*J. Symbolic Computation* (2002) **33**, 209–220
doi:10.1006/jsco.2001.0501
Available online at http://www.idealibrary.com on IDEAL®

# Gröbner Bases in Orders of Algebraic Number Fields

DAVID ANDREW SMITH†

*15986 Arrowhead Road 102, Danville, IL 61834, U.S.A.*

We prove that any order **O** of any algebraic number field $K$ is a reduction ring. Rather than showing the axioms for a reduction ring hold, we start from scratch by well-ordering **O**, defining a division algorithm, and demonstrating how to use it in a Buchberger algorithm which computes a Gröbner basis given a finite generating set for an ideal. It is shown that our theory of Gröbner bases is equivalent to the ideal membership problem and in fact, a total of eight characterizations are given for a Gröbner basis. Additional conclusions and questions for further investigation are revealed at the end of the paper.


## 1. Introduction

In the 1960s Bruno Buchberger presented his first critical-pair-completion algorithm, now called Buchberger's algorithm. Since then Gröbner bases have become a powerful tool in computational algebra and algebraic geometry. What is not as well known is that Buchberger (1985, 1987) has also shown a way of computing Gröbner bases in the integers. This is not as trivial as it may seem. In the polynomials, for example, it is possible to separate every element into a *head* part and an *other* part, and then formulate Gröbner bases. Overcoming this difficulty, Buchberger has given a list of axioms of every ring, called a reduction ring, satisfying them, we are guaranteed that Gröbner bases can be computed using a critical-pair-completion algorithm. Since then, Stifter (1985, 1987) has generalized the notion of a reduction ring; with more freedom to formulate the theory of Gröbner bases, she was able to show reduction rings can have zero divisors and that the Gaussian integers are a reduction ring. Buchberger and Stifter also showed various hereditary properties (see later); in particular, the reduction ring property is hereditary from $R$ to $R[x_1, \ldots, x_n]$.

An alternate version of reduction rings has appeared in Madlener and Reinert (1998); however, the construction of a Gröbner basis is left as an assumption. We show that orders of algebraic number fields are reduction rings in the sense of both papers; however, to guarantee the construction of a Gröbner basis we more closely follow Buchberger and Stifter's approach. Yet we do not show their axioms hold, per se; we take a more hands on approach similar to the exposition in Adams *et al.* (1994) and Cox *et al.* (1997) for polynomial rings.

We define Gröbner bases in orders of algebraic number fields and show that computing Gröbner bases solves the ideal membership problem. We base our exposition on Buchberger's landmark proof of the Generalized Newman Lemma which can be found in Buchberger *et al.* (1983) together with Becker *et al.* (1993). Roughly, his lemma gives

†E-mail: david@mathparty.com

0747–7171/02/020209 + 12 $35.00/0 

us a way to formulate a proof that a Gröbner basis can be computed in an order of an algebraic number field, given a finite set as input.

We first describe a division algorithm, which works for any order $\mathbf{O}$ of any number field and which is based on the algorithm in Stifter's dissertation; namely, not every element can be used as a multiplier. Only algebraic integers of the form $aF_i$ where $a$ is a non-zero integer and $\{F_0, F_1, \ldots, F_{d-1}\}$ is a $\mathbf{Z}$-basis for $\mathbf{O}$, will be allowed as multipliers. So we fix a lexicographical ordering on the $\mathbf{Z}$-basis of $\mathbf{O}$ and use a well-ordering on the integers and extend these two orderings to $\mathbf{O}$. Once an ordering is given, the division algorithm we formulate is quite easy and natural. A side effect of this restriction upon the multipliers is that not every singleton will be a Gröbner basis as is the case in the integers.

We define Gröbner bases as Buchberger did for general reduction rings; specifically, a finite subset $G$ is a Gröbner basis when $\rightarrow_G$ has one of the equivalent properties in the Generalized Newman Lemma (Buchberger–Newman Lemma presented later) where $\rightarrow_G$ can roughly be thought of as one step in the division algorithm. Having a Gröbner basis $G$ of an ideal $\mathbf{Id}(G)$ is proven to be equivalent to the ideal membership problem of $\mathbf{Id}(G)$. We also define critical pairs as Buchberger and Stifter did for general reduction rings. The crucial point is that we are able to show that the $\alpha$ that satisfies $\gamma_1 \underline{\triangle}_{i,j}^{\alpha} \gamma_2$ has a certain form; and this will aid in computing Gröbner bases and in the proof of Buchberger's algorithm.

## 2. A Division Algorithm for Orders

To describe a division algorithm we fix a number field $K = \mathbf{Q}(\theta)$ where $\theta$ is an algebraic integer and $\deg(K) = d$ and an order $\mathbf{O}$ of $K$ with $\mathbf{Z}$-basis $\{F_0, F_1, \ldots, F_{d-1}\}$.

Definition. Let $<_{\mathbf{z}}$ be defined on the integers as $0 <_{\mathbf{z}} -1 <_{\mathbf{z}} 1 <_{\mathbf{z}} -2 <_{\mathbf{z}} 2 <_{\mathbf{z}} \cdots$. Then extend $<_{\mathbf{z}}$ to $\mathbf{O}$ by

$$\sum_{k=0}^{d-1} a_k F_k <_{\mathbf{o}} \sum_{k=0}^{d-1} b_k F_k \Leftrightarrow \ \exists\, i \text{ such that } a_i <_{\mathbf{z}} b_i \text{ and } \forall j > i, a_j = b_j.$$

Definition. A multiplier in $\mathbf{O}$ is any element of the form $aF_i$ where $i \in \{0, 1, \ldots, d-1\}$ and $a$ is a non-zero integer.

Given a $\gamma$ in $\mathbf{O}$ we define a reduction (a strictly antisymmetric) relation on $\mathbf{O}$ by,

$$\rightarrow_\gamma := \{(\alpha, \beta) \mid \exists \text{ a multiplier } m \text{ such that } \beta = \alpha - m\gamma \text{ and } \beta <_{\mathbf{o}} \alpha\}$$

and we write, $\alpha \rightarrow_{(m,\gamma)} \beta$ or sometimes $\alpha \rightarrow_\gamma \beta$.

To have a division algorithm capable of supporting a theory of Gröbner bases we need to have a way to compute $\alpha \rightarrow_\gamma \beta$. That is, given algebraic integers $\alpha$ and $\gamma$, we want to have a way of finding a multiplier $m$ such that $\beta = \alpha - m\gamma <_{\mathbf{o}} \alpha$. Even more specifically, given $\alpha, \gamma \in \mathbf{O}$ and $i$ we want to find a non-zero integer $a$ such that for $m = aF_i$ we have $\beta := \alpha - m\gamma <_{\mathbf{o}} \alpha$.

If there is such an $m$ then we say that $\alpha$ is reducible modulo $\gamma$ to $\beta$ by $m$. Further, if there is no $m' \in \mathbf{O}$ such that $\beta \rightarrow_{(m',\gamma)}$ for any $i$, then $\beta$ is called a normal form of $\alpha$ modulo $\gamma$. Specifically, we denote $\rightarrow_G$ to mean the $(\alpha, \beta) \in \mathbf{O} \times \mathbf{O}$ such that there exists $m$ with $\alpha \rightarrow_{(m,g)} \beta$ for some $g \in G$. Following Becker *et al.* (1993) and Buchberger (1987)

we denote $\overset{*}{\to}_G$, $\leftrightarrow_G$, and $\overset{*}{\leftrightarrow}_G$ as the reflexive-transitive closure of $\to_G$, the symmetric closure of $\to_G$, and the reflexive-transitive closure of $\leftrightarrow_G$, respectively. Buchberger (1985, 1987) discusses reduction processes on the integers using $<_{\mathbf{Z}}$. To obtain a normal form for a given $a$ modulo a given $c$ Buchberger mentions a simple iterative function which finds the multiplier.

