Dynamical Gröbner bases over Dedekind rings

Amina Hadj Kacem ([1]), Ihsen Yengui ([2])

April 7, 2010

Abstract

In this paper, we extend the notion of "dynamical Gröbner bases" introduced by the second author to Dedekind rings (with zero divisors). As an application, we dynamically solve the ideal membership problem and compute a generating set for the syzygy module over multivariate polynomial rings with coefficients in Dedekind rings. We also give a partial positive answer to a conjecture about Gröbner rings.

Key words : Gröbner basis, dynamical Gröbner basis, ideal membership problem, principal rings, Dedekind rings, Gröbner rings, constructive mathematics.

Introduction

First, let us say a few words about constructive algebra. Constructive algebra can be seen as an abstract version of computer algebra. In computer algebra, one attempts to construct efficient algorithms for solving "concrete problems given in an algebraic formulation". A problem is "concrete" if its hypotheses and conclusion have a computational content.

Constructive algebra can be understood as a first "preprocessing" step for computer algebra that leads to the discovery of general algorithms, even if they are not efficient. Moreover, in constructive algebra, one tries to give general algorithms for solving virtually "any" theorem of abstract algebra. Therefore, a first task in constructive algebra is often to define the computational content hidden in hypotheses that are formulated in a very abstract way. For example, what is a good constructive definition of a local ring, a valuation ring, an arithmetical ring, a ring of Krull dimension ≤ 2, and so on? A good constructive definition must be equivalent to the usual definition given in classical mathematics; it must have a computational content, and it must be satisfied by the usual objects (of usual mathematics) that satisfy the abstract definition.

Let us consider the classical theorem that states "any polynomial P in $\mathbf{K}[X]$ is a product of irreducible polynomials ($\mathbf{K}$ a field)". This leads to an interesting problem. It seems like no general algorithm could give the solution to this theorem. What, then, is the constructive content of this theorem? A possible answer is as follows: when performing computations with P, proceed as if its decomposition is known in irreducibles. At the beginning, proceed as if P were irreducible. If something strange appears (the gcd of P and another polynomial Q is a strict divisor of P), use this fact to improve the decomposition of P.

This trick was invented in computer algebra as the D5-philosophy [10, 12, 22]. Following this computational trick, one is able to compute inside the algebraic closure $\widetilde{\mathbf{K}}$ of $\mathbf{K}$ even if it is not possible to "construct" $\widetilde{\mathbf{K}}$.

The foregoing has been referred to as the "dynamical evaluation" (of the algebraic closure). Because the method for computing Gröbner bases introduced by the second author in [30] is directly inspired by this trick, these bases were named "dynamical Gröbner bases".

[1] Department of Mathematics, Faculty of Sciences of Sfax, 3000 Sfax, TUNISIA.
[2] Department of Mathematics, Faculty of Sciences of Sfax, 3000 Sfax, TUNISIA, email: ihsen.yengui@fss.rnu.tn.

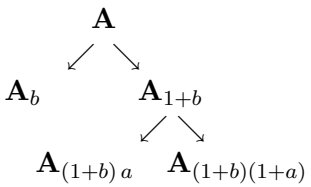
From a logical point of view, the "dynamical evaluation" gives a constructive substitute for two highly nonconstructive tools of abstract algebra: the Third Excluded Middle and Zorn's Lemma. These tools are required in order to "construct" complete prime factorization of ideals in Dedekind rings: the dynamical evaluation allows the fully computational content of this "construction" to be found. The paper [8] is an excellent reference regarding the foundations of dynamical methods in algebra.

The constructive rewriting of "abstract local-global principles" is very important. In classical proofs using this kind of principle, the argument is "let us see what happens after localization at an arbitrary prime ideal of $\mathbf{R}$". From a computational point of view, prime ideals are overly abstract objects, particularly if one wishes to deal with a general commutative ring. In the constructive rereading, the argument is "let us see what happens when the ring is a residually discrete local ring", i.e., if $\forall x$, $(x \in \mathbf{R}^\times \text{ or } \forall y\,(1+xy) \in \mathbf{R}^\times)$. If a constructive proof is obtained in this particular case, the process can be completed by "dynamically evaluating an arbitrary ring $\mathbf{R}$ as a residually discrete local ring". For example, in this paper, Dedekind rings will behave dynamically as valuation rings.

This paper can be thought as a continuation of [30]. In order to avoid repetition, it is assumed that the reader has a copy of [30] in hand. The notion of "dynamical Gröbner bases" introduced in [30] for principal rings is extended to Dedekind rings with zero divisors. It is worth pointing out that dynamical Gröbner bases represent a new alternative for computation with multivariate polynomials over Noetherian rings. Contrary to the methods that have been proposed, which suggest that for Noetherian rings the analog of Gröbner bases over fields should be computed, (see for example [1, 4, 21, 23, 29]), a dynamical substitute is proposed. Instead of a Gröbner basis describing the situation globally, use a finite number of Gröbner bases, not over the base ring, but over comaximal localizations of this ring. At each localization, the computation behaves as if a valuation ring were present. In a word, it is somewhat like Serre's method in "Corps locaux" [27] but follows the lazy fashion of computer algebra [2, 8, 10, 12, 13, 30, 31, 32]. Borrowing words from [23], the difference between our approach and classical approaches is well illustrated by the following example: a Gröbner basis of the ideal $\langle 2X_1,\, 3X_2\rangle$ in $\mathbb{Z}[X_1, X_2]$ is $\{2X_1,\, 3X_2\}$ according to Trinks [29], $\{2X_1,\, 3X_2,\, X_1X_2\}$ according to Buchberger [4], and $\{(\mathbb{Z}[\frac{1}{2}, X_1, X_2], \{X_1,\, 3X_2\}),\, (\mathbb{Z}[\frac{1}{3}, X_1, X_2], \{2X_1,\, X_2\})\}$ for us.

An essential property of a Dedekind domain is that its integral closure in a finite algebraic extension of its quotient field remains a Dedekind domain. This property is difficult to capture from an algorithmic point of view if one requires complete prime factorization of ideals (see [20]). Besides, even if such factorization is possible in theory, one rapidly encounters impracticable methods that involve huge complexities such as factorizing the discriminant. In [5], Buchmann and Lenstra proposed to compute inside rings of integers without using a $\mathbb{Z}$-basis. An important algorithmic fact is that it is always easier to obtain partial factorization for a family of natural integers, i.e., a decomposition of each of these integers into a product of factors picked in a family of pairwise coprime integers (see [3, 2]). This is the strategy adopted when computing dynamical Gröbner bases. The use of dynamical Gröbner bases provides a way to overcome such difficulties.

Another feature of the use of dynamical Gröbner bases is that it enables one to easily resolve the delicate problem caused by the appearance of zero divisors as leading coefficients (see [6]). Cai and Kapur concluded their paper [6] by mentioning the open question of how to generalize Buchbergers's algorithm for Boolean rings (see also [16], in which Boolean rings are used to model prepositional calculus). As a typical example of a problematical situation, Cai and Kapur used the case where the base ring is $\mathbf{A} = (\mathbb{Z}/2\mathbb{Z})[a, b]$ with $a^2 = a$ and $b^2 = b$. In that case, the method they proposed does not work due to the fact that an annihilator of $ab+a+b+1 \in \mathbf{A}$ can be either a or b; thus, there may exist non-comparable multi-annihilators for an element in $\mathbf{A}$. Dynamical Gröbner bases allow one to fairly overcome this difficulty. As a matter of fact, in this specific case, a computation of a dynamical Gröbner base made up of three Gröbner bases on localizations of $\mathbf{A}$ will be conducted. For $x \in \mathbf{A}$, denoting $\mathbf{A}_x := \mathbf{A}[\frac{1}{x}]$, this can be represented by the following binary tree:



Of course, at each leaf of the tree above, the problem Cai and Kapur pointed disappears completely. Thus, by systematizing the dynamical construction above, it is directly shown that dynamical Gröbner bases could be a satisfactory solution to this open problem.

