The syzygy theorem for Bézout rings

Maroua Gamanda[*], Henri Lombardi[**], Stefan Neuwirth[**,1], and Ihsen Yengui[*,2]

[*]Département de mathématiques, Faculté des sciences de Sfax, Université de Sfax, 3000 Sfax, Tunisia, marwa.gmenda@hotmail.com, ihsen.yengui@fss.rnu.tn.
[**]Laboratoire de mathématiques de Besançon, Université Bourgogne Franche-Comté, 25030 Besançon Cedex, France, henri.lombardi@univ-fcomte.fr, stefan.neuwirth@univ-fcomte.fr.

Abstract

We provide constructive versions of Hilbert's syzygy theorem for $\mathbb{Z}$ and $\mathbb{Z}/N\mathbb{Z}$ following Schreyer's method. Moreover, we extend these results to arbitrary coherent strict Bézout rings with a divisibility test for the case of finitely generated modules whose module of leading terms is finitely generated.

MSC 2010: 13D02, 13P10, 13C10, 13P20, 14Q20

Keywords: Syzygy theorem, free resolution, monomial order, Schreyer's monomial order, Schreyer's syzygy algorithm, dynamical Gröbner basis, valuation ring, Gröbner ring, strict Bézout ring.

Contents

Introduction 2

1 Gröbner bases for modules over a discrete ring 2

[1]Supported by the French "Investissements d'avenir" program, project ISITE-BFC (contract ANR-15-IDEX-03).
[2]Supported by the John Templeton Foundation (ID 60842).

2 The algorithms **6**
The context . . . 6
The division algorithm . . . 6
The S-polynomial algorithm . . . 7
Buchberger's algorithm . . . 9
The syzygy algorithm for terms . . . 10
Schreyer's syzygy algorithm . . . 10

3 The algorithms in the case of a valuation ring **11**

4 Termination of Buchberger's algorithm for a Bézout ring **13**
When is a valuation ring a Gröbner ring? . . . 17

5 The syzygy theorem and Schreyer's algorithm for a valuation ring **19**

6 The syzygy theorem and Schreyer's algorithm for a Bézout ring **25**
The case of the integers . . . 27
The case of $\mathbb{Z}/N\mathbb{Z}$ . . . 28

References **30**

Introduction

This paper is written in the framework of Bishop style constructive mathematics (see [2, 3, 11, 12]). It can be seen as a sequel to the papers [10, 16]. The main goal is to obtain constructive versions of Hilbert's syzygy theorem for Bézout domains of Krull dimension ≤ 1 with a divisibility test and for coherent zero-dimensional Bézout rings with a divisibility test (e.g. for $\mathbb{Z}$ and $\mathbb{Z}/N\mathbb{Z}$, see [11, 13, 18, 19]) following Schreyer's method. These two cases are instances of Gröbner rings. Moreover, we extend these results to arbitrary coherent strict Bézout rings with a divisibility test for the case of finitely generated modules whose module of leading terms is finitely generated.

1 Gröbner bases for modules over a discrete ring

General context. In this article, $\mathbf{R}$ is a commutative ring with unit, $X_1, \ldots, X_n$ are n indeterminates ($n \geq 1$), $\mathbf{R}[\underline{X}] = \mathbf{R}[X_1, \ldots, X_n]$, $\mathbf{H}_m \simeq$

$\mathbb{A}^m(\mathbf{R}[\underline{X}])$ is a free $\mathbf{R}[\underline{X}]$-module with basis $(e_1, \ldots, e_m)$ $(m \geq 1)$, and $>$ is a monomial order on $\mathbf{H}_m$ (see Definition 1.3).

We start with recalling the following constructive definitions.

Definition 1.1.

- $\mathbf{R}$ is *discrete* if it is equipped with a zero test: equality is decidable.
- $\mathbf{R}$ is *zero-dimensional* and we write $\dim \mathbf{R} \leq 0$ if

$$\forall a \in \mathbf{R}\ \exists k \in \mathbb{N}\ \exists x \in \mathbf{R}\ \ a^k(ax-1) = 0.$$

- $\mathbf{R}$ has Krull dimension ≤ 1 and we write $\dim \mathbf{R} \leq 1$ if

$$\forall a, b \in \mathbf{R}\ \exists k, \ell \in \mathbb{N}\ \exists x, y \in \mathbf{R}\ \ b^\ell(a^k(ax-1)+by) = 0.$$

- Let U be an $\mathbf{R}$-module. The *syzygy module* of a p-tuple $(v_1, \ldots, v_p) \in U^p$ is

$$\mathrm{Syz}(v_1, \ldots, v_p) \coloneqq \{\, (b_1, \ldots, b_p) \in \mathbf{R}^n \,;\, b_1 v_1 + \cdots + b_p v_p = 0 \,\}.$$

The syzygy module of a single element v is the *annihilator* $\mathrm{Ann}(v)$ of v.

