On Buchberger's Method of Solving Systems of Algebraic Equations*

Wolfgang Trinks

Mathematisches Institut II, Universität Karlsruhe (TH), 7500 Karlsruhe, Germany

Communicated by H.W. Leopoldt
(received February 28, 1978)

Abstract

An algorithm of Bruno Buchberger's is extended to polynomial rings over a Noetherian ring. In a specialized version, it can be used for computing *elimination ideals*. Over fields, it provides the determination of the minimal prime ideals which contain the given ideal, except that the primeness must be proved with other methods. Estimates for computing time are not given.

Introduction

The system of equations

$$F_\mu(X_1, \ldots, X_n) = 0 \qquad (1 \le \mu \le m) \tag{$\dagger$}$$

with polynomials F_μ of degree d_μ needs to be solved.

If the coefficient ring $\mathfrak{r}$ is the field $\mathbb{C}$ and we seek solutions $(x_1, \ldots, x_n)$ in $\mathbb{C}^n$, we are often interested only in approximations $(\widetilde{x}_1, \ldots, \widetilde{x}_n)$. If in addition $m = n$ holds, then *in general* the number L of solutions is finite and $N = \prod_{\mu=1}^{m} d_\mu$ is an upper bound for L, i.e. $L = N$ holds. In this situation, it is possible in principle to find $(\widetilde{x}_1, \ldots, \widetilde{x}_n)$ using a homotopy method: we choose a system of equations $G_\mu(X_1, \ldots, X_n) = 0$, G_μ of degree d_μ, whose N solutions are known (e.g. $G_\mu(X_1, \ldots, X_n) = X_\mu^{d_\mu} - 1$), and each of the N solutions $(x_{i1}(t) \ldots, x_{in}(t))$ of the system follows $H_\mu(t; X_1, \ldots, X_n) := tF_\mu(X_1, \ldots, X_n) + (1-t)G_\mu(X_1, \ldots, X_n) = 0$ as t varies along a suitable curve (in $\mathbb{C}$) from 0 to 1. This approach was used by Drexler [5] for example.

Without such extra assumptions, the problem posed at the outset belongs to the basic tasks of ideal theory in the commutative ring $\mathfrak{R} = \mathfrak{r}[X_1, \ldots, X_n]$: we find all minimal elements of the set $\{\mathfrak{P} \in \operatorname{Spec} \mathfrak{R} \mid \mathfrak{P} \supseteq \mathfrak{A}\}$, where $\mathfrak{A}$ is the $\mathfrak{R}$-ideal generated by the F_μ. When $\mathfrak{r}$ is a field, this and other basic tasks have been treated theoretically at least since Grete Hermann [7]. (We note however some corrections: Seidenberg [12].) For Noetherian rings, Richman [14] worked on the same thing. However, these algebraic methods were not built for practically implementable algorithms.

Journal of Number Theory **10** (1978): 475-488. Translated by Michael P. Abramson.

Buchberger [1] suggested an algorithm (when $\mathfrak{r}$ is a field) in which the generating set of the ideal $\mathfrak{A}$ is first brought into a certain normal form, and then this is used to produce a set of residue class representatives modulo $\mathfrak{A}$. For ideals of dimension 0, this is enough to determine the zeros. Recently, Buchberger [2] tackled this subject again and established the uniqueness of the normal form from his previous work.

In addition to Buchberger himself, Schrader [11] also implemented the algorithm on a computer (Univac 1108) and thereby came to the same conclusion concerning the uniqueness of the normal form. Computational methods for finding zeros continue to arise which are simpler than what Buchberger suggested. Lauer [9] also implemented the algorithm and generalized it for Euclidean rings $\mathfrak{r}$, a variant of which is for Noetherian integral domains $\mathfrak{r}$. Unfortunately, he did not combine everything into a uniform proof.

It appears that simple modifications to Buchberger's algorithm are necessary if we want to find zeros in higher dimensions as well. Except for this, all of the essential properties of the algorithm still hold when we replace the ground field by an arbitrary Noetherian ring.

Although Buchberger's proofs continue to hold mutatis mutandis, this last generalization in particular requires so many technical changes that a new version of the algorithm cannot be avoided.

In one special case, a method for the *successive elimination of variables* emerges, for which termination after finitely many steps, but without an estimate for that number, is known. (Unrealistically coarse estimates would be useless for applications.)

The efficiency of the actual zero calculations must be carefully considered. For ideals of dimension 0 and with a field as the underlying ring, a method is described for finding zeros, where only the large computing time of Buchberger's algorithm (and eventually for the prime decomposition of the resulting polynomials) remains unsatisfactory. For ideals of dimension greater than 0, there does not seem to be any practical method for verifying that the resulting ideals are prime.

Finally, a computed example is at least carried out. The solution of this system was noted by Matzat [10]. This is why I implemented and published the version of Buchberger's algorithm written in 1976.

0 Assumptions and Notation

Let $\mathfrak{r}$ be a commutative Noetherian ring with unity, $\mathfrak{R} = \mathfrak{r}[X_1, \ldots, X_n]$. a, b, c, … will be elements of $\mathfrak{r}$ and $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, … subsets of $\mathfrak{r}$. Corresponding upper-case letters usually mean the same for $\mathfrak{R}$.

For the ring $\mathfrak{r}$, we assume that the ring operations can be carried out constructively, and also the following:[1]

> For $b \in \mathfrak{r}$ and $\mathfrak{a} \trianglelefteq \mathfrak{r}$ (the ideal $\mathfrak{a}$ might be given by a basis), let an element $\rho(b, \mathfrak{a}) \in \mathfrak{r}$ be computable, such that $\rho(b, \mathfrak{a})$ depends only on the residue class of b modulo $\mathfrak{a}$, that is, $\rho(b, \mathfrak{a}) \equiv b \bmod \mathfrak{a}$, and $\rho(b, \mathfrak{a}) = 0$ if and only if $b \in \mathfrak{a}$. (1)

> If the coefficients a_σ, $b \in \mathfrak{r}$ of the linear equation $\sum_{\sigma=1}^{s} a_\sigma x_\sigma = b$ are given, then a specific solution (if it exists) and a basis for the $\mathfrak{r}$-module of solutions of the homogeneous equation $\sum_{\sigma=1}^{s} a_\sigma y_\sigma = 0$ are computable. (2)

(From here on, *basis* means a finite generating set of a Noetherian modules over $\mathfrak{r}$ or $\mathfrak{R}$, and specifically of an ideal. Minimality is not required.)

---

[1] Note in translation: the expression $\mathfrak{a} \trianglelefteq \mathfrak{r}$ denotes $\mathfrak{a}$ being an ideal in $\mathfrak{r}$.