It is true that all the examples given in this paper are over $\mathbb{Z}/n\mathbb{Z}$ or over rings of integers having a $\mathbb{Z}$-basis and that such problems can be treated directly in most software systems such as `MAGMA` [19] and `SINGULAR` [28] without using a dynamical approach. Dynamical Gröbner bases are potentially more appropriate for dealing with Dedekind rings, which are intractable to this type of computer algebra software. However, the computations are restricted to small, simple examples because all of the work must be done by hand. For lack of an implementation of dynamical Gröbner bases, a practical comparison with other methods is impossible. A serious analysis of improvements to the dynamical method proposed is therefore outside the scope of this paper. No doubt, almost all the improvements that have been made in cases where the base ring is a field will prove to be easily adaptable to the dynamical context. Our goal is simply to introduce the main lines of the computation of dynamical Gröbner bases over Dedekind rings, with the hope that in the future dynamical Gröbner bases will be implemented in one of the available computer algebra systems. Of course, in such cases, one must take into account the considerable number of optimizations that have been made in recent years for the purpose of speeding up Buchberger's algorithm in cases where the base ring is a field (the faster version was given in [14]). The interested reader can refer to [15] for a modern introduction to this subject.

The computation of syzygies (that is, relations between the generators of a module) and the submodule membership problem are central to homological algebra and represent the two principal tools required for the resolution of linear systems over rings. The first is used for testing particular solutions and the second for solving the homogeneous associated system. These two major problems have been chosen to illustrate our dynamical computation with multivariate polynomials over Dedekind rings. The resolution of a finitely-generated module is nothing but the computation of iterated syzygies of its presentation matrix. It is worth mentioning that in the examples given in this paper are restricted to the computation of the first syzygy because the computation is done by hand, as explained above. The method used for the computation of syzygies over multivariate polynomials with coefficients in a field@ is not the optimal one. As a matter of fact, the algorithms implemented in computer algebra systems that compute such syzygies (`SINGULAR` for example) are largely inspired by Schreyer's original proof [25, 26]. Moreover, by performing reductions between the generators, one can obtain a more balanced presentation of the syzygy module. Here, it is emphasized that the classical approach can be adapted to the dynamical setting; thorough optimization of the approach remains to be done.

Another important issue raised in the present work is the "*Gröbner Ring Conjecture*" [30] stating that a valuation ring is Gröbner if and only if its Krull dimension is ≤ 1. Recall that according to [30] a ring $\mathbf{R}$ is said to be *Gröbner* if for each $n \in \mathbb{N}$ and each finitely-generated ideal I of $\mathbf{R}[X_1, \ldots, X_n]$, fixing a monomial order on $\mathbf{R}[X_1, \ldots, X_n]$, the ideal $\{\mathrm{LT}(f), f \in I\}$ of $\mathbf{R}[X_1, \ldots, X_n]$ formed by the leading terms of the elements of I is finitely-generated. It is proven that a Gröbner valuation ring must have Krull dimension ≤ 1, giving a partial positive answer to this conjecture.

All rings considered are unitary and commutative. The undefined terminology is standard, as in [9] and [20].

1 Dynamical Gröbner bases over Dedekind rings

Constructive definitions of arithmetical rings and Dedekind rings are needed.

Definition 1 (Constructive definition of arithmetical rings and Dedekind rings [11])

(*i*) S is said to be a *multiplicative subset* of a ring $\mathbf{R}$ if

$$S \subseteq \mathbf{R}, 1 \in S \text{ and } \forall\, x, y \in S,\ xy \in S.$$

For $x_1, \ldots, x_r \in \mathbf{R}$, $\mathcal{M}(x_1, \ldots, x_r)$ will denote the multiplicative subset of $\mathbf{R}$ generated by $x_1, \ldots, x_r$, that is,

$$\mathcal{M}(x_1, \ldots, x_r) = \{x_1^{n_1} \cdots x_r^{n_r}, n_i \in \mathbb{N}\}.$$

Such a multiplicative subset is said to be finitely-generated. If S is a multiplicative subset of a ring $\mathbf{R}$, the localization of $\mathbf{R}$ at S is the ring $S^{-1}\mathbf{R} = \{\frac{x}{s}, x \in \mathbf{R}, s \in S\}$ in which the elements of S are forced into being invertible. Note that we do not suppose that $0 \notin S$ and thus the ring $S^{-1}\mathbf{R}$ may be trivial ($1 = 0$). Trivial rings are too important to be disregarded [24, 31]

If $x \in \mathbf{R}$, the localization of $\mathbf{R}$ at the multiplicative subset $\mathcal{M}(x)$ will be denoted by $\mathbf{R}_x$. Moreover, by induction, for each $x_1, \ldots, x_k \in \mathbf{R}$, it is defined that $\mathbf{R}_{x_1.x_2.....x_k} := (\mathbf{R}_{x_1.x_2.....x_{k-1}})_{x_k}$.

If $S_1, \ldots, S_k$ are multiplicative subsets of $\mathbf{R}$, we say that $S_1, \ldots, S_k$ are *comaximal* if

$$\forall s_1 \in S_1, \ldots, s_n \in S_n,\ \exists\, a_1, \ldots, a_n \in \mathbf{R} \ \mid\ \sum_{i=1}^{n} a_i s_i = 1.$$

(*ii*) A ring $\mathbf{R}$ (not necessarily integral) is said to be arithmetical if, for any $x_1, x_2 \in \mathbf{R}$, there exist $u, v, w \in \mathbf{R}$ such that:

$$\begin{cases} ux_2 = vx_1 \\ wx_2 = (1-u)x_1. \end{cases}$$

Thus, x_1 divides x_2 in the ring $\mathbf{R}_u$, x_2 divides x_1 in the ring $\mathbf{R}_{1-u}$, and the multiplicative subsets $\mathcal{M}(u)$ and $\mathcal{M}(1-u)$ are obviously comaximal. This is not surprising, because we know that if we localize an arithmetical ring at a prime ideal, we find a valuation ring. An arithmetical domain is called a Prüfer domain.

(*iii*) A ring $\mathbf{R}$ is said to be a Dedekind ring if it is arithmetical, strongly discrete (we have an algorithm for the ideal membership problem) and Noetherian (any ascending chain of finitely generated ideals pauses).

1.1 How to construct a dynamical Gröbner basis over a Dedekind ring ?

Let $\mathbf{R}$ be a Dedekind ring, $I = \langle f_1, \ldots, f_s \rangle$ a nonzero finitely-generated ideal of $\mathbf{R}[X_1, \ldots, X_n]$, and fix a monomial order $>$ on $\mathbf{R}[X_1, \ldots, X_n]$ (throughout this paper by monomial order we mean a global ordering [15]). The purpose is to construct a dynamical Gröbner basis G for I.