- An $\mathbf{R}$-module U is *coherent* if the syzygy module of every p-tuple of elements of U is finitely generated,[1] i.e. if there is an algorithm providing a finite system of generators for the syzygies, and an algorithm that represents each syzygy as a linear combination of the generators. $\mathbf{R}$ is *coherent* if it is coherent as an $\mathbf{R}$-module. It is well known that a module is coherent iff on the one hand any intersection of two finitely generated submodules is finitely generated, and on the other hand the annihilator of every element is a finitely generated ideal.
- $\mathbf{R}$ is *local* if, for every element $x \in \mathbf{R}$, either x or $1+x$ is invertible.
- $\mathbf{R}$ is *equipped with a divisibility test* if, given $a, b \in \mathbf{R}$, one can answer the question $a \in ?\ \langle b \rangle$ and, in the case of a positive answer, one can explicitly provide $c \in \mathbf{R}$ such that $a = bc$.
- $\mathbf{R}$ is *strongly discrete* if it is equipped with a membership test for finitely generated ideals, i.e. if, given $a, b_1, \ldots, b_p \in \mathbf{R}$, one can answer the question $a \in ?\ \langle b_1, \ldots, b_p \rangle$ and, in the case of a positive answer, one can explicitly provide $c_1, \ldots, c_p \in \mathbf{R}$ such that $a = c_1 b_1 + \cdots + c_p b_p$.

[1] In contradistinction to Bourbaki and to the Stacks project, we do not require U to be finitely generated.

- $\mathbf{R}$ is a *valuation ring*[2] if every two elements are comparable w.r.t. division, i.e. if, given $a, b \in \mathbf{R}$, either $a \mid b$ or $b \mid a$. A valuation ring is a local ring; it is coherent iff the annihilator of any element is principal. A valuation domain is coherent. A valuation ring is strongly discrete iff it is equipped with a divisibility test.

- $\mathbf{R}$ is a *Bézout ring* if every finitely generated ideal is principal, i.e. of the form $\langle a\rangle = \mathbf{R}a$ with $a \in \mathbf{R}$. A Bézout ring is strongly discrete iff it is equipped with a divisibility test; it is coherent iff the annihilator of any element is principal. To be a valuation ring is to be a Bézout local ring (see [11, Lemma IV-7.1]).

- A Bézout ring $\mathbf{R}$ is *strict* if for all $b_1, b_2 \in \mathbf{R}$ we can find $d, b_1', b_2', c_1, c_2 \in \mathbf{R}$ such that $b_1 = db_1'$, $b_2 = db_2'$, and $c_1b_1' + c_2b_2' = 1$. Valuation rings and Bézout domains are strict Bézout rings; a quotient or a localisation of a strict Bézout ring is again a strict Bézout ring (see [11, Exercise IV-7 pp. 220–221, solution pp. 227–228]). A zero-dimensional Bézout ring is strict (because it is a "Smith ring", see [7, Exercice XVI-9 p. 355, solution p. 526] and [11, Exercise IV-8 pp. 221-222, solution p. 228]).

Remark 1.2. In some cases, e.g. euclidean domains or polynomial rings over a discrete field, a strongly discrete ring is equipped with a *division algorithm* which, for arbitrary $a \in \mathbf{R}$ and $(b_1, \ldots, b_p) \in \mathbf{R}^p$, provides an expression $a = c_1'b_1 + \cdots + c_p'b_p + e$ with *quotients* $c_1', \ldots, c_p'$ and a *remainder* e, where $e = 0$ iff $a \in \langle b_1, \ldots, b_p\rangle$. When a strongly discrete ring is not equipped with a division algorithm, we shall consider that the division is trivial if $a \notin \langle b_1, \ldots, b_p\rangle$: the quotients vanish and $e = a$. In the case of Bézout rings, dividing a by $(b_1, \ldots, b_p)$ amounts to dividing a by the gcd d of $(b_1, \ldots, b_p)$, since $a = c'd + e$ can be read as $a = (c'c_1)b_1 + \cdots + (c'c_p)b_p + e$, where $d = c_1b_1 + \cdots + c_pb_p$.