For a division algorithm in $\mathbf{O}$, we first compute the table of products,

$$F_jF_k = s_{j,k,0}F_0 + s_{j,k,1}F_1 + \cdots + s_{j,k,d-1}F_{d-1}$$

which puts $F_jF_k$ in basis form. For a given $i$, we want to find $a \in Z$ such that $\alpha - aF_i\gamma <_{\mathbf{O}} \alpha$. Writing $\alpha = \sum_{k=0}^{d-1} a_kF_k$ and using the table to obtain integers $t_l$ with $F_i\gamma = \sum_{k=0}^{d-1} t_kF_k$, we see that we want to find an integer $a$ such that

$$\sum_{k=0}^{d-1}(a_k - at_k)F_k <_{\mathbf{O}} \sum_{k=0}^{d-1} a_kF_k.$$

Now we are led to find $a$ such that $a_{d-1} \to_{(a,t_{d-1})}$. To do this reduction in the integers, we can use Buchberger's procedure mentioned earlier. But we actually have different cases to consider. Suppose $p$ is such that $a_{p+1} = a_{p+2} = \cdots = a_{d-1} = 0$ and $a_p \neq 0$. Then to have reduction we must have $t_{p+1} = t_{p+2} = \cdots = t_{d-1} = 0$ and $t_p \neq 0$. If there is no $a$ such that $a_p \to_{(a,t_p)}$ (in the integers) then $\alpha$ is not reducible module $\gamma$ w.r.t. this $i$. If we cannot find a multiplier for any $i$ then $\alpha$ is not reducible modulo $\gamma$.

Here is an example of one possible step in the division algorithm. Let $\theta = \sqrt[3]{19}$ and $K = Q(\theta)$. Then we have an integral basis $\{1, \theta, \frac{\theta^2+\theta+1}{3}\} = \{1, F_1, F_2\}$ for $\mathbf{O} = \mathbf{Z}_K$. Reduce $\alpha = 15 - 24F_1 - 35F_2$ modulo $\gamma = -12 - 4F_1 + 8F_2$ w.r.t. $i = 1$. We first compute, $F_1F_1 = -1 - F_1 + 3F_2$, $F_1F_2 = 6 + F_2$, and $F_2F_2 = 4 + 2F_1 + F_2$. We want to find $a \in Z$ such that $\alpha - aF_1\gamma <_{\mathbf{O}} \alpha$. Writing this in basis form,

$$(15 - 52a) + (-24 + 8a)F_1 + (-35 + 4a)F_2 <_{\mathbf{O}} 15 - 24F_1 - 35F_2.$$

Thus, we are led to find $a$ such that $-35 \to_{(a,-4)}$. So we let $a = 9$ and obtain,

$$15 - 24F_1 - 35F_2 \to_{(9F_1,-12-4F_1+8F_2)} -453 + 48F_1 + F_2.$$

## 3. Gröbner Bases and Ideal Membership

If there exists $\gamma \in \mathbf{O}$ such that $\alpha \overset{*}{\to}_G \gamma$ and $\beta \overset{*}{\to}_G \gamma$, then we say $\alpha$ and $\beta$ have a common successor, denoted by $\alpha \downarrow_G \beta$. If $\gamma, \mu_1, \ldots, \mu_t \in \mathbf{O}$ with $\mu_i \prec \gamma$ for $i = 1, \ldots, t$ such that $\alpha = \mu_1 \leftrightarrow_G \mu_2 \leftrightarrow_G \cdots \leftrightarrow_G \mu_{t-1} \leftrightarrow \mu_t = \beta$, then we say $\alpha$ and $\beta$ are connected below $\gamma$, denoted by $\alpha \overset{*}{\leftrightarrow}_{\prec\gamma,G} \beta$. The proof of the following theorem can be found in Becker *et al.* (1993) and Buchberger *et al.* (1983).

THEOREM 3.1. (BUCHBERGER–NEWMAN LEMMA) *The following are equivalent properties for $\to_G$. For any $a, b, c \in \mathbf{O}$:*

- **a.** *$\to_G$ is locally confluent if ($a \to_G b$ and $a \to_G c$) $\Rightarrow b \downarrow_G c$;*
- **b.** *$\to_G$ is confluent if ($a \overset{*}{\to}_G b$ and $a \overset{*}{\to}_G c$) $\Rightarrow b \downarrow_G c$;*
- **c.** *$\to_G$ has unique normal forms if ($a \overset{*}{\to}_G b$, $a \overset{*}{\to}_G c$, and $b$ and $c$ are $\to_G$-maximal) $\Rightarrow b = c$;*
- **d.** *$\to_G$ has the Church–Rosser property if $a \overset{*}{\leftrightarrow}_G b \Rightarrow a \downarrow_G b$; and*

**e.** $\rightarrow_G$ *has the Buchberger property if* $(a \rightarrow_G b$ *and* $a \rightarrow_G c) \Rightarrow b \overset{*}{\leftrightarrow}_{\prec a,G} c$.

Definition. (Gröbner Basis) Let $G$ be a finite subset of $\mathbf{O}$. Then $G$ is called a Gröbner basis if $\rightarrow_G$ has one of the equivalent properties in the Buchberger–Newman Lemma. Moreover, a Gröbner basis $G$ is a reduced Gröbner basis when every $g \in G$ is in normal form w.r.t. $G \backslash \{g\}$.

*Elementary observations.* The converse to the Church–Rosser property always holds. If $\alpha \rightarrow_{(m,\gamma)} \beta$, then $\alpha+\delta \downarrow_\gamma \beta+\delta$, because either $\alpha+\delta \rightarrow_{(m,\gamma)} \beta+\delta$ or $\alpha+\delta \leftarrow_{(-m,\gamma)} \beta+\delta$ ($<_{\mathbf{O}}$ is linear). In particular, for non-zero $\delta$ and $\gamma$, $\delta \downarrow_\gamma \delta - m\gamma$ holds for any multiplier $m$.

Theorem 3.2. *Let $C$ be a finite subset of $\boldsymbol{O}$. Then $\overset{*}{\leftrightarrow}_C$ and $\equiv_C$ are equivalent.*

Proof. Suffiency is straightforward. Conversely, suppose $\alpha \equiv_C \beta$. Then there exists $\alpha_k \in \mathbf{O}$, and $\gamma_k \in C$ such that $\beta = \alpha + \sum_{k=1}^{t} \alpha_k \gamma_k$. Let $M$ be the set of all multipliers for $\mathbf{O}$. Then there are $m_{1,k}, \ldots, m_{l,k} \in M$ such that $\alpha_k = \sum_{i=1}^{l} m_{i,k}$. So, $\beta = \alpha + \sum_{k=1}^{t-1} \alpha_k \gamma_k + (\sum_{i=1}^{l} m_{i,t})\gamma_t$. Using $m_{1,t}, \ldots, m_{l,t}$, we apply the rule $\delta \downarrow_{\gamma_k} (\delta - m_{i,t}\gamma_k)$, $l$ times to obtain,

$$\beta \downarrow_{\gamma_t} \left( \alpha + \sum_{k=1}^{t-1} \alpha_k \gamma_k + \left( \sum_{k=1}^{l-1} m_{k,t} \right) \gamma_t \right) \downarrow_{\gamma_t} \ldots \downarrow_{\gamma_t} \left( \alpha + \sum_{k=1}^{t-1} \alpha_k \gamma_k \right).$$

