View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Institutional Repository of the Freie Universität Berlin

SERIE B — INFORMATIK

Computing Sums of Radicals in Polynomial Time[◇]

Johannes Blömer*

B 93–13
August 1993

Abstract

For sums of radicals $\sum_{i=1}^{k} v_i \sqrt[d_i]{\rho_i}$, where v_i, ρ_i are elements of some real algebraic number field $\mathbf{Q}(\alpha)$, $\sqrt[d_i]{\rho_i} \in \mathbf{R}$, we present a deterministic polynomial time algorithm to decide whether the sum is zero. The time is polynomial in the number of bits required to represent α, the v_i's, ρ_i's and d_i's. The algorithm can be extended to sums of complex radicals over certain complex algebraic number fields.

[◇]This research was supported by the ESPRIT Basic Research Action No. 3075 (ALCOM II). A preliminary version of this paper appeared in *Proc. of the 32nd Symposium on Foundations of Computer Science*, 1991.
*Institut für Informatik, Fachbereich Mathematik und Informatik, Institut für Informatik, Freie Universität Berlin, Takustraße 9, D-14195 Berlin, Germany.

1 Introduction

A standard problem in Computer Algebra as well as in other areas of Computer Science is to decide whether some complicated expression, which may be given as a result of symbolic computations, is zero or, more general, contained in some field, for example the field of rational numbers. In this paper results theorems from algebraic number theory we show how to solve this problem for a large class of expressions in polynomial time.

Consider for example a sum S of the form $S = \sum_{i=1}^{k} c_i \sqrt[d_i]{q_i}$ with $c_i, q_i \in \mathbf{Q}, d_i \in \mathbf{N}$ such that $\sqrt[d_i]{q_i} \in \mathbf{R}$. We prove that the question whether this sum is zero or, more general, rational can be decided in time polynomial in the number of bits necessary to represent S. Observe that sums of the form described above play an important role in various geometric problems (e.g. Euclidean shortest paths, Euclidean traveling salesman tours). It is not known how to decide efficiently whether such a sum is positive. Although our result concerning these sums obviously relates to this question it has only little effect on the complexity of determining the sign of a sum of radicals. In fact, it only shows that if the latter problem is in NP then it is already in NP$\cap$co-NP.

In the main part of the paper we describe an algorithm that applies to sums of a much more general form than the one mentioned above. In fact, the algorithm can be applied to sums $S = \sum_{i=1}^{k} v_i \sqrt[d_i]{\rho_i}$, where $v_i, \sqrt[d_i]{\rho_i}$ are elements of some algebraic number field $\mathbf{Q}(\alpha)$ and the extension $\mathbf{Q}(\alpha, \sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ is a so-called admissible radical extension of $\mathbf{Q}(\alpha)$.

These extensions are basically defined by the following property: *Any p-th root of unity, p a prime, that can be written as*

$$\gamma \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i}, \ \gamma \in \mathbf{Q}(\alpha), \ e_i \in \mathbf{Z},$$

is already an element of $\mathbf{Q}(\alpha)$.

In particular, if $\mathbf{Q}(\alpha, \sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k}) \subset \mathbf{R}$ then the extension is admissible.

The algorithm for sums of radicals over algebraic number fields is based on the following corollary to a theorem due to M. Kneser [13]:
Let $\mathbf{Q}(\alpha, \sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$ *be an admissible radical extension of* $\mathbf{Q}(\alpha)$ *such that*

$$\frac{\sqrt[d_i]{\rho_i}}{\sqrt[d_j]{\rho_j}} \notin \mathbf{Q}(\alpha) \text{ for all } i \neq j,$$

then the elements of the set $\{\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k}\}$ *are linearly independent over* $\mathbf{Q}(\alpha)$.

Special cases of Kneser's theorem have first been shown by Besicovitch [5], Mordell [21], and Siegel [22]. If $\mathbf{Q}(\alpha)$ contains a primitive d_i-th root of unity for all i then the theorem follows immediately from Kummer theory (see [4]).

Using Kneser's theorem the question whether a sum of radicals over $\mathbf{Q}(\alpha)$ is zero basically reduces to the question whether certain ratios of radicals are contained in the algebraic number field $\mathbf{Q}(\alpha)$.

We describe an algorithm solving this problem that runs in polynomial time. Given a ratio of radicals $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$ using Newton iteration we first compute an approximation to the ratio. Using this approximation the lattice basis reduction is applied to determine an element in $\mathbf{Q}(\alpha)$ such that if the ratio is in $\mathbf{Q}(\alpha)$ then it must be this element. Finally, we use a recent algorithm of Ge [8] to decide whether the ratio and the element computed in

the previous step are equal. We also present a simple probabilistic algorithm (of Monte-Carlo-type) that can replace Ge's result.

2 Linear dependence between radicals

In this section we study linear relations between radicals. Based on a result due to Kneser [13] we prove that under certain conditions the elements in a finite set of radicals are linearly independent if any two of them are linearly independent.

Throughout this section we assume that F is a subfield of the complex numbers $\mathbf{C}$. An element $\gamma \in \mathbf{C}$ is called algebraic over F if it is a root of some polynomial $p(X) \in F[X]$. The smallest degree polynomial with leading coefficient 1 and root γ is called the minimal polynomial of γ.

A field $E \supset F$ is called an algebraic extension of F if each element in E is algebraic over F. An element $\gamma \in \mathbf{C}$ is called a *radical* over F iff

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

for some positive integer d.

Hence radicals are solutions of equations of the form $X^d - \rho = 0$, $\rho \in F$, $d \in \mathbf{N}$, and are therefore algebraic over F.

Although d and ρ alone do not uniquely specify a number, throughout 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 (This will be made more precise in Section 4.).

Definition 2.1 *An algebraic extension E of F is called a* **radical extension** *iff it has the form $E = F(\sqrt[d_1]{\rho_1}, \ldots, \sqrt[d_k]{\rho_k})$ for a finite number of radicals $\sqrt[d_i]{\rho_i}$ over F.*

As it turns out it is convenient to characterize radical extensions via group theory. Let E be an algebraic extension of F. By F^* and E^* denote the multiplicative groups $F\backslash\{0\}$ and $E\backslash\{0\}$, respectively. Assume $E = F(G)$ is generated by the elements of a subgroup G of E^*, i.e. E is the smallest field containing F and G. Throughout this section for a group G denote by $\Gamma(G)$ the group $F^*G := \{\beta\gamma | \beta \in F^*, \gamma \in G\}$.

With these notations E is a radical extension iff the factor group $\Gamma(G)/F^*$ is finite. In fact, if E is a radical extension as defined in Definition 2.1 then it is also generated by the group $G = \left\{ \beta \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i} \mid e_i \in \mathbf{Z},\ \beta \in F^* \right\}$. In this case $G = \Gamma(G)$.

On the other hand, if E is generated by a group G such that $\Gamma(G)/F^*$ is finite then

i) For any element γ in G an integer $d = d(\gamma)$ exists such that $\gamma^d \in F^*$

ii) A finite subset H of G exists such that any element of G can be written as a product of an element in H and an element in F^*,

i.e. E is generated by a subset H satisfying (ii), a finite set of radicals over F.

As Kneser [13] has shown for a large class of radical extensions $E = F(G)$ the degree of the extension can be determined by looking only at the group $\Gamma(G)$.

Definition 2.2 *A radical extension $E = F(G)$ is called* **admissible** *if it satisfies the following two 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 $\sqrt{-1} \in F^*$.

Theorem 2.3 (Kneser) *If $E = F(G)$ is an admissible radical extension then the degree of E over F is the same as the index of F^* in $\Gamma(G)$, i.e. the number of elements of the factor group $\Gamma(G)/F^*$.*

Observe that the degree of the radical extension $E = F(G)$ is always at most the index of $\Gamma(G)$ in F^*.

Before we derive some corollaries from Kneser's theorem let us describe important classes of admissible radical extensions.

Example 2.4 *The first class consists of those radical extensions E that are contained in the real numbers $\mathbf{R}$. 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 [22].

Example 2.5 *A radical extension $F(\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ 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 $G = \Gamma(G) = \left\{ \beta \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i} \mid e_i \in \mathbf{Z}, \beta \in F^* \right\}$ 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 G its d-th power lies in F. Moreover, we claim that for each γ in G the smallest integer k such that γ^k is in F divides d. The fact that $F(G)$ is admissible follows from this claim.

To prove the claim let k be the smallest integer such that $\gamma^k \in F$ for $\gamma \in G$. 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.

However, not all radical extensions are admissible. The simplest counterexamples are the extensions $F(\zeta)$, where ζ is a root of unity not contained in F. On the other hand, by enlarging F any radical extension $E = F(G)$ can be made admissible: One simply has to adjoin to F the appropriate roots of unity.

The main algorithm of this paper is based on the following 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: By $G = \Gamma(G)$ denote the group $\left\{ \beta \prod_{i=1}^{k} \sqrt[d_i]{\rho_i}^{e_i} \mid e_i \in \mathbf{Z},\ \beta \in F^* \right\}$.

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 S be a complete system of representatives. Not all radicals $\sqrt[d_i]{\rho_i}$ need to be an element of S. 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 S. Replacing each s_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. □

For the analysis of our main algorithm one more corollary to Kneser's theorem is needed.

Corollary 2.7 *Let $\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}$ be radicals over F such that $F(\sqrt[d_1]{\rho_1})$ and $F(\sqrt[d_2]{\rho_2})$ are admissible radical extensions. Denote the greatest common divisor of d_1, d_2 by d. If $\sqrt[d_1]{\rho_1} / \sqrt[d_2]{\rho_2} \in F$ then $\sqrt[d_1]{\rho_1}^d, \sqrt[d_2]{\rho_2}^d \in F$.*

Proof: $\sqrt[d_1]{\rho_1} / \sqrt[d_2]{\rho_2} \in F$ implies $(\sqrt[d_1]{\rho_1} / \sqrt[d_2]{\rho_2})^d \in F$. Hence

$$\sqrt[d_1]{\rho_1}^d = \gamma \sqrt[d_2]{\rho_2}^d$$

for some $\gamma \in F$.

We claim that the degree of $\sqrt[d_1]{\rho_1}^d$ over F is a divisor of $d_1' = d_1/d$ and that likewise the degree of $\sqrt[d_2]{\rho_2}^d$ over F is d_2'/d. We proof this only for $\sqrt[d_1]{\rho_1}^d$.

$\sqrt[d_1]{\rho_1}^d = \sqrt[d_1']{\rho_1}$ for a d_1'-th root of ρ_1. Since $F(\sqrt[d_1]{\rho_1})$ is an admissible radical extension so is $F(\sqrt[d_1']{\rho_1}) \subset F(\sqrt[d_1]{\rho_1})$. By Theorem 2.3 the degree of $\sqrt[d_1']{\rho_1}$ over F is the smallest integer k such that $\sqrt[d_1']{\rho_1}^k$ is in F^*. As in the discussion of the second class of admissible extensions one shows that k divides d_1'.

Returning to our original problem observe that the equality $\sqrt[d_1]{\rho_1}^d = \gamma \sqrt[d_2]{\rho_2}^d$ implies that $\sqrt[d_1]{\rho_1}^d$ and $\sqrt[d_2]{\rho_2}^d$ have the same degree over F. Since this degree is a divisor of d_1', d_2' and since $\gcd(d_1', d_2') = 1$ the degree must be 1, hence $\sqrt[d_1]{\rho_1}^d, \sqrt[d_2]{\rho_2}^d \in F$. □

For the sake of completeness let us mention one more corollary to Kneser's theorem although this will not be used in the sequel.