Definition 1.3 (Monomial orders on finite-rank free $\mathbf{R}[\underline{X}]$-modules, see [1, 5])**.**

(1) A *monomial* in $\mathbf{H}_m$ is a vector of type $\underline{X}^\alpha e_\ell$ $(1 \leq \ell \leq m)$, where $\underline{X}^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ is a monomial in $\mathbf{R}[\underline{X}]$; the index ℓ is the *position* of the monomial. The set of monomials in $\mathbf{H}_m$ is denoted by $\mathbb{M}_n^m$, with $\mathbb{M}_n^1 \cong \mathbb{M}_n$ (the set of monomials in $\mathbf{R}[\underline{X}]$). E.g., $X_1X_2^3e_2$ is a monomial in $\mathbf{H}_m$, but $2X_1e_3$, $(X_1 + X_2^3)e_2$ and $X_1e_2 + X_2^3e_3$ are not.

[2]Here we follow Kaplansky's definition: $\mathbf{R}$ may have nonzero zerodivisors. In [19] it is required that a valuation ring be strongly discrete. We prefer to add this hypothesis when the argument requires it, so as to discriminate the algorithms that rely on the divisibility test from those that do not.

If $M = \underline{X}^\alpha e_\ell$ and $N = \underline{X}^\beta e_k$, we say that M *divides* N if $\ell = k$ and $\underline{X}^\alpha$ divides $\underline{X}^\beta$. E.g., $X_1 e_1$ divides $X_1 X_2 e_1$, but does not divide $X_1 X_2 e_2$. Note that in the case that M divides N, there exists a monomial $\underline{X}^\gamma$ in $\mathbf{R}[\underline{X}]$ such that $N = \underline{X}^\gamma M$: in this case we define $N/M := \underline{X}^\gamma$; e.g., $(X_1 X_2 e_1)/(X_1 e_1) = X_2$.

A *term* in $\mathbf{H}_m$ is a vector of type cM, where $c \in \mathbf{R}\setminus\{0\}$ and $M \in \mathbb{M}_n^m$. We say that a term cM *divides* a term $c'M'$, with $c, c' \in \mathbf{R}\setminus\{0\}$ and $M, M' \in \mathbb{M}_n^m$, if c divides c' and M divides M'.

(2) A *monomial order* on $\mathbf{H}_m$ is a relation $>$ on $\mathbb{M}_n^m$ such that

(i) $>$ is a total order on $\mathbb{M}_n^m$,

(ii) $\underline{X}^\alpha M > M$ for all $M \in \mathbb{M}_n^m$ and $\underline{X}^\alpha \in \mathbb{M}_n \setminus \{1\}$,

(iii) $M > N \implies \underline{X}^\alpha M > \underline{X}^\alpha N$ for all $M, N \in \mathbb{M}_n^m$ and $\underline{X}^\alpha \in \mathbb{M}_n$.

Note that, when specialised to the case $m = 1$, this definition coincides with the definition of a monomial order on $\mathbf{R}[\underline{X}]$.

When $\mathbf{R}$ is discrete, any *nonzero* vector $h \in \mathbf{H}_m$ can be written as a sum of terms

$$h = c_t M_t + c_{t-1} M_{t-1} + \cdots + c_1 M_1,$$

with $c_\ell \in \mathbf{R} \setminus \{0\}$, $M_\ell \in \mathbb{M}_n^m$, and $M_t > M_{t-1} > \cdots > M_1$. We define the *leading coefficient*, *leading monomial*, and *leading term* of h as in the ring case: $\mathrm{LC}(h) = c_t$, $\mathrm{LM}(h) = M_t$, $\mathrm{LT}(h) = c_t M_t$. Letting $M_t = \underline{X}^\alpha e_\ell$ with $\underline{X}^\alpha \in \mathbb{M}_n^m$ and $1 \le \ell \le m$, we say that α is the *multidegree of* h and write $\mathrm{mdeg}(h) = \alpha$, and that the index ℓ is the *leading position* of h and write $\mathrm{LPos}(h) = \ell$.

We stipulate that $\mathrm{LT}(0) = 0$ and $\mathrm{mdeg}(0) = -\infty$, but we do not define $\mathrm{LPos}(0)$.