Repeating this procedure $t-1$ more times (i.e. for each $\gamma_k$) we obtain,

$$\beta = \left( \alpha + \sum_{k=1}^{t-1} \alpha_k \gamma_k + \left( \sum_{k=1}^{l} m_{k,t} \right) \gamma_t \right) \downarrow_{\gamma_t} \ldots \downarrow_{\gamma_1} \alpha.$$

Applying the converse to the Church–Rosser property $t \times l$ times it follows that $\alpha \overset{*}{\leftrightarrow}_C \beta$. □

Theorem 3.3. (Ideal Membership) *Let $G$ be a finite subset of $\boldsymbol{O}$. Then the following are equivalent:*

*(i) $G$ is a Gröbner basis;*
*(ii) $\alpha \in \boldsymbol{Id}(G) \Rightarrow \alpha \overset{*}{\rightarrow}_G 0$; and*
*(iii) $0 \neq \alpha \in \boldsymbol{Id}(G) \Rightarrow \alpha$ is reducible w.r.t. $G$*

*where $\boldsymbol{Id}(G)$ denotes the ideal generated by $G$.*

Proof. Using Theorem 3.2, (i)⇒(ii) follows easily; and (ii)⇒(iii) is straightforward. (iii)⇒(i): Suppose $\beta \overset{*}{\rightarrow}_G \beta_1, \beta \overset{*}{\rightarrow}_G \beta_2, \beta_1$ and $\beta_2$ are normal forms of $\beta$ w.r.t. $G$, and $\beta_1 \neq \beta_2$. Then $\beta_1 - \beta_2 \in \mathbf{Id}(G)$ and by assumption $\beta_1 - \beta_2 \rightarrow_G \sigma = \beta_1 - \beta_2 - m\gamma$ where $\gamma \in G$. First suppose $\sigma = 0$. Then, $\beta_1 \downarrow \beta_2$ implies $\beta_1 \leftrightarrow_G \beta_2$. This contradicts that $\beta_1$ and $\beta_2$ are normal forms of $\beta$ w.r.t. $G$ with $\beta_1 \neq \beta_2$. If $\sigma \neq 0$, then it follows $\beta_1 \downarrow_G \beta_1 - m\gamma$ and $\beta_2 \downarrow_G \beta_2 - m\gamma$. Also, $(\beta - m\gamma) \downarrow_G (\beta_1 - m\gamma)$ and $(\beta - m\gamma) \downarrow_G (\beta_2 - m\gamma)$. Then,

$\beta_1 \overset{*}{\leftrightarrow}_G (\beta_1 - m\gamma) \overset{*}{\leftrightarrow}_G (\beta - mg) \overset{*}{\leftrightarrow}_G (\beta_2 - m\gamma) \overset{*}{\leftrightarrow}_G \beta_2$. So we again contradict that $\beta_1$ and $\beta_2$ are normal forms of $\beta$ w.r.t. $G$ with $\beta_1 \neq \beta_2$. Therefore, (iii) implies $\rightarrow_G$ has unique normal forms. □

## 4. Buchberger's Algorithm

Notice that in order to check whether a finite subset $G$ is a Gröbner basis one needs to check that every element $\alpha$ has, for example, a unique normal form modulo a potential $G$. Buchberger's ingenious idea is to reduce the amount of checking to a finite set of elements. As we will see, the correct definitions will be:

Definition. (Irrelative) Let $\gamma_1, \gamma_2 \in \mathbf{O}$ and suppose $m_1 = aF_i$ and $m_2 = bF_j$ are multipliers. Then $(m_1, \gamma_1)$ and $(m_2, \gamma_2)$ are called irrelative when $\gamma_1 \neq \gamma_2$ or when $\gamma_1 = \gamma_2$ and $i \neq j$.

Definition. (Non-Trival Common Reducible) Let $\gamma_1, \gamma_2 \in \mathbf{O}$ and suppose there exists an $\alpha$ in $\mathbf{O}$ such that there exist $m_1 = aF_i$ and $m_2 = bF_j$ with $\leftarrow_{(m_2,\gamma_2)} \alpha \rightarrow_{(m_1,\gamma_1)}$ and $(m_1, \gamma_1)$ and $(m_2, \gamma_2)$ are irrelative; and there does not exist $m_1'$ and $m_2'$ with $\leftarrow_{(m_2',\gamma_2)}$ $\alpha \rightarrow_{(m_1',\gamma_1)}$, $(\alpha - m_1'\gamma_1) \rightarrow_{(m_2',\gamma_2)}$ or $(\alpha - m_2'\gamma_2) \rightarrow_{(m_1',\gamma_1)}$, $(m_1', \gamma_1)$ and $(m_2', \gamma_2)$ are irrelative, and $m_1' = aF_i$ and $m_2' = bF_j$ in case $\gamma_1 = \gamma_2$. Then $\alpha$ is called a non-trivial common reducible for $\gamma_1$ and $\gamma_2$ and is denoted by $\gamma_1 \triangle_{i,j}^{\alpha} \gamma_2$. Further, if there does not exist $\alpha' <_{\mathbf{o}} \alpha$ such that $\gamma_1 \triangle_{i,j}^{\alpha'} \gamma_2$, then $\alpha$ is called the least non-trival common reducible w.r.t. $\gamma_1$ and $\gamma_2$ and denoted by $\gamma_1 \underline{\triangle}_{i,j}^{\alpha} \gamma_2$.

It is proven later that if $\gamma_1 \underline{\triangle}_{i,j}^{\alpha} \gamma_2$, then $\alpha = aF_k$ for some non-zero integer $a$ and some $k$. For now we will concentrate on computing such $a$ and $k$ and Gröbner bases. Buchberger gave the following functions for computing an $a$ such that $c_1 \underline{\triangle}^{a} c_2$ in the integers. Namely,

$$a = LCRInt(c_1, c_2) := \max_{<_{\mathbf{Z}}} \{LRInt(c_1), LRInt(c_2)\}$$

where

$$LRInt(c) := \begin{cases} \frac{|c|}{2} & \text{if } c \text{ is even} \\ -\frac{|c|+1}{2} & \text{if } c \text{ is odd.} \end{cases}$$

Using these functions and the following proof of the lemma, we can easily compute the $k$ and integer $a$ such that $\gamma_1 \underline{\triangle}_{i,j}^{aF_k} \gamma_2$ in $\mathbf{O}$. Here is an example: let $\theta = \sqrt[3]{19}$, $K = Q(\theta)$, and $\mathbf{O} = \mathbf{Z}_K$. Using the integral basis $\{1, \theta, \frac{\theta^2+\theta+1}{3}\} = \{F_0, F_1, F_2\}$, with $\gamma = 6 - 3F_1 + 12F_2$, $i = 1$, and $j = 2$, find the $aF_k$ such that $\gamma \underline{\triangle}_{1,2}^{aF_k} \gamma$. We first compute, $F_1F_1 = -1 - F_1 + 3F_2$, $F_1F_2 = 6 + F_2$, and $F_2F_2 = 4 + 2F_1 + F_2$. Then we compute $F_1\gamma = 75 + 9F_1 + 3F_2$ and $F_2\gamma = 30 + 24F_1 + 15F_2$. We see that $k$ must be 2 and $a = LCRInt(3, 15) = -8$. Therefore,

$$6 - 3F_1 + 12F_2 \underline{\triangle}_{1,2}^{-8F_2} 6 - 3F_1 + 12F_2.$$

Theorem 4.1. (Buchberger's Algorithm) *Let $C$ be a non-empty finite subset of $\boldsymbol{O}$.*