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ and $I = \mathbb{N} \cup \{-1\}$. (The additional element -1 saves us from having to distinguish cases.) For $i = (i_1, \ldots, i_n) \in I$, let $X^i := \prod_{\nu=1}^{n} X_\nu^{i_\nu}$, and we write $A = \sum_{i \in I} a_i X^i$ for $A \in \mathfrak{R}$, where it is always implicitly assumed that $a_{-1} = 0$ and almost all $a_i = 0$. $i \mid j$ will mean $i_\nu \leq j_\nu$ $(1 \leq \nu \leq n)$, and $i \nmid j$ the opposite. For the element $-1 \in I$, we add: $1 \mid i$ for $i \in I$, and $i \nmid -1$ for $i \neq -1$. If $E \subseteq I$ is a finite set, then $\operatorname{lcm}(E)$ will denote the least upper bound of E in I relative to the partial order $\mid$. In addition, let I be given a linear order $\leq$ which agrees with $\mid$ as follows:

$$i \mid j \quad \text{implies} \quad i \leq j \qquad (i, j \in I) \tag{3}$$

$$i \leq j \quad \text{implies} \quad i + k \leq j + k \qquad (i, j, k \in I \setminus \{-1\}) \tag{4}$$

Later, we will write $i < j$ or $j > i$ for $i \leq j \neq i$ quite often. The terms *minimum* and *minimal* applied to the subsets of I always relate to the relation $\mid$, and *least element* to $\leq$; similarly for *maximum*, when not explicitly stated otherwise.

For $A = \sum_{i \in I} a_i X^i$, let $\partial A := \max_{\leq}\{i \in I \mid a_i \neq 0 \text{ or } i = -1\}$ be the degree of A (hence this $\max_{\leq}$ differs from the definition just stated) and $f_A := a_{\partial A}$ be the *leading coefficient* of A. Let $\mathfrak{M} \subseteq \mathfrak{R}$. We define the ideal $\mathfrak{a}_i(\mathfrak{M})$ $(i \in I)$ of $\mathfrak{r}$ relative to $\mathfrak{M}$ and $\leq$ as follows: Let $\mathfrak{a}_i(\mathfrak{M})$ be the $\mathfrak{r}$-ideal generated by $\{f_A \mid A \in \mathfrak{M} \text{ and } \partial A \mid i\}$. If $\mathfrak{M}$ is fixed, we just write $\mathfrak{a}_i$. In addition, let $\mathfrak{B} = \mathfrak{B}(\mathfrak{M}) := \big\{B = \sum_{i \in I} b_i X^i \in \mathfrak{R} \mid b_i = \rho(b_i, \mathfrak{a}_i) \text{ for all } i\big\}$ with ρ as in (1).

1 Definitions and Lemmas

Lemma 1. (a) *There are no (infinite) sequences* (i^λ), $i^\lambda \in I$, $\lambda \in \mathbb{N}$, *with the property that for* $\lambda < \mu$, $i^\lambda \nmid i^\mu$ *holds.*

(b) *A set* $J \subseteq I$ *is finite if* $i \neq j$ *implies* $i \nmid j$ *for all* $i, j \in J$.

(c) *There are no (infinite) sequences* (i^λ) *with* $i^\lambda > i^\mu$ *for* $\lambda < \mu$.

Proof. (a) It is easy to see for $n = 0$ or 1. Let $m \in \mathbb{N}$ be the smallest number such that the claim can be disproved by a sequence (i^λ), $i^\lambda \in \mathbb{N}^m$. This contains the subsequence $(j^\mu) = (i^{\lambda_\mu})$, $\mu \in \mathbb{N}$, in which, for the index m, the sequence j_m^μ, for instance, does not decrease. But then we would have also found such a sequence (k^μ) in $\mathbb{N}^{m-1}$, with $k^\mu = (j_1^\mu, \ldots, j_{m-1}^\mu)$, contradicting the definition of m. (b) follows immediately. (c) is implied by (3). ☐

Lemma 2. *Let* $(\mathfrak{a}_{ip})$ *be a double sequence* $(i \in I, p \in \mathbb{N})$ *of ideals in the Noetherian ring* $\mathfrak{r}$, *where*

$$i \mid j \quad \textit{implies} \quad \mathfrak{a}_{ip} \subseteq \mathfrak{a}_{jp} \tag{5}$$

$$p \leq q \quad \textit{implies} \quad \mathfrak{a}_{ip} \subseteq \mathfrak{a}_{iq}. \tag{6}$$

holds for all indices. By (6), $\mathfrak{a}_i := \bigcup_{p \in \mathbb{N}} \mathfrak{a}_{ip}$ *is also an ideal of* $\mathfrak{r}$. *Then*

(a) *The set* $\mathcal{Z} := \{\mathfrak{a}_i \mid i \in I\}$ *is finite.*

(b) *The set* $K := \{i \in I \mid i \text{ is minimal such that } \mathfrak{a}_i = \mathfrak{b} \text{ for some } \mathfrak{b} \in \mathcal{Z}\}$ *is finite.*

(c) *There is an* $N \in \mathbb{N}$ *such that* $\mathfrak{a}_{iN} = \mathfrak{a}_i$ *for all* $i \in I$.

Proof. By assuming that $\mathcal{Z}$ is not finite, we will construct a sequence (i^λ) that contradicts Lemma 1(a) by means of the following *algorithm*:

To start, let $\mathcal{Y} := \varnothing$, $\ell := 0$.

$$\text{Let } \mathfrak{b} \text{ be a maximal element of } \mathcal{Z}/\mathcal{Y}.\ (\mathfrak{r} \text{ is Noetherian}) \tag{7}$$

$$J := \{i \in I \mid i \text{ minimal with } \mathfrak{a}_i = \mathfrak{b}\}.\ \text{By definition of } \mathcal{Z}, \text{ we have } J \neq \varnothing. \tag{8}$$

(5) and (6) together immediately imply:

$$i \mid j \text{ implies } \mathfrak{a}_i \subseteq \mathfrak{a}_j. \tag{5'}$$

Thus by Lemma 1(b), J is finite. Now to construct the sequence (i^λ), let the i^λ be already defined for $\lambda < \ell$. If $i = i^\lambda$ with $\lambda < \ell$, then $\mathfrak{a}_i \not\subseteq \mathfrak{b}$, since otherwise (7) would be violated, and thus by (5'), $i \nmid j$ for $j \in J$. For $j \neq j' \in J$, $j \nmid j'$ holds by definition. If $J = \{j^1, \ldots, j^s\}$ for instance, then we set $i^{\ell-1+\sigma} := j^\sigma$ $(1 \leq \sigma \leq s)$ and $\ell := \ell + s$, and also $\mathcal{Y} := \mathcal{Y} \cup \{\mathfrak{b}\}$. Go to (7).