(3) A monomial order on $\mathbf{R}[\underline{X}]$ gives rise to the following canonical monomial order on $\mathbf{H}_m$: for monomials $M = \underline{X}^\alpha e_\ell$ and $N = \underline{X}^\beta e_k \in \mathbb{M}_n^m$, let us define that

$$M > N \quad \text{if} \quad \left| \begin{array}{l} \text{either } \underline{X}^\alpha > \underline{X}^\beta \\ \text{or both } \underline{X}^\alpha = \underline{X}^\beta \text{ and } \ell < k. \end{array} \right.$$

This monomial order is called *term over position* (TOP) because it gives more importance to the monomial order on $\mathbf{R}[\underline{X}]$ than to the vector position. E.g., when $X_2 > X_1$, we have

$$X_2 e_1 > X_2 e_2 > X_1 e_1 > X_1 e_2.$$

Definition 1.4 (Gröbner bases and Schreyer's monomial order)**.** Let $\mathbf{R}$ be a discrete ring. Consider $G = (g_1, \ldots, g_p)$, $g_j \in \mathbf{H}_m \setminus \{0\}$, and the finitely generated submodule $U = \langle g_1, \ldots, g_p \rangle = \mathbf{R}[\underline{X}]g_1 + \cdots + \mathbf{R}[\underline{X}]g_p$ of $\mathbf{H}_m$.

(1) The *module of leading terms* of U is $\mathrm{LT}(U) \coloneqq \langle\, \mathrm{LT}(u)\ ;\ u \in U \,\rangle$.

(2) G is a *Gröbner basis* for U if $\mathrm{LT}(U) = \langle \mathrm{LT}(G) \rangle \coloneqq \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_p) \rangle$.

(3) Let $(\epsilon_1, \ldots, \epsilon_p)$ be the canonical basis of $\mathbf{R}[\underline{X}]^p$. *Schreyer's monomial order induced by* $>$ *and* $(g_1, \ldots, g_p)$ on $\mathbf{R}[\underline{X}]^p$ is the order denoted by $>_{g_1,\ldots,g_p}$, or again by $>$, defined as follows:

$$\underline{X}^\alpha \epsilon_\ell > \underline{X}^\beta \epsilon_k \quad \text{if} \quad \left| \begin{array}{l} \text{either } \mathrm{LM}(\underline{X}^\alpha g_\ell) > \mathrm{LM}(\underline{X}^\beta g_k) \\ \text{or both } \mathrm{LM}(\underline{X}^\alpha g_\ell) = \mathrm{LM}(\underline{X}^\beta g_k) \text{ and } \ell < k. \end{array} \right.$$

Schreyer's monomial order is defined on $\mathbf{R}[\underline{X}]^p$ in the same way as when $\mathbf{R}$ is a discrete field (see [8, p. 66]).

2 The algorithms

The context

Let us now present the algorithms to be discussed in this article in a form that adapts as well to the case where $\mathbf{R}$ is a coherent valuation ring with a divisibility test as to the case where $\mathbf{R}$ is a coherent strict Bézout ring with a divisibility test (note that the former case is the local case of the latter). This is achieved by appeals to "**find** ... **such that** ..." commands that will adapt to the corresponding framework. I.e., the following context is needed for the algorithms, except that coherence and strictness is not used in the division algorithm and that the divisibility test is not used for the computation of S-polynomials.

Context 2.1. The algorithms take place in a coherent strict Bézout ring $\mathbf{R}$ with a divisibility test. In the local case, $\mathbf{R}$ is a coherent valuation ring with a divisibility test.

The division algorithm

This algorithm takes place in Context 2.1 for $\mathbf{R}$; note however that coherence and strictness are not used here. Like the classical division algorithm for

$\mathbf{F}[\underline{X}]^m$ with $\mathbf{F}$ a discrete field (see [19, Algorithm 211]), this algorithm has the following goal.

$$\begin{array}{rl}\textbf{Input} & h \in \mathbf{H}_m,\ h_1, \ldots, h_p \in \mathbf{H}_m \setminus \{0\}.\\ \textbf{Output} & q_1, \ldots, q_p \in \mathbf{R}[\underline{X}] \text{ and } r \in \mathbf{H}_m \text{ such that}\\ & \begin{cases} h = q_1 h_1 + \cdots + q_p h_p + r,\\ \mathrm{LM}(h) \geq \mathrm{LM}(q_j)\,\mathrm{LM}(h_j) \text{ whenever } q_j \neq 0,\\ T \notin \langle \mathrm{LT}(h_1), \ldots, \mathrm{LT}(h_p)\rangle \text{ for each term } T \text{ of } r. \end{cases}\end{array}$$

Definition and notation 2.2. The vector r is called *a remainder of h on division by $H = (h_1, \ldots, h_p)$* and is denoted by $r = \overline{h}^H$.