Dynamical version of Buchberger's Algorithm

This algorithm is analogous to the dynamical version of Buchberger's Algorithm over principal rings given in [30]. The details of this analogy are described herein. For Noetherian valuation rings, the algorithm works similarly to Buchberger's Algorithm. The only difference occurs when it must handle two incomparable (under division) elements a, b in $\mathbf{R}$. In this situation, one should first compute $u, v, w \in \mathbf{R}$ such that

$$\begin{cases} ub = va \\ wb = (1-u)a. \end{cases}$$

Now, one opens two branches: the computations are pursued in $\mathbf{R}_u$ and $\mathbf{R}_{1+u\mathbf{R}} := \{\frac{x}{y}, x \in \mathbf{R} \text{ and } \exists\, z \in \mathbf{R} \mid y = 1+zu\}$. At each new branch, if $S = \overline{S(f,g)}^{G'} \neq 0$ where G' is the current Gröbner basis, then

S must be added to G'. This algorithm must terminate after a finite number of steps. Indeed, if it does not terminate, this is due to the coefficient and not to the monomials because $\mathbb{N}^n$ is well ordered (see Dickson's Lemma [9], page 69). That is, the dynamical version of Buchberger's Algorithm would produce infinitely many polynomials g_i with the same multidegree, such that $\langle \mathrm{LC}(g_1)\rangle \subset \langle \mathrm{LC}(g_2)\rangle \subset \langle \mathrm{LC}(g_2)\rangle \subset \cdots$; this is in contradiction to the fact that a Dedekind ring is Noetherian.

Note that contrary to [30], we use the localization $\mathbf{R}_{1+u\mathbf{R}}$ instead of $\mathbf{R}_{1-u}$ in order to avoid redundancies. To see this, let us take as an example $\mathbf{R} = \mathbb{Z}$ and $u = 4$. In the ring $\mathbb{Z}_{1+4\mathbb{Z}}$, all the integers that are coprime to 4 become units (for instance $15 \in \mathbb{Z}_{1+4\mathbb{Z}}^{\times}$), while in the ring $\mathbb{Z}_3$, only the $\pm 3^k$ ($k \in \mathbb{Z}$) become units ($15 \notin \mathbb{Z}_3^{\times}$).

• Dynamical division algorithm (the dynamical analogue of the division algorithm in the case of a Noetherian valuation ring): suppose that one is required to divide a term $aX^{\alpha} = \mathrm{LT}(f)$ by another term $bX^{\beta} = \mathrm{LT}(g)$ with X^{β} divides X^{α} (note that this is only possible when X^{β} divides X^{α} and b divides a, as in the classical approach).

In the ring $\mathbf{R}_{1+u\mathbf{R}}$: $f = \frac{w}{1-u}\frac{X^{\alpha}}{X^{\beta}}g + r$ ($\mathrm{mdeg}(r) < \mathrm{mdeg}(f)$) and the division is pursued with f replaced by r.

In the ring $\mathbf{R}_u$: $\mathrm{LT}, (f)$ is not divisible by $\mathrm{LT}(g)$ and thus $f = \overline{f}^{\{g\}}$.

• Dynamical computation of the S-pairs: suppose that one wishes to compute $S(f, g)$ with $\mathrm{LT}(f) = aX^{\alpha}$ and $\mathrm{LT}(g) = bX^{\beta}$. Denote $\gamma = (\gamma_1, \ldots, \gamma_n)$, with $\gamma_i = \max(\alpha_i, \beta_i)$ for each i.

In the ring $\mathbf{R}_{1+u\mathbf{R}}$: $S(f, g) = \frac{X^{\gamma}}{X^{\alpha}}f - \frac{w}{1-u}\frac{X^{\gamma}}{X^{\beta}}g$.

In the ring $\mathbf{R}_u$: $S(f, g) = \frac{v}{u}\frac{X^{\gamma}}{X^{\alpha}}f - \frac{X^{\gamma}}{X^{\beta}}g$.

2 The ideal membership problem over Dedekind rings

Definition 2 Let $\mathbf{R}$ be a ring, $f, g \in \mathbf{R}[X_1, \ldots, X_n]\backslash\{0\}$, $I = \langle f_1, \ldots, f_s\rangle$ a nonzero, finitely-generated ideal of $\mathbf{R}[X_1, \ldots, X_n]$, and $>$ a monomial order on $\mathbf{R}[X_1, \ldots, X_n]$.

1) For $g_1, \ldots, g_t \in \mathbf{R}[X_1, \ldots, X_n]$, $G = \{g_1, \ldots, g_t\}$ is said to be a *special Gröbner basis* for I if $I = \langle g_1, \ldots, g_t\rangle$, the set $\{\mathrm{LC}(g_1), \ldots, \mathrm{LC}(g_t)\}$ is totally ordered under division and for each $i \neq j$, $\overline{S(g_i, g_j)}^{G} = 0$.

   Note that when $\mathbf{R}$ is a field, this definition coincides with the classical definition of Gröbner bases [9, 15]. Also, where $\mathbf{R}$ is a valuation ring, we retrieve the definition given in [30].

2) A set $G = \{(S_1, G_1), \ldots, (S_k, G_k)\}$ is said to be a *dynamical Gröbner basis* for I if $S_1, \ldots, S_k$ are finitely-generated comaximal multiplicative subsets of $\mathbf{R}$ and in each localization $(S_i^{-1}\mathbf{R})[X_1, \ldots, X_n]$, G_i is a special Gröbner basis for $\langle f_1, \ldots, f_s\rangle$.

The following proposition is similar to Proposition 12 of [30].

Proposition 3 *Let $\mathbf{R}$ be a Dedekind ring, $I = \langle f_1 \ldots, f_s\rangle$ be a nonzero finitely-generated ideal of $\mathbf{R}[X_1, \ldots, X_n]$, $f \in \mathbf{R}[X_1, \ldots, X_n]$ and fix a monomial order on $\mathbf{R}[X_1, \ldots, X_n]$. Suppose that $G = \{g_1, \ldots, g_t\}$ is a special Gröbner basis for I in $\mathbf{R}[X_1, \ldots, X_n]$. Then, $f \in I$ if and only if $\overline{f}^{G} = 0$.*

Proof Of course, if $\overline{f}^{G} = 0$, then $f \in \langle g_1, \ldots, g_t\rangle = I$. For the converse, suppose that $f \in I$ and that the remainder r of f on division by G in $\mathbf{R}[X_1, \ldots, X_n]$ is nonzero. This means that $\mathrm{LT}(r)$ is not divisible by any of $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t)$.
Observe that G is also a Gröbner basis for $\langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}_{\mathfrak{p}}[X_1, \ldots, X_n]$ for each prime ideal $\mathfrak{p}$ of $\mathbf{R}$. Let $\mathfrak{p}$ be any prime ideal of $\mathbf{R}$. Because G is also a Gröbner basis for $\langle f_1, \ldots, f_s\rangle$ in $\mathbf{R}_{\mathfrak{p}}[X_1, \ldots, X_n]$, $\mathrm{LM}(r)$ is divisible by at least one of $\mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_t)$, but for each g_i such that $\mathrm{LM}(g_i)$ divides $\mathrm{LM}(r)$, $\mathrm{LC}(g_i)$ does not divide $\mathrm{LM}(r)$. Let $g_{i_1}, \ldots, g_{i_k}$ be such polynomials and suppose that