By Lemma 1(a), this algorithm must terminate. This can only happen in such a way that $\mathcal{Z}/\mathcal{Y} = \varnothing$ in (7), and thus $\mathcal{Z}$ is finite, proving (a). In (b), K is the union of all finite sets J that appear in (8) (until termination), so it is itself finite. Now let $N_i := \min\{p \in \mathbb{N} \mid \mathfrak{a}_{ip} = \mathfrak{a}_i\}$ for each $i \in I$. Then $i \mid j$ implies $\mathfrak{a}_{iN_i} = \mathfrak{a}_i \subseteq \mathfrak{a}_j = \mathfrak{a}_{jN_j}$, so again by (6), $i \mid j$ and $\mathfrak{a}_i = \mathfrak{a}_j$ imply $N_i \geq N_j$. With $N := \max\limits_{i \in K} N_i$, (c) is proved. ☐

Definition 1. Let $\mathfrak{M} \subseteq \mathfrak{R}$ be finite, with say m elements. Furthermore, define $J = J(\mathfrak{M}) := \big\{\mathrm{lcm}\,\{\partial A \mid A \in \mathfrak{G}\} \bigm| \mathfrak{G} \subseteq \mathfrak{M}\big\}$ to be the set of all possible least common multiples of degrees of elements of $\mathfrak{M}$; J is finite. Let $\mathfrak{m}_j := \left\{(\ldots, y_A, \ldots) \in \mathfrak{r}^m \;\middle|\; \sum\limits_{A \in \mathfrak{M}} f_A y_A = 0,\ y_A = 0 \text{ for } \partial A \nmid j\right\}$ and $\{(\ldots, y_A^\tau, \ldots) \mid 1 \leq \tau \leq t_j\}$ be a basis for $\mathfrak{m}_j$ (which is computable by (2)) for $j \in J$. Then the polynomials $S_j^\tau := \sum\limits_{A \in \mathfrak{M}} A\, y_A^\tau X^{j - \partial A}$ $(1 \leq \tau \leq t_j)$ are called the *S-polynomials* of $\mathfrak{M}$ of level j. Let $\mathfrak{G}_j$ be the $\mathfrak{r}$-module that is generated by them.

Definition 2. Let $\mathfrak{M} \subseteq \mathfrak{R}$ be finite and $i \in I$. For $A \in \mathfrak{M}$, let $d_A \in \mathfrak{r}$ be found such that $d_A = 0$ whenever $\partial A \nmid i$. Then the set $(i, (d_A))$ is called a *D(ifference)-expression* (*relative to* $\mathfrak{M}$), and the polynomial $D := \sum\limits_{A \in \mathfrak{M}} A\, d_A X^{i - \partial A}$ is called the *D-polynomial* of $(i, (d_A))$. For $F, G \in \mathfrak{R}$, we write $(i, (d_A)) : F \longrightarrow G$ if $F - D = G$. We write $F \longrightarrow^i G$ if there exists (d_A) such that $(i, (d_A)) : F \longrightarrow G$, and $F \longrightarrow G$ if this is the case for any $i \in I$. We will write $\longrightarrow_{\mathfrak{M}}$ if it would be otherwise unclear to which set $\mathfrak{M}$ this notation relates.

Definition 3. Let $\mathfrak{M} \subseteq \mathfrak{R}$ be finite. A sequence $\Delta = (i^\lambda, (d_A^\lambda))_{\lambda \in \mathbb{N}}$ of D-expressions is called a *D-sequence* if it is always the case that $i^{\lambda+1} \leq i^\lambda$ and $i^{\lambda+1} < i^\lambda$ for $i^\lambda \neq -1$. By Lemma 1(c), $i^\lambda = -1$ for all $\lambda \geq \ell$ for instance, and by Definition 2, $d_A^\lambda = 0$ for such λ. Thus for $F \in \mathfrak{R}$, the sequence (F_λ) with $F_0 = F$ and $(i^\lambda, (d_A^\lambda)) : F_\lambda \longrightarrow F_{\lambda+1}$ becomes stationary. If $F_\ell = G$, then we write $\Delta : F \twoheadrightarrow G$, and we write $F \twoheadrightarrow G$ if there exists such a Δ. $\partial\Delta := i^0$ is called the *degree of the D-sequence* Δ. Let $F \twoheadrightarrow^{<j} G$ be shorthand for "there is a D-sequence $\Delta : F \twoheadrightarrow G$ with $\partial\Delta < j$" (defined similarly for $\leq$). $\twoheadrightarrow_{\mathfrak{M}}$ will be written if $\mathfrak{M}$ would be otherwise ambiguous.

In what follows, let $\mathfrak{M} \subset \mathfrak{R}$ be a fixed finite subset. All terminology (such as $\mathfrak{a}_i$, $\mathfrak{B}$, $\longrightarrow$, $\twoheadrightarrow$, S_j^τ, …) is relative to this.

Lemma 3. *For $F \in \mathfrak{M}$ with $\partial F = i$, there is a $G \in \mathfrak{B}$ with $F \twoheadrightarrow^{\leqslant i} G$. The computation of G is constructive.* (It remains open whether there are several such G; see Lemma 6.)

Proof. We provide an algorithm. Let $j^\lambda := \max_{\leq} \{i \in I \mid f_i \neq \rho(f_i, \mathfrak{a}_i) \text{ or } i = -1\}$ and $F_\lambda = \sum_{i \in I} f_i X^i$ (with $F_0 = F$). If $j^\lambda = -1$, then $F_\lambda \in \mathfrak{B}$ already, and the *trivial* D-sequence ($i^\mu = -1$ and $d^\mu_A = 0$ for all $\mu \geq \lambda$ and all $A \in \mathfrak{M}$) has the required property. Now let $j = j^\lambda \neq -1$, $f_j = b$, and $\rho(f_j, \mathfrak{a}_j) = c$. We can calculate c using (1), and any solution (d^λ_A) of $\sum_{A \in \mathfrak{M},\, \partial A \mid j} f_A d^\lambda_A = b - c$ using (2). Let $d^\lambda_A = 0$ for $\partial A \nmid j$. We compute $F_{\lambda+1}$ by $(j^\lambda, (d^\lambda_A)) : F_\lambda \longrightarrow F_{\lambda+1}$, and apply the same process to $F_{\lambda+1}$. By Lemma 1(c), since the sequence of j^λ is strictly decreasing, we arrive at a $j^\ell = -1$ after finitely many steps, thus $F_\ell \in \mathfrak{B}$. □

Lemma 4/Definition 4. *Let $F \in \mathfrak{R}$ and $\partial F = i$. Then there is a $G \in \mathfrak{R}$ such that $F \twoheadrightarrow_{\mathfrak{M}} G$ and either $G = 0$ or $f_G \notin \mathfrak{a}_{\partial G}$. G can be computed and is called an $\mathfrak{M}$-remainder of F.*

Proof. A weakening of Lemma 3. □

Lemma 5. (a) *$F \twoheadrightarrow^{\leqslant i} \overline{F}$ and $G \twoheadrightarrow^{\leqslant i} \overline{G}$ imply $F + G \twoheadrightarrow^{\leqslant i} \overline{F} + \overline{G}$.*

(b) *$F \twoheadrightarrow^{\leqslant i} G$ implies $aF \twoheadrightarrow^{\leqslant i} aG$ $\quad (a \in \mathfrak{r})$.*