This notation would gain in precision if it included the dependence of the remainder on the algorithm mentioned in Remark 1.2.

Division algorithm 2.3.

```
1  local variables  j : {1,...,p},  D : subset of {1,...,p},
2                   c, c_j, d, e : R,  h' : H_m;
3  q_1 ← 0;  ...  ;  q_p ← 0;  r ← 0;  h' ← h;
4  while h' ≠ 0 do
5     D ← { j ; LM(h_j) | LM(h') };
6     find d, c_j (j ∈ D) such that
7        d = gcd(LC(h_j))_{j∈D} = Σ_{j∈D} c_j LC(h_j);
8     find c, e such that
9        LC(h') = cd + e  (with e = 0 iff d divides LC(h'), see Remark 1.2);
10    for j in D do
11       q_j ← q_j + cc_j(LM(h')/ LM(h_j))
12    od;
13    r ← r + e LM(h');
14    h' ← h' − Σ_{j∈D} cc_j(LM(h')/ LM(h_j))h_j − e LM(h')
15 od
```

By convention, if D is empty, then $d = 0$. At each step of the algorithm, the equality $h = q_1 h_1 + \cdots + q_p h_p + h' + r$ holds while $\mathrm{mdeg}(h')$ decreases.

Note that in the case of a valuation ring, the gcd d is an $\mathrm{LC}(h_{j_0})$ dividing all the $\mathrm{LC}(h_j)$, and the Bézout identity may be given by setting $c_{j_0} = 1$ and $c_j = 0$ for $j \neq j_0$: see Algorithm 3.1.

The S-polynomial algorithm

This algorithm takes also place in Context 2.1 for $\mathbf{R}$. Note however that the divisibility test is not used here; only the zero test is used. This algorithm

is a key tool for constructing a Gröbner basis and has been introduced by Buchberger [4] for the case where the base ring is a discrete field. It has the following goal.

Input $f, g \in \mathbf{H}_m \setminus \{0\}$.
Output the S-polynomial given by $b\underline{X}^\beta$ and $a\underline{X}^\alpha$ as $\mathrm{S}(f,g) = b\underline{X}^\beta f - a\underline{X}^\alpha g$: if $f = g$, then $b\underline{X}^\beta = b$ is a generator of $\mathrm{Ann}(\mathrm{LC}(f))$ and $a\underline{X}^\alpha = 0$; otherwise, if $\mathrm{LM}(f) = \underline{X}^\mu e_i$ and $\mathrm{LM}(g) = \underline{X}^\nu e_i$, then $\mathrm{S}(f,g) = b\underline{X}^{(\nu-\mu)^+} f - a\underline{X}^{(\mu-\nu)^+} g$ with $b\,\mathrm{LC}(f) = a\,\mathrm{LC}(g)$, $\gcd(a,b) = 1$; otherwise, $\mathrm{S}(f,g) = 0$.

Here $\alpha^+ = (\max(\alpha_1, 0), \ldots, \max(\alpha_n, 0))$ is the *positive part* of $\alpha \in \mathbb{Z}^n$.

S-polynomial algorithm 2.4.

```
1  local variables a, b : R, μ, ν : N^n;
2  if f = g then
3    find b such that Ann(LC(f)) = ⟨b⟩;
4    S(f, f) ← bf
5  else
6    if LPos(f) ≠ LPos(g) then
7      S(f, g) ← 0
8    else
9      μ ← mdeg(f); ν ← mdeg(g);
10     find a, b such that
11       gcd(a, b) = 1,
12       a gcd(LC(f), LC(g)) = LC(f),
13       b gcd(LC(f), LC(g)) = LC(g);
14     S(f, g) ← bX^(ν−μ)^+ f − aX^(μ−ν)^+ g
15   fi
16 fi
```

Note the following important properties of $\mathrm{S}(f,g)$:

- If $\mathrm{LM}(f) = \underline{X}^\mu e_i$ and $\mathrm{LM}(g) = \underline{X}^\nu e_i$, then either $\mathrm{S}(f,g) = 0$ or $\mathrm{LM}(\mathrm{S}(f,g)) < \underline{X}^{\sup(\mu,\nu)} e_i$; if $\mathrm{LPos}(f) \neq \mathrm{LPos}(g)$, then $\mathrm{S}(f,g) = 0$;
- $\mathrm{S}(\underline{X}^\delta f, \underline{X}^\delta g) = \underline{X}^\delta \mathrm{S}(f,g)$ for all $\delta \in \mathbb{N}^n$.