*Then the following algorithm computes a Gröbner basis for* $\boldsymbol{Id}(C)$. *Input: A finite subset* $C$ *of* $\boldsymbol{O}$. *Output: A finite subset* $G$ *such that* $\boldsymbol{Id}(G) = \boldsymbol{Id}(C)$ *and* $G$ *is a a Gröbner basis for* $\boldsymbol{Id}(G)$. *Initialize: Set* $G = C$ *and* $\Delta = \{(\gamma_1, \gamma_2, \alpha, i, j) \mid \gamma_1 \underline{\triangle}^{\alpha}_{i,j} \gamma_2,\ \gamma_1, \gamma_2 \in G\}$. *Loop: Do while* $\Delta \neq \emptyset$. *Take an element out of* $\Delta$, *say* $(\gamma_1, \gamma_2, \alpha, i, j)$. *Set* $\Delta = \Delta \backslash \{(\gamma_1, \gamma_2, \alpha, i, j)\}$ *and compute,* $\alpha \rightarrow_{(m_1,\gamma_1)} \zeta_1, \alpha \rightarrow_{(m_2,\gamma_2)} \zeta_2$ *where* $m = aF_i$, $m_2 = bF_j$, *and* $(m_1, \gamma_1)$ *and* $(m_2, \gamma_2)$ *are irrelative and compute normal forms of* $\zeta_1$ *and* $\zeta_2$ *w.r.t.* $G$, *obtaining* $\zeta_1'$ *and* $\zeta_2'$, *respectively. If* $\gamma := \zeta_1' - \zeta_2' = 0$ *then repeat loop. Otherwise, set* $G = G \cup \{\gamma\}$ *and* $\Delta = \Delta \cup \{(\gamma', \gamma, \alpha, i, j) \mid \gamma' \underline{\triangle}^{\alpha}_{i,j} \gamma,\ \gamma' \in G\}$.

Continuing with the previous example, we show one possible step in the computation of a Gröbner basis for the ideal generated by $\gamma = 6 - 3F_1 + 12F_2$. Initialize $G = \{\gamma\}$ and take out $(6 - 3F_1 + 12F_2, 6 - 3F_1 + 12F_2, -8F_2, 1, 2)$ of $\Delta$. We compute (the multipliers can be from the previous example):

$$-8F_2 \rightarrow_{(-3F_1, 6-3F_1+12F_2)} 225 + 27F_1 + F_2$$

and

$$-8F_2 \rightarrow_{(-F_2, 6-3F_1+12F_2)} 30 + 24F_2 + 7F_2.$$

Notice that $225 + 27F_1 + F_2$ is already a normal form w.r.t. $6 - 3F_1 + 12F_2$. Compute a normal form of $30 + 24F_2 + 7F_2$ w.r.t. $G$:

$$\begin{aligned} 30 + 24F_2 + 7F_2 &\rightarrow_{(-1, 6-3F_1+12F_2)} 24 + 27F_1 - 5F_2 \\ &\rightarrow_{(-2F_1, 6-3F_1+12F_2)} 174 + 45F_1 + F_2. \end{aligned}$$

Since $(225 + 27F_1 + F_2) - (174 + 45F_1 + F_2) \neq 0$ we update $G$ and $\Delta$.

The proof of Buchberger's algorithm uses the following two lemmas.

LEMMA 4.1. *If* $\gamma_1 \underline{\triangle}^{\alpha}_{i,j} \gamma_2$, *then* $\alpha = aF_k$ *for some non-zero integer* $a$ *and some* $k$.

PROOF. We are assuming there exist multipliers $m_1 = a_1 F_i$ and $m_2 = a_2 F_j$ such that $\alpha \rightarrow_{(m_1,\gamma_1)}$, $\alpha \rightarrow_{(m_2,\gamma_2)}$, and $(m_1, \gamma_1)$ and $(m_2, \gamma_2)$ are irrelative. Then we have

$$\sum_{l=0}^{d-1} (\alpha_l - a_1 t_l) F_l <_{\mathbf{o}} \alpha >_{\mathbf{o}} \sum_{l=0}^{d-1} (\alpha_l - a_2 s_l) F_l \tag{1}$$

where the $t_l$ and $s_l$ are obtained by putting $F_i\gamma_1$ and $F_j\gamma_2$ in basis form, respectively.

Case 1. Assume that $\alpha_{d-1} \neq 0$ and at least one other $\alpha_i$ is non-zero.

Subcase 1A: Assume that $a_1 t_{d-1}$ and $a_2 s_{d-1}$ are both non-zero. Then we have $\alpha_{d-1} \rightarrow_{(a_1, t_{d-1})}$ and $\alpha_{d-1} \rightarrow_{(a_2, s_{d-1})}$. Therefore, $\alpha_{d-1} F_{d-1} \rightarrow_{(m_1,\gamma_1)}$ and $\alpha_{d-1} F_{d-1} \rightarrow_{(m_2,\gamma_2)}$ and $(m_1, \gamma_1)$ and $(m_2, \gamma_2)$ are irrelative.

Now assume for a contradiction that there exist multipliers $m_1' = a_1' F_{i'}$ and $m_2' = a_2' F_{j'}$ such that

$$\leftarrow_{(m_1',\gamma_1)} \alpha_{d-1} F_{d-1} - m_2'\gamma_2 \leftarrow_{(m_2',\gamma_2)} \alpha_{d-1} F_{d-1} \rightarrow_{(m_1',\gamma_1)}$$

and $(m_1', \gamma_1)$ and $(m_2', \gamma_2)$ are irrelative (also assume $i' = i$ and $j' = j$ incase $\gamma_1 = \gamma_2$). But then,

$$\leftarrow_{(m_1',\gamma_1)} \alpha - m_2'\gamma_2 \leftarrow_{(m_2',\gamma_2)} \alpha \rightarrow_{(m_1',\gamma_1)}$$

which is a contradiction to $\gamma_1 \triangle_{i,j}^{\alpha} \gamma_2$. The case for when $\gamma_1$ and $\gamma_2$ are switched in the above three sentences is analogous. So $\gamma_1 \triangle_{i,j}^{\alpha_{d-1}F_{d-1}} \gamma_2$ and since $\alpha_{d-1}F_{d-1} <_{\mathbf{o}} \alpha$ we have a contradiction to $\gamma_1 \underline{\triangle}_{i,j}^{\alpha} \gamma_2$.

Subcase 1B: Assume in (1) that $a_1 t_{d-1}$ and $a_2 s_{d-1}$ are not both non-zero, then (1) becomes

$$\sum_{l=0}^{p} (\alpha_l - a_1 t_l) F_l <_{\mathbf{o}} \alpha >_{\mathbf{o}} \sum_{l=0}^{q} (\alpha_l - a_2 s_l) F_l$$

where the $p$ and $q$ satisfy:

$$t_{p'} = 0 \ \forall \ p' > p, \qquad t_p \neq 0, \qquad s_{q'} = 0 \ \forall \ q' > q, \qquad \text{and} \qquad s_q \neq 0.$$

If we have $p < q$, then

$$(\alpha_p F_p \rightarrow_{(m_1,\gamma_1)} \qquad \text{and} \qquad sF_p = 0) \Rightarrow \alpha - m_2\gamma_2 \rightarrow_{(m_1,\gamma_1)}.$$

If we have $q < p$, then

$$(\alpha_q F_q \rightarrow_{(m_2,\gamma_2)} \qquad \text{and} \qquad tF_q = 0) \Rightarrow \alpha - m_1\gamma_1 \rightarrow_{(m_2,\gamma_2)}.$$

Both of these cases contradict $\gamma_1 \triangle_{i,j}^{\alpha} \gamma_2$. Therefore $p = q$. But a contradiction for this case is easily achieved as in subcase 1A. All subcases considered, it follows that if $\alpha_{d-1}$ is non-zero then all other $\alpha_i$ must be zero.