(c) *$F \twoheadrightarrow^{\leqslant i} G$ implies $X^j F \twoheadrightarrow^{\leqslant i+j} X^j G$ $\quad (i, j \in I,\ i \neq -1 \neq j)$.*

(d) *The same as* (a), (b), *and* (c) *with $<$ instead of $\leqslant$.*

(e) *The same as* (a), (b), *and* (c) *without the additional $\leqslant i$ and $\leqslant i + j$.*

(f) *Let $\mathfrak{A}$ be the $\mathfrak{R}$-ideal generated by $\mathfrak{M}$. Then $F \in \mathfrak{A}$ implies $F \twoheadrightarrow 0$.*

Proof. (a) Let $(i^\lambda, (c^\lambda_A))_{\lambda \in \mathbb{N}} : F \twoheadrightarrow^{\leqslant i} \overline{F}$ and $(j^\mu, (d^\mu_A))_{\mu \in \mathbb{N}} : G \twoheadrightarrow^{\leqslant i} \overline{G}$. $K = \{i^\lambda \mid \lambda \in \mathbb{N}\} \cup \{j^\mu \mid \mu \in \mathbb{N}\}$ is finite. Let $K = \{k^0, k^1, \ldots, k^\ell\}$, for instance, with $k^0 > k^1 > \cdots > k^\ell = -1$. Let $k^\nu := -1$ for $\nu > \ell$ and $e^\nu_A := \sum_\lambda c^\lambda_A\, \delta(i^\lambda, k^\nu) + \sum_\mu d^\mu_A\, \delta(j^\mu, k^\nu)$, where $\delta(\cdot, \cdot)$ denotes the Kronecker symbol. Then clearly $(k^\nu, (e^\nu_A))_{\nu \in \mathbb{N}} : F + G \twoheadrightarrow^{\leqslant i} \overline{F} + \overline{G}$. (b), (c), (d) and(e) are even simpler to prove. (f) Suppose for example $F = \sum_{A \in \mathfrak{M}} AC_A$ with $C_A \in \mathfrak{R}$. In view of $A \twoheadrightarrow 0$ for $A \in \mathfrak{M}$, we set $C_A = \sum_{i \in I} c_{Ai} X^i$ ($c_{Ai} \in \mathfrak{r}$) and apply (a), (b), (c), and (e). □

2 The Algorithm of Bruno Buchberger

The algorithm, that is the subject of our interest, consists of different transformations of an initial set of polynomials. It will be shown that the result does not depend on how we choose the sequence of transformations. Certainly, the running time is strongly dependent on this, but it appears that only a heuristic choice is known (see [1]).

Let $\mathfrak{A}$ be an ideal of $\mathfrak{R}$ and $\mathfrak{M}$ a basis for $\mathfrak{A}$. Let $\mathfrak{M}_0 := \mathfrak{M}$ and $\mathfrak{M}_{p+1}$ be formed from $\mathfrak{M}_p$ by performing the following actions:

(A) Let $G \neq 0$ be an $\mathfrak{M}_p$-remainder (Definition 4) of an S-polynomial of $\mathfrak{M}_p$ (Definition 1). Set $\mathfrak{M}_{p+1} := \mathfrak{M}_p \cup \{G\}$.

(B) Let $F \in \mathfrak{M}_p$, $\mathfrak{N} := \mathfrak{M}_p \setminus \{F\}$ and G an $\mathfrak{N}$-remainder of F. Set $\mathfrak{M}_{p+1} := \mathfrak{N} \cup \{G\}$.

(C) Let $F_1, \dots, F_s \in \mathfrak{M}_p$ be polynomials *of the same degree*, $U \in GL_s(\mathfrak{r})$ and $(G_1, \dots, G_s) = (F_1, \dots, F_s)\,U$. (The G_σ do not necessarily have the same degree.) Set

$$\mathfrak{M}_{p+1} := (\mathfrak{M}_p \setminus \{F_1, \dots, F_s\}) \cup \{G_1, \dots, G_s\}.$$

(D) $\mathfrak{M}_{p+1} := \mathfrak{M}_p \setminus \{0\}$.

Let $\mathfrak{a}_{ip} = \mathfrak{a}_i(\mathfrak{M}_p)$. Note that this double sequence satisfies the hypotheses of Lemma 2. More precisely, $\mathfrak{a}_{j,p+1} \supsetneqq \mathfrak{a}_{jp}$ certainly holds for $j = \partial G$ after completing one (A) step. It follows that after finitely many steps of (A), with (B), (C), and (D) interspersed ad libitum, (A) can no longer be executed because $\Delta : S \twoheadrightarrow_{\mathfrak{M}_p} 0$ for all S-polynomials S of $\mathfrak{M}_p$, of which there are indeed only finitely many, and which are considered as arbitrary D-sequences Δ in Lemmas 3 and 4. All D-polynomials and S-polynomials are contained in $\mathfrak{A}$, thus every set $\mathfrak{M}_p$ is a basis of $\mathfrak{A}$.

Definition 5. A basis $\mathfrak{G}$ of the ideal $\mathfrak{A} \trianglelefteq \mathfrak{R}$ is called a *Gröbner basis* (after Wolfgang Gröbner) if for all of the S-polynomials S, we have $\Delta : S \twoheadrightarrow_{\mathfrak{G}} 0$ for the D-sequence Δ chosen in Lemma 4. The algorithm just described for computing a Gröbner basis $\mathfrak{G}$ from an arbitrary basis $\mathfrak{M}$ of $\mathfrak{A}$ is called *Buchberger's algorithm.*

(It is easy to convince oneself that the theoretically unnecessary steps (B), (C), and (D) cannot be omitted in practice during computation.)

Lemma 6. *Let* $\mathfrak{G}$ *be a Gröbner basis of* $\mathfrak{A}$*, all terms* (*such as* $\mathfrak{a}_i$, $\mathfrak{B}$, $\longrightarrow$, $\twoheadrightarrow$, S_j^τ, ...) *relating to the set* $\mathfrak{G}$*. Then the following holds: Let* $F \in \mathfrak{R}$ *and* $G, \overline{G} \in \mathfrak{B}$*. Then* $F \twoheadrightarrow G$ *and* $F \twoheadrightarrow \overline{G}$ *imply* $G = \overline{G}$*.*