$\mathrm{S}(f,f)$ is called the *auto-S-polynomial* of f. It is designed to produce cancellation of the leading term of f by multiplying f with a generator of the annihilator of $\mathrm{LC}(f)$. If the leading coefficient of f is regular, then $\mathrm{S}(f,f) = 0$ as in the discrete field case. In case $\mathbf{R}$ is a domain, this algorithm is not

supposed to compute auto-S-polynomials and we can remove lines 2–5 and 16: if nevertheless executed with $f = g$, it yields $\mathrm{S}(f, f) = 0$.

The S-polynomial $\mathrm{S}(f, g)$ is designed to produce cancellation of the leading terms of f and g. It is worth pointing out that $\mathrm{S}(f, g)$ is not uniquely determined (up to a unit) when $\mathbf{R}$ has nonzero zerodivisors. Also $\mathrm{S}(g, f)$ is generally not equal (up to a unit) to $\mathrm{S}(f, g)$ (in the discrete field case, this ambiguity is taken care of by making the S-polynomial monic). These issues are repaired through the consideration of the auto-S-polynomials $\mathrm{S}(f, f)$ and $\mathrm{S}(g, g)$.

Note that in the case of a valuation ring, the computation of the coefficients a, b is particularly easy: see Algorithm 3.2.

Buchberger's algorithm

This algorithm takes place in Context 2.1 for $\mathbf{R}$. Here coherence, strictness, and the divisibility test are used. Concerning the termination of the algorithm, see Section 4.

This algorithm has the following goal.

Input $g_1, \ldots, g_p \in \mathbf{H}_m \setminus \{0\}$.
Output a Gröbner basis $(g_1, \ldots, g_p, \ldots, g_t)$ for $\langle g_1, \ldots, g_p \rangle$.

Buchberger's algorithm 2.5.

```
1  local variables S : H_m , i, j, u : N;
2  t ← p;
3  repeat
4    u ← t;
5    for i from 1 to u do
6      for j from i to u do
7        S ← S(g_i, g_j)^(g_1,...,g_u) by Algorithms 2.4 and 2.3;
8        if S ≠ 0 then
9          t ← t + 1;
10         g_t ← S
11       fi
12     od
13   od
14 until t = u
```

This algorithm is almost the same algorithm as in the case where the base ring is a discrete field. The modifications are in the definition of S-polynomials, in the consideration of the auto-S-polynomials, and in the division of terms (see Item (1) of Definition 1.3). In line 7, the algorithm may be

sped up by computing the remainder w.r.t. $(g_1, \ldots, g_t)$ instead of $(g_1, \ldots, g_u)$ only.

Remark 2.6. If the algorithm terminates, then we can transform the obtained Gröbner basis into a Gröbner basis $(g'_1, \ldots, g'_{t'})$ such that no term of an element g'_j lies in $\langle \operatorname{LT}(g'_k) \,;\, k \neq j \rangle$ by replacing each element of the Gröbner basis with a remainder of it on division by the other nonzero elements and by repeating this process until it stabilises. Such a Gröbner basis is called a *pseudo-reduced Gröbner basis*.

The syzygy algorithm for terms

This algorithm takes also place in Context 2.1 for $\mathbf{R}$. Note however that the divisibility test is not used here; only the zero test is used. It has the following goal.

Input terms $T_1, \ldots, T_p \in \mathbf{H}_m$.
Output a generating system $(\mathrm{S}_{i,j})_{1 \leq i \leq j \leq p, \operatorname{LPos}(T_j) = \operatorname{LPos}(T_i)}$ for $\operatorname{Syz}(T_1, \ldots, T_p)$.

In this algorithm, $(\epsilon_1, \ldots, \epsilon_p)$ is the canonical basis of $\mathbf{R}[\underline{X}]^p$.