$\mathrm{LC}(g_{i_1})/\mathrm{LC}(g_{i_2})/\cdots/\mathrm{LC}(g_{i_k})$ (we can make this hypothesis by definition of a special Gröbner basis). Because the base ring is a Dedekind ring, we can write $\langle \mathrm{LC}(g_{i_1})\rangle = \mathfrak{p}_1^{\alpha_1}\cdots\mathfrak{p}_\ell^{\alpha_\ell}$ and $\langle \mathrm{LC}(r)\rangle = \mathfrak{p}_1^{\beta_1}\cdots\mathfrak{p}_\ell^{\beta_\ell}$, where the p_i are distinct prime ideals of $\mathbf{R}$, and $\alpha_i, \beta_i \in \mathbb{N}$. Necessarily, there exists $1 \leq i_0 \leq \ell$ such that $\alpha_{i_0} > \beta_{i_0}$. But this would imply that the problem persists in the ring $\mathbf{R}_{\mathfrak{p}_{i_0}}[X_1,\ldots,X_n]$, in contradiction to the fact that G is a Gröbner basis for $\langle f_1,\ldots,f_s\rangle$ in $\mathbf{R}_{\mathfrak{p}_{i_0}}[X_1,\ldots,X_n]$. □

Theorem 4 (Dynamical gluing) *Let $\mathbf{R}$ be a Dedekind ring, $I = \langle f_1,\ldots,f_s\rangle$ be a nonzero finitely generated ideal of $\mathbf{R}[X_1,\ldots,X_n]$, $f \in \mathbf{R}[X_1,\ldots,X_n]$ and fix a monomial order on $\mathbf{R}[X_1,\ldots,X_n]$. Suppose that $G = \{(S_1,G_1),\ldots,(S_k,G_k)\}$ is a dynamical Gröbner basis for I in $\mathbf{R}[X_1,\ldots,X_n]$. Then, $f \in I$ if and only if $\overline{f}^{G_i} = 0$ in $(S_i^{-1}\mathbf{R})[X_1,\ldots,X_n]$ for each $1 \leq i \leq k$.*

Proof The proof is identical to the proof of Theorem 13 in [30]. □

3 Application to the Syzygy module

3.1 Syzygy modules over valuation rings

The following theorem gives a generating set for syzygies of monomials with coefficients in a valuation ring. It is a generalization of Proposition 8 ([9], page 104) to valuation rings.

Theorem 5 (Syzygy-generating set of monomials over valuation rings)
Let $\mathbf{V}$ be a valuation ring, $c_1,\ldots,c_s \in \mathbf{V}\setminus\{0\}$, and $M_1,\ldots,M_s$ be monomials in $\mathbf{V}[X_1,\ldots,X_n]$. Denoting $LCM(M_i,M_j)$ by $M_{i,j}$, the syzygy module $\mathrm{Syz}(c_1M_1,\ldots,c_sM_s)$ *is generated by:*

$$\{S_{ij} \in \mathbf{V}[X_1,\ldots,X_n]^s \mid 1 \leq i < j \leq s\},$$

where

$$S_{ij} = \begin{cases} \frac{M_{i,j}}{M_i}e_i - \frac{c_i}{c_j}\frac{M_{i,j}}{M_j}e_j & \text{if } c_j \mid c_i \\ \frac{c_j}{c_i}\frac{M_{i,j}}{M_i}e_i - \frac{M_{i,j}}{M_j}e_j & \text{else.} \end{cases}$$

Here, $(e_1,\ldots,e_s)$ is the canonical basis of $\mathbf{V}[X_1,\ldots,X_n]^{s\times 1}$.

Proof One has only to slightly modify the original proof in case $\mathbf{V}$ is a field [9].

□

Notation 6 Let $\mathbf{V}$ be a valuation ring, $>$ a monomial order, $f_1,\ldots,f_s \in \mathbf{V}[X_1,\ldots,X_n]\setminus\{0\}$, and $\{g_1,\ldots,g_t\}$ a Gröbner basis for $\langle f_1,\ldots,f_s\rangle$. Let $c_i = LC(g_i)$, and $M_i = LM(g_i)$. In order to determine the syzygy module $\mathrm{Syz}(f_1,\ldots,f_s)$, we will first compute $\mathrm{Syz}(g_1,...,g_t)$. Recall that for each $1 \leq i < j \leq t$, the S-polynomial of g_i and g_j is given by:

$$S(g_i,g_j) = \begin{cases} \frac{M_{ij}}{M_i}g_i - \frac{c_i}{c_j}\frac{M_{ij}}{M_j}g_j & \text{if } c_j \mid c_i \\ \frac{c_j}{c_i}\frac{M_{ij}}{M_i}g_i - \frac{M_{ij}}{M_j}g_j & \text{else.} \end{cases}$$

For some $h_{ijk} \in \mathbf{V}[X_1,...,X_n]$, we have

$$S(g_i,g_j) = \sum_{k=1}^{t} g_k h_{ijk} \text{ with } \mathrm{mdeg}(S(g_i,g_j)) = max_{1\leq k\leq t}\mathrm{mdeg}(g_k h_{ijk}) \ (\star).$$

(The polynomials h_{ijk} are given by the division algorithm.)
Let:

$$\epsilon_{ij} = \begin{cases} \frac{M_{ij}}{M_i}e_i - \frac{c_i}{c_j}\frac{M_{ij}}{M_j}e_j & \text{if } c_j \mid c_i \\ \frac{c_j}{c_i}\frac{M_{ij}}{M_i}e_i - \frac{M_{ij}}{M_j}e_j & \text{else.} \end{cases}$$

And

$$s_{ij} = \epsilon_{ij} - \sum_{k=1}^{t} e_k h_{ijk}.$$

Theorem 7 *(Syzygy module of a Gröbner basis over a valuation ring) With the previous notations,*

$$\mathrm{Syz}(g_1,\dots,g_t)=\langle s_{ij}\mid 1\leq i<j\leq t\rangle.$$

Proof One has only to slightly modify the original proof in case $\mathbf{V}$ is a field [9].

□

Denoting by $F=[f_1\cdots f_s]$ and $G=[g_1\cdots g_t]$, there exist two matrices, S and T, respectively of size $t\times s$ and $s\times t$ such that $F=GS$ and $G=FT$. We can first compute a generating set $\{s_1,\dots,s_r\}$ for $\mathrm{Syz}(G)$. For each $i\in\{1,\dots,r\}$, we have $0=Gs_i=(FT)s_i=F(Ts_i)$; therefore, $\langle Ts_i\mid\ i\in\{1,\dots,r\}\rangle\subseteq\mathrm{Syz}(F)$. Also, denoting by $\mathbf{I}_s$ the identity matrix of size $s\times s$, we have

$$F(\mathbf{I}_s-TS)=F-FTS=F-GS=F-F=0.$$

This equality shows that the columns $r_1,\dots,r_s$ of $\mathbf{I}_s-TS$ are also in $\mathrm{Syz}(F)$. The converse holds, as stated by the following theorem, the proof of which is identical to that in the case in which the base ring is a field [9].

Theorem 8 *(Syzygy computation over valuation rings: general case) With the previous notations, we have*

$$\mathrm{Syz}(f_1,\dots,f_s)=\langle Ts_1,\dots,Ts_r,r_1,\dots,r_s\rangle.$$

Example 9 Let $f_1=2XY, f_2=3Y^3+3, f_3=X^2-3X\in\mathbf{V}[X,Y]=(\mathbb{Z}/4\mathbb{Z})[X,Y]$, and $F=[f_1\ f_2\ f_3]$. Computing a Gröbner basis for $\langle f_1,f_2,f_3\rangle$ using the lexicographic order with $X>Y$ as monomial order, we obtain:

$S(f_1,f_2)=Y^2f_1-2Xf_2=2X=:f_4$,

$S(f_1,f_3)=Xf_1-2Yf_3=2XY\xrightarrow{f_1}0$,

$S(f_2,f_3)=X^2f_2-3Y^3f_3=3X^2+XY^3\xrightarrow{f_3}X+XY^3\xrightarrow{f_2}0$,

$f_1\xrightarrow{f_4}0$, $S(f_2,f_4)=2Xf_2-Y^3f_4=2X\xrightarrow{f_4}0$,

$S(f_3,f_4)=2f_3-Xf_4=2X\xrightarrow{f_4}0$.