Proof. Let $\Delta : F \twoheadrightarrow G$ and $\overline{\Delta} : F \twoheadrightarrow \overline{G}$. If $\partial\Delta = \partial\overline{\Delta} = -1$ (Definition 3), then the statement is true since $G = F = \overline{G}$. Suppose therefore that $\max_{\le}(\partial\Delta, \partial\overline{\Delta}) = i \neq -1$ and the claim is already proved for D-sequences of smaller degree than i. First we see, without loss of generality, that $\partial\Delta = \partial\overline{\Delta}$. (Indeed if, for example, $\partial\Delta < i$ and $\Delta = (i^\lambda, (d_A^\lambda))_{\lambda\in\mathbb{N}}$, then we set $k^0 := i$, $c_A^0 := 0$ and $k^{\lambda+1} := i^\lambda$, $c_A^{\lambda+1} := d_A^\lambda$ ($\lambda \in \mathbb{N}$). With $\Gamma := (k^\mu, (c_A^\mu))_{\mu\in\mathbb{N}}$, we have $\partial\Gamma = i$ and $\Gamma : F \twoheadrightarrow G$.) Now let $(i^0, (d_A^0))$ resp. $(i^0, (\overline{d}_A^0))$ be the first D-expressions (Definition 2), i.e. $i = i^0$, from Δ resp. $\overline{\Delta}$, and say

$$(i^0, (d_A^0)) : F \longrightarrow H \qquad (i^0, (\overline{d}_A^0)) : F \longrightarrow \overline{H}. \tag{9}$$

Then by Definition

$$H \overset{<i}{\twoheadrightarrow} G \qquad \overline{H} \overset{<i}{\twoheadrightarrow} \overline{G}. \tag{10}$$

Let $j := \operatorname{lcm}\left\{\partial A \;\middle|\; A \in \mathfrak{G},\ \partial A \mid i\right\}$, in particular $j \mid i$, and let $f, g, \overline{g}, h, \overline{h}$ be the coefficients of X^i in $F, G, \overline{G}, H, \overline{H}$. Since coefficients of degree $\geq i$ will no longer be changed by (10), and since $G, \overline{G} \in \mathfrak{B}$, it follows that $g = h = \rho(f, \mathfrak{a}_i) = \overline{h} = \overline{g}$. Therefore, the polynomials $D = F - H$ and $\overline{D} = F - \overline{H}$ corresponding to (9) have the same coefficients of X^i, and hence $S = D - \overline{D}$ lies in $X^{i-j}\mathfrak{G}$ (Definition 1). Lemma 5 implies $S \twoheadrightarrow^{<i} 0$ since the S-polynomials S_j^τ at level j (that generate $\mathfrak{G}_j$ as an $\mathfrak{r}$-module) have one degree $\partial S_j^\tau < j$, and $S_j^\tau \twoheadrightarrow^{<j} 0$ by assumption on $\mathfrak{G}$. On the other hand, $H + S \twoheadrightarrow^{<i} G + 0 = G$ holds by Lemma 5. Since $H + S = \overline{H} \twoheadrightarrow_{<i} \overline{G}$, $G = \overline{G}$ by induction hypothesis. □

The result of our efforts thus far are presented as

Theorem. *Given an arbitrary basis $\mathfrak{M}$ of the ideal $\mathfrak{A} \trianglelefteq \mathfrak{R}$, we can use Buchberger's algorithm to compute a Gröbner basis $\mathfrak{G}$, which have the following equivalent properties ((13) was the definition):*

For every $F \in \mathfrak{R}$, there is exactly one $G \in \mathfrak{B}(\mathfrak{G})$ with $F \twoheadrightarrow_{\mathfrak{G}} G$. ($\mathfrak{B}(\mathfrak{G})$ is a set of representatives of $\mathfrak{R}/\mathfrak{A}$.) (11)

For all $i \in I$, $\mathfrak{a}_i(\mathfrak{A}) = \mathfrak{a}_i(\mathfrak{G})$. (So in particular, $\mathfrak{B}(\mathfrak{G}) = \mathfrak{B}(\mathfrak{A})$ is independent of $\mathfrak{G}$.) (12)

For all S-polynomials S of level j of $\mathfrak{G}$, $\Delta : S \twoheadrightarrow_{\mathfrak{G}} G$ holds with the D-sequence Δ arbitrarily chosen in Lemma 4. (13)

Proof. (11) follows from (13) by Lemma 6. Now suppose (12) were false. If $\mathfrak{a}_i(\mathfrak{A}) \supsetneqq \mathfrak{a}_i(\mathfrak{G})$, then there is an $F \in \mathfrak{A}$ with $f_F \notin \mathfrak{a}_{\partial F}(\mathfrak{G})$. Lemma 5(f) claims $F \twoheadrightarrow 0$ and Lemma 3 produces a $G \in \mathfrak{B}$, $G \neq 0$, with $F \twoheadrightarrow G$. This contradicts (11). If (12) holds, then Lemmas 3 and 4 actually produce $F \twoheadrightarrow^{<j} 0$ for all $F \in \mathfrak{A}$ with $\partial F < j$. □

Sometimes we desire a Gröbner basis determined with less arbitrariness. Thus for ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathfrak{r}$, let a set of representatives $\beta(\mathfrak{a}, \mathfrak{b}) = \{a_1, \ldots, a_s\} \subset \mathfrak{a}$ of a basis $\{a_1 + \mathfrak{b}, \ldots, a_s + \mathfrak{b}\}$ be computable from $(\mathfrak{a} + \mathfrak{b})/\mathfrak{b}$, and without loss of generality, with $\rho(a_\sigma, \mathfrak{b}) = a_\sigma$ for $\sigma = 1, \ldots, s$ and $s = 0$ if $\mathfrak{a} \leq \mathfrak{b}$. Now let $\mathfrak{A} \trianglelefteq \mathfrak{R}$ and $\mathfrak{G}$ be a Gröbner basis of $\mathfrak{A}$. Because of the uniqueness of $\mathfrak{B}$ by (12), it follows that (by using $\mathfrak{A}$, $\mathfrak{r}$, the choice of variables $X_1, \ldots, X_n$, the relation $\leq$ on I and the formation of ρ and β) we obtain a uniquely determined Gröbner basis $\mathfrak{H}$ of $\mathfrak{A}$ as follows: let K be the set designated in Lemma 2(b) applied to the *double sequence* $\mathfrak{a}_{ip} = \mathfrak{a}_i(\mathfrak{A})$, then denote the sets $\mathfrak{a}_k = \mathfrak{a}_k(\mathfrak{A})$, $\mathfrak{b}_k = \sum\limits_{k \neq j | k} \mathfrak{a}_j$ and $\beta(\mathfrak{a}_k, \mathfrak{b}_k) = \{a_{k1}, \ldots, a_{ks_k}\}$. Furthermore, $-a_{k\sigma} X^k \twoheadrightarrow_{\mathfrak{G}} A_{k\sigma} \in \mathfrak{B}$ holds for $\sigma = 1, \ldots, s_k$. Then $\mathfrak{H} = \{a_{k\sigma} X^k + A_{k\sigma} \mid k \in K, 1 \leq \sigma \leq s_k\}$ is such a Gröbner basis.