As mentioned already in the proof above, 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 $X^k - \rho^k$, where $\rho^k \in F$. 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 $d \in \mathbf{N}$, $\gamma \in F$.

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 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 2.8 *Let $F(G)$ be an admissible radical extension of F. Assume that H is a subgroup of G containing F^*. Then the degree of E over $F(H)$ is the index of $\Gamma(H)$ in $\Gamma(G)$, i.e. the number of elements of the factor group $\Gamma(G)/\Gamma(H)$.*

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 [10]) 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 $\Gamma(G)$. □

As a consequence from this corollary we get for example that the only real radicals that are contained in a real radical extension $F(G)$ are the obvious ones, they are exactly the elements of $\Gamma(G)$.

3 The rational case

To demonstrate the basic features of our algorithm in this section we restrict ourselves to real radicals over the rational numbers.

So suppose that we are given a set of real radicals $\{\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_k]{q_k}\}$ over the rational numbers. We want to check whether these radicals are linearly independent. Likewise, we want to determine whether a given linear combination of these radicals with coefficients in $\mathbf{Q}$ is zero.

Due to Corollary 2.6 we only have to check for any pair of radicals $\sqrt[d_i]{q_i}$, $\sqrt[d_j]{q_j}$ whether their ratio is a rational number. As will be seen later, using Corollary 2.7 this property in turn can be tested by determining for three radicals over $\mathbf{Q}$ whether they are rational. So let us consider this problem first. From unique factorization follows

Lemma 3.1 *Let $q \in \mathbf{Q}$, $q = \frac{a}{b}$, $\gcd(a, b) = 1$ and $d \in \mathbf{N}$. Then $\sqrt[d]{q} \in \mathbf{Q}$ if and only if $\sqrt[d]{a} \in \mathbf{Z}$ and $\sqrt[d]{b} \in \mathbf{Z}$.*

We now show how to check in polynomial time whether an integer is a d-th power.

Lemma 3.2 *It can be decided in polynomial time whether $\sqrt[d]{z} \in \mathbf{Z}$ and, if so, it can also be computed in polynomial time.*

Proof: We may assume $d \leq \log z$. Otherwise $X^d - z = 0$ has a solution in $\mathbf{Z}$ if and only if $z = 1$ or $z = -1$. Furthermore we can restrict ourselves to positive integers.

The integer $z' \in \mathbf{Z}$ such that if $\sqrt[d]{z} \in \mathbf{Z}$ then $\sqrt[d]{z} = z'$ can be determined by a binary search on the integers in the interval $I = [0, 2^{\lceil \frac{l}{d} \rceil}]$, where $l = \lceil \log z \rceil + 1$. In each step of the binary search we have to determine whether an element $\hat{z}$ from I if raised to the d-th power is smaller or larger than z or equal to z. The d-th power is computed by successive

squaring. Also observe that we may stop when a power of $\hat{z}$ has been computed that is larger than z. Hence the binary search can be done in polynomial time. □

Theorem 3.3 *Let $\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}$ be l-bit radicals over Q. It can be decided in polynomial time whether the ratio of these radicals is in* $\mathbf{Q}$. *Furthermore if the ratio is rational it can be computed in polynomial time.*

Proof: First the greatest common divisor d of d_1 and d_2 is computed.

By Corollary 2.7 if $\sqrt[d_1]{q_1}/\sqrt[d_2]{q_2} \in \mathbf{Q}$ then $\sqrt[d_i]{q_i}^d = \sqrt[d_i']{q_i} = q_i' \in \mathbf{Q}$, $i = 1, 2$. By Lemma 3.1 we can check whether this is the case by applying the algorithm leading to the previous lemma to d_i' and the numerator and denominator of q_i, $i = 1, 2$.

Then we compute q_1'/q_2' and determine (using again Lemma 3.1 and Lemma 3.2) whether

$$\sqrt[d]{\frac{q_1'}{q_2'}} \in \mathbf{Q}.$$

All steps can be done in polynomial time. □

Combining this result with Corollary 2.6 leads to

Corollary 3.4 *Let $\{\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_k]{q_k}\}$ be a set of real radicals over* $\mathbf{Q}$. *It can be decided in polynomial time whether this set is linearly independent over* $\mathbf{Q}$.

Moreover, for any sum $S = \sum_{i=1}^{k} v_i \sqrt[d_i]{q_i}$ it can be decided in polynomial time whether it is zero.

Proof: To check whether the set of radicals is linearly independent it suffices to apply the algorithm of the previous theorem to the $\frac{k(k-1)}{2}$ different ratios of radicals.

To check whether a sum $S = \sum_{i=1}^{k} v_i \sqrt[d_i]{q_i}$ is zero first use the algorithm of Theorem 3.3 to partition $R = \{\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_k]{q_k}\}$ into subsets $R_1, \ldots, R_h$ such that two radicals are in the same subset if and only if their ratio is rational. To simplify the notation assume $\sqrt[d_i]{q_i} \in R_i$, $i = 1, \ldots, h$. Also the rational numbers r_{ij} are computed such that if $\sqrt[d_j]{q_j}/\sqrt[d_i]{q_i} \in \mathbf{Q}$ then $\sqrt[d_j]{q_j}/\sqrt[d_i]{q_i} = r_{ij}$. Hence

$$S = \sum_{i=1}^{k} v_i \sqrt[d_i]{q_i} = \sum_{i=1}^{h} \left(\sum_{\sqrt[d_j]{q_j} \in R_i} v_j r_{ij} \right) \sqrt[d_i]{q_i}.$$

Since for any pair of different radicals in $R' = \{\sqrt[d_1]{q_1}, \sqrt[d_2]{q_2}, \ldots, \sqrt[d_h]{q_h}\}$ their ratio is not a rational number, by Corollary 2.6 $S = 0$ if and only if

$$\sum_{\sqrt[d_j]{q_j} \in R_i} v_j r_{ij} = 0, \text{ for } i = 1, \ldots, h.$$

These sums can be computed in polynomial time. By Theorem 3.3 the previous steps can also be done in polynomial time. □

4 Background and an outline of the general algorithm

In the remainder of this paper we generalize the results of the previous section to radicals over algebraic number fields. This section surveys the fundamental definitions from algebraic number theory and explains the problems that have to be solved to achieve the general result on sums of radicals over algebraic number fields.

An algebraic number field E is a finite extension of $\mathbf{Q}$. As is well-known any algebraic number field can be generated by a single algebraic number α, i.e. $E = \mathbf{Q}(\alpha)$ is the smallest field containing $\mathbf{Q}$ and α. If α is a root of a polynomial $p(X) = \sum_{i=0}^{n} p_i X^i, p_i \in \mathbf{Z}$ such that p has relatively prime coefficients, $p_n > 0$, and p is the smallest degree polynomial with root α then p called the minimal polynomial of α. The different roots $\alpha_0 = \alpha, \alpha_1, \ldots, \alpha_{n-1}$ of the minimal polynomial of α are called the conjugates of α.

The mappings $\sigma_j, j = 0, \ldots, n-1$, which are defined as follows

$$\begin{aligned} \sigma_j : \mathbf{Q}(\alpha) &\rightarrow \mathbf{Q}(\alpha_j) \\ \sum_{i=0}^{n-1} q_i \alpha^i &\rightarrow \sum_{i=0}^{n-1} q_i \alpha_j^i, \end{aligned}$$

are called the (n distinct) *embeddings of* $\mathbf{Q}(\alpha)$ *into the complex numbers.* The σ_j's are field isomorphisms (see [19]) and the fields $\mathbf{Q}(\alpha)$ are called the *conjugate fields* of $\mathbf{Q}(\alpha)$.

The number

$$\Delta = \Delta(\alpha) = \left(\prod_{0=i<j=n-1} (\alpha_i - \alpha_j) \right)^2$$

is called the *discriminant* of α.

The *ring of algebraic integers* (or simply *integers*) in $\mathbf{Q}(\alpha)$, denoted by R_α, is the set of all $\beta \in \mathbf{Q}(\alpha)$ such that there exists an integer polynomial $f(X) = \sum_{i=0}^{n} f_i X^i$ with $f_n = 1$ and $f(\beta) = 0$. This set endowed with the usual addition and multiplication in $\mathbf{C}$ forms a ring (cf. [19]).

We may assume that α itself is an algebraic integer. If α is not and $p(X) = \sum_{i=0}^{n} p_i X^i$ is the minimal polynomial of α then $p_n \alpha$ is an integer and generates the same field. If α is an algebraic integer then $\mathbf{Z}[\alpha]$ is a subring of R_α. Since we cannot afford to compute a basis for R_α itself we will need a superset of R_α as well.

A proof for the following lemma can be found in [19].

Lemma 4.1 *Let α an algebraic integer. Then $\Delta(\alpha) \in \mathbf{Z}$ and the ring of integers R_α of $\mathbf{Q}(\alpha)$ is contained in the $\mathbf{Z}-$module $G = (\mathbf{Z}/\Delta) \oplus (\mathbf{Z}/\Delta)\,\alpha \oplus \ldots \oplus (\mathbf{Z}/\Delta)\,\alpha^{n-1}$, i.e., any number in R_α can be uniquely written as $\frac{1}{\Delta} \sum_{i=0}^{n-1} c_i \alpha^i$, $c_i \in \mathbf{Z}$.*

Note that the inclusion is always strict.

Next a few words on the number of bits needed to encode number fields, elements in these fields, and radicals over number fields. The representation for an algebraic number field we use is the one that has been used for example by Loos [17]. In order to distinguish $\mathbf{Q}(\alpha)$ from its conjugate fields we assume that $\mathbf{Q}(\alpha)$ is specified by the minimal polynomial p of α and an isolating rectangle R, that is, a rectangle that contains no root of p except α. It follows from the root separation bound (cf. [20]) that if $|p_i| < 2^l$ for all i then R can be specified using $\mathcal{O}(n \log n + nl)$ bits. That is, $\mathbf{Q}(\alpha)$ can be encoded using $\mathcal{O}(n \log n + nl)$ bits.

However, for the sake of simplicity our theorems and algorithms we will never explicitly mention the rectangle R.

In number theory usually an element β of an algebraic number field $\mathbf{Q}(\alpha)$ is described by an n-tuple $(q_0, q_1, \ldots, q_{n-2}, q_{n-1}) \in \mathbf{Q}^n$ such that $\rho = \sum_{i=0}^{n-1} q_i \alpha^i$. In this paper we assume instead that β is encoded by an $(n+1)$-tuple $(b, b_0, b_1, \ldots, b_{n-2}, b_{n-1}) \in \mathbf{Z}^{n+1}$ such that $\beta = \frac{1}{b} \sum_{i=0}^{n-1} b_i \alpha^i$. Moreover, we assume $\gcd(b, b_0, b_1, \ldots, b_{n-1}) = 1$ and $b > 0$. The integer b will be called the *denominator* of ρ. By computing the least common multiple of the denominators of the q_i we can easily go from one representation to the other. In any case, the total input size of ρ is a linear in n and the maximum bit size of the integers p_i, b, b_i.