Syzygy algorithm for terms 2.7.

```
1  local variables i, j : {1, ..., p} ,  J : subset of {1, ..., p} ,
2                  a, b : R ,  α, β : N^n ;
3  for i from 1 to p do
4    J ← { j ≥ i ; LPos(T_j) = LPos(T_i) } ;
5    for j in J do
6      compute b X^β, a X^α such that S(T_i, T_j) = b X^β T_i − a X^α T_j
7                by Algorithm 2.4 ;
8      S_{i,j} ← b X^β ε_i − a X^α ε_j
9    od
10 od
```

Schreyer's syzygy algorithm

This algorithm takes also place in Context 2.1 for $\mathbf{R}$. It has the following goal.

Input a Gröbner basis $(g_1, \ldots, g_p)$ for a submodule of $\mathbf{H}_m$.
Output a Gröbner basis $(u_{i,j})_{1 \leq i \leq j \leq p, \operatorname{LPos}(g_j) = \operatorname{LPos}(g_i)}$ for $\operatorname{Syz}(g_1, \ldots, g_p)$ w.r.t. Schreyer's monomial order induced by $>$ and $(g_1, \ldots, g_p)$.

In this algorithm, $(\epsilon_1, \ldots, \epsilon_p)$ is the canonical basis of $\mathbf{R}[\underline{X}]^p$.

Schreyer's syzygy algorithm 2.8.

```
1  local variables i, j : {1, ..., p}, J : subset of {1, ..., p},
2                  a, b : R, α, β : N^n, q_ℓ : R[X];
3  for i from 1 to p do
4    J ← { j ≥ i ; LPos(g_j) = LPos(g_i) };
5    for j in J do
6      compute bX^β, aX^α such that S(g_i, g_j) = bX^β g_i − aX^α g_j
7              by Algorithm 2.4;
8      compute q_1, ..., q_p such that
9        S(g_i, g_j) = q_1 g_1 + ··· + q_p g_p by Algorithm 2.3 (note that
10         LM(S(g_i, g_j)) ≥ LM(q_ℓ) LM(g_ℓ) whenever q_ℓ ≠ 0);
11     u_{i,j} ← bX^β ε_i − aX^α ε_j − q_1 ε_1 − ··· − q_p ε_p
12   od
13 od
```

The polynomials $q_1, \dots, q_p$ of lines 8–10 may have been computed while constructing the Gröbner basis.

Remark 2.9. For an arbitrary system of generators $(h_1, \dots, h_r)$ for a submodule U of $\mathbf{H}_m$, the syzygy module of $(h_1, \dots, h_r)$ is easily obtained from the syzygy module of a Gröbner basis for U (see [19, Theorem 296]).

3 The algorithms in the case of a valuation ring

This is the case of a local Bézout ring. We consider a coherent valuation ring $\mathbf{R}$ with a divisibility test. In this case, we get simplified versions of the algorithms given in Section 2. We recover the algorithms given in [16, 19], but for modules instead of ideals. In particular, we generalise Buchberger's algorithm to convenient valuation rings and modules. Note that the algorithm given in [16] contains a bug which is corrected in the corrigendum [17] to the papers [10, 16].

Division algorithm 3.1 (see [19, Definition 226])**.** Let $\mathbf{R}$ be a valuation ring with a divisibility test. In the Division algorithm 2.3, instead of defining the set D and finding the gcd d, one may look out for the first $\mathrm{LT}(h_i)$ such that $\mathrm{LT}(h_i)$ divides $\mathrm{LT}(h')$; in case of success, the algorithm proceeds with this index i, and the Bézout identity of line 7 is not needed.

```
1  local variables i : {1, ..., p}, c : R, h' : H_m, notdiv : boolean;
2  q_1 ← 0; ... ; q_p ← 0; r ← 0; h' ← h;
```

```
3  while h' ≠ 0 do
4    i ← 1;
5    notdiv ← true;
6    while i ≤ p and notdiv do
7      if LT(h_i) | LT(h') then
8        find c such that c LC(h_i) = LC(h');
9        q_i ← q_i + c(LM(h')/LM(h_i));
10       h' ← h' − c(LM(h')/LM(h_i))h_i;
11       notdiv ← false
12     else
13       i ← i + 1
14     fi
15   od;
16   if notdiv then
17     r ← r + LT(h');
18     h' ← h' − LT(h')
19   fi
20 od
```