Case 2. Suppose $\alpha_{d-1} = 0$, $\alpha_{d-2}$ is non-zero and at least one of the other $\alpha_i$ is non-zero besides $\alpha_{d-2}$ . Then (1) becomes

$$\sum_{l=0}^{d-2} (\alpha_l - a_1 t_l) F_l <_{\mathbf{o}} \alpha >_{\mathbf{o}} \sum_{l=0}^{d-2} (\alpha_l - a_2 s_l) F_l.$$

Now apply case 1 with $d-1$ replaced by $d-2$, obtaining the conclusion that, if $\alpha_{d-2}$ is non-zero then all other $\alpha_i$ are zero.

Continue this argument until the last step, where we reach the conclusion that if $\alpha_2$ and $\alpha_1$ are both non-zero and all other $\alpha_i$ are zero, then we have a contradiction. So finally, we conclude that if any two of the $\alpha_i$ are non-zero then we get a contradiction, which implies that exactly one of the $\alpha_i$ is non-zero. □

LEMMA 4.2. *Let $G$ be a finite subset of $\boldsymbol{O}$ and suppose that for any $\gamma_1, \gamma_2 \in G$ and $\alpha'$ such that $\gamma_1 \underline{\triangle}_{i,j}^{\alpha'} \gamma_2$ there exists $n_1 = a'F_i$ and $n_2 = b'F_j$ such that $\alpha' \rightarrow_{(n_1,\gamma_1)}$, $\alpha' \rightarrow_{(n_2,\gamma_2)}$, $\alpha' - n_1\gamma_1 \overset{*}{\leftrightarrow}_{<_{\boldsymbol{o}}\alpha',G} \alpha' - n_2\gamma_2$, and $(n_1,\gamma_1)$ and $(n_2,\gamma_2)$. Then for any $\alpha$ in $\boldsymbol{O}$ with $\gamma_1 \triangle_{i,j}^{\alpha} \gamma_2$, there exists $m_1 = aF_i$ and $m_2 = bF_j$ such that $\alpha \rightarrow_{(m_1,\gamma_1)}$, $\alpha \rightarrow_{(m_2,\gamma_2)}$, $(\alpha - m_1\gamma_1) \overset{*}{\leftrightarrow}_{<_{\boldsymbol{o}}\alpha,G} (\alpha - m_2\gamma_2)$, and $(m_1,\gamma_1)$ and $(m_2,\gamma_2)$ are irrelative.*

PROOF. Suppose $\gamma_1 \triangle^{\alpha} \gamma_2$. Since $<_{\mathbf{o}}$ is a well-order there must exist $\alpha' \leq \alpha$ such that $\gamma_1 \underline{\triangle}_{i,j}^{\alpha'} \gamma_2$. By assumption, there exist multipliers $n_1$ and $n_2$ such that $\alpha' \rightarrow_{(n_1,\gamma_1)} \zeta_1$, $\alpha' \rightarrow_{(n_2,\gamma_2)} \zeta_2$, $\zeta_1 \overset{*}{\leftrightarrow}_{<_{\mathbf{o}}\alpha',G} \zeta_2$, and $(n_1,\gamma_1)$ and $(n_2,\gamma_2)$ are irrelative. Thus, there exist $\mu_1, \ldots, \mu_t$ in $\mathbf{O}$ and $\gamma_1, \ldots, \gamma_{t-1}$ in $G$ such that $\mu_1, \ldots, \mu_t <_{\mathbf{o}} \alpha'$ and

$$\alpha' - n_1\gamma_1 = \mu_1 \leftrightarrow_{\gamma_1} \mu_2 \leftrightarrow_{\gamma_2} \cdots \leftrightarrow_{\gamma_{t-2}} \mu_{t-1} \leftrightarrow_{\gamma_{t-1}} \mu_t = \alpha' - n_2\gamma_2. \tag{2}$$

Case 1. Suppose $\alpha' = sF_k$ and that $\alpha'$ and $\alpha$ have the same sign in the $k$th component. We know that (2) implies

$$\alpha - n_1\gamma_1 = \mu + \mu_1 \downarrow_{\gamma_1} \mu + \mu_2 \downarrow_{\gamma_2} \cdots \downarrow_{\gamma_{t-2}} \mu + \mu_{t-1} \downarrow_{\gamma_{t-1}} \mu + \mu_t = \alpha - n_2\gamma_2,$$

with $\mu = \alpha - \alpha'$. From the converse to the Church–Rosser property we have

$$\alpha - n_1\gamma_1 = \mu + \mu_1 \overset{*}{\leftrightarrow}_{\gamma_1} \mu + \mu_2 \overset{*}{\leftrightarrow}_{\gamma_2} \overset{*}{\leftrightarrow}_{\gamma_{t-2}} \mu + \mu_{t-1} \overset{*}{\leftrightarrow}_{\gamma_{t-1}} \mu + \mu_t = \alpha - n_2\gamma_2.$$

In this case it suffices to take $m_1 = n_1$ and $m_2 = n_2$, because if $\alpha'$ and $\alpha$ have the same sign in the $k$th component then $\alpha' + (-\alpha' + \mu_i) = \mu_i <_{\mathbf{o}} \alpha'$ implies $\mu + \mu_i = \alpha + (-\alpha' + \mu_i) <_{\mathbf{o}} \alpha$. Using $m_1 = n_1$, we have $\zeta_2 \rightarrow_{(m_2,\gamma_2)} \alpha \rightarrow_{(m_1,\gamma_1)} \zeta_1$, $\zeta_1 \overset{*}{\leftrightarrow}_{<_{\mathbf{o}}\alpha',G} \zeta_2$, and $(m_1, \gamma_1)$ and $(m_2, \gamma_2)$ are irrelative.

Case 2. Suppose $\alpha'$ and $\alpha$ have different signs in the $k$th component. Multiplying (2) through by $-1$, using $\mu = \alpha + \alpha'$, and the converse to the Church–Rosser property, it follows that

$$\alpha + n_1\gamma_1 = \mu - \mu_1 \overset{*}{\leftrightarrow}_{\gamma_1} \mu - \mu_2 \overset{*}{\leftrightarrow}_{\gamma_2} \overset{*}{\leftrightarrow}_{\gamma_{t-2}} \mu - \mu_{t-1} \overset{*}{\leftrightarrow}_{\gamma_{t-1}} \mu - \mu_t = \alpha + n_2\gamma_2.$$

Letting $m_1 = -n_1$ and $m_2 = -n_2$ suffices because if $\alpha'$ and $\alpha$ have different signs in the $k$th component then $\alpha' + (-\alpha' + \mu_i) = \mu_i <_{\mathbf{o}} \alpha'$ implies $\mu - \mu_i = \alpha - (-\alpha' + \mu_i) <_{\mathbf{o}} \alpha$. □

Notice that in the proof, if $n_1 = aF_i$ and $n_2 = bF_j$ then $m_1 = \pm aF_i$ and $m_2 = \pm bF_j$. This is important for the next theorem.

THEOREM 4.2. (GRÖBNER BASIS CRITERION) *Let $G$ be a finite subset of $\boldsymbol{O}$. Then $G$ is a Gröbner basis if and only if for any $\gamma_1, \gamma_2 \in G$ and $\alpha$ such that $\gamma_1 \underline{\triangle}^{\alpha}_{i,j} \gamma_2$ there exists multipliers $m_1 = aF_i$ and $m_2 = bF_j$ such that $\alpha \rightarrow_{(m_1,\gamma_1)}$, $\alpha \rightarrow_{(m_2,\gamma_2)}$, $(\alpha - m_1\gamma_1) \overset{*}{\leftrightarrow}_{<_o\alpha,G} (\alpha - m_2\gamma_2)$, and $(m_1, \gamma_1)$ and $(m_2, \gamma_2)$ are irrelative.*

PROOF. Sufficiency is trivial by considering the definitions of Buchberger's property and $\gamma_1 \underline{\triangle}^{\alpha}_{i,j} \gamma_2$.