The question whether a sum of radicals $S = \sum_{i=1}^{k} v_i \sqrt[d_i]{\rho_i},\ v_i, \rho_i \in \mathbf{Q}(\alpha)$, is zero clearly depends on the values of the radicals $\sqrt[d_i]{\rho_i}$. Hence in the algorithms to be described below it is assumed that a radical $\sqrt[d]{\rho}$ is given by d, ρ, and a positive integer k between 0 and $d-1$ such that

$$\sqrt[d]{\rho} = \zeta_d^k |\rho|^{\frac{1}{d}} \left(\cos \frac{1}{d}\phi + i \sin \frac{1}{d}\phi \right),$$

where $\phi \in (-\pi, \pi]$ denotes the angle of ρ when written in polar coordinates, $|\rho|^{\frac{1}{d}}$ is the positive d-th root, and $\zeta_d = \cos \frac{2\pi}{d} + i \sin \frac{2\pi}{d}$. For the sake of brevity, the integer k will not be mentioned explicitly.

In summary, the input size of a set of radicals $\{\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k}\}$ over an algebraic number field is polynomial in the degree of the field, in the bit size of the coefficients of the minimal polynomial of α, in the bit size of the coefficients of the ρ_i's, and in $\log d_i$, $i = 1, 2, \ldots, k$.

Before we can outline the basic algorithm we have to address one more question. The main algorithm that decides whether a sum of radicals $S = \sum_{i=1}^{k} v_i \sqrt[d_i]{\rho_i},\ v_i, \rho_i \in \mathbf{Q}(\alpha)$, is zero, is correct only if $\mathbf{Q}(\alpha, \sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ is an admissible radical extension of $\mathbf{Q}(\alpha)$. How do we guarantee this property? As mentioned in Section 2, if $\mathbf{Q}(\alpha)$ and the radicals $\sqrt[d_i]{\rho_i}$ are real then the extension $\mathbf{Q}(\alpha, \sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ is admissible. This is the situation that is most appropriate to our algorithms. The algorithm will be polynomial in the input parameters mentioned above and these parameters are mutually independent.

However, if the radicals $\sqrt[d_i]{\rho_i}$ are complex numbers, in general there is no satisfying way to guarantee admissibility. To check whether $\mathbf{Q}(\alpha, \sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ is admissible we know no better way than determining all roots of unity in $\Gamma(G)$ (using the notation from Section 1). The methods of this paper lead to an algorithm for this problem. Its run time, however, will be exponential in k. But given that much time we can determine whether a sum of radicals is zero by a brute force bit comparison test.

By Example 2.5 in Section 2 we can avoid this problem by replacing $\mathbf{Q}(\alpha)$ by the field containing $\mathbf{Q}(\alpha)$ and for all primes p dividing $\prod d_i$ a primitive p-th root of unity. Using standard methods in algorithmic algebraic number field (see [17]) a generating element for this field can be found. However, the degree of this field and the complexity of the following algorithms will again be exponential in k, leaving us with the same problem as before.

We nevertheless describe our algorithms in the general setting of admissible extension for two reasons. First, considering arbitrary admissible extensions instead of real radical extension does not add anything to the problem. The same algorithms can be used. And second, there are cases in which a complex radical extension is admissible without

assuming a ground field $\mathbf{Q}(\alpha)$ of exponential degree. In fact, the degree may even be of the order $\max\{\log d_i\}$. Consider for example the case in which the d_i's are huge powers of a single small prime or of constantly many small primes. In these cases our algorithm will also run in time polynomial in the input size.

Finally let us briefly outline the main algorithm. Due to Corollary 2.6 deciding whether $S = \sum_{i=1}^{k} v_i \sqrt[d_i]{\rho_i} = 0$ can basically be reduced to k^2 tests whether a ratio of radicals $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$ is in $\mathbf{Q}(\alpha)$. Our main task is to describe an algorithm for this problem. Since the ring of integers in $\mathbf{Q}(\alpha)$ is in general not a unique factorization domain we really have to work with ratios and cannot, as in the rational case, restrict ourselves to roots of algebraic integers.

The algorithm that decides whether a ratio of radicals is in $\mathbf{Q}(\alpha)$ has three phases. In the first one the ratio is approximated. In the second one, this approximation is used to determine an element in $\mathbf{Q}(\alpha)$ such that if the ratio is in $\mathbf{Q}(\alpha)$ then it must be this element. In the third step, it is checked whether the ratio of radicals really equals the number determined in the second phase.

The first step is done using Newton iteration. In the second phase we use a variant of the Kannan, Lenstra, Lovász algorithm (cf. [12]) to reconstruct exact representations of algebraic numbers from approximations.

For the third phase we present two different solution. The first one is deterministic and based on a recent result of Ge [8]. The second one is a very simple probabilistic algorithm.

We describe the second phase first in order to determine the quality of the approximation that has to be computed in the first phase. But before we can do so, several bounds on polynomials and representations of algebraic numbers have to be shown.

5 Some basic bounds

Let $p = \sum_{i=0}^{n} p_i X^i \in \mathbf{C}[X]$ be a polynomial with complex coefficients. The *length* $|p|_2$ of p denotes the euclidean length $\left(\sum_{i=0}^{n} |p_i|^2\right)^{\frac{1}{2}}$ of the vector $(p_0, \ldots, p_n)$.

The *measure* $M(p)$ of p is defined as

$$M(p) = |p_n| \prod_{j=0}^{n-1} \max\{1, |\alpha_j|\}.$$

$M(p)$ satisfies

$$M(p) \leq |p|_2$$

(see [20] and [28]). Combining the bound for the measure of a polynomial with Hadamard's bound for the determinant of a matrix yields an upper bound for the discriminant of a polynomial p (see for example [14], [28]).

Lemma 5.1 *Let α be an algebraic integer with minimal polynomial p. The discriminant Δ of α satisfies*

$$|\Delta|^{\frac{1}{2}} < n^n |p|_2^n.$$

Next we deduce some bounds on the representation size of algebraic numbers. For an algebraic number $\beta = \beta_0$ of degree m its *infinity norm* $[\beta]_\infty$ is defined as the maximum of the absolute values of its conjugates. If β is an element of the algebraic number field $\mathbf{Q}(\alpha)$ given by the representation $\beta = \frac{1}{b}\sum_{i=0}^{n-1} b_i\alpha^i$, $b, b_i \in \mathbf{Z}$, $\gcd(b, b_0, b_1, \ldots, b_{n-1}) = 1$, and if the distinct field embeddings of $\mathbf{Q}(\alpha)$ over $\mathbf{Q}$ are σ_j, $j = 0, \ldots, n-1$, then $[\beta]_\infty = \max\{|\sigma_0(\beta)|, |\sigma_1(\beta)|, \ldots, |\sigma_{n-1}(\beta)|\}$.

The infinity norm is subadditive and submultiplicative, i.e.

(i) $[\alpha + \beta]_\infty \leq [\alpha]_\infty + [\beta]_\infty$,

(ii) $[\alpha\beta]_\infty \leq [\alpha]_\infty[\beta]_\infty$.

For $\beta \in \mathbf{Q}(\alpha)$ as above $[\beta]$ is defined as $\max\{|b|, |b_0|, |b_1|, \ldots, |b_{n-1}|\}$. We will call $[\beta]$ the *coefficient size* or *representation size* of β with respect to $\mathbf{Q}(\alpha)$. $[\beta]$ depends on the field $\mathbf{Q}(\alpha)$ and the generator α. But it will always be clear which field $\mathbf{Q}(\alpha)$ and which generator we are referring to, therefore we do not mention them explicitly in the symbol $[\beta]$.

The following lemma bounds the coefficient size of β with respect to its infinity norm. Formulated differently the lemma has already been shown by Weinberger, Rothschild [27] and others (see [14], [15], [28]). So we omit its proof.

Lemma 5.2 *Let $\mathbf{Q}(\alpha)$ be an algebraic number field, where α is an algebraic integer with minimal polynomial p. Then any element β of the ring of integers R_α of $\mathbf{Q}(\alpha)$ satisfies*

$$[\beta] < n^{2n}|p|_2^{2n}[\beta]_\infty.$$

We also need to bound the infinity norm of β and of β^{-1} by the coefficient size. First let us recall from Loos' paper on resultants [17] how to construct for an element $\beta = \frac{1}{b}\sum_{i=0}^{n-1} b_i\alpha^i, b_i \in \mathbf{Z}$, an integer polynomial whose roots are the conjugates of β.

Let $f(X) = \sum_{i=0}^{n} f_i X^i$ and $g(X) = \sum_{i=0}^{m} g_i X^i$ be polynomials over an arbitrary commutative ring R. The determinant of the following $(n+m)\times(n+m)$-matrix M that consists of m rows of shifted coefficients of f and n rows of shifted coefficients of g

$$M = \begin{bmatrix}
f_n & f_{n-1} & f_{n-2} & \cdots & f_1 & f_0 & & \\
 & f_n & f_{n-1} & \cdots & \cdots & f_1 & f_0 & \\
 & \ddots & & & & & & \\
 & & & f_n & f_{n-1} & \cdots & f_1 & f_0 \\
g_m & g_{m-1} & \cdots & g_1 & g_0 & & & \\
 & g_m & g_{m-1} & \cdots & g_1 & g_0 & & \\
 & \ddots & & & & & & \\
 & & & g_m & g_{m-1} & \cdots & g_1 & g_0
\end{bmatrix}$$

is called the *resultant* $\operatorname{res}(f, g)$ of f and g.

Lemma 5.3 (Loos) *Let $\beta = \frac{1}{b}\sum_{i=0}^{n-1} b_i\alpha^i, b, b_i \in \mathbf{Z}$ be an element of $\mathbf{Q}(\alpha)$. Denote by $B(Y)$ the polynomial $B(Y) = \sum_{i=0}^{n-1} b_i Y^i$. Then the resultant $r(X) \in \mathbf{Z}[X]$ of $bX - B(Y)$ and $p(Y)$ taken with respect to the ring $\mathbf{Z}[X]$ has roots $\sigma_j(\beta), j = 0, \ldots, n-1$. Here p is the minimal polynomial of α and the σ_j's are the distinct field embeddings of $\mathbf{Q}(\alpha)$.*

To bound the length of the resultant polynomial of the previous lemma the following generalization of Hadamard's bound is used (see [9], [28]).

Lemma 5.4 (Goldstein-Graham) *Let $M(X) = (M_{ij}(X))$ be an $n \times n$-matrix whose entries are polynomials with complex coefficients. Denote by m_{ij} the L_1-norm of $M_{ij}(X)$, that is, the sum of the absolute values of the coefficients of M_{ij}. Furthermore define M' as $M' = (m_{ij})$. Then the polynomial $\det M(X) \in \mathbf{C}[X]$ satisfies*

$$|\det M(X)|_2 \leq H(M').$$

Combining these results yields

Lemma 5.5 *Let $\mathbf{Q}(\alpha)$ and β be as above. Then*

(i) β and β^{-1} are roots of polynomials r and r', respectively, whose length is bounded by

$$|r|_2 = |r'|_2 < n^{2n}|p|_2^n[\beta]^n$$

(ii)

$$[\beta]_\infty < 3[\beta]|p|_2^n$$

and

$$[\beta^{-1}]_\infty < n^{2n}|p|_2^n[\beta]^n.$$

Proof: We may choose r to be the polynomial from Lemma 5.3. Moreover, if

$$r(X) = \sum_{i=0}^{n} r_i X^i,\ r_i \in \mathbf{Z},$$

then β^{-1} is a root of

$$r'(X) = \sum_{i=0}^{n} r_{n-i} X^i.$$

Hence $|r|_2 = |r'|_2$. To get the bound on $|r|_2$ apply the Graham-Goldstein bound to the matrix defining r which shows

$$|r|_2 = |r'|_2 < |p|_2^n \left(\sum_{i=1}^{n-1} |b_i|^2 + (|b_0| + |b|)^2 \right)^{\frac{n}{2}} \leq |p|_2^n (n+3)^{\frac{n}{2}} [\beta]^n < n^{2n}|p|_2^n[\beta]^n.$$

Since $[\beta^{-1}]_\infty \leq M(r') \leq |r'|_2$ this proves the bound for $[\beta^{-1}]_\infty$.