Incidentally, everything works similarly if we replace the $\mathfrak{R}$-submodule $\mathfrak{A}$ in $\mathfrak{R}^1$ by a submodule $\mathfrak{A}$ of $\mathfrak{R}^m$ for arbitrary m, except that the system of equations in (2) appears with m equations, and the mappings ρ and β corresponding to submodules of $\mathfrak{r}^m$ must be defined. One can verify this by going through the proof; easier by "idealization": We replace $\mathfrak{R}$ by $\mathfrak{R}[T_1, \ldots, T_m] = \mathfrak{R}'$, embed $\mathfrak{R}^m$ in $\mathfrak{R}'$ using $\iota : (0, \ldots, 0, 1_{(\mu)}, 0, \ldots, 0) \mapsto T_\mu$ and, instead of considering the $\mathfrak{R}$-modules generated by $F_1, \ldots, F_s$, consider the $\mathfrak{R}'$-ideal generated by $\{\iota(F_1), \ldots, \iota(F_s)\} \cup \{T_\mu T_\nu \mid 1 \leq \mu, \nu \leq m\}$. [It is clear from actual computation that the T_μ no longer appear!] Clearly the basic task from (1) is solved by Buchberger's algorithm for the ring $\mathfrak{R}$ instead of $\mathfrak{r}$. We still desire a method that solves (2) in $\mathfrak{R}$ instead of $\mathfrak{r}$, if only for aesthetic reasons.

3 Application to the Computing of Zeros

One order on I for which (3) and (4) hold is clearly the lexicographic order $\leq_\ell$. For $i, j \in \mathbb{N}^n$, $i \leq_\ell j$ holds if and only if the first non-vanishing of the numbers $j_n - i_n$, $j_{n-1} - i_{n-1}$, …, $j_1 - i_1$ is positive.

Now let $\Theta \in GL_n(\mathbb{R})$, $\Theta = (\theta_{\mu\nu})$ and $\theta_{\mu\nu} \geq 0$. Then (3) and (4) also hold for $\leq_\Theta$, defined by $i \leq_\Theta j$ if and only if $i\Theta \leq_\ell j\Theta$. (Thus the i and j are viewed as row vectors.)

In [1] the order is given by

$$\Theta_B = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

For partitioning systems of $n_1 + n_2 = n$ variables via elimination, we can use orders of this type

$$\leq_\Theta \quad \text{with} \quad \Theta = \left(\begin{array}{cc|cccc|cccc} 1 & 0 & 1 & 0 & \dots & 0 & & & & \\ 1 & 0 & 0 & 1 & \dots & 0 & & & & \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & & & 0 & \\ 1 & 0 & 0 & 0 & \dots & 1 & & & & \\ 1 & 0 & 0 & 0 & \dots & 0 & & & & \\ \hline 0 & 1 & & & & & 1 & 0 & \dots & 0 \\ 0 & 1 & & & & & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & & 0 & & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & & & & & 0 & 0 & \dots & 1 \\ 0 & 1 & & & & & 0 & 0 & \dots & 0 \end{array}\right) \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\\vdots\\1\\1\end{array}}\right\} n_1 \\ \left.\vphantom{\begin{array}{c}0\\0\\\vdots\\0\\0\end{array}}\right\} n_2 \end{array} . \tag{14}$$

Now we insert them in the

Corollary. (a) *Let $n = n_1 + n_2$ and $\leq$ be an order on I of type* (14). *Let $\mathfrak{G}$ be a Gröbner basis of the ideal $\mathfrak{A} \trianglelefteq \mathfrak{R}$ with respect to the order $\leq$. Let $\mathfrak{R}' = \mathfrak{r}[X_1, \dots, X_{n_1}]$. Then $\mathfrak{G}' := \mathfrak{G} \cap \mathfrak{R}'$ is a Gröbner basis of $\mathfrak{A}' := \mathfrak{A} \cap \mathfrak{R}'$.*

(b) *Let ϕ be the canonical monomorphism $\phi : \mathfrak{R}'/\mathfrak{A}' \xrightarrow{\sim} (\mathfrak{R}' + \mathfrak{A})/\mathfrak{A} \hookrightarrow \mathfrak{R}/\mathfrak{A}$ under the assumptions of* (a). *Then ϕ is an isomorphism if and only if $\mathfrak{a}_{i^\nu}(\mathfrak{G}) = \mathfrak{r}$* (*with i^ν defined by $X^{i^\nu} = X_\nu$*) *for $\nu > n_1$.*

(c) *If $\leq$ is the lexicographic order, $\mathfrak{R}_\nu = \mathfrak{r}[X_1, \dots, X_\nu]$* ($0 \leq \nu \leq n$), *and $\mathfrak{G}$ is a Gröbner basis of $\mathfrak{A} \trianglelefteq \mathfrak{R}$ formed using $\leq$, then $\mathfrak{G}_\nu := \mathfrak{G} \cap \mathfrak{R}_\nu$ is a Gröbner basis of $\mathfrak{A}_\nu := \mathfrak{A} \cap \mathfrak{R}_\nu$.*

(d) *Let $F_1, \dots, F_m \in \mathfrak{R}$, $\mathfrak{R}' = \mathfrak{r}[F_1, \dots, F_m]$, and $\mathfrak{A} \trianglelefteq \mathfrak{R}$. Then $\mathfrak{A}' = \mathfrak{A} \cap \mathfrak{R}'$ can be computed.*

Proof. (a) By virtue of Lemma 3, Lemma 5(f) and (11), the elements $A \in \mathfrak{G} \setminus \mathfrak{G}'$ are not used to compute the $\mathfrak{G}$-remainder of an $F \in \mathfrak{A}'$. (b) By (12), this is precisely $\mathfrak{B} \subseteq \mathfrak{R}'$. (c) is an iteration of (a). (d) goes as follows: Let $T_1, \dots, T_m$ be new indeterminates, $\widetilde{\mathfrak{R}} = \mathfrak{R}[T_1, \dots, T_m]$ and $\widetilde{\mathfrak{A}}$ be the ideal in $\widetilde{\mathfrak{R}}$ generated by $\mathfrak{A}$ and $\{T_1 - F_1, \ \dots, \ T_m - F_m\}$. Using (a), we compute $\widetilde{\mathfrak{A}} \cap \mathfrak{r}[T_1, \dots, T_m]$ and replace T_μ in the result by F_μ. □

If $\mathfrak{r}$ is a field, then we are familiar with elimination based on the successive formation of resultants. (Collins [3] based his quantifier elimination method on this.) But it does not always possess the precision expressed in Corollary (c). For general $\mathfrak{r}$, it remains to be seen how far Corollary (c) advances the finding of zeros of $\mathfrak{A}$ (thus the minimal elements of $\{\mathfrak{P} \in \operatorname{Spec} \mathfrak{R} \mid \mathfrak{P} \supseteq \mathfrak{A}\}$). Among other things, we certainly require

