(\zeta_d, \mu_1, \ldots, \mu_h)$ of F.

According to Lemma 2.8 the trace of the left-hand side is exactly the degree of the extension $F(\zeta_d, \mu_1, \ldots, \mu_h)$. Denote this degree by D. The trace of the right-hand side is exactly the trace of ζ'/ζ, which is a d-th root of unity. If D' is the degree of $F(\zeta_d, \mu_1, \ldots, \mu_h)$ over $F\left(\frac{\zeta'}{\zeta}\right)$ then the trace of the right-hand side is D' times the trace of ζ'/ζ taken with respect to the extension $F\left(\frac{\zeta'}{\zeta}\right)$ of F. If the equality above is correct than the latter trace must be exactly D/D', the degree of $F\left(\frac{\zeta'}{\zeta}\right)$.

The trace of ζ'/ζ is the sum of its conjugates, all of which are d-th roots of unity. Moreover, since it is assumed that ζ'/ζ is not in F, there are at least 2 different conjugates. By the triangle inequality a sum of n roots of unity, not all the same, are in absolute value strictly less than n. Hence the trace of ζ'/ζ with respect to $F\left(\frac{\zeta'}{\zeta}\right)$ is in absolute value strictly less than D/D'. This shows that if ζ'/ζ is not in F then

$$\left(1 + \zeta_1\mu_1 + \cdots + \zeta_h\mu_h\right) = \frac{\zeta'}{\zeta} \left(1 + \zeta'_1\mu_1 + \cdots + \zeta'_h\mu_h\right)$$

cannot be correct.

So assume $\zeta'/\zeta' = \gamma \in F$. In that case, we must show that

$$(\gamma - 1) + (\zeta_1 - \zeta_1')\mu_1 + \cdots + (\zeta_h - \zeta_h')\mu_h = 0$$

is impossible.

This is a relation between the elements of $\{1, \mu_1, \ldots, \mu_h\}$ over F. As mentioned before these elements are linearly independent, hence the relation can hold if and only if all coefficients are zero. In particular, $\gamma = 1$ or equivalently, $\zeta = \zeta'$. But then for at least one index j between 1 and h the roots of unity ζ_j, ζ_j' are different. In which case, $(\gamma - 1) + (\zeta_1 - \zeta_1')\mu_1 + \cdots + (\zeta_h - \zeta_h')\mu_h \neq 0$, too. This proves the claim and hence the theorem. $\Box$

3 Roots of Unity in Radical Extensions of the Rational Numbers

As an application of the results of the previous section we now show the following theorem.

Theorem 3.1 *Let $F = \mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k})$ be a real radical extension of $\mathbf{Q}$. If ζ_m is a primitive m-th root of unity then $F(\zeta_m)$ contains at most $24m$ different roots of unity. Moreover, the constant 24 is best possible, i.e., there are real radical extensions F of $\mathbf{Q}$ and $m \in \mathbf{N}$ such that $F(\zeta_m)$ contains exactly $24m$ different roots of unity.*

Proof: First we reformulate the problem a bit.

Lemma 3.2 *The number M of roots of unity in $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$ is the maximum of all numbers N such that $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$ contains a primitive N-th root of unity. Moreover, m divides M.*

Proof: Assume the field contains no primitive M-th root of unity, instead assume $N < M$ is the largest number such that $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$ contains an N-th primitive root of unity. Then $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$ contains a primitive N-th root of unity and a primitive K-th root of unity for $\gcd(N, K) = 1$, $K > 1$. This implies that $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$ also contains a primitive KN-th root of unity. This contradicts the maximality of N, so $M = N$.

But then all roots of unity in $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$ must be a power of ζ_M. In particular, the primitive m-th roots of unity ζ_m must be a power of ζ_M. This is possible if and only if m divides M. $\Box$

In view of these facts we can reformulate the original problem. We have to determine the largest multiple M of m such that $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m) = \mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_M)$ for primitive m-th and M-th roots of unity ζ_m, ζ_M.