Thus, $\{f_2,f_3,f_4\}$ is a Gröbner basis for $\langle f_1,f_2,f_3\rangle$ in $\mathbf{V}[X,Y]$. Denoting by $G=[f_2\ f_3\ f_4]$, we have $G=FT$ with $T=\begin{pmatrix}0&0&Y^2\\1&0&-2X\\0&1&0\end{pmatrix}$ and $F=GS$ with $S=\begin{pmatrix}0&1&0\\0&0&1\\Y&0&0\end{pmatrix}$.

Computing $s_{ij}=\epsilon_{ij}-\sum_{k=1}^{t}e_kh_{ijk}$ for all $i<j$, we obtain:

$$s_{12}=(X^2-3X,-3Y^3-3,0),s_{13}=(2X,0,-Y^3-1),s_{23}=(0,2,-X-1).$$

And so

$$Ts_{12}=\begin{pmatrix}0\\X^2-3X\\-3Y^3-3\end{pmatrix},Ts_{13}=\begin{pmatrix}-Y^5-Y^2\\4X+2XY^3\\0\end{pmatrix},Ts_{23}=\begin{pmatrix}-XY^2-Y^2\\2X^2+2X\\2\end{pmatrix}.$$

Moreover, we have $\mathbf{I}_3-TS=\begin{pmatrix}1-Y^3&0&0\\2XY&0&0\\0&0&0\end{pmatrix}$. So, denoting the first column of $\mathbf{I}_3-TS$ by r_1, we have:

$$\mathrm{Syz}(F)=\langle Ts_{12},Ts_{13},Ts_{23},r_1\rangle$$

$$=\langle {}^{\mathrm{t}}(-XY^2-Y^2,2X^2+2X,2),\ {}^{\mathrm{t}}(-Y^5-Y^2,4X+2XY^3,0),\ {}^{\mathrm{t}}(0,X^2-3X,-3Y^3-3),\ {}^{\mathrm{t}}(1-Y^3,2XY,0)\rangle.$$

3.2 Computing dynamically a generating set for syzygies of polynomials over Dedekind rings

Let $\mathbf{R}$ be a Dedekind ring and consider $f_1, \ldots, f_s \in \mathbf{R}[X_1, \ldots, X_n] \setminus \{0\}$. Our goal is to compute a generating set for $\mathrm{Syz}(f_1, \ldots, f_s)$. We must first compute a dynamical Gröbner basis $G = \{(S_1, G_1), ..., (S_k, G_k)\}$ for the ideal $\langle f_1, \ldots, f_s\rangle$ of $\mathbf{R}[X_1, \ldots, X_n]$. Denoting by $H_j = \{h_{j,1}, ..., h_{j,p_j}\}$ a generating set for $\mathrm{Syz}(f_1, \ldots, f_s)$ over $(S_j^{-1}\mathbf{R})[X_1, \ldots, X_n]$, $1 \leq j \leq k$, for each $1 \leq i \leq p_j$, there exists $d_{j,i} \in S_j$ such that $d_{j,i}h_{j,i} \in \mathbf{R}[X_1, \ldots, X_n]$. Under these hypotheses, we have:

Theorem 10 *(Syzygies over Dedekind rings) As an $\mathbf{R}[X_1, \ldots, X_n]$-module,*

$$\mathrm{Syz}(f_1, \ldots, f_s) = \langle d_{1,1}h_{1,1}, \ldots, d_{1,p_1}h_{1,p_1}, \ldots, d_{k,1}h_{k,1}, \ldots, d_{k,p_k}h_{k,p_k}\rangle.$$

Proof It is clear that $\langle d_{1,1}h_{1,1}, \ldots, d_{1,p_1}h_{1,p_1}, \ldots, d_{k,1}h_{k,1}, \ldots, d_{k,p_k}h_{k,p_k}\rangle \subseteq \mathrm{Syz}(f_1, \ldots, f_s)$. For the converse, let $h \in \mathrm{Syz}(f_1, \ldots, f_s)$ over $\mathbf{R}[X_1, \ldots, X_n]$. It is also a syzygy for $(f_1, \ldots, f_s)$ over $(S_j^{-1}\mathbf{R})[X_1, \ldots, X_n]$ for each $1 \leq j \leq k$. Hence, for some $d_j \in S_j$, $d_jh \in \langle d_{j,1}h_{j,1}, \ldots, d_{j,p_j}h_{j,p_j}\rangle$ over $\mathbf{R}[X_1, \ldots, X_n]$. On the other hand, as $S_1, \ldots, S_k$ are comaximal multiplicative subsets of $\mathbf{R}$, there exist $\alpha_1, \ldots, \alpha_k \in \mathbf{R}$ such that $\sum_{j=1}^k \alpha_j d_j = 1$. From the fact that $h = \sum_{j=1}^k \alpha_j d_j h$, we infer that $h \in \langle d_{1,1}h_{1,1}, \ldots, d_{1,p_1}h_{1,p_1}, \ldots, d_{k,1}h_{k,1}, \ldots, d_{k,p_k}h_{k,p_k}\rangle$ over $\mathbf{R}[X_1, \ldots, X_n]$. □

A dynamical method for computing the syzygy module for polynomials over a Dedekind ring

Let $\mathbf{R}$ be a Dedekind ring and consider $f_1, \ldots, f_s \in \mathbf{R}[X_1, \ldots, X_n] \setminus \{0\}$. Our goal is to describe a dynamical method of computing a generating set for $\mathrm{Syz}(f_1, \ldots, f_s)$. This method works in the same way as the case in which the base ring is a Noetherian valuation ring (Paragraph 3.1). Here we add the Noetherian hypothesis so that the dynamical version of Buchberger's algorithm terminates. The only difference occurs when one has to handle two incomparable (under division) elements a, b in $\mathbf{R}$. In that situation, one should first compute $u, v, w \in \mathbf{R}$ such that

$$\begin{cases} ub = va \\ wb = (1-u)a. \end{cases}$$

Now, one opens two branches: the computations are pursued in $\mathbf{R}_u$ and $\mathbf{R}_{1+u\mathbf{R}}$.

4 An example

Let $I = \langle f_1 = 3XY + 1,\ f_2 = (4+2\theta)Y + 9\rangle$ in $\mathbf{R} := \mathbb{Z}[\theta][X, Y]$ where $\theta = \sqrt{-5}$.

Let us fix the lexicographic order with $X > Y$ as monomial order.

a) Computing a dynamical Gröbner basis

We will first compute a dynamical Gröbner basis for I in $\mathbb{Z}[\theta][X, Y]$. The details of the computations will be given for one leaf only. Because $x_1 := 3$ and $x_2 := 4 + 2\theta$ are not comparable, we have to find $u, v, w \in \mathbb{Z}[\theta]$ such that:

$$\begin{cases} ux_2 = vx_1 \\ wx_2 = (1-u)x_1. \end{cases}$$

A solution of this system is given by: $u = 5 + 2\theta$, $v = 6\theta$, $w = -3$. Then we can open two branches:

$$\begin{array}{ccc} & \mathbb{Z}[\theta] & \\ & \swarrow \quad \searrow & \\ \mathbb{Z}[\theta]_{4+2\theta} & & \mathbb{Z}[\theta]_{5+2\theta} \end{array}$$

In $\mathbb{Z}[\theta]_{5+2\theta}$:

$S(f_1, f_2) = \frac{6\theta}{5+2\theta} f_1 - X f_2 = -9X + \frac{6\theta}{5+2\theta} =: f_3,$

$S(f_1, f_3) = -3f_1 - Yf_3 = -\frac{6\theta}{5+2\theta}Y - 3 =: f_4$,
$S(f_1, f_4) = -\frac{2\theta}{5+2\theta}f_1 - Xf_4 = 3X - \frac{2\theta}{5+2\theta} =: f_5$,
$f_2 \xrightarrow{f_4} 0$, $f_3 \xrightarrow{f_5} 0$,
$S(f_1, f_5) = f_1 - Yf_5 = \frac{2\theta}{5+2\theta}Y + 1 =: f_6$,
$f_4 \xrightarrow{f_6} 0$, $S(f_2, f_5) = Xf_2 - \frac{6\theta}{5+2\theta}Yf_5 \xrightarrow{f_5, f_6} 0$.