To show necessity suppose $\alpha \rightarrow_{(n_1,\gamma_1)} \zeta_1$ and $\alpha \rightarrow_{(n_2,\gamma_2)} \zeta_2$ for $\gamma_1, \gamma_2 \in G$, $n_1 = aF_i$, $n_2 = bF_j$, and $\alpha \in \mathbf{O}$. In all the subcases that follow it will be shown that $\zeta_1 \overset{*}{\leftrightarrow}_{<_{\mathbf{o}}\alpha,G} \zeta_2$.

Case 1. Suppose $\gamma_1 = \gamma_2 := \gamma$.

Subcase 1.1: Suppose $i = j$. If $\zeta_1 = \zeta_2$ then done. Otherwise, either $\zeta_1 <_{\mathbf{o}} \zeta_2$ or conversely. If the latter holds then $\alpha \rightarrow_{(n_1,\gamma_1)} \zeta_1 \rightarrow_{(n_1-n_2,\gamma_1)} \zeta_2$ follows and so $\zeta_1 \overset{*}{\leftrightarrow}_{<_{\mathbf{o}}\alpha,G} \zeta_2$. Similarly for $\zeta_1 <_{\mathbf{o}} \zeta_2$.

Subcase 1.2: Suppose there exists $n_1', n_2'$ such that $n_1' = a'F_i$, $n_2' = b'F_j$ and

$$_{(n_1',\gamma)} \leftarrow \alpha - n_2'\gamma \; _{(n_2',\gamma)} \leftarrow \alpha \rightarrow_{(n_1',\gamma)}. \tag{3}$$

Then $\alpha - n_1'\gamma - n_2'\gamma \downarrow_{\gamma} \alpha - n_2'\gamma$ and $\alpha - n_1'\gamma \downarrow_{\gamma} \alpha - n_1'\gamma - n_2'\gamma$; so it follows that, $\alpha - n_1'\gamma \overset{*}{\leftrightarrow}_{\prec\alpha,\gamma} \alpha - n_2'\gamma$. By subcase 1.1, and $\alpha \rightarrow_{(n_1,\gamma)} \zeta_1$, it follows that $\zeta_1 \overset{*}{\leftrightarrow}_{\prec\alpha,\gamma} \alpha - n_1'\gamma$. Similarily, $\zeta_2 \overset{*}{\leftrightarrow}_{\prec\alpha,\gamma} \alpha - n_2'\gamma$. Whence, $\zeta_1 \overset{*}{\leftrightarrow}_{\prec\alpha,\gamma} \zeta_2$.

Subcase 1.3: Suppose there exists $n_1', n_2'$ such that $\alpha \rightarrow_{(n_1',\gamma)}$, $\alpha \rightarrow_{(n_2',\gamma)}$, $\alpha - n_1'\gamma \rightarrow_{(n_2',\gamma)}$, $n_1' = aF_i$, and $n_2' = bF_j$. Analogous to subcase 1.2.

Subcase 1.4: Suppose subcases 1.1, 1.2, and 1.3 do not hold. Then $\gamma \triangle^{\alpha}_{i,j} \gamma$. Now

Lemma 4.2 holds, so there exists multipliers $m_1 = aF_i$ and $m_2 = bF_j$ such that $\alpha \rightarrow_{(m_1,\gamma)} \zeta_1'$ and $\alpha \rightarrow_{(m_2,\gamma)} \zeta_2'$, $\zeta_1' \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_2'$, and $(m_1,\gamma)$ and $(m_2,\gamma)$ are irrelative. Moreover, by the remark after Lemma 4.2, $(m_1,\gamma)$ and $(n_1,\gamma)$ are not irrelative and $(m_2,\gamma)$ and $(n_2,\gamma)$ are not irrelative. Suppose $\zeta_1 <_{\mathbf{O}} \zeta_1'$ and $\zeta_2 <_{\mathbf{O}} \zeta_2'$. Applying the reasoning in subcase 1.1, $\zeta_1' \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_1$ and $\zeta_2' \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_2$. For the other subcases we also obtain $\zeta_1' \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_1$ and $\zeta_2' \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_2$. Therefore, $\zeta_1 \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_2$.

Case 2. Suppose $\gamma_1 \neq \gamma_2$.

Subcase 2.1: Suppose there exists $n_1', n_2'$ such that $\alpha \rightarrow_{(n_1',\gamma_1)}$, $\alpha \rightarrow_{(n_2',\gamma_2)}$, $\alpha - n_1'\gamma_1 \rightarrow_{(n_2',\gamma_2)}$. Analogous to subcase 1.2.

Subcase 2.1: Suppose there exists $n_1', n_2'$ such that $\alpha \rightarrow_{(n_1',\gamma_1)}$, $\alpha \rightarrow_{(n_2',\gamma_2)}$, $\alpha - n_2'\gamma_2 \rightarrow_{(n_1',\gamma_1)}$. Analogous to subcase 1.2.

Subcase 2.3: Suppose none of the above cases hold. Then $\gamma_1 \triangle_{i,j}^{\alpha} \gamma_2$. Again Lemma 4.2 holds, so there exist multipliers $m_1 = aF_i$ and $m_2 = bF_j$ such that $\alpha \rightarrow_{(m_1,\gamma_1)} \zeta_1'$ and $\alpha \rightarrow_{(m_2,\gamma_2)} \zeta_2'$, $\zeta_1' \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_2'$, and $(m_1,\gamma_1)$ and $(m_2,\gamma_2)$ are irrelative. Finally by case 1, $\zeta_1' \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_2$ and $\zeta_1 \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_2'$. Whence, $\zeta_1 \overset{*}{\leftrightarrow}_{<_{\mathbf{O}}\alpha,G} \zeta_2$. □

Proof. (Of Buchberger's Algorithm) The correctness of the algorithm follows exactly as in Buchberger (1985, 1987). Termination: Define $Red(G) = \{\alpha \in \mathbf{O} \mid \alpha \rightarrow_G\}$. It also follows from Buchberger (1985, 1987) that the algorithm, if it does not terminate, gives rise to the following strictly ascending chain of subsets:

$$Red(G_0) \subset Red(G_1) \subset \cdots \subset Red(G_k) \subset Red(G_{k+1}) \subset \cdots$$

which is impossible: note that $Red(\gamma)$ has a finite complement for any $\gamma$ (and hence so does $Red(G)$ for any finite subset $G$). Whence, the above strictly ascending chain leads to the strictly descending chain of finite sets $Red(G_1)' \supset Red(G_2)' \supset \cdots$ which is impossible. □

## 5. Further Conclusions and Applications

*Hereditary properties.* As noted above, Stifter (1985, 1987) generalized the notion of a reduction ring and showed that the reduction ring property is hereditary from $R$ to $R[\underline{X}]$ where $\underline{X} = \{x_1, \ldots, x_n\}$. Moreover, Stifter (1991) was able to show that the reduction property is hereditary from $R$ to $R^m$ where $R^m$ is the ring defined using (componentwise) the operations from $R$; and also[†] to $R/I$ where $I$ is an ideal in $R$. Hence one can compute Gröbner bases in the rings:

$$\mathbf{O}, \mathbf{O}^m, \mathbf{O}/I, \mathbf{O}[\underline{X}], \mathbf{O}^m[\underline{X}], \qquad \text{and} \qquad (\mathbf{O}/I)[\underline{X}].$$

In a different direction, one can easily show how to compute Gröbner bases in $\mathbf{O}$ as a module over a subring which contains the integers and show how to solve the submodule membership problem. Simply move the multipliers. For example, suppose $K = \mathbf{Q}(\alpha)$ is a given algebraic number field with $\theta = \sqrt[3]{19}$, $\mathbf{O} = \mathbf{Z}_K$, and $S = \mathbf{Z}[\theta]$. Then $\mathbf{O} \neq S$ and one can choose the multipliers as $a\theta^i$ where $a$ is a non-zero integer and

[†]Assuming that the well-founded partial ordering on $R$ is actually a well-order and that $R/I$ has a finite number of zero divisors. Both assumptions hold for orders of algebraic number fields.