Instead of answering this question for the field $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$ we will answer it for $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_{m'})$ where $m' = \operatorname{lcm}(4, m)$. The number M deduced in this way will be an upper bound on the number of roots of unity in $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_m)$.

Assume that the prime factorization of m' is given by $m' = 2^e \prod_{i=1}^{l} p_i^{e_i}$, p_i prime, $e, e_i \in \mathbf{N}$, $e \geq 2$. Then M can be written as $M = 2^{e'} \prod_{i=1}^{l'} q_i^{f_i} \prod_{i=1}^{l} p_i^{e_i}$, q_i prime, $e', f_i \in \mathbf{N}$, $e' \geq e$. The q_i's need not be distinct from the p_i's.

If $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_{m'}) = \mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_M)$ then the first field must be the same as $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_{M_i})$, for all $i = 0, 1, \ldots, l'$, where $M_0 = 2^{e'} \prod_{i=1}^{l} p_i^{e_i}$ and $M_i = q_i^{f_i} 2^e \prod_{i=1}^{l} p_i^{e_i}$ for $i > 0$. We will show that this is possible only for $e' - e = 1$ and $q_i^{f_i} = 3$. This implies $M \leq 6m' \leq 24m$ and will therefore prove the upper bound of the theorem.

To prove the claim we consider for each M_i, $i = 0, 1, \ldots, l'$, a field E_i such that if $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_{m'}) = \mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_{M_i})$ then E_i must be a subfield of this field. Hence the degrees of $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_{m'})$ and of $\mathbf{Q}(\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}, \zeta_{M_i})$ over E_i have to be the same. From this condition the claim will follow.

We will choose the field E_i to be the field generated by the real radicals $\sqrt[d_1]{n_1}, \ldots, \sqrt[d_k]{n_k}$ and all real square roots in $\mathbf{Q}(\zeta_{M_i})$.

Lemma 3.3 *Let $m \in \mathbf{N}$ such that $4|m$. If $m = 2^e \prod_{i=1}^{l} p_i^{e_i}$, $e_i \geq 1$, $e \geq 2$, is the prime factorization of m then the subfield of $\mathbf{Q}(\zeta_m)$ generated by all real square roots in $\mathbf{Q}(\zeta_m)$ is $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_l})$ if $e = 2$ and $\mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_l}, \sqrt{2})$ if $e > 2$.*

Proof: First all quadratic subfields of $\mathbf{Q}(\zeta_m)$ will be determined. By Galois theory these subfields correspond to subgroups of the Galois group of $\mathbf{Q}(\zeta_m)$ over $\mathbf{Q}$ of order $\frac{\varphi(m)}{2}$, $\varphi(m) = [\mathbf{Q}(\zeta_m) : \mathbf{Q}]$. The Galois group of this extension is isomorphic to $\mathbf{Z}_m^*$, the multiplicative group of integers taken modulo m between 1 and m which are relatively prime to m. In particular, it is abelian. By the following result due to G. Birkhoff [3] the number of quadratic subfields of $\mathbf{Q}(\zeta_m)$ equals the number of subgroups of $\mathbf{Z}_m^*$ of order 2.

Lemma 3.4 (Birkhoff) *If G is an abelian group of order n then the number of subgroups of order $\frac{n}{d}$, $d|n$, equals the number of subgroups of order d.*

$\mathbf{Z}_m^*$ can be written as a direct product

$$\mathbf{Z}_m^* = \mathbf{Z}_{2^e}^* \times \mathbf{Z}_{p_1^{e_1}}^* \times \mathbf{Z}_{p_2^{e_2}}^* \times \cdots \times \mathbf{Z}_{p_l^{e_l}}^*,$$

where $\mathbf{Z}_{p_i^{e_i}}^*$ is a cyclic group of order $p_i^{e_i - 1}(p_i - 1)$ and $\mathbf{Z}_{2^e}^*$ is either a cyclic group of order 2 or a direct product of two cyclic groups C_1, C_2, one of order 2 and the other of order 2^{e-2}.