To prove the better bound on $[\beta]_\infty$ observe that p is non-linear and irreducible hence its length is at least $\sqrt{2}$. $[\beta]_\infty \leq [\beta] \max\{\sum_{i=0}^{n-1} |\sigma_j(\alpha)|^i\}$, where the maximum is over all field embeddings σ_j of $\mathbf{Q}(\alpha)$. Since $[\alpha]_\infty \leq |p|_2$ we get

$$\sum_{i=0}^{n-1} |\sigma_j(\alpha)|^i \leq \sum_{i=1}^{n-1} |p|_2^i \leq \frac{|p|_2^n - 1}{|p|_2 - 1}$$

and the bound for $[\beta]_\infty$ follows from $|p|_2 - 1 \geq \sqrt{2} - 1 > \frac{1}{3}$. □

We apply the previous results to derive a bound on the representation size of a ratio of radicals over $\mathbf{Q}(\alpha)$.

Lemma 5.6 *Let* $\mathbf{Q}(\alpha)$ *be as before. Assume* $\sqrt[d_1]{\rho_1}$, $\sqrt[d_2]{\rho_2}$ *are radicals over* $\mathbf{Q}(\alpha)$ *such that* $\mathbf{Q}(\alpha, \rho_1, \rho_2)$ *is an admissible radical extension of* $\mathbf{Q}(\alpha)$. *If* $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2} \in \mathbf{Q}(\alpha)$ *then*

$$\left[\frac{\sqrt[d_1]{\rho_1}}{\sqrt[d_2]{\rho_2}}\right] < 3n^{6n}|p|_2^{5n}[\rho_1]^2[\rho_2]^{2n}.$$

Proof: First we prove a bound on the denominator of $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$.

By Lemma 2.7 $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2} \in \mathbf{Q}(\alpha)$ implies $\sqrt[d_1]{\rho_1}^d \in \mathbf{Q}(\alpha)$, $\sqrt[d_2]{\rho_2}^d \in \mathbf{Q}(\alpha)$, where $d = \gcd(d_1, d_2)$. Furthermore let $d_1' = d_1/d$, $d_2' = d_2/d$.

Hence $\sqrt[d_1]{\rho_1}^d$ is a root of

$$X^{d_1'} - \rho_1$$

and $\sqrt[d_2]{\rho_2}^{-d}$ is a root of

$$X^{d_2'} - \frac{1}{\rho_2}.$$

$\sqrt[d_1]{\rho_1}$ is a solution to the equation $X^{d_1} - \rho_1 = 0$. Let b be the denominator of ρ_1. $b\sqrt[d_1]{\rho_1}$ is a solution to $X^{d_1} - b^{d_1}\rho_1 = 0$. Since $b^d\rho_1$ is an algebraic integer $b\sqrt[d_1]{\rho_1}$ is an algebraic integer, too.

We need a similar result for $\frac{1}{\sqrt[d_2]{\rho_2}^d}$. Again we only need to bound the size of a rational integer b' such that $b'\frac{1}{\rho_2}$ is an algebraic integer.

It is well-known that if $\frac{1}{\rho_2}$ is a root of the polynomial $r \in \mathbf{Z}[X]$ whose leading coefficient is r_m then $r_m\frac{1}{\rho_2}$ is an algebraic integer. By Lemma 5.5 $\frac{1}{\rho_2}$ is root of a polynomial r whose length $|r|_2$ is bounded by $n^{2n}|p|_2^n[\rho_2]^n$. This gives the bound on b'. Moreover, combined with the bound on b it shows that an integer c, $|c| < |p|_2^n n^{2n}[\rho_1][\rho_2]^n$ exists such that $c\left(\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}\right)^d$ is an algebraic integer. Next observe that $\frac{\sqrt[d_1]{\rho_1}}{\sqrt[d_2]{\rho_2}}$ is a root of

$$X^d - \left(\frac{\sqrt[d_1]{\rho_1}}{\sqrt[d_2]{\rho_2}}\right)^d,$$

which is by assumption a polynomial over $\mathbf{Q}(\alpha)$. As before we conclude that $c\left(\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}\right)$ is an algebraic integer.

By Lemma 5.2 and the submultiplicativity of the infinity norm

$$\left[c\frac{\sqrt[d_1]{\rho_1}}{\sqrt[d_2]{\rho_2}}\right] < 3n^{2n}|p|_2^{2n}|c|[\rho_1]_\infty[\rho_2^{-1}]_\infty.$$

Since $c\frac{\sqrt[d_1]{\rho_1}}{\sqrt[d_2]{\rho_2}}$ is an algebraic integer its denominator is bounded by $|\Delta|$, where Δ is the discriminant of α (see Lemma 4.1). Hence the denominator of $\frac{\sqrt[d_1]{\rho_1}}{\sqrt[d_2]{\rho_2}}$ is bounded by $|c||\Delta|$. Using the bound on c from above, the bound for Δ (Lemma 5.1), and the bounds for $[\rho_1]_\infty, [\rho_2^{-1}]_\infty$ from Lemma 5.5, the lemma follows. □

The important thing to notice here is that the bounds are independent of d. This may seem quite surprising but it only reflects the fact that the size of the coefficients of a factor of a polynomial depends only on the degree of the factor and on the size of the coefficients of the polynomial but not on its degree (see for example [14], [27]).

6 Lattice basis reduction and reconstructing algebraic numbers

In this section we answer the following questions:
Given an approximation $\overline{\gamma}$ to an element $\gamma \in \mathbf{Q}(\alpha)$ and a guarantee that the integer coefficients c, c_i in $\gamma = \frac{1}{c}\sum_{i-0}^{n-1} c_i\alpha^i$ are bounded in absolute value by 2^B. Can the coefficients c, c_i be computed exactly? How good do we have to choose the approximation $\overline{\gamma}$?

We will show that a variant of the Kannan, Lenstra, Lovász algorithm to reconstruct minimal polynomials (see [12]) can be used to solve this problem.

Given a set V of vectors $V = \{\underline{v_1}, \ldots, \underline{v_m}\} \subset \mathbf{R}^n$, the lattice $\Lambda(V)$ generated by these vectors is the set

$$\Lambda(V) = \left\{ \sum_{i=1}^{m} z_i \underline{v_i} \mid z_i \in \mathbf{Z} \right\}$$

of vectors that can be written as linear integer combinations of the vectors in V. The vectors $\underline{v_i}$ will be described as the columns of an $(n \times m)$-matrix, which is also called V.

If we assume that the columns in V are linearly independent any vector $\underline{v} \in \Lambda(V)$ can be identified with a unique vector $(z_1, \ldots, z_m) \in \mathbf{Z}^m$ such that $\underline{v} = \sum_{i=1}^{m} z_i\underline{v_i}$. Using the matrix V this reads as $\underline{v} = V(z_1, \ldots, z_m)^T$.

Observe that a lattice is a discrete object. So the length of a shortest vector taken with respect to the euclidean length $\|.\|_2$ is uniquely defined although there may be many different vectors of this length. It is not known whether a shortest vector can be computed in polynomial time. However, in their break-through work on polynomial factorization Lenstra et al. [16] used the concept of a *reduced basis* of a lattice to show that in polynomial time a vector can be computed that is not too large compared with a shortest vector.

We will not define exactly what a reduced basis is, instead we just state its basic properties in the following lemma.

Lemma 6.1 *Given a lattice $\Lambda(V)$, $V = \{\underline{v_1}, \ldots, \underline{v_m}\} \subset \mathbf{Z}^n$, a reduced basis of $\Lambda(V)$ can be computed in polynomial time.*

The length of the shortest vector in a reduced basis of $\Lambda(V)$ differs from the length of a shortest non-zero vector in the lattice by at most a factor of $2^{\frac{m-1}{2}}$.

As mentioned, both properties were originally proven in [16]. The lattice reduction algorithm of [16] has been improved by various authors. The best run times so far are due to Schnorr [23] and Schönhage [25].

The next theorem establishes the relationship between shortest vectors in a reduced basis and representations of algebraic numbers.

Theorem 6.2 *Let $\mathbf{Q}(\alpha)$ be an algebraic number field, where α is an algebraic integer with minimal polynomial $p(X) = \sum_{i=0}^{n} p_i X^i, p_n = 1, p_i \in \mathbf{Z}$. Let γ be an element in $\mathbf{Q}(\alpha)$ such that $[\gamma] < 2^B$, $B \geq 1$. Assume s and ϵ are real numbers satisfying*

$$s > 2^{2n^2} 2^{4n} n^n |p|_2^n 2^{4Bn}, \quad \epsilon = 4s^{-1}.$$

Moreover, suppose $\overline{\gamma}, \overline{\alpha}$ are approximations to γ and α, respectively, such that the following estimates hold for the real and imaginary parts $\Re, \Im$ of γ, α

$$|\Re(\overline{\gamma}) - \Re(\gamma)| < \frac{1}{2}\epsilon, \quad |\Im(\overline{\gamma}) - \Im(\gamma)| < \frac{1}{2}\epsilon,$$

$$|\Re(\overline{\alpha}^i) - \Re(\alpha^i)| < \frac{1}{2}\epsilon, \;\; |\Im(\overline{\alpha}^i) - \Im(\alpha^i)| < \frac{1}{2}\epsilon, \; \forall i \in \{1, 2, \ldots, n-1\}.$$

If $\Lambda(V)$ is generated by the columns of the following $(n+3) \times (n+1)$ matrix

$$V = \begin{bmatrix} s\Re(\overline{\gamma}) & s & s\Re(\overline{\alpha}) & s\Re(\overline{\alpha}^2) & \ldots & s\Re(\overline{\alpha}^{n-1}) \\ s\Im(\overline{\gamma}) & 0 & s\Im(\overline{\alpha}) & s\Im(\overline{\alpha}^2) & \ldots & s\Im(\overline{\alpha}^{n-1}) \\ 1 & 0 & \ldots & & & 0 \\ 0 & 1 & 0 & \ldots & & 0 \\ & & \ddots & & & \\ & & & \ldots & & \\ 0 & 0 & \ldots & & 0 & 1 \end{bmatrix},$$

then the shortest vector $\underline{g} = V(c, c_0, c_1, \ldots, c_{n-1})^T$ of a reduced basis of $\Lambda(V)$ satisfies

$$\gamma = \frac{-1}{c} \sum_{i=0}^{n-1} c_i \alpha^i.$$

Moreover, $\gcd(c, c_0, c_1, \ldots, c_{n-1}) = 1$.

Proof: The columns in V are linearly independent. Each vector $\underline{v} \in \Lambda(V)$ can be identified with a unique vector $(z, z_0, z_1, \ldots, z_{n-1}) \in \mathbf{Z}^{n+1}$ such that $\underline{v} = V(z, z_0, z_1, \ldots, z_{n-1})^T$. Every vector $(z, z_0, z_1, \ldots, z_{n-1}) \in \mathbf{Z}^{n+1}$ in turn can be identified with a unique polynomial $v(X, Y) = zX + \sum_{i=0}^{n-1} z_i Y^i$ in the two variables X and Y. Hence there is a one-to-one correspondence between vectors $\underline{v} \in \Lambda(V)$ and certain polynomials $v(X, Y) \in \mathbf{Z}[X, Y]$.