$i \in \{0, 1, \ldots, deg(K) - 1\}$. One could simply follow the above three sections in detail and construct a theory of Gröbner bases in these (non-trivial) modules. Further, in this way, we can compute Gröbner bases in any free finitely generated Abelian group.

One could also compute Gröbner bases in $\mathbf{O}[\underline{X}]^m$ as an $\mathbf{O}[\underline{X}]$-module, or even as a $\mathbf{O}$-module by simply following Adams *et al.* (1994) and adapting the theory to the case for $\mathbf{O}$ instead of a field.

Apparently, one can construct Gröbner bases in $R[\underline{X}]$ as a $R[\underline{U}]$-module where $\underline{U} \subseteq \underline{X}$ and $R$ is a field or any order of an algebraic number field. Simply move the multipliers; that is, only let monomials in $\underline{U}$ be multipliers. Of course one has to modify the $S$-polynomial, but this is easily achieved.

Finally, take any reduction domain $R$ with $R$-basis $\{b_1, \ldots, b_n\}$. Construct a theory of Gröbner bases for $Rb_1 \oplus \cdots \oplus Rb_n$.

*Ideal algorithms.* The following algorithms for $R[\underline{X}]$ can be found in one or more of Adams *et al.* (1994), Becker *et al.* (1993) and Cox *et al.* (1997) where $R$ is a field or a PID. We note that the proofs carry over to $\mathbf{O}[\underline{X}]$ (recall $\mathbf{O}$ is not necessarily a PID) and we make the important observation that the algorithms also hold for the coefficient ring $\mathbf{O}$. That is to say, we can compute the ideal intersection, quotient, saturation, and the Chinese Remainder theorem in $\mathbf{O}$ by computing Gröbner bases in $\mathbf{O}[\underline{X}]$. In the following theorem when $\underline{X} = \emptyset$ we simply mean $\mathbf{O}[\underline{X}] = \mathbf{O}$.

THEOREM 5.1. *Let $\prec_T$ be a term order on $T(\underline{X})$ that is an elimination order on $\underline{U} \subseteq \underline{X}$.*

- **a.** [*Elimination*] *If $G$ is a Gröbner basis of $I$ in $\boldsymbol{O}[\underline{X}]$, then $G \cap \boldsymbol{O}[\underline{U}]$ is a Gröbner basis of $I_{\underline{U}}$ in $\boldsymbol{O}[\underline{U}]$.*
- **b.** [*Intersection*] *Let $I_1, \ldots, I_m \lhd \boldsymbol{O}[\underline{X}]$, and let $J = \boldsymbol{Id}(\{1 - \sum_{i=1}^m y_i\} \cup \bigcup_{i=1}^m y_i I_i)$ in $\boldsymbol{O}[\underline{X}, \underline{Y}]$, where $y_1, \ldots, y_m$ are indeterminates not in $\underline{X}$. Then, $\cap_{i=1}^m I_i = J_{\underline{X}}$.*
- **c.** [*Quotient*] *To compute a basis for the ideal quotient $I : J$ where $I = \boldsymbol{Id}(f_1, \ldots, f_s)$ and $J = \boldsymbol{Id}(g_1, \ldots, g_t)$, first compute a basis of $\boldsymbol{Id}(f_1, \ldots, f_s) \cap \boldsymbol{Id}(g_i)$ for each $i = 1, \ldots, t$ obtaining say $\{h_{1,i}, \ldots, h_{u,i}\}$. Then divide each $h_{i,j}$ by $g_i$ obtaining $\{\frac{h_{1,i}}{g_i}, \ldots, \frac{h_{u,i}}{g_i}\}$ a basis of $I : \boldsymbol{Id}(g_i)$ for each $i$. Then $J = \boldsymbol{Id}(g_1, \ldots, g_t) = \sum_{i=1}^t \boldsymbol{Id}(g_i)$ and $I : J = I : \sum_{i=1}^t \boldsymbol{Id}(g_i) = \bigcap_{i=1}^t I : \boldsymbol{Id}(g_i)$.*
- **d.** [*Saturation*] *Let $I = \boldsymbol{Id}(f_1, \ldots, f_m)$ in $\boldsymbol{O}[\underline{X}], 0 \neq f \in \boldsymbol{O}[\underline{X}]$, and let $J = \boldsymbol{Id}(I, 1 - yf)$ in $\boldsymbol{O}[\underline{X}, y]$. Then, $I : f^\infty := \bigcup_{i=1}^\infty I : f^i = J_{\underline{X}}$. Moreover, let $J_{\underline{X}}$ have basis $\{g_1, \ldots, g_m\}$ where each $g_i$ has the form $h_i(1 - yf) + \sum_{j=1}^k h_{ij} f_j$ where $1 \leq i \leq m$ and $h_i, h_{i,j} \in \boldsymbol{O}[\underline{X}, y]$. Then $s := max\{deg(h_{ij}) \mid 1 \leq i \leq m, 1 \leq j \leq k\}$ has the property $I : f^s = I : f^\infty$.*
- **e.** [*Chinese Remainder Theorem*] *Given $f_i \in \boldsymbol{O}[\underline{X}]$ and ideals $I_i$ in $\boldsymbol{O}[\underline{X}]$, for $1 \leq i \leq m$, let $\prec_T$ be a term order on $T(\underline{X})$ that is also an elimination order on $\underline{X} \subseteq \underline{X} \cup \underline{Y}$ where $\underline{Y} = \{y_1, \ldots, y_m\}$ are indeterminates not in $\underline{X}$. Also let $G$ be a Gröbner basis of $J = \boldsymbol{Id}(\{1 - \sum_{i=1}^m y_i\} \cup \bigcup_{i=1}^m y_i I_i)$ w.r.t. $\prec_T$ in $\boldsymbol{O}[\underline{X}, \underline{Y}]$, $\boldsymbol{f} = (f_1, \ldots, f_m)$, and finally let $h$ be the unique normal form of $f^* = \sum_{i=1}^m y_i f_i$ modulo $G$. Then the following are equivalent: (i) $A_{\boldsymbol{f}} = \bigcap_{i=1}^m (f_i + I_i) \neq \emptyset$, (ii) $h \in \boldsymbol{O}[\underline{X}]$, and (iii) $h \in A_{\boldsymbol{f}}$. Moreover, the following hold: (iv) $A_{\boldsymbol{f}} = h + \bigcap_{i=1}^m I_i$, (v) $h$ is the least element in $A_{\boldsymbol{f}}$ w.r.t. $\prec_T$ and $\ll_o$, (vi) $g \in A_{\boldsymbol{f}} \Leftrightarrow h$ is the normal form of $g$ modulo $G \cap \boldsymbol{O}[\underline{X}]$.*

*Primary decomposition.* In fact, because we have shown that $\mathbf{O}$ is a reduction ring,

Rutman (1992) has shown how to compute primary decompositions for submodules in $\mathbf{O}[x_1, \ldots, x_n]^m$ as an $\mathbf{O}[x_1, \ldots, x_n]$-module.

We will outline how to compute the primary decomposition for a given ideal $I$ in $\mathbf{Z}_K[x_1, \ldots, x_n] = \mathbf{Z}_K[\underline{X}]$.