Because 2 and 3 are not comparable under division in $\mathbb{Z}[\theta]_{5+2\theta}$, we open two new branches:

$$\begin{array}{ccc} & \mathbb{Z}[\theta]_{5+2\theta} & \\ \swarrow & & \searrow \\ \mathbb{Z}[\theta]_{(5+2\theta).3} & & \mathbb{Z}[\theta]_{(5+2\theta).2} \end{array}$$

In $\mathbb{Z}[\theta]_{(5+2\theta).3}$:

$S(f_1, f_6) = \frac{2\theta}{3(5+2\theta)}f_1 - Xf_6 = -\frac{1}{3}f_5 \xrightarrow{f_5} 0$,
$S(f_5, f_6) = \frac{2\theta}{3(5+2\theta)}Yf_5 - Xf_6 = \frac{20}{3(5+2\theta)^2}Y - X \xrightarrow{f_5} \frac{20}{3(5+2\theta)^2}Y - \frac{2\theta}{3(5+2\theta)} \xrightarrow{f_6} 0$.

Thus, $G_1 = \{3XY+1,\ 3X - \frac{2\theta}{5+2\theta},\ \frac{2\theta}{5+2\theta}Y + 1\}$ is a special Gröbner basis for $\langle 3XY+1,\ (4+2\theta)Y+9\rangle$ in $\mathcal{M}(5+2\theta, 3)^{-1}\mathbb{Z}[\theta] = \mathbb{Z}[\theta]_{(5+2\theta).3}$.

In $\mathbb{Z}[\theta]_{(5+2\theta).2}$:

$G_2 = \{3XY+1,\ 3X - \frac{2\theta}{5+2\theta},\ \frac{2\theta}{5+2\theta}Y + 1\}$ is a special Gröbner basis for $\langle 3XY+1,\ (4+2\theta)Y+9\rangle$.

In $\mathbb{Z}[\theta]_{(4+2\theta)}$:

$G_3 = \{3XY+1,\ (4+2\theta)Y+9,\ \frac{-27}{4+2\theta}X + 1\}$ is a special Gröbner basis for $\langle 3XY+1,\ (4+2\theta)Y+9\rangle$.

Finally, in $\mathbb{Z}[\theta]$: The dynamical evaluation of the problem of constructing a Gröbner basis for I produces the following evaluation tree:

$$\begin{array}{ccccc} & & \mathbb{Z}[\theta] & & \\ & \swarrow & & \searrow & \\ \mathbb{Z}[\theta]_{4+2\theta} & & & & \mathbb{Z}[\theta]_{5+2\theta} \\ & & & \swarrow & \searrow \\ & & \mathbb{Z}[\theta]_{(5+2\theta).3} & & \mathbb{Z}[\theta]_{(5+2\theta).2} \end{array}$$

The obtained dynamical Gröbner basis of I is

$$G = \{(\mathbf{R}[\frac{1}{5+2\theta}],\ G_1),\ (\mathbf{R}[\frac{1}{4+2\theta}],\ G_3)\}.$$

b) Computing the syzygy module

Denoting by $F = [f_1\ f_2]$, we will compute a generating set for $\mathrm{Syz}(F)$.

In $\mathbb{Z}[\theta]_{(5+2\theta).3}$:

Denoting by $G = [g_1\ g_2\ g_3]$ with $g_1 = 3XY+1$, $g_2 = 3X - \frac{2\theta}{5+2\theta}$, $g_3 = \frac{2\theta}{5+2\theta}Y + 1$, we have $G = FT$ with $T = \begin{pmatrix} 1 & 3X - \frac{2\theta}{5+2\theta} + \frac{6\theta}{5+2\theta}XY & -3XY + \frac{2\theta}{5+2\theta}Y - \frac{6\theta}{5+2\theta}XY^2 + 1 \\ 0 & -X^2Y & X^2Y^2 \end{pmatrix}$, and $F = GS$ with $S = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 9 \end{pmatrix}$. $\mathbf{I}_2 - TS = \begin{pmatrix} 0 & 27XY - 9 - (4+2\theta)Y + 3(4+2\theta)XY^2 \\ 0 & 1 - 9X^2Y^2 \end{pmatrix}$,
$r_1 = \begin{pmatrix} 27XY - 9 - (4+2\theta)Y + 3(4+2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \in \mathrm{Syz}(F)$,

$s_{12} = {}^{\mathrm{t}}(1, -Y, -1), s_{13} = {}^{\mathrm{t}}(\frac{2\theta}{3(5+2\theta)}, \frac{1}{3}, -X), s_{23} = {}^{\mathrm{t}}(0, \frac{2\theta}{3(5+2\theta)}Y + \frac{1}{3}, -X + \frac{2\theta}{3(5+2\theta)})$,
$Ts_{12}=\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $Ts_{13}=\begin{pmatrix} 3X^2Y + \frac{4+2\theta}{3}X^2Y^2 \\ \frac{-1}{3}X^2Y - X^3Y^2 \end{pmatrix}$, and $Ts_{23} = Ts_{13}$. Thus, over $\mathbb{Z}[\theta]_{(5+2\theta).3}[X, Y]$,

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} 3X^2Y + \frac{4+2\theta}{3}X^2Y^2 \\ \frac{-1}{3}X^2Y - X^3Y^2 \end{pmatrix}, \begin{pmatrix} 27XY - 9 - (4+2\theta)Y + 3(4+2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle.$$

In $\mathbb{Z}[\theta]_{(5+2\theta).2}$:

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} \frac{9X^2Y(5+2\theta+2\theta Y)}{2\theta} \\ \frac{-(5+2\theta)(3X^3Y^2+X^2Y)}{2\theta} \end{pmatrix}, \begin{pmatrix} 27XY - 9 - (4+2\theta)Y + 3(4+2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle.$$

In $\mathbb{Z}[\theta]_{(4+2\theta)}$:

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} -\frac{9}{4+2\theta} - Y \\ \frac{1}{4+2\theta} + \frac{3XY}{4+2\theta} \end{pmatrix} \rangle.$$

Finally, in $\mathbb{Z}[\theta]$: Over $\mathbb{Z}[\theta][X, Y]$, we have

$$\mathrm{Syz}(F) = \langle \begin{pmatrix} -(4+2\theta)Y - 9 \\ 3XY + 1 \end{pmatrix}, \begin{pmatrix} 27XY - 9 - (4+2\theta)Y + 3(4+2\theta)XY^2 \\ 1 - 9X^2Y^2 \end{pmatrix} \rangle = \langle \begin{pmatrix} -(4+2\theta)Y - 9 \\ 3XY + 1 \end{pmatrix} \rangle.$$

c) The ideal membership problem Suppose that we must deal with the ideal membership problem:

$$f = (4\theta - 1)X^2Y + 6\theta XY^2 + 9\theta X^2 + 3X - 4Y - 9 \ \in ? \ I = \langle f_1 = 3XY + 1, \ f_2 = (4+2\theta)Y + 9 \rangle$$

in $\mathbb{Z}[\theta][X, Y]$ where $\theta = \sqrt{-5}$.