Lemma 7. *Let $\mathfrak{R}$ be a commutative Noetherian ring, $\mathfrak{R}' \leq \mathfrak{R}$ a subring (with the same 1). Let $\mathfrak{A} \trianglelefteq \mathfrak{R}$, $\mathfrak{A}' = \mathfrak{A} \cap \mathfrak{R}'$, $\mathfrak{A}' = \bigcap_{\tau=1}^{t} \mathfrak{B}'_\tau$ with ideals $\mathfrak{B}'_\tau \trianglelefteq \mathfrak{R}'$. Then $\mathfrak{B} := \bigcap_{\tau=1}^{t} \mathfrak{B}_\tau$ with $\mathfrak{B}_\tau := \mathfrak{B}'_\tau\mathfrak{R} + \mathfrak{A}$ is an ideal of $\mathfrak{R}$ with the property $\mathfrak{A} \subseteq \mathfrak{B} \subseteq \sqrt{\mathfrak{A}}$ (radical), thus with the same zeros as $\mathfrak{A}$.*

Proof. $\mathfrak{A} \subseteq \mathfrak{B}$ is clear since $\mathfrak{A} \subseteq \mathfrak{B}_\tau$. Now let $\mathfrak{P} \supseteq \mathfrak{A}$ be a prime ideal of $\mathfrak{R}$. Then $\mathfrak{P}' := \mathfrak{P} \cap \mathfrak{R}'$ is a prime ideal of $\mathfrak{R}'$ with $\mathfrak{P}' \supseteq \mathfrak{A}'$, thus $\mathfrak{P}' \supseteq \mathfrak{B}'_\tau$ for some τ. Then for this τ, $\mathfrak{P} \supseteq \mathfrak{B}'_\tau\mathfrak{R} + \mathfrak{A} = \mathfrak{B}_\tau$ holds, so $\mathfrak{P} \supseteq \mathfrak{B}$. ☐

Naturally, if the $\mathfrak{B}'_\sigma$ are prime, the $\mathfrak{B}_\sigma$ need not be prime in general. Practical methods, for verifying that the components $\mathfrak{B}_\sigma$ of a decomposition (found in some way) are prime, seem not to exist in this context.

Although this also applies when $\mathfrak{r}$ is a field, this special case ought to be pursued a little further. Therefore, *let $\mathfrak{r}$ be a field.* Then the gcd of two elements in the unique factorization domain $\mathfrak{R}$ can be computed using the Euclidean algorithm [8, pp. 89-90]. Furthermore, the *Principal Ideal Theorem* holds: Every ideal in $\mathfrak{R}$ of co-dimension one is divisible by a proper principal ideal [15, p. 175]. We now write $\mathfrak{A} \sim \mathfrak{B}$ whenever $\sqrt{\mathfrak{A}} = \sqrt{\mathfrak{B}}$. Let $\mathfrak{A} \trianglelefteq \mathfrak{R}$ be given by a basis $\{A_1, \ldots, A_s\}$. If $C = \gcd(A_1, \ldots, A_s)$ and we set $B_\sigma := A_\sigma / \gcd(A_\sigma, C^N)$ (N large), then we obtain a decomposition $\mathfrak{A} \sim C\mathfrak{R} \cap (B_1\mathfrak{R} + \ldots + B_s\mathfrak{R}) = \mathfrak{C} \cap \mathfrak{B}$, where C can now be further decomposed into prime factors and $\mathfrak{B}$ is an ideal of dimension smaller than $n-1$. Then instead of $\mathfrak{B}$, we decompose $\mathfrak{B}' = \mathfrak{B} \cap \mathfrak{r}[X_1, \ldots, X_{n-1}]$ (the intersection is computed using Corollary (a)) and apply the decomposition of $\mathfrak{B}'$ as in Lemma 7.

In order to obtain the prime decomposition at the conclusion of this procedure, we must first carry out *general transformations* in the style of Hermann [7]: We would have to adjoin independent variables $U_{\mu\nu}$ ($1 \leq \mu, \nu \leq n$) to the ground field $\mathfrak{r}$, replace $X_\mu = \sum_\nu U_{\mu\nu} Y_\nu$, and perform all computations in $\mathfrak{r}(U_{11}, \ldots, U_{nn})[Y_1, \ldots, Y_n]$. Instead, we can at best carry out the computation for a special $(u_{\mu\nu}) \in GL_n(\mathfrak{r})$. Anyway:

(a) We *almost always* obtain a prime decomposition. (This means the set of $(u_{\mu\nu})$ for which this isn't so, is the set of zeros of an ideal $\widetilde{\mathfrak{a}} \trianglelefteq \mathfrak{r}[U_{11}, \ldots, U_{nn}]$, $\widetilde{\mathfrak{a}} \neq \{0\}$).

(b) If the mapping ϕ appearing in Corollary (a) is to be an isomorphism, we have the problem of switching to one with fewer variables.

Incidentally, the prime decomposition of polynomials may still be a substantial numerical problem. See [16], which also indicates further literature.

4 Remarks

The choice of order $\leq$ on I has a strong influence on the number of elements of a Gröbner basis and the number of non-zero monomials in the basis polynomials. In this regard, the order used by both Buchberger [1, 2] and Schrader [11] is convenient, but is unsuitable for *elimination problems.*

Buchberger's advice to work first with S-polynomials of the smallest level is advantageous. We note that $X^{j-i}\mathfrak{G}_i \subseteq \mathfrak{G}_j$ holds for $i \mid j$, and to determine the S-polynomials of level j, we just append a set of basis representatives of the $\mathfrak{r}$-module $\mathfrak{G}_j/\mathfrak{T}_j$, where $\mathfrak{T}_j = \sum_{i|j\neq i} \sum_{k|(j-i)} X^k \mathfrak{G}_i$. (This is all taken into account in [1, 2]. How this can be made clear depends on the "linear algebra in $\mathfrak{r}$".)

The requirement that (2) be practically satisfiable severely limits the possible rings $\mathfrak{r}$. For principal ideal rings, it suffices for the gcd of two elements to be constructively representable as a linear combination. In Dedekind rings, it suffices to assume that some basic ideal theoretic problems are solvable constructively, so that (2) follows. For the ring of integers in a number field, these conditions, for example, are satisfied; compare [13], [6], [4, pp. 91-102, 144-155] for this. Completely generally, we desperately wish that not just any basis for the solution module of a homogeneous linear system of equations over the ground ring $\mathfrak{r}$ were computable, but rather one with a minimal number of elements.

One can ask at this point whether it is easy to guarantee, in nontrivial cases, that the functions ρ and β are well-defined. But by examining the proof, we see that the values of ρ and β may be dependent on the specific sets of generators given, $(a_1, \ldots, a_s)$ of $\mathfrak{a}$ and $(b_1, \ldots, b_t)$ of $\mathfrak{b}$, or even from the presentation of the elements of $\mathfrak{r}$ that appear. This does not affect the algorithm, but rather in a corresponding way the assertions of uniqueness about $\mathfrak{B}(\mathfrak{A})$ and $\mathfrak{H}$.