Each subgroup of order 2 of $\mathbf{Z}_m^*$ must be cyclic. Hence we have to determine all elements in $\mathbf{Z}_m^*$ of order 2. By the above representation for $\mathbf{Z}_m^*$ these elements correspond to products $h_1 h_2 g_1 \cdots g_l$, where $h_1 \in C_1, h_2 \in C_2, g_i \in \mathbf{Z}_{p_i^{e_i}}^*$ and each element is either the unit element of that group or an element of order 2. If $e = 2$ then we have to dismiss the second factor.

Any cyclic group of order d contains for each divisor d' of d exactly one element of order d'. Hence there are $2^{l+1} - 1$ or $2^{l+2} - 1$ elements of order 2 in $\mathbf{Z}_m^*$ depending on whether $e = 2$ or $e > 2$. The -1-terms occurs because we are not allowed to take the unit element from each subgroup. Accordingly, $\mathbf{Q}(\zeta_m)$ has either $2^{l+1} - 1$ or $2^{l+2} - 1$ quadratic subfields.

Next observe that $\mathbf{Q}(\zeta_{p_i}), \mathbf{Q}(\zeta_4)$ are subfields of $\mathbf{Q}(\zeta_m)$. And if $8|m$ then $\mathbf{Q}(\zeta_8)$ is also a subfield. A well-known result in algebraic number theory (see for example [5]) states that the unique quadratic subfield of $\mathbf{Q}(\zeta_{p_i})$ is generated by $\sqrt{(-1)p_i}$ if $p_i \equiv 3 \bmod 4$ and is generated by $\sqrt{p_i}$ if $p_i \equiv 1 \bmod 4$. Moreover, $\mathbf{Q}(\zeta_8)$ has the three quadratic subfields generated by $\sqrt{-1}, \sqrt{2}$, and by $\sqrt{-2}$.

Therefore $\mathbf{Q}(\zeta_m)$ contains

$$\sqrt{(-1)^{f_1}2^{f_2}p_1^{f_3}\cdots p_l^{f_{l+2}}},$$

where each f_i is either 0 or 1 and in case $e = 2$ f_2 is always 0.

These square roots generate pairwise distinct quadratic subfields of $\mathbf{Q}(\zeta_m)$. Since this yields $2^{l+1} - 1$ or $2^{l+2} - 1$ distinct quadratic fields depending on whether $e = 2$ or $e > 2$ these must be all quadratic subfields. Hence a real square root that is contained $\mathbf{Q}(\zeta_m)$ must generate one of the fields

$$\mathbf{Q}\left(\sqrt{2^{f_2}p_1^{f_3}\cdots p_l^{f_{l+2}}}\right),\ f_i = 0, 1,\ f_2 = 0 \text{ if } e = 2.$$

Since all these fields are contained in $\mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_l})$ if $e = 2$ and in $\mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_l}, \sqrt{2})$ if $e > 2$ the lemma follows. □

Denote the field generated by the real square roots contained in $\mathbf{Q}(\zeta_{M_i})$ and by the real radicals $\sqrt[d_1]{n_1}, \dots, \sqrt[d_k]{n_k}$ by E_i. Hence $E_i \subset \mathbf{Q}(\zeta_{M_i})$ and $\mathbf{Q}(\sqrt[d_1]{n_1}, \dots, \sqrt[d_k]{n_k}, \zeta_{M_i}) = E_i(\zeta_{M_i})$. Moreover, if $\zeta_{M_i} \in \mathbf{Q}(\sqrt[d_1]{n_1}, \dots, \sqrt[d_k]{n_k}, \zeta_{m'})$ then $E_i(\zeta_{m'}) = E_i(\zeta_{M_i})$. In particular, the degree of $E_i(\zeta_{m'})$ over E_i must be equal to the degree of $E_i(\zeta_{M_i})$ over E_i.

We need the following result from Galois Theory (see for example [8]).