Let us first execute the dynamical division algorithm of f by $G_1 = \{f_1 = 3XY + 1, \ f_5 = -3X + \frac{2\theta}{5+2\theta}, \ f_6 = \frac{2\theta}{5+2\theta}Y + 1\}$ in the ring $\mathbb{Z}[\theta]_{(5+2\theta).3}[X, Y]$.
With the same notations as in [9], one obtains:

q_1	q_5	q_6	p
$\frac{4\theta-1}{3}X$	0	0	$6\theta XY^2 + 9\theta X^2 + \frac{10-4\theta}{3}X - 4Y - 9$
$\frac{4\theta-1}{3}X + 2\theta Y$	0	0	$9\theta X^2 + \frac{10-4\theta}{3}X - (4+2\theta)Y - 9$
$\frac{4\theta-1}{3}X + 2\theta Y$	$-3\theta X$	0	$-(4+2\theta)Y - 9$
$\frac{4\theta-1}{3}X + 2\theta Y$	$-3\theta X$	-9	0

Thus, the answer to this ideal membership problem in the ring $\mathbb{Z}[\theta]_{(5+2\theta).3}[X, Y]$ is positive and one obtains:

$f = (\frac{4\theta-1}{3}X + 2\theta Y)f_1 - 3\theta X f_5 - 9f_6$.

But since

$f_5 = (\frac{-6\theta}{5+2\theta}XY - 3X + \frac{2\theta}{5+2\theta})f_1 - X^2Y f_2$, and
$f_6 = (\frac{-6\theta}{5+2\theta}XY^2 - 3XY + \frac{2\theta}{5+2\theta}Y + 1)f_1 - X^2Y^2 f_2$, one infers that

$$f = [\frac{-90}{5+2\theta}X^2Y + 9\theta X^2 + \frac{54\theta}{5+2\theta}XY^2 + 27XY + \frac{6\theta+15}{5+2\theta}X - 4Y - 9]f_1 + [3\theta X^3Y + 9X^2Y^2]f_2.$$

Seeing that 3 does not appear in the denominators of the relation above, we can say that we have a positive answer to our ideal membership problem in the ring $\mathbb{Z}[\theta]_{5+2\theta}[X, Y]$ without dealing with the leaf $\mathbb{Z}[\theta]_{(5+2\theta).2}$. Clearing the denominators, we obtain:

$$(5+2\theta)f = [-90X^2Y+45(\theta-2)X^2+54\theta XY^2+27(5+2\theta)XY+(6\theta+15)X-4(5+2\theta)Y-9(5+2\theta)]f_1$$
$$+[15(\theta-2)X^3Y+9(5+2\theta)X^2Y^2]f_2. \qquad (A)$$

It remains to execute the dynamical division algorithm of f by $G_2 = \{f_1 = 3XY+1,\ f_7 = -\frac{27}{4+2\theta}X+1,\ f_8 = Y+\frac{9}{4+2\theta}\}$ in the ring $\mathbb{Z}[\theta]_{4+2\theta}[X,Y]$. The division is as follows:

q_1	q_7	q_8	p
0	0	$(4\theta-1)X^2$	$6\theta XY^2-\frac{81}{4+2\theta}X^2+3X-4Y-9$
$2\theta Y$	0	$(4\theta-1)X^2$	$\frac{-81}{4+2\theta}X^2+3X-(4+2\theta)Y-9$
$2\theta Y$	$3X$	$(4\theta-1)X^2$	$-(4+2\theta)Y-9$
$2\theta Y$	$3X$	$(4\theta-1)X^2-(4+2\theta)$	0

Thus, the answer to this ideal membership problem in the ring $\mathbb{Z}[\theta]_{4+2\theta}[X,Y]$ is positive and one obtains:

$f = 2\theta Y f_1 + 3Xf_7 + ((4\theta-1)X^2-(4+2\theta))f_8.$

But since

$f_7 = f_1 - \frac{3}{4+2\theta}Xf_2$, and
$f_8 = (Y+\frac{9}{4+2\theta})f_1 - \frac{3}{4+2\theta}XYf_2$, one infers that

$$(4+2\theta)f = [(14\theta-44)X^2Y+9(4\theta-1)X^2-4(4+2\theta)Y+3(4+2\theta)X-9(4+2\theta)]f_1$$
$$+[-9X^2-3(4\theta-1)X^3Y+3(4+2\theta)XY]f_2. \qquad (B)$$

Using the Bezout identity $(5+2\theta)-(4+2\theta)=1$, $(A)-(B)\Rightarrow$

$$f = [(46-14\theta)X^2Y+9(\theta-9)X^2+54\theta XY^2+27(5+2\theta)XY+3X-4Y-9]f_1$$
$$+[3(9\theta-11)X^3Y+9(5+2\theta)X^2Y^2+9X^2-3(4+2\theta)X]f_2,$$

a complete positive answer.

5 The Gröbner Ring Conjecture

Recall that accordingly to [30], a ring $\mathbf{R}$ is said to be *Gröbner* if for each $n\in\mathbb{N}$ and each finitely-generated ideal I of $\mathbf{R}[X_1,\dots,X_n]$, fixing a monomial order on $\mathbf{R}[X_1,\dots,X_n]$, the ideal $\{\mathrm{LT}(f), f\in I\}$ of $\mathbf{R}[X_1,\dots,X_n]$ formed by the leading terms of the elements of I is finitely-generated. The first example of a ring that is not Gröbner was given in [30]. This example corresponds to a valuation domain $\mathbf{V}$ whose valuation group is $\mathbb{Z}\times\mathbb{Z}$ equipped with the lexicographic order ($\dim\mathbf{V}=2$). The author of [30] was unable to prove that this works for any valuation domain whose Krull dimension is ≥ 2. We propose hereafter to establish this fact in the general setting, giving a partial positive answer to the conjecture given in [30] to which, for convenience, we will refer as the Gröbner Ring Conjecture.

The Gröbner Ring Conjecture: *A valuation ring is Gröbner if and only if its Krull dimension is* ≤ 1.

Recall that a ring $\mathbf{R}$ has Krull dimension ≤ 1 if and only if

$$\forall a,b\in\mathbf{R},\ \ \exists n\in\mathbb{N},\ \ \exists x,y\in\mathbf{R}\ \ \mid\ \ a^n(b^n(1+xb)+ya)=0. \qquad (1)$$

This is a constructive substitute for the classical abstract definition (see [7, 17, 18]). For a valuation domain, it is easy to see that (1) amounts to the fact that the valuation group is archimedean.

Theorem 11 *For an integral valuation ring* $\mathbf{V}$*, we have* (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) *where:*

(i) $\mathbf{V}$ *is a Gröbner ring.*

(ii) *For any* $m \in \mathbb{N}$*, if* J *is a finitely-generated ideal of* $\mathbf{V}[X_1, \ldots, X_m]$ *then* $J \cap \mathbf{V}$ *is a principal ideal* $\mathbf{V}$*.*

(iii) $\dim \mathbf{V} \leq 1$.