The euclidean norm $\|\underline{v}\|_2$ of a vector $\underline{v} \in \Lambda(V)$ satisfies

$$\|\underline{v}\|_2^2 = s^2 |v(\overline{\gamma}, \overline{\alpha})|^2 + |z|^2 + \sum_{i=0}^{n-1} |z_i|^2.$$

Consider the vector $\underline{g} = V(c, c_0, \ldots, c_{n-1})^T$ and the polynomial $g(X, Y) = cX + \sum_{i=0}^{n-1} c_i Y^i$, corresponding to the representation $\gamma = \frac{-1}{c} \sum_{i=0}^{n-1} c_i \alpha^i$, $c, c_i \in \mathbf{Z}$.

$g(\gamma, \alpha) = 0$ hence

$$|g(\overline{\gamma}, \overline{\alpha})| = |g(\overline{\gamma}, \overline{\alpha}) - g(\gamma, \alpha)| \leq$$

$$\leq |c||\overline{\gamma} - \gamma| + \sum_{i=1}^{n-1} |c_i||\overline{\alpha}^i - \alpha^i| \leq n 2^B \epsilon,$$

since by assumption $|c| < 2^B$, $|c_i| < 2^B$ for all $i = 0, \ldots, n-1$. So the length ℓ of a shortest vector in a reduced basis for $\Lambda(V)$ satisfies (see Lemma 6.1)

$$\ell \leq 2^{\frac{n}{2}} \|\underline{g}\|_2 = 2^{\frac{n}{2}} \left(s^2 |g(\overline{\gamma}, \overline{\alpha})|^2 + |c|^2 + \sum_{i=0}^{n-1} |c_i|^2 \right)^{\frac{1}{2}} \leq$$

$$\leq 2^{\frac{n}{2}} ((\epsilon s n 2^B)^2 + (n 2^B)^2)^{\frac{1}{2}} \leq 2^{\frac{n}{2}} (\epsilon s + 1) n 2^B.$$

By choice of ϵ and s

$$\ell < 2^{2n+B}.$$

Next we claim that for any vector $\underline{v} \in \Lambda(V)$ whose euclidean norm $\|\underline{v}\|_2$ is smaller than 2^{2n+B} the corresponding polynomial $v(X,Y)$ satisfies $v(\gamma,\alpha)=0$.

To prove the claim first note that

$$\|\underline{v}\|_2 = \left(s^2 |v(\overline{\gamma},\overline{\alpha})|^2 + |z|^2 + \sum_{i=0}^{n-1} |z_i|^2 \right)^{\frac{1}{2}} \leq 2^{2n+B}$$

implies

$$|v(\overline{\gamma},\overline{\alpha})| \leq 2^{2n+B} s^{-1} \text{ and}$$
$$|z| \leq 2^{2n+B},\ |z_i| \leq 2^{2n+B},\ i=0,\ldots,n-1.$$

From $|v(\overline{\gamma},\overline{\alpha})| \leq 2^{2n+B} B s^{-1}$ we deduce

$$|v(\gamma,\alpha)| \leq |v(\gamma,\alpha) - v(\overline{\gamma},\overline{\alpha})| + |v(\overline{\gamma},\overline{\alpha})| \leq$$
$$\leq 2^{2n+B} n\epsilon + 2^{2n+B} s^{-1} = 2^{2n+B} s^{-1}(4n+1) < 2^{4n+B} s^{-1},$$

where the bound on $|v(\gamma,\alpha) - v(\overline{\gamma},\overline{\alpha})|$ follows in exactly the same way as the corresponding bound for g shown above.

By assumption on the representation size of γ a non-zero integer c, $|c| < 2^B$, exists such that $c\gamma \in \mathbf{Z}[\alpha]$. Consider the norm

$$\mathrm{no}(cv(\gamma,\alpha)) = \prod_{j=0}^{n-1} cv(\sigma_j(\gamma),\sigma_j(\alpha))$$

of $cv(\gamma,\alpha)$. Since $cv(\gamma,\alpha)$ is an algebraic integer this is a rational integer (see for example [19]). Hence

$$\left| c^n \prod_{j=0}^{n-1} v(\sigma_j(\gamma),\sigma_j(\alpha)) \right| \in \mathbf{N} \cup \{0\}.$$

We show that the product is smaller than 1 and hence must be zero.

$$\left| c^n \prod_{j=0}^{n-1} v(\sigma_j(\gamma),\sigma_j(\alpha)) \right| = |c^n||v(\gamma,\alpha)| \prod_{j=1}^{n-1} |v(\sigma_j(\gamma),\sigma_j(\alpha))| <$$

$$s^{-1} 2^{4n+B(n+1)} \prod_{j=1}^{n-1} |v(\sigma_j(\gamma),\sigma_j(\alpha))| \leq s^{-1} 2^{4n+B(n+1)} \prod_{j=1}^{n-1} \left(|z\sigma_j(\gamma)| + \sum_{i=0}^{n-1} |z_i \sigma_j(\alpha^i)| \right).$$

Using the above estimates for $|z|$ and $|z_i|$ this shows

$$\left| c^n \prod_{j=0}^{n-1} v(\sigma_j(\gamma),\sigma_j(\alpha)) \right| < s^{-1} 2^{2n^2} 2^{4n} 2^{2Bn} \prod_{j=1}^{n-1} \left(|\sigma_j(\gamma)| + \sum_{i=0}^{n-1} |\sigma_j(\alpha^i)| \right).$$

Writing $\sigma_j(\gamma)$ as $\frac{1}{c}\sum_{i=0}^{n-1} c_i \sigma_j(\alpha)^i$, combining corresponding powers of $\sigma_j(\alpha)$, and expanding the product yields $n^{(n-1)}$ terms each of which is smaller than $(2^B+1)^{n-1} M(p)^{n-1}$, where $M(p)$ is the measure of p.

Hence by applying $M(p) \leq |p|_2$ we get

$$\left| c^n \prod_{j=0}^{n-1} v(\sigma_j(\gamma), \sigma_j(\alpha)) \right| < s^{-1} 2^{2n^2} 2^{4n} n^{n-1} 2^{4Bn} |p|_2^{n-1}.$$

By choice of s the claim follows.

Since $c \neq 0$ $\left| c^n \prod_{j=0}^{n-1} v(\sigma_j(\gamma), \sigma_j(\alpha)) \right| = 0$ implies that one factor in $\prod_{j=0}^{n-1} v(\sigma_j(\gamma), \sigma_j(\alpha))$ is zero. But these factors are conjugates of each other. Hence if one of them is zero all are, which proves our claim that $\|\underline{v}\| < 2^{2n+B}$ implies $v(\gamma, \alpha) = 0$.

Applying this result to the shortest vector $\underline{g}$ in a reduced basis of the lattice $\Lambda(V)$ shows that $\underline{g}$ corresponds to a polynomial $g(X, Y) = cX + \sum_{i=0}^{n-1} c_i Y^i$ such that $g(\gamma, \alpha) = 0$. This proves the first part of the theorem.

To prove the second claim observe that if $\gcd(c, c_0, \ldots, c_{n-1}) \neq 1$ we would find a vector $\underline{g'} = V(c', c'_0, \ldots, c'_{n-1})^T \in \Lambda(V)$ such that $\gcd(c', c'_0, \ldots, c'_{n-1}) = 1$ and $g'(\gamma, \alpha) = 0$. The unique representation of elements of $\mathbf{Q}(\alpha)$ as rational linear combinations of powers of α shows $\underline{g'} = \frac{c'}{c}\underline{g}$. Since $\gcd(c', c'_0, \ldots, c'_{n-1}) = 1$ the integer c cannot properly divide c'. On the other hand, $\underline{g'}$ can be written as an integer linear combination of the vectors in the reduced basis. Since the elements of the basis are linearly independent even over $\mathbf{Q}$, this representation must be $\underline{g'} = \frac{c'}{c}\underline{g}$. But then $\frac{c'}{c} = +1$ or $\frac{c'}{c} = -1$ which proves the second claim of the theorem. □

The proof above is based on ideas of Lovász [18] but replaces a brute force estimate by $M(p) \leq |p|_2$. Applying this modification to Lovász' analysis of the corresponding bounds for minimal polynomials leads to an improvement of his bounds by a factor of n. Thus this analysis can be used to deduce the same bounds as in [12].

By choice of s and ϵ we can assume that the entries of the matrix V in Theorem 6.2 are integers, hence combining this theorem with Lemma 6.1 gives

Theorem 6.3 *Let $\mathbf{Q}(\alpha)$ be an algebraic number field, where α is an algebraic integer with minimal polynomial $p(X) = \sum_{i=0}^{n} p_i X^i, p_n = 1, p_i \in \mathbf{Z}$, $|p|_2 < 2^l$. Let γ be an element in $\mathbf{Q}(\alpha)$ such that $[\gamma] < 2^B$. Assume $\epsilon > 0$ satisfies*

$$\log \frac{1}{\epsilon} > 2n^2 + 4n + n \log n + nl + 4nB.$$

Moreover, suppose that approximations $\overline{\gamma}, \overline{\alpha}$ to γ and α, respectively, are given such that the following estimates hold for the real and imaginary parts $\Re, \Im$ of γ, α

$$|\Re(\overline{\gamma}) - \Re(\gamma)| < \frac{1}{2}\epsilon, \quad |\Im(\overline{\gamma}) - \Im(\gamma)| < \frac{1}{2}\epsilon,$$

$$|\Re(\overline{\alpha}^i) - \Re(\alpha^i)| < \frac{1}{2}\epsilon, \quad |\Im(\overline{\alpha}^i) - \Im(\alpha^i)| < \frac{1}{2}\epsilon, \ \forall i \in \{1, 2, \ldots, n-1\}.$$

Then the representation of γ as $\gamma = \frac{1}{c}\sum_{i=0}^{n-1} c_i \alpha^i$, $c, c_i \in \mathbf{Z}$, $|c|, |c_i| < 2^B$, can be computed in time polynomial in n, l, B.

Combining Lemma 5.6 with Theorem 6.3 shows

Corollary 6.4 *Suppose* $\sqrt[d_1]{\rho_1}$, $\sqrt[d_2]{\rho_2}$ *are radicals over an algebraic number field* $\mathbf{Q}(\alpha)$ *such that* $\mathbf{Q}(\alpha, \rho_1, \rho_2)$ *is an admissible radical extension of* $\mathbf{Q}(\alpha)$. *Here* α *is an algebraic integer with minimal polynomial* $p(X) = \sum_{i=0}^{n} p_i X^i, p_n = 1, p_i \in \mathbf{Z},\ |p|_2 < 2^l$. *Let* $[\rho_1], [\rho_2] < 2^L$ *and assume that* $\epsilon > 0$ *satisfies*

$$\log \frac{1}{\epsilon} > 28n^2(\log n + l + L).$$

Moreover, suppose that approximations $\overline{\gamma}, \overline{\alpha}$ *to* $\gamma = \sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$ *and* α, *respectively, are given such that the following estimates hold*

$$|\Re(\overline{\gamma}) - \Re(\gamma)| < \frac{1}{2}\epsilon,\ \ |\Im(\overline{\gamma}) - \Im(\gamma)| < \frac{1}{2}\epsilon,$$

$$|\Re(\overline{\alpha}^i) - \Re(\alpha^i)| < \frac{1}{2}\epsilon,\ \ |\Im(\overline{\alpha}^i) - \Im(\alpha^i)| < \frac{1}{2}\epsilon,\ \forall i \in \{1, 2, \ldots, n-1\}.$$

Then integers $c, c_0, \ldots, c_{n-1}$ *such that if* $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2} \in \mathbf{Q}(\alpha)$ *then* $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2} = \frac{1}{c}\sum_{i=0}^{n-1} c_i \alpha^i$ *can be computed in time polynomial in* $n, l,$ *and* L.