Theorem 3.5 *Let E be a Galois extension of the field K. Denote the Galois group of this extension by G. Assume furthermore that F is an arbitrary extension of K and denote by EF the smallest field containing E and F. Then the field EF is a Galois extension of F and the Galois group of $EF : F$ is isomorphic to the subgroup of G corresponding to the extension $E : F \cap E$.*

Applying this theorem to $K = \mathbf{Q}$, $E = \mathbf{Q}(\zeta_{M_i}), F = E_i$ and to $K = \mathbf{Q}$, $E = \mathbf{Q}(\zeta_{m'})$, $F = E_i$ shows that $E_i(\zeta_{m'}) = E_i(\zeta_{M_i})$ implies

$$[\mathbf{Q}(\zeta_{m'}) : \mathbf{Q}(\zeta_{m'}) \cap E_i] = [\mathbf{Q}(\zeta_{M_i}) : \mathbf{Q}(\zeta_{M_i}) \cap E_i],\ i = 0, 1, \dots, l'.$$

Next we determine how the intersections look like.

Lemma 3.6 *Let $\sqrt[d_1]{n_1}, \dots, \sqrt[d_k]{n_k}$ be real radicals and ζ_m be a primitive m-th root of unity. By E denote the subfield of $\mathbf{Q}(\sqrt[d_1]{n_1}, \dots, \sqrt[d_k]{n_k}, \zeta_m)$ that is generated by the radicals $\sqrt[d_i]{n_i}$ and by the real square roots contained in $\mathbf{Q}(\zeta_m)$. Then $E \cap \mathbf{Q}(\zeta_m)$ is the field generated by the real square roots in $\mathbf{Q}(\zeta_m)$.*

Proof: Since $E \cap \mathbf{Q}(\zeta_m)$ is a subfield of the real radical extension E it must be generated by real radicals (see Theorem 2.9 and recall from Example 2.4 that E is an admissible radical extension of $\mathbf{Q}$).

Since $E \cap \mathbf{Q}(\zeta_m)$ is a real radical extension contained in $\mathbf{Q}(\zeta_m)$ it must be generated by square roots (see Lemma 2.8). By the same lemma, the field generated by all real square roots in $\mathbf{Q}(\zeta_m)$ is the largest possible subfield of $\mathbf{Q}(\zeta_m)$ generated by real radicals.

By definition of E this field is also a subfield of E. The lemma follows. $\Box$

Combining Lemma 3.3 and Lemma 3.6 shows

- If $e > 2$ then
$$F_i = \mathbf{Q}(\zeta_{M_i}) \cap E_i = \mathbf{Q}(\sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_l}, \sqrt{q_i}),\ i = 1, 2, \ldots, l',$$
and
$$F = \mathbf{Q}(\zeta_{m'}) \cap E_i = F_0 = \mathbf{Q}(\zeta_{M_0}) \cap E_0 = \mathbf{Q}(\sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_l}).$$
- If $e = e' = 2$ then
$$F_i = \mathbf{Q}(\zeta_{M_i}) \cap E_i = \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_l}, \sqrt{q_i}),\ i = 1, 2, \ldots, l',$$
and
$$F = \mathbf{Q}(\zeta_{m'}) \cap E_i = F_0 = \mathbf{Q}(\zeta_{M_0}) \cap E_0 = \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_l}) \text{ for all } i$$
- If $e = 2$, $e' > 2$ then
$$F_i = \mathbf{Q}(\zeta_{M_i}) \cap E_i = \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_l}, \sqrt{q_i}),\ i = 1, 2, \ldots, l',$$
$$F_0 = \mathbf{Q}(\zeta_{M_0}) \cap E_0 = \mathbf{Q}(\sqrt{2}, \sqrt{p_1}, \ldots, \sqrt{p_l}),$$
and
$$F = \mathbf{Q}(\zeta_{m'}) \cap E_i = \mathbf{Q}(\sqrt{p_1}, \ldots, \sqrt{p_l}) \text{ for all } i.$$