Proof "(i) $\Rightarrow$ (ii)" Let J be a finitely-generated ideal of $\mathbf{V}[X_1, \ldots, X_m]$. Because $\mathbf{V}$ is a Gröbner ring, $\langle \mathrm{LT}(J) \rangle$ is finitely-generated, say $\langle \mathrm{LT}(J) \rangle = \langle h_1, \ldots, h_s \rangle$ where $h_1, \ldots, h_s$ are terms. We can suppose that $h_1 \in \mathbf{V}$ and $h_2, \ldots, h_s \notin \mathbf{V}$. By virtue of Lemma 3 of [30], we infer that $J \cap \mathbf{V} = \langle h_1 \rangle$.

"(ii) $\Rightarrow$ (iii)" Let us denote by v and G respectively the valuation and the valuation group associated with $\mathbf{V}$ and consider $a, b \in \mathrm{Rad}(\mathbf{V})$ (the Jacobson radical of $\mathbf{V}$). Our goal is to find $n \in \mathbb{N}$ such that $v(b) \leq n\, v(a)$, or equivalently, such that b divides a^n.
Let us denote by I the ideal of $\mathbf{V}[X]$ generated by $g_1 = aX + 1$ and $g_2 = b$. Because I finitely-generated $I \cap \mathbf{V}$ is principal, write $I \cap \mathbf{V} = \langle c \rangle$. Because $c \in I$, it can be written in the form

$$c = U(X).(aX + 1) + V(X).b,$$

with $U(X), V(X) \in \mathbf{V}[X]$. Supposing that $\deg V \leq k$ and evaluating X at $\frac{-1}{a}$, we obtain that $c = V(\frac{-1}{a})b$ and thus b divides $c\, a^k$. This means that $v(b) \leq v(c\, a^k)$, or equivalently, $v(c) \geq v(\frac{b}{a^k})$.

It is worth pointing out that for any $m \in \mathbb{N}$, if a^m divides b then $\frac{b}{a^m} \in I$ as $S(g_1, g_2) = (\frac{b}{a})g_1 - Xg_2 = \frac{b}{a} =: g_3 \in I, \ldots, g_{m+1} := \frac{b}{a^{m-1}} \in I$, $g_{m+2} := \frac{b}{a^m} = \frac{b}{a^m}(aX + 1) - Xg_{m+1} \in I$.

If a^k does not divide b, we are done by taking $n = k$; otherwise $v(c) = v(\frac{b}{a^k})$ because $c/\frac{b}{a^k}$ and necessarily $I \cap \mathbf{V} = \{x \in \mathbf{V} \mid v(x) \geq v(\frac{b}{a^k})\}$. Thus $\frac{b}{a^{k+1}} \notin I$, b divides a^{k+1}, and we are done by taking $n = k + 1$.

□

Corollary 12 *If a Prüfer domain is Gröbner, then its Krull dimension is* ≤ 1.

References

[1] Adams W.-W., Laustaunau P. *An introduction to Gröbner bases.* Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.

[2] Bernstein D. *Fast ideal arithmetic via lazy localization.* In: H. Cohen (Ed.), Algorithmic Number Theory, Proceeding of the Second International Symposium, ANTS-II, Talence, France, May 18-23, 1996, in: Lecture Notes in Comput. Sci., vol. 1122, Springer-Verlag, Berlin, 1996, pp. 27-34.

[3] Bernstein D. *Factoring into coprimes in essentially linear time.* J. Algorithms **54** (2005) 1-30.

[4] Buchberger B. *A critical pair/completion algorithm for finitely generated ideals in rings.* In: Springer Lectures Notes in Computer Science **171** (1984) 137-155.

[5] Buchmann J., Lenstra H. *Approximating rings of integers in number fields.* J. Théor. Nombres Bordeaux **6 (2)** (1994) 221-260.

[6] Cai Y., Kapur D. *An algorithm for computing a Gröbner basis of a polynomial ideal over a ring with zero divisors.* University of New Mexico, Technical Report (2003). `www.cs.unm.edu/ treport/tr/03-12/GB.pdf`

[7] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings*, in: Commutative ring theory and applications. Eds: Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 477–499.

[8] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra: Effective Nullstellensätze*. Annals of Pure and Applied Logic **111** (2001) 203–256.

[9] Cox D., Little J., O'Shea D. *Ideals, varieties and algorithms*. 2nd edition, New York, Springer-Verlag, 1997.

[10] Della Dora J., Dicrescenzo C., Duval D. *About a new method for computing in algebraic number fields*. In Caviness B.F. (Ed.) EUROCAL '85. Lecture Notes in Computer Science 204, 289–290. Springer (1985).

[11] Ducos L., Quitté C., Lombardi H., Salou M. *Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind*. Journal of Algebra **281** (2004) 604–650.

[12] Duval D., Reynaud J.-C. *Sketches and computation (Part II) Dynamic evaluation and applications*. Mathematical Structures in computer Sciences **4** (1994) 239–271.

[13] Ellouz A., Lombardi H., Yengui I. *A constructive comparison of the rings* $\mathbf{R}(X)$ *and* $\mathbf{R}\langle X\rangle$ *and application to the Lequain-Simis induction theorem*, J. Algebra **320** (2008) 521-533.

[14] Faugère J.-C. *A new efficient algorithm for computing Gröbner bases without reduction to zero* (F_5). In Proc. ISSAC (2002).

[15] Greuel G.-M., Pfister G. *A Singular introduction to commutative algebra*. Springer Verlag Berlin, Heidelberg, New York, 2002. 2nd Edition: 2008.

[16] Kapur D., Narendran P. *An equational approach to theoretical proving in first-order predicate calculus*. IJCAI (1985) 1146-1153.

[17] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique*. Math. Zeitschrift **242** (2002) 23–46.

[18] Lombardi H., Quitté C., Yengui I. *Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa*. J. Pure Appl. Algebra **212** (2008) 1575–1582.

[19] Magma (Computational Algebra Group within School of Maths and Statistics of University of Sydney): `http://magma.maths.usyd.edu.au/magma`

[20] Mines R., Richman R., Ruitenburg W. *A Course in Constructive Algebra*. Universitext, Springer-Verlag, 1988.

[21] Möller H.-M. *On the construction of Gröbner bases using syzygies*. J. Symb. Comp. **6** (1988) 345–359.

[22] Mora T. *Solving Polynomial Equation Systems I: The Kronecker-Duval Philosophy*. Cambridge University Press (2003).

[23] Pauer F. *Gröbner bases with coefficients in rings*. J. Symb. Comp. **42** (2007) 1003–1011.

[24] Richman F. *Non trivial uses of trivial rings*. Proc. Amer. Math. Soc. **103** (1988) 1012–1014.

[25] Schreyer F.-O. *Syzygies of canonical curves and special linear series*. Math. Ann. **275** (1986).

[26] Schreyer F.-O. *A standard basis approach to Syzygies of canonical curves*. J. Reine Angew. Math. **421** (1991) 83-123.

[27] Serre J.-P. *Local fields*. Trans. M.J. Greenberg, New York, Springer-Verlag, 1979.

[28] SINGULAR (Decker W., Greuel G.-M., Pfister G., Schönemann H.): A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern: `http://www.singular.uni-kl.de`

[29] Trinks W. *Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen*. J. Number Theory **10** (1978) 475–488.

[30] Yengui I. *Dynamical Gröbner bases*. J. Algebra **301** (2006) 447–458.

[31] Yengui I. *Making the use of maximal ideals constructive*. Theoretical Computer Science **392** (2008) 174-178.

[32] Yengui I. *Stably free modules over* $\mathbf{R}[X]$ *of rank* $>\dim\mathbf{R}$ *are free*. Mathematics of Computation, To appear.