7 Approximating radicals and ratios of radicals

In this section we show how to compute efficiently the approximations required by Corollary 6.4. First the approximations to $\alpha^i,\ i = 1, \ldots, n-1$, are considered.

Lemma 7.1 *Let* α *be root of the polynomial* $p(X) = \sum_{i=0}^{n} p_i x^i, p_n = 1, p_i \in \mathbf{Z}, |p|_2 < 2^l$. *An approximation* $\overline{\alpha}$ *to* α *satisfying* $|\alpha^i - \overline{\alpha}^i| < \epsilon$ *for all* $i < n$, *can be computed in time polynomial in* $n, l,$ *and* $\log \frac{1}{\epsilon}$.

Proof: Using standard estimates one can show that if $x \in \mathbf{C}$ satisfies $|x| < 2^m$ and ϵ is less than $2^{-(m+1)}$ then an approximation $\overline{x}$ to x with absolute error less than ϵ satisfies

$$|\overline{x}^i - x^i| < \epsilon 2^{2(m+1)i}.$$

Hence if $\epsilon' := \epsilon 2^{-2(l+1)n}$ then an approximation $\overline{\alpha}$ with $|\alpha - \overline{\alpha}| < \epsilon'$ will lead to approximations as required. Applying Schönhages approximation algorithm [24] the lemma follows. □

The main difficulty in approximating a ratio of radicals $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$ is to keep the run time polynomial in $\log d_i,\ i = 1, 2$. To achieve such a run time Newton iteration is used. We first show how to approximate a single real radical.

Lemma 7.2 *Suppose* $\sqrt[d]{\rho}$ *is real radical over a real algebraic number field* $\mathbf{Q}(\alpha)$, *where* α *is an algebraic integer with minimal polynomial* $p(X) = \sum_{i=0}^{n} p_i X^i, p_n = 1, p_i \in \mathbf{Z},\ |p|_2 < 2^l$. *Assume* $[\rho] < 2^L$. *For any* $\epsilon >$ *an approximation to* $\sqrt[d]{\rho}$ *with absolute error less than* ϵ *can be computed in time polynomial in* $n, l, L, \log d,$ *and* $\log \frac{1}{\epsilon}$.

Proof: From the Mean-Value-Theorem follows that if x is a complex numbers satisfying $2^{-m} < |x| < 2^m$, $0 < \epsilon < 2^{-(m+1)}$, and $\overline{x}$ is such that $|\overline{x} - x| < \epsilon$ then

$$\left| x^{\frac{1}{d}} - \overline{x}^{\frac{1}{d}} \right| < 2^{m+1}\epsilon.$$

Since $|\rho| < 2^{nl+L+2}$ (Lemma 5.5) it suffices to approximate ρ and to approximate the d-th root of the approximation to ρ. Using the same argument as in Lemma 7.1 a good approximation to α yields a good approximation to ρ. Due to the bounds in Lemma 5.5 we can also determine the sign of ρ in polynomial time. Therefore in the remainder of the proof we show how to approximate $\sqrt[d]{\rho}$ assuming ρ is positive and is given exactly. Moreover, the bound for $|\rho|$ in Lemma 5.5 implies that it is enough to show how to approximate a $\sqrt[d]{\rho}$ with relative error ϵ.

Considering d as constant this has already been done. (see for example [2]). In our case, however, d is part of the input. So we will describe and analyze the approximation algorithm in more detail. As mentioned we use Newton iteration.

$\sqrt[d]{\rho}$ is a root of $x^d - \rho$, hence the iteration is given by

$$x_{i+1} = \left(1 - \frac{1}{d}\right) x_i + \frac{1}{d} \frac{\rho}{x_i^{d-1}}.$$

First let us pretend that we could compute x_{i+1} exactly from x_i. As is well known given a good initial approximation x_0 then Newton iteration has a quadratic convergence, which means that $\log\log \frac{1}{\epsilon}$ iterations suffice to get an approximation with relative error ϵ.

We need to determine how good the initial approximation has to be. To do so assume x_i is an approximation to $\sqrt[d]{\rho}$ with relative error ϵ_i, i.e., $\sqrt[d]{\rho} = (1 - \epsilon_i)x_i$. Then

$$|\sqrt[d]{\rho} - x_{i+1}| < \left| \sqrt[d]{\rho} - \left(1 - \frac{1}{d}\right)(1 - \epsilon_i)\sqrt[d]{\rho} + \frac{1}{d}\sqrt[d]{\rho} \left(\frac{1}{1 - \epsilon_i}\right)^{d-1} \right|.$$

Since $\left(\frac{1}{1-\epsilon_i}\right)^{d-1} = \sum_{j=0}^{\infty} \binom{d-2+j}{d-2} \epsilon_i^j$ we get

$$|\sqrt[d]{\rho} - x_{i+1}| < \sqrt[d]{\rho} \left(1 - \epsilon_i^2 \frac{1}{d} \sum_{j=0}^{\infty} \binom{d+j}{d-2} \epsilon^j\right).$$

Hence the relative error ϵ_{i+1} is

$$\epsilon_i^2 \frac{1}{d} \sum_{j=0}^{\infty} \binom{d+j}{d-2} \epsilon_i^j = \epsilon_i^2 (d-1) \sum_{j=0}^{\infty} \frac{1}{(j+1)(j+2)} \binom{d+j}{d} \epsilon_i^j <$$

$$< \epsilon_i^2 (d-1) \sum_{j=0}^{\infty} \binom{d+j}{d} \epsilon_i^j = \epsilon_i^2 (d-1) \left(\frac{1}{1-\epsilon_i}\right)^{d+1}.$$

Assume $\epsilon_i < \frac{1}{2(d+1)}$. Then

$$\epsilon_{i+1} < \epsilon_i^2 (d-1) \left(\frac{1}{1 - \frac{1}{2(d+1)}}\right)^{d+1} < \epsilon_i^2 (d-1)\sqrt{e},$$

using $1 + x < e^x$ for all x.

It follows that an initial approximation with relative error $\frac{1}{2(d+1)}$ suffices to guarantee quadratic convergence.

Now x_{i+1} can not be computed exactly from x_i. However, computing it with relative error ϵ_i^2 still yields quadratic convergence. These approximations can be computed in time $\log d, L$, and $\log \epsilon_i$. Hence except for the computation of the initial approximation x_0 the Newton iteration can be done in time polynomial in $\log d, L$, and $\log \epsilon$.

To get the initial approximation x_0 that guarantees quadratic convergence, as in Lemma 3.1 we can use a binary search technique on the interval $[1, \rho]$, if $\rho > 1$, or on the interval $[\rho, 1]$, if $\rho < 1$. Again this can be done in polynomial time due to the upper bound on $|\rho|$ given in Lemma 5.5. This finally proves the lemma. □

Now we consider the general case. Recall that we assume that a radical $\sqrt[d]{\rho}$ is given by ρ and an integer k such that $\sqrt[d]{\rho} = \zeta_d^k |\rho|^{\frac{1}{d}} \left(\cos \frac{1}{d}\phi + i \sin \frac{1}{d}\phi\right)$, where $\phi \in (-\pi, \pi]$ denotes the angle of ρ when written in polar coordinates, $|\rho|^{\frac{1}{d}}$ is the positive d-th root, and $\zeta_d = \cos \frac{2\pi}{d} + i \sin \frac{2\pi}{d}$.

Lemma 7.3 *Suppose $\mathbf{Q}(\alpha)$ is a number field generated by the algebraic integer α, whose minimal polynomial is $p(X) = \sum_{i=0}^{n} p_i X^i \in \mathbf{Z}[X], |p|_2 < 2^l$. If $d_1, d_2 \in \mathbf{N}$ and $\rho_1, \rho_2 \in \mathbf{Q}(\alpha)$ satisfy $[\rho_1], [\rho_2] < 2^L$ then for any $\epsilon > 0$ the ratio $\sqrt[d_1]{\rho_1} / \sqrt[d_2]{\rho_2}$ can be approximated with absolute error ϵ in time polynomial in $n, l, L, \log d_1, \log d_2$, and $\log \frac{1}{\epsilon}$.*

Proof: To prove the lemma note that by Lemma 5.5, not only $|\sqrt[d_1]{\rho_1}| < \max\{1, |\rho_1|\} < 2^{nl+L+2}$ but also $|\sqrt[d_2]{\rho_2}^{-1}| < \max\{1, |\rho_2^{-1}|\} < 2^{2(n \log n|+nl+nL)}$. Computing $\sqrt[d_1]{\rho_1}$ with absolute error $\epsilon 2^{-2(n \log n+nl+nL+1)}$ and $\sqrt[d_2]{\rho_2}^{-1}$ with absolute error $\epsilon' = \epsilon 2^{-(nl+L+4)}$ therefore suffices to prove the lemma.

Using standard estimates it can be shown that first approximating $\sqrt[d_2]{\rho_2}$ with absolute error less than $\epsilon' 2^{-4(n \log n+nl+nL+1)}$ and then computing the inverse of this approximation with absolute error less than $\frac{1}{2}\epsilon'$ suffices to compute the required approximation to $\sqrt[d_2]{\rho_2}^{-1}$. Computing the inverse can be done in polynomial time using Newton iteration (see for example [6]).

Hence we only need to show how to approximate a single radical $\sqrt[d]{\rho}$ in polynomial time. By the upper bound on $|\rho|$ given in Lemma 5.5 it suffices to show how to approximate $|\rho|^{\frac{1}{d}}$ (interpreted as the positive real root), $\cos \frac{1}{d}\phi_\rho + i \sin \frac{1}{d}\phi_\rho$, and $\zeta_d^k = \cos \frac{2k\pi}{d} + i \sin \frac{2k\pi}{d}$ efficiently.

Since an approximation to ρ with absolute error less than ϵ automatically yields an approximation to $|\rho|$ with absolute error less than ϵ, approximating $|\rho|^{\frac{1}{d}}$ can be analyzed by the previous lemma.

Next recall that the derivative of sin and cos is bounded by 1. Hence if $\overline{x}$ is an approximation to x with error less that $\epsilon \sin \overline{x}$ or $\cos \overline{x}$ is an approximation to $\sin x$ and $\cos x$ with (absolute or relative) error ϵ, too. Now Brent's results [6] on approximating π, sin, and cos can be used to approximate $\zeta_d^k = \cos \frac{2k\pi}{d} + i \sin \frac{2k\pi}{d}$.

Accordingly, in order to show how to approximate $\cos \frac{1}{d}\phi_\rho + i \sin \frac{1}{d}\phi_\rho$ we only need to show how to approximate ϕ_ρ.

Observe that $\phi_\rho = \arctan\left(\frac{\Im\rho}{\Re\rho}\right)$. The derivative of arctan is bounded in absolute value by π and Brent [6] also showed how to approximate arctan efficiently. Therefore it remains to show how to approximate $\frac{\Im\rho}{\Re\rho}$. Since we can approximate ρ we can also approximate the real and imaginary part of ρ. Finally we can efficiently approximate the ratio $\frac{\Im\rho}{\Re\rho}$ by

approximating $\Im\rho$ and $\frac{1}{\Re\rho}$ separately, provided we can derive good upper and lower bounds on $\Im\rho$ and $\Re\rho$, respectively. A good upper bound on the imaginary part follows from the upper bound on $[\rho]_\infty$ given in Lemma 5.5. It remains to derive a lower bound on $\Re\rho$.