Since field degrees are multiplicative
$$\frac{\varphi(M_i)}{\varphi(m')} = \frac{[\mathbf{Q}(\zeta_{M_i}) : \mathbf{Q}]}{[\mathbf{Q}(\zeta_{m'}) : \mathbf{Q}]} = \frac{[F_i : \mathbf{Q}]}{[F : \mathbf{Q}]}.$$

First consider $i = 0$ and assume $e' > e$. In this case
$$\frac{\varphi(M_0)}{\varphi(m')} = 2^{e'-e}$$
but
$$\frac{[F_0 : \mathbf{Q}]}{[F : \mathbf{Q}]} = 2$$
if $e = 2$. Otherwise this ratio is 1. Hence if $e = 2$ then e' can be at most 3 and if $e > 2$ then $e = e'$.

For $i > 0$ we can use a similar argument.
$$\frac{\varphi(M_i)}{\varphi(m')} = q_i^{f_i - 1}(q_i - 1)$$
if q_i is distint from all p_i's. Otherwise
$$\frac{\varphi(M_i)}{\varphi(m')} = q_i^{f_i}.$$

On the other hand

$$\frac{[F^{(i)} : \mathbf{Q}]}{[F : \mathbf{Q}]} = 2$$

or

$$\frac{[F^{(i)} : \mathbf{Q}]}{[F : \mathbf{Q}]} = 1$$

depending on whether q_i is distinct from the p_j's or not.

Hence $q_i^{f_i-1}(q_i - 1) = 2$ or $q_i^{f_i} = 2$. The second case is impossible for an odd prime and the first one is possible if and only if $q_i = 3$ and $f_i = 1$. As mentioned this proves the upper bound.

It remains to show that this bound is optimal. To do so let m be a positive integer such that $\gcd(24, m) = 1$. Moreover let m be divisible by a prime p satisfying $p \equiv 3 \bmod 4$. Consider $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{p}, \zeta_m)$, where ζ_m is a primitive m-th root of unity.

As noted above $\mathbf{Q}(\zeta_m)$ contains $\sqrt{-p}$. Hence $\sqrt{-1} \in \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{p}, \zeta_m)$. Therefore this field contains

$$\frac{1}{\sqrt{2}}(1 + \sqrt{-1}) \text{ and } \frac{1}{2}(1 - \sqrt{-3}).$$

The first number is a primitive 8-th root of unity and the second one a primitive 3-rd root of unity. This implies that $\mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt{p}, \zeta_m)$ contains a $24m$-th primitive root of unity. □

As an immediate corollary we obtain

Corollary 3.7 *A k-th root of unity can be written as a rational combination of rational numbers, $\sqrt{-1}$, and real radicals over $\mathbf{Q}$ if and only if k divides* 24.

References

[1] E. Artin, *Galois Theory*, University of Notre Dame Press, 1942.

[2] A. S. Besicovitch, "On the linear independence of fractional powers of integers", *Journal of the London Mathematical Society* Vol. 15,pp. 3-6, 1940.

[3] G. Birkhoff, "Subgroups of abelian groups", *Proceedings of the London Mathematical Society* 2. Series Vol. 38, pp. 385-401, 1935.

[4] N. Jacobson, *Basic Algebra I*, W. H. Freeman and Company, 1974.

[5] G. J. Janusz, *Algebraic Number Fields*, Academic Press, 1973.

[6] R. Kannan, A. K. Lenstra, L. Lovász, "Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers", *Mathematics of Computation* Vol. 50, No. 181, pp. 235-250, 1988

[7] M. Kneser, "Lineare Abhängigkeit von Wurzeln", *Acta Arithmetica* Vol. 26, pp. 307-308, 1974/75.

[8] S. Lang, *Algebra* , Addison-Wesley, 1965.

[9] D. A. Marcus, *Number Fields*, Springer-Verlag, 1977.

[10] L. J. Mordell, “On the linear independence of algebraic numbers”, *Pacific Journal of Mathematics*, Vol. 3,pp. 625-630, 1953.

[11] C. L. Siegel, “Algebraische Abhängigkeit von Wurzeln”, *Acta Arithmetica*, Vol. 21, pp. 59-64, 1971.