5 On Implementation

Since in the course of Buchberger's algorithm, the number of equations normally grows (or at least stays the same), we cannot work with (floating-point) approximations of the coefficients (given initially perhaps as rational numbers). The numerators and denominators of the coefficients grow quickly in the course of computation. It is therefore necessary to be able to compute with numbers of arbitrary size and to make the memory allocation of a coefficient dynamic. (This problem goes away of course if, for example, we take $\mathfrak{r}$ to be a finite field $\mathbb{F}_q$ or another finite ring.) Overall, the memory requirements are so large that we may need to work with peripheral memory.

In the program written for the Univac 1108 of the University of Karlsruhe, I satisfied these postulates except for the last one. Although its main aim here is speed (it is essentially written in Univac assembly language, and hence is not portable), the running times for even simple looking examples are considerable. I cannot give an estimate for this any more than I can for memory requirements.

One of the systems of equations follows, whose solutions by Matzat [10] allow us to specify the function fields and number fields with specific Galois groups. We assume that we could have solved it numerically with homotopy methods. In order to obtain the exact solution from the approximation, which is our only interest here, we would have needed even more non-trivial deliberations and computations.

The ideal $\mathfrak{A} \trianglelefteq \mathbb{Q}[W, P, Z, T, S, B]$ is generated by the polynomials

$$\begin{aligned}
F_1 &= 45P + 35S - 165B - 36\\
F_2 &= 35P + 40Z + 25T - 27S\\
F_3 &= 15W + 25PS + 30Z - 18T - 165B^2\\
F_4 &= -9W + 15PT + 20ZS\\
F_5 &= WP + 2ZT - 11B^3\\
F_6 &= 99W - 11SB + 3B^2
\end{aligned}$$

If we choose the lexicographic order with $W > P > Z > T > S > B$, then using the algorithm, we obtain a Gröbner basis of $\mathfrak{A}$ of polynomials $G_1, \ldots, G_6$, where G_σ contains only σ variables.

However, the numerators and denominators of the coefficients have magnitudes up to 10^{160}, so they will not be expressed here. G_1 is a polynomial in $\mathbb{Q}[B]$ of degree 10, that has two prime factors of degrees 2 and 8. The factor of degree 2 is

$$F_7 = B^2 + \frac{33}{50}B + \frac{2673}{10000}.$$

It factors over $\mathbb{Q}(\sqrt{-11})$, as it must have done after the derivation of the system of equations.

Since we are only interested in those zeros of $\mathfrak{A}$ that have coordinates in $\mathbb{Q}(\sqrt{-11})$, the algorithm would now be applied once more to the prime ideal $\mathfrak{P} = \mathfrak{A} + F_7\mathfrak{R}$. The result is the Gröbner basis $\{H_1, \ldots, H_6\}$ of $\mathfrak{P}$:

$$\begin{aligned}
H_1 &= W + \frac{19}{120}B + \frac{1323}{20000} \\
H_2 &= P - \frac{31}{18}B - \frac{153}{200} \\
H_3 &= Z + \frac{49}{36}B + \frac{1143}{2000} \\
H_4 &= T - \frac{37}{15}B + \frac{27}{250} \\
H_5 &= S - \frac{5}{2}B - \frac{9}{200} \\
H_6 &= F_7.
\end{aligned}$$

Thus all of the coordinates of interesting zeros are determined.

Eleven minutes were required for the computation of the G_σ, and another three minutes for the H_σ (after F_7 was known). It should be noted that a Gröbner basis for $\mathfrak{A}$ relative to the order $\leq_{\Theta_B}$ could not be computed in an hour. (The Univac 1108 requires 0.75 μsec for adding two 36-bit numbers.)

References

[1] B. Buchberger. *Ein Algorithmisches Kriterium für die Lösbarkeit eines Algebraischen Gleichungsystems* [*An Algorithmic Method for the Solvablity of a System of Algebraic Equations*]. Aeq. Math. **4** (1969): 374-383 [English translation by M. Abramson in *Gröbner Bases and Applications.* London Math. Society Lecture Note Series **251**. Cambridge, 1998, 535-545].

[2] B. Buchberger. *On Certain Bases of Polynomial Ideals.* Report No. 53 of the Institute for Mathematics of the University of Linz (Austria), May 1976. Abridged version: *Some Properties of Gröbner Bases for Polynomial Ideals.* ACM SIGSAM Bulletin **10**/4 (1976): 19-24.

[3] *G. Collins. *Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition.* Automata Theory and Formal Languages, Second GI Conference. Springer LNCS **33**, 1975, 134-183.

[4] C. Curtis, I. Reiner. *Representation Theory of Finite Groups and Associative Algebras.* Interscience, 1962.

[5] F. Drexler. *Eine Methode zur Berechnung sämtlicher Lösungen eines Polynomgleichungsystems* [*A Method for Calculating all the Solutions of a System of Polynomial Equations*]. Dissertation, Linz/Munich, 1976 [published in Numerische Mathematik **29** (1977): 45-58].

[6] W. Franz. *Elementarteilertheorie in Algebraische Körper* [*Elementary Divisor Theory of Algebraic Fields*]. Journal der Reine und Angewandte Mathematik **172** (1932): 149-161.

[7] *G. Herrman. *Die Frage der Endlich Vielen Schritten in der Theorie der Polynomideale* [*The Question of Finitely Many Steps in Polynomial Ideal Theory*]. Math. Ann. **95** (1925): 736-788 [English translation by M. Abramson in *ACM SIGSAM Bulletin* **32**/3 (1998): 8-30].

[8] J. König. *Einleitung in die Allgemeine Theorie der Algebraische Grössen* [*Introduction to the General Theory of Algebraic Quantities*]. Leipzig: B.G. Teubner, 1903.

[9] M. Lauer. *Kanonische Repräsentanten für die Restklassen nach einem Polynomideal* [*Canonical Representatives for the Residue Classes Modulo a Polynomial Ideal*]. Report No. 13 of the Computer Algebra Working Group, Kaiserslautern, 1976.

[10] B. Matzat. *Zur Konstruktion von Zahl- und Funktionenkörper mit Vorgegeben Galoisgruppe* [*On the Construction of Number Fields and Function Fields with Fixed Galois Group*]. To appear, 1978 [published in Journal der Reine und Angewandte Mathematik **349** (1984): 179-220].

[11] R. Schrader. *Zur Konstruktiven Idealtheorie.* Diplomarbeit, Universität Karlsruhe, 1976.

[12] A. Seidenberg. *Constructions in Algebra.* Trans. AMS **197** (1973): 273-313.

[13] E. Steinitz. *Rechteckige Systeme und Moduln in Algebraischen Zahlkörpern* [*Rectangular Systems and Modules in Algebraic Number Fields*] I, II. Math. Ann. **71** (1912): 328-354, **72** (1912): 297-345.

[14] F. Richman. *Constructive Aspects of Noetherian Rings.* Proc. AMS **44** (1974): 436-441.

[15] B. van der Waerden. *Algebra II*, Fifth edition. Springer, 1967.

[16] P. Wang. *Factoring Multivariate Polynomials over Algebraic Number Fields.* Mathematics of Computation **30** (1976): 324-336.

The works denoted by * contain many further pointers to the literature.