By the root separation bound the difference between two different roots of a polynomial $f = \sum_{i=0}^{m} f_i X^i \in \mathbf{C}[X]$, is at least $n^{-(n+2)/2}|f|_2^{1-n}|\Delta(f)|^{1/2}$, where $\Delta(f)$ is the discriminant of f (see [20]).

By Lemma 5.3 and Lemma 5.5 we know that ρ is a root of a polynomial whose degree is bounded by n and whose length is at most $n^2|p|_2^n[\rho]^n$. Next consider $i\rho$, $i = \sqrt{-1}$. Its minimal polynomial is $f(\frac{1}{i}X)$. Moreover $|\Re\rho| = \frac{1}{2}|i\rho + \overline{i\rho}|$, where $\overline{i\rho}$ is the complex conjugate of $i\rho$. But $-\overline{i\rho}$ is also a root of $f(\frac{1}{i}X)$. To deduce a lower bound on $|\Re\rho|$ we may therefore apply the root separation bound. Observing that the discriminant of a polynomial in $\mathbf{Z}[i][X]$ is an element of $\mathbf{Z}[i]$ (see for example [11]) and therefore satisfies $|\Delta(f)| \geq 1$, this yields

$$|\Re\rho| > 2^{-2n^2(\log n - l - L) - n\log n - 1}.$$

Since the logarithm of this bound in polynomial in the input size of ρ this suffices for our purposes and the lemma follows. □

Recall that the absolute error ϵ required for the approximations in Corollary 6.4 needs to be only of the order $\mathcal{O}(n^2(\log n + l + L)$ hence the results of this section can be summarized in

Corollary 7.4 *Approximations to* α, $\sqrt[d_1]{\rho_1}$, *and* $\sqrt[d_2]{\rho_2}$ *as required by Corollary 6.4 can be determined in polynomial time.*

8 Testing for equality.

In the previous sections it has been shown how to compute the coefficients of a number $\gamma \in \mathbf{Q}(\alpha)$ such that if a ratio of radicals $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$ is contained in $\mathbf{Q}(\alpha)$ then $\gamma = \sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$. But it still remains to verify this equality.

In this section we first describe a deterministic algorithm that solves this problem. This result is based on a recent algorithm of Ge [8]. Ge's algorithm is complicated and as an alternative we describe a simple probabilistic probabilistic algorithm to determine whether γ equals the ratio $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$. Let us first state Ge's result.

Theorem 8.1 (Ge) *Let* $\mathbf{Q}(\alpha)$ *be an algebraic number field, where* α *is an algebraic integer with minimal polynomial* $p(X) = \sum_{i=0}^{n} p_i X^i, p_n = 1, p_i \in \mathbf{Z}$, $|p|_2 < 2^l$. *Assume that* ρ_i, $i = 1, \ldots, k$, *are elements of* $\mathbf{Q}(\alpha)$ *with* $[\rho_i] < 2^L$ *and assume furthermore that* $m_i \in \mathbf{Z}$, $i = 1, \ldots, k$. *It can be decided in time polynomial in* n, l, L, *and* $\max\{\log m_i\}$ *whether* $\prod_{i=1}^{k} \rho_i^{m_i} = 1$.

Applying this result to our problem yields

Corollary 8.2 *Given the element* γ *from Corollary 6.4 it can be decided in polynomial time whether* $\gamma = \sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$.

Proof: Using Ge's algorithm we first determine in polynomial time whether $\gamma^{d_1 d_2}\rho_2^{d_1} = \rho_1^{d_2}$. If equality does not hold then $\gamma \neq \sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$, too.

However, even if $\gamma^{d_1 d_2}\rho_2^{d_1} = \rho_1^{d_2}$ this does not necessarily imply that $\gamma = \sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$. All that can be deduced from this equality is that $\gamma\sqrt[d_2]{\rho_2}$ is a d_1-th root of ρ_1. It does not show that it is the root denoted by $\sqrt[d_1]{\rho_1}$. To check whether it is $\sqrt[d_1]{\rho_1}$ a bit comparison test is applied.

If $\gamma\sqrt[d_2]{\rho_2}$ is a d_1-th root of ρ_1 it can be written as $\zeta\sqrt[d_1]{\rho_1}$, where ζ is a d_1-th root of unity. Hence $|\gamma\sqrt[d_2]{\rho_2} - \sqrt[d_1]{\rho_1}| = |\zeta - 1||\sqrt[d_1]{\rho_1}|$. By Lemma 5.5 $|\sqrt[d_1]{\rho_1}| > 2^{-(2n\log n + nl + nL)}$. Moreover, two d_1-th roots of unity have distance at least $2^{-\log d_1 - 1}$. To verify this bound recall that the d_1-th roots of unity correspond to the vertices of a regular d_1-gon inscribed in the unit circle in the plane.

Together, this shows that if $\gamma\sqrt[d_2]{\rho_2} \neq \sqrt[d_1]{\rho_1}$ although $\gamma^{d_1 d_2}\rho_2^{d_1} = \rho_1^{d_2}$ then $\gamma\sqrt[d_2]{\rho_2}$ and $\sqrt[d_1]{\rho_1}$ differ by at least $\epsilon = 2^{-(2n\log n + nl + nL + 1)}$. Hence in the final step of the algorithm we compute $\sqrt[d_1]{\rho_1}$ and $\gamma\sqrt[d_2]{\rho_2}$ with precision at least ϵ. Using the results of the previous section this can be done in polynomial time. □

Remark that if $\mathbf{Q}(\alpha)$, $\sqrt[d_1]{\rho_1}$, and $\sqrt[d_2]{\rho_2}$ are real then the bit comparison test is not necessary. In fact, in this case $\gamma^{d_1 d_2}\rho_2^{d_1} = \rho_1^{d_2}$ implies $\gamma\sqrt[d_2]{\rho_2} = \sqrt[d_1]{\rho_1}$ or $-\gamma\sqrt[d_2]{\rho_2} = \sqrt[d_1]{\rho_1}$. In both cases the ratio $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$ is in $\mathbf{Q}(\alpha)$.

In the remainder of this section we show how to replace Ge's algorithm by a simple probabilistic algorithm. The algorithms will decide whether $\gamma^{d_1 d_2}\rho_2^{d_1} = \rho_1^{d_2}$ correctly with probability at least $\frac{1}{2}$. Applying the algorithm repeatedly yields any desired error probability.

Assume $b_1, b_2, c \in \mathbf{Z}$ such that $b_i\rho_i \in \mathbf{Z}[\alpha]$, $c\gamma \in \mathbf{Z}[\alpha]$. Define $\tilde{\rho}_i := b_i\rho_i$ and $\tilde{\gamma} := c\gamma$. Then $\gamma^{d_1 d_2}\rho_2^{d_1} = \rho_1^{d_2}$ is equivalent to

$$b_1^{d_2}\tilde{\rho}_2{}^{d_1}\tilde{\gamma}^{d_1 d_2} - b_2^{d_1}c^{d_1 d_2}\tilde{\rho}_1{}^{d_2} = 0,$$

which is an equation in $\mathbf{Z}[\alpha]$. Denote the algebraic number on the left-hand side of the equation by $\Gamma \in \mathbf{Z}[\alpha]$. The probabilistic algorithm works as follows:

ALGORITHM **Probablistic Checking**:

(1) Set $C := 14d_1d_2(n\log n + nl + nL)$.

(2) Randomly choose $48\log C$ integers from the interval $I = [1, 2^{4\log C}]$.

(3) For each integer z chosen in Step (2) compute the coefficients of Γ taken modulo z by reducing after each arithmetic operation in $\mathbf{Z}[\alpha]$ the coefficients of the result modulo z.

(4) If for each z the coefficients of Γ taken modulo z are zero then output $\Gamma = 0$, otherwise output $\Gamma \neq 0$.

Three things remain to be done. It has to be shown that in Step (3) the algorithm really determines the coefficients of Γ taken modulo z. Then the run time has to be analyzed. And finally it has to be shown that the error probability is less than $\frac{1}{2}$. The correctness of Step (3) follows from the next lemma.

Lemma 8.3 *Let $\rho_1, \rho_2 \in \mathbf{Z}[\alpha]$, $z \in \mathbf{Z}$, and denote by $(\rho_i)_z$ the number that is obtained by reducing the coefficients of ρ_i modulo z. Then*

$$((\rho_1)_z + (\rho_2)_z)_z = (\rho_1 + \rho_2)_z$$

and

$$((\rho_1)_z(\rho_2)_z)_z = (\rho_1\rho_2)_z$$

using arithmetic in $\mathbf{Z}[\alpha]$.

Proof: For the addition nothing has to be done.

For the multiplication it suffices to show that for two integer polynomials g_1, g_2

$$\left(\left(\left((g_1)_p\right)_z\left((g_2)_p\right)_z\right)_p\right)_z = \left((g_1g_2)_p\right)_z,$$

where $(f)_p$ denotes the polynomial f modulo the polynomial p.

Let $r_i = (g_i)_p$. Furthermore let

$$r_i = r_i' + z\overline{r_i},$$

with $r_i' = (r_i)_z$.

Then

$$\left(\left(\left((g_1)_p\right)_z\left((g_2)_p\right)_z\right)_p\right)_z = \left((r_1'r_2')_p\right)_z.$$

By definition

$$\left((g_1g_2)_p\right)_z = \left((r_1r_2)_p\right)_z.$$

Now

$$(r_1r_2)_p = \left(r_1'r_2'\right)_p + z\left(r_1'\overline{r_2} + r_2'\overline{r_1} + \overline{r_1r_2}\right)_p,$$

since for a non-constant polynomial p the homomorphism $\mathbf{Z}[X] \to (\mathbf{Z}[X])_p$ induces an isomorphism of $\mathbf{Z}$ onto itself.

From the previous equality we finally get

$$(r_1r_2)_p = \left(r_1'r_2'\right)_p,$$

which proves the lemma. □

Remark that

$$\left(\left(\left((g_1)_p\right)_z\left((g_2)_p\right)_z\right)_p\right)_z = \left((g_1g_2)_p\right)_z$$

is *not* correct if z is a non-constant polynomial.

Due to the following four facts the run time of the algorithm is polynomial. First, polynomially many integers z are chosen in Step (2), second, the size of each z is bounded by a polynomial in the input size. Third, arithmetic in $\mathbf{Z}[\alpha]$ can be done in polynomial time (see [17]) and, fourth, the reduction steps can be performed in polynomial time (see [1]).

It remains to analyze the error probability of the algorithm. First observe that if $\Gamma = 0$ then the algorithm will give the correct answer. On the other hand, if the algorithm answers $\Gamma \neq 0$ this answer is also correct since the algorithm found an integer z such that the coefficients of Γ are non-zero modulo z. Hence z witnesses $\Gamma \neq 0$.

Call an integer *unlucky* if it divides all coefficients of Γ or, equivalently, the gcd of these coefficients. Otherwise we call z *lucky*. If $\Gamma \neq 0$ then exactly the unlucky numbers will lead

to an incorrect answer of the algorithm. Hence to prove the claim that the algorithm gives the correct answer with probability at least $\frac{1}{2}$ we have to show that among the integers z chosen in Step (2) with probability at least $\frac{1}{2}$ one number is lucky.

We need a bound on the gcd of the coefficients in Γ.