The basic idea is that prime factorization of ideals in the maximal order is well-understood and so one can rely on Kalkbrener (1998) to lift the unique factorization algorithm in $\mathbf{Z}_K$ to a primary decomposition algorithm in $\mathbf{Z}_K[\underline{X}]$. In Cohen (1995, 2000) there are algorithms, namely Algorithms 2.4.4, 4.8.17, and 6.2.9 in Cohen (1995) and Algorithm 2.3.22 in Cohen (2000) which compute the unique factorization for an ideal $I$ in $\mathbf{Z}_K$. These algorithms have been implemented in Pari. Here is the main idea: let $\mathbf{N} = \prod_{i=1}^{s} p_i^{a_i}$ be the unique factorization, in the integers, of the norm of $I$, (i.e. the cardinality of the finite ring $\mathbf{Z}_K/I$), let $p_i\mathbf{Z}_K = \prod_{j=1}^{t} P_{ij}$ be unique factorizations, for $1 \leq i \leq s$, and let $v_{P_{ij}}(I)$ be the valuation of $I$ at $P_{ij}$. Then, $I = \prod_{ij} P_{ij}^{v_{P_{ij}}(I)}$ is the unique factorization. Notice that this is actually a reduced primary decomposition of $I$. To see this, reindex the $P_{ij}$ to get $P_k$, where $1 \leq k \leq \ s + t$, and notice that $rad(Q_k := P_k^{v_{P_k}(I)}) = P_k$. Since a power of a maximal ideal $P$ is $P$-primary and since the $Q_k$ are pairwise comaximal (because the $P_k$ are, see Zariski *et al.*, 1958), we have the reduced primary decomposition:

$$I = Q_1 \cap Q_2 \cap \cdots \cap Q_{s+t}.$$

In Kalkbrener (1998), a system of representations, in any Nötherian commutative ring with identity $R$, is defined. The usefulness of systems of representations is based on Kalkbrener's algorithm lifting theorem. For a well-motivated and constructive proof as well as the directions for computing a primary decomposition from a system of representations in $\mathbf{Z}_K[x_1, \ldots, x_n]$ (see Kalkbrener, 1998). Note that since we can compute Gröbner bases for the elimination, intersection, quotient, and saturation ideals in both $\mathbf{Z}_K$ and $\mathbf{Z}_K[x_1, \ldots, x_n]$ and since unique factorization computes the radical of an ideal as well as a primary decomposition of an ideal, the assumptions of Kalkbrener's algorithm lifting theorem hold for $\mathbf{Z}_K$.

## 6. Questions

(1) [Orderings] In the earlier theory, we used the orderings $<_{\mathbf{Z}}$ and $<_{\mathbf{O}}$. To see what properties of these orderings we used consult Lemma 4.1 and Theorem 4.2. The question is what other orderings can be used? Obviously, some other lexicographical ordering on the **Z**-basis could be used and Buchberger (1985, 1987) has considered other orderings on the integers. Which other orderings are possible?

(2) [Improvements] The Buchberger algorithm given previously is quite generic, so what improvements can be made? Moreover, what role does coefficient explosion play in, say, $\mathbf{O}[x_1, \ldots, x_n]$? Our division algorithm is *different* than the algorithm in Adams *et al.* (1994). More specifically, the coefficients play a *different* role in reduction, for example, see Adams *et al.* (1994, p. 203) and compare with the division algorithm given earlier for $\mathbf{O}[x_1, \ldots, x_n]$.

(3) [Integral-Basis] Can a theory of Gröbner bases be developed which solves the subring membership problem for subrings of orders which contain the integers (i.e. SAGBI-bases)? If so, if we consider an order in which a **Z**-basis is not known as a subring of an

order in which a **Z**-basis is known (i.e. cyclotomic orders), then can computing Gröbner bases for subrings lead to an algorithm for finding a **Z**-basis for the order in question?

(4) [Primary Decomposition] Can the theory of Gröbner bases for orders be used to give an algorithm for primary decomposition of ideals in (not necessarily maximal) orders? If so, we can use Kalkbrener's theorem again to extend such a decomposition to polynomial rings over orders? Rutman's theory shows how to compute primary decomposition for $\mathbf{O}[x_1, \ldots, x_n]^m$ as an $\mathbf{O}[x_1, \ldots, x_n]$-module. Can we give a primary decomposition algorithm for submodules in $\mathbf{O}[x_1, \ldots, x_n]^m$ as an **O**-module? Can these primary decomposition algorithms (for both the ideal and submodule case) be realized under just one general algorithm?

(5) [Relative Extensions] Let $L$ be an algebraic number field extension of $K$. If we know that $\mathbf{Z}_L$ is a free $\mathbf{Z}_K$-module and if we have a $\mathbf{Z}_K$-basis, in fact Cohen (2000) shows how to compute one, then can we construct a theory of Gröbner bases in terms of the arithmetic of the relative extension, thus repeating the conclusions of this paper as well as questions (1)–(4)?

## Acknowledgements

I would like to thank Drs B. Buchberger, W. Adams, T. Luo, and S. Smith for their support of reduction rings, this paper, my future, and my present, respectively, as well as the referees for their valuable comments.

## References

Adams, W., Loustaunau, P. (1994). *An Introduction to Gröbner Bases*, Providence, RI, American Mathematical Society.

Becker, T., Weispfenning, V. (1993). *Gröbner Bases*, New York, Springer.

Buchberger, B., Winkler, F. (1983). A criterion for eliminating unnecessary reductions in the Knuth–Bendix algorithm. *Algebra, Comb. Logic Comput. Sci.*, **42**, 849–869.

Buchberger, B. (1985). A critical-pair completion algorithm for finitely generated ideals in rings. In *Extended Version: RISC-Linz Series RISC-83-21.0*, University of Linz.

Buchberger, B. (1987). A critical-pair/completion algorithm in reduction rings. In Borger, E., Hasenjager, G., Rodding, D. eds, *Proceedings of Logic and Machines: Decision Problems and Complexity*, volume 171 of LNCS, pp. 137–161. New York, Springer.

Cohen, H. (1995). *A Course in Computational Algebraic Number Theory*, New York, Springer.

Cohen, H. (2000). *Advanced Topics in Computational Algebraic Number Theory*, New York, Springer.

Cox, D., Little, J., O'Shea, D. (1997). *Ideals, Varieties, and Algorithms*, New York, Springer.

Kalkbrener, M. (1998). Algorithmic properties of polynomial rings. *J. Symb. Comput.*, **26**, 525–581.

Madlener, K., Reinert, B. (1998). *Gröbner bases in non-commutative reduction rings. Gröbner Bases and Applications (Proc. of the 33 years of Gröbner Bases Conference)*. Volume 251 of the *London Mathematical Society Lecture Notes Series*, pp. 408–420. Cambridge, U.K., Cambridge University Press.

Rutman, E. (1992). Gröbner bases and primary decomposition of modules. *J. Symb. Comput.*, **14**, 483–503.

Stifter, S. (1985). Gröbner bases over the integers and in general reduction rings. Diploma Thesis. RISC-series RISC-85-28.0, University of Linz.

Stifter, S. (1987). A generalization of reduction rings. *J. Symb. Comput.*, **3**, 351–364.

Stifter, S. (1991). The reduction ring property is hereditary. *J. Algebra*, **140**, 399–414.

Stifter, S. (1993). Gröbner bases of modules over reduction rings. *J. Algebra*, **159**, 54–63.

Zariski, O., Samuel, P. (1958). *Commutative Algebra*, Princeton, NJ, D. Van Nostrand.

*Received 13 February 2001*
*Accepted 29 August 2001*