Lemma 8.4 *Let $\rho_1, \ldots \rho_d \in \mathbf{Z}[\alpha]$ such that $[\rho_i] < 2^L$, $i = 1, 2, \ldots, d$, and α is as usual. Then the coefficients of $\prod_{i=1}^{d} \rho_i$ are bounded in absolute value by $2^{d(\log n + n(l+1)+L)}$.*

Proof: Let $R_i(X) = \sum_{j=0}^{n-1} r_j^{(i)} X^j$ be defined by $R_i(\alpha) = \rho_i$. Hence computing the coefficients of $\prod \rho_i$ is the same as computing the coefficients of $\prod R_i(X) \bmod p(X)$, where p is the minimal polynomial of α.

$\prod R_i(X)$ is a polynomial of degree $(n-1)d$ and its coefficients are bounded in absolute value by $2^{d(\log n + L)}$. Write $\prod R_i(X)$ as $\sum_{i=0}^{d(n-1)} m_i X^i$ and consider the following matrix:

$$d(n-1)-n+1 \text{ rows} \left\{ \begin{bmatrix} 1 & p_{n-1} & & \cdots & p_1 & p_0 & & \\ & 1 & p_{n-1} & \cdots & \cdots & p_1 & p_0 & \\ & \ddots & & & & & & \\ & & 1 & p_{n-1} & \cdots & & p_1 & p_0 \\ m_{d(n-1)} & m_{d(n-1)-1} & \cdots & & \cdots & \cdots & m_1 & m_0 \end{bmatrix} \right.$$

Using Gauss-elimination this matrix can be transformed into an upper triangular matrix

$$d(n-1)-n+1 \text{ rows} \left\{ \begin{bmatrix} 1 & p_{n-1} & p_{n-2} & \cdots & p_1 & p_0 & & \\ & 1 & p_{n-1} & \cdots & \cdots & p_1 & p_0 & \\ & \ddots & & & & & & \\ & & 1 & p_{n-1} & \cdots & & p_1 & p_0 \\ & & 0 & m'_{n-1} & m'_{n-2} & \cdots & m'_1 & m'_0 \end{bmatrix} \right.$$

It follows that m'_i are the coefficients of $\prod R_i(X)$ modulo $p(X)$.

We have to analyze this process. Denote by L_i an upper bound on the absolute values on the entries in the last row after the i-th step of the Gauss-elimination. In particular, $L_0 \leq 2^{d(\log n + L)}$. We have $L_{i+1} \leq |p|_\infty L_i + L_i = (|p|_\infty + 1) L_i$. Hence

$$L_i \leq (|p|_\infty + 1)^i 2^{d(\log n + L)}.$$

As we have to apply $d(n-1)-n$ steps in the Gauss-elimination the lemma follows from $|p|_\infty < 2^l$. □

Recall from Lemma 5.6 that $|b_1|, |b_2|, |c|, [\rho'_1], [\rho'_2], [\gamma'] < 2^{6(n \log n + nl + nL)}$. Hence the previous lemma gives a bound of

$$14 d_1 d_2 (n \log n + nl + nL) = C$$

for the bit size of the coefficients of Γ. Accordingly, the gcd of the coefficients in Γ is bounded by 2^C.

Unfortunately, an integer $z \in \mathbf{Z}$ may have almost $z^{\frac{\ln 2}{\ln \ln z}}$ different divisors (cf. [3]). This is the main reason why we cannot show directly that most numbers in I are lucky. Instead

we will show that most primes in I are lucky and that by choosing randomly $48C$ numbers from I with probability $\frac{1}{2}$ at least one of them is a lucky prime.

First note that any integer z has at most $\log z / \log\log z$ different prime divisors (see [3]). Hence the gcd of the coefficients of Γ has at most C distinct prime divisors.

On the other hand, the number of primes less than an integer x is a least $\frac{1}{6}x/\ln x$ (see [3]). Hence the number of primes in I is at least $\frac{1}{6}2^{4\log C}/4\log C > 2^{\log C+2}$, which shows that a random prime in I is unlucky with probability at most $\frac{1}{4}$.

It also follows from the lower bound on the number of primes less than x that a random number in I is composite with probability at most $1-\frac{1}{24C}$. Therefore the probability that none of the numbers chosen in Step (2) is prime is bounded by $(1-\frac{1}{24C})^{48C}$.

Since $\left(1-\frac{1}{24C}\right)^{24C} \leq \frac{1}{e}$, the probability that no prime has been chosen in Step (2) is bounded by $e^{-2} < \frac{1}{4}$.

Now there are two ways we may fail to hit upon a lucky integer. First no prime may have been chosen. Second, even if a prime has been chosen it may not be lucky. Both cases happen independently and with probability at most $\frac{1}{4}$. This shows that the error probability is of the algorithm **Probabilistic Checking** is at most $\frac{1}{2}$. Summarizing it has been shown

Lemma 8.5 *The algorithm* **Probabilistic Checking** *runs in polynomial time and gives the correct answer with probability at least* $\frac{1}{2}$.

9 Putting things together

The results of the previous three sections can be summarized in the following theorem.

Theorem 9.1 *Suppose* $\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}$ *are radicals over an algebraic number field* $\mathbf{Q}(\alpha)$ *such that* $\mathbf{Q}(\alpha,\rho_1,\rho_2)$ *is an admissible radical extension of* $\mathbf{Q}(\alpha)$. *Furthermore let* α *be an algebraic integer with minimal polynomial* $p(X)=\sum_{i=0}^{n} p_i X^i, p_n = 1, p_i \in \mathbf{Z}$, $|p|_2 < 2^l$ *and assume* $[\rho_1],[\rho_2] < 2^L$. *It can be decided in time polynomial in* n, l, L, *and* $\log d_1, \log d_2$ *whether the ratio* $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2}$ *is an element of* $\mathbf{Q}(\alpha)$. *If so, the representation* $\sqrt[d_1]{\rho_1}/\sqrt[d_2]{\rho_2} = \frac{1}{c}\sum_{i=0}^{n-1} c_i\alpha^i$, $c, c_i \in \mathbf{Z}$, *can also be computed in polynomial time.*

As in the rational case due to Corollary 2.6 this result immediately extends to sums of radicals.

Theorem 9.2 *Let* $\{\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k}\}$ *be a set of radicals over the algebraic number field* $\mathbf{Q}(\alpha)$ *such that* $\mathbf{Q}(\alpha, \sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k})$ *is an admissible radical extension of* $\mathbf{Q}(\alpha)$. *Assume that* α *is an algebraic integer whose minimal polynomial has degree* n *and has length* $|p|_2 < 2^l$. *Furthermore assume that* $[\rho_i] < 2^L, i = 1,2,\ldots,k$. *It can be decided in time polynomial in* n, l, L, *and* $\max\{\log d_i\}$ *whether a sum* $S = \sum_{i=1}^{k} v_i \sqrt[d_i]{\rho_i}$, $v_i \in \mathbf{Q}(\alpha)$, $[v_i] < 2^L$, *is zero.*

Proof: First using the algorithm of the previous theorem the set $\{\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_k]{\rho_k}\}$ is partioned into subsets $R_1, \ldots R_h$ such that two radicals are in the same subset if and only if their ratio is an element of $\mathbf{Q}(\alpha)$. To simplify the notation assume $\sqrt[d_i]{\rho_i} \in R_i$, $i = 1,\ldots,h$. This partitioning can be done in polynomial.

Also in polynomial time elements ν_{ij} can be computed such that if $\sqrt[d_j]{\rho_j}/\sqrt[d_i]{\rho_i} \in \mathbf{Q}(\alpha)$ then $\sqrt[d_j]{\rho_j}/\sqrt[d_i]{\rho_i} = \nu_{ij}$. So

$$S = \sum_{i=1}^{k} v_i \sqrt[d_i]{\rho_i} = \sum_{i=1}^{h} \left(\sum_{\sqrt[d_j]{\rho_j} \in R_i} v_j \nu_{ij} \right) \sqrt[d_i]{\rho_i}.$$

Since for any pair of different radicals in $R' = \{\sqrt[d_1]{\rho_1}, \sqrt[d_2]{\rho_2}, \ldots, \sqrt[d_h]{\rho_h}\}$ their ratio is not in $\mathbf{Q}(\alpha)$ we conclude by Corollary 2.6 that $S = 0$ if and only if

$$\sum_{\sqrt[d_j]{\rho_j} \in R_i} v_j \nu_{ij} = 0 \text{ for } i = 1, \ldots, h.$$

Since arithmetic in $\mathbf{Q}(\alpha)$ can be done in polynomial time (cf. [17]) the bound given in Lemma 5.6 for the coefficient size of the elements μ_{ij} implies that these sums can be computed in polynomial time. In particular, it can be decided in polynomial time whether they are zero. □

Acknowledgement The author thanks Helmut Alt, Emo Welzl, and Chee Yap. Helmut Alt drew my attention to several efficient approximation algorithms and Emo Welzl suggested improvements for the probabilistic algorithm in section 8. Chee Yap not only introduced me to the problem considered in this paper. A solution to the problem whether a sum of square roots is zero was in fact joint work with Chee Yap. Moreover, in his course on Computer Algebra I first learned about the basic techniques used in this paper. His class notes, soon to be published [28], were an invaluable help.

References

[1] A. V. Aho, J. E. Hopcroft, J. D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, 1975.

[2] H. Alt, "Comparison of arithmetic functions with respect to Boolean circuit depth", *Proceedings of the 16th Symposium on Theory of Computing*, pp. 466-470, 1984.

[3] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.

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

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

[6] R. P. Brent, "Fast multiple-precision evaluation of elementary functions", *Journal of the ACM*, Vol. 23, pp. 242-251, 1976.

[7] W. S. Brown, "On Euclid's algorithm and the computation of polynomial greatest common divisors", *Journal of the ACM*, Vol. 18, pp. 478-504, 1971.

[8] G. Ge ,"Testing equalities of multiplicative representations in polynomial time", to appear in *Proceedings 34th Symposium on Foundations of Computer Science*, 1993.

[9] A. J. Goldstein, R. L. Graham, "A Hadamard-type bound on the coefficients of a determinant of a polynomial", *SIAM Review* Vol. 16, pp. 394-395, 1974.

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

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

[12] 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.

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

[14] S. Landau, "Factoring polynomials over algebraic number fields", *SIAM Journal on Computing* Vol. 14, No. 1, pp. 184-195, 1985.

[15] L. Langemyr, S. McCallum, "The computation of greatest common divisors over an algebraic number field", *Journal of Symbolic Computation*, Vol. 8, pp. 429-448, 1989.

[16] A. K. Lenstra, H. W. Lenstra, L. Lovász, "Factoring polynomials with rational coefficients", *Mathematische Annalen*, Vol. 261, pp. 515-534, 1982.

[17] R. Loos, "Computing in algebraic extensions", *Computing*, Suppl. 4, pp. 173-187, 1982.

[18] L. Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*, SIAM, 1986.

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

[20] M. Mignotte, *Mathematics for Computer Algebra*, Springer-Verlag, 1992.

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

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

[23] C. P. Schnorr, "A more efficient algorithm for lattice basis reduction", *Journal of Algorithms* Vol. 9, pp. 47-62, 1988.

[24] A. Schönhage, "The fundamental theorem of algebra in terms of computational complexity", *Preliminary Report*, Universität Tübingen, 1982.

[25] A. Schönhage, "Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm", *Proc. 11th ICALP*, LNCS 172, pp. 437-447, 1984.

[26] B. L. van der Waerden, *Algebra I*, Springer Verlag, 1975.

[27] P. J. Weinberger, L. P. Rothschild, "Factoring polynomials over algebraic number fields", *ACM Transactions on Mathematical Software*, Vol. 2, pp. 335-350, 1976.

[28] C.-K. Yap, *Fundamental Problems in Algorithmic Algebra*, Princeton University Press, to appear 1993.