S-polynomial algorithm 3.2 (see [19, Definition 229])**.** Let $\mathbf{R}$ be a coherent valuation ring. We define the *S-polynomial* of two nonzero vectors in $\mathbf{H}_m$ by the S-polynomial algorithm 2.4. In this algorithm, the finding of a, b in lines 10-13 will take the following simple form, typical for valuation rings:

find a, b **such that**
$a\,\mathrm{LC}(g) = b\,\mathrm{LC}(f)$ with $a = 1$ or $b = 1$

This does not rely on the divisibility test: the explicit disjunction "a divides b or b divides a" is sufficient. When we have a divisibility test, the following expression arises for $\mathrm{S}(f, g)$ with $f \neq g$, $\mathrm{LPos}(f) = \mathrm{LPos}(g)$, $\mathrm{mdeg}(f) = \mu$, $\mathrm{mdeg}(g) = \nu$:

$$\mathrm{S}(f,g) = \begin{cases} \underline{X}^{(\nu-\mu)^+} f - a\underline{X}^{(\mu-\nu)^+} g & \text{if } \mathrm{LC}(g) \mid \mathrm{LC}(f), \text{ where } \mathrm{LC}(f) = a\,\mathrm{LC}(g) \\ b\underline{X}^{(\nu-\mu)^+} f - \underline{X}^{(\mu-\nu)^+} g & \text{otherwise, where } b\,\mathrm{LC}(f) = \mathrm{LC}(g). \end{cases}$$

Note also that the annihilator $\mathrm{Ann}(\mathrm{LC}(f))$ appearing in the computation of the auto-S-polynomial is principal because $\mathbf{R}$ is a coherent valuation ring: there is a b such that $\mathrm{Ann}(\mathrm{LC}(f)) = b\mathbf{R}$ (b being defined up to a unit, see [11, Exercise IX-7]).

Example 3.3 (S-polynomials over $\mathbf{R} = \mathbb{F}_2[Y]/\langle Y^r\rangle$, $r \geq 2$, a generalisation of [19, Example 231]). The ring $\mathbf{R} = \mathbb{F}_2[Y]/\langle Y^r\rangle = \mathbb{F}_2[y]$ (where

$y = \overline{Y}$) is a zero-dimensional coherent valuation ring with nonzero zerodivisors ($\mathrm{Ann}(y^k) = \langle y^{r-k}\rangle$). Each nonzero element a of this ring may be written in a unique way as $y^k(1+yb)$ with $k = 0, \dots, r-1$ and $1+yb$ a unit. Let $f \neq g \in \mathbf{R}[\underline{X}]\setminus\{0\}$ and $\mu = \mathrm{mdeg}(f)$, $\nu = \mathrm{mdeg}(g)$. If $\mathrm{LC}(g) = y^k(1+yb)$ and $\mathrm{LC}(f) = y^\ell(1+yc)$, then

$$\mathrm{S}(f,g) = \begin{cases} \underline{X}^{(\nu-\mu)^+} f - (1+yc)(1+yb)^{-1}y^{\ell-k}\underline{X}^{(\mu-\nu)^+} g & \text{if } k \le \ell \\ (1+yb)(1+yc)^{-1}y^{k-\ell}\underline{X}^{(\nu-\mu)^+} f - \underline{X}^{(\mu-\nu)^+} g & \text{if } k > \ell \end{cases}$$
$$\underset{\text{up to a unit}}{=} \begin{cases} (1+yb)\underline{X}^{(\nu-\mu)^+} f - (1+yc)y^{\ell-k}\underline{X}^{(\mu-\nu)^+} g & \text{if } k \le \ell \\ (1+yb)y^{k-\ell}\underline{X}^{(\nu-\mu)^+} f - (1+yc)\underline{X}^{(\mu-\nu)^+} g & \text{if } k > \ell. \end{cases}$$

For the computation of the auto-S-polynomial $\mathrm{S}(f,f)$, two cases may arise:

- If $\mathrm{LC}(f)$ is a unit, then $\mathrm{S}(f,f) = 0$.
- If $\mathrm{LC}(f)$ is y^k ($k > 0$) up to a unit, then $\mathrm{S}(f,f) = y^{r-k}f$.

E.g., with $r = 2$, using the lexicographic order for which $X_2 > X_1$ and considering the polynomials $f = yX_2 + X_1$ and $g = yX_1 + y$, we have:

$$\mathrm{S}(f,g) = X_1 f - X_2 g = X_1^2 + yX_2,\ \ \mathrm{S}(f,f) = yf = yX_1,\ \ \mathrm{S}(g,g) = yg = 0.$$

4 Termination of Buchberger's algorithm for a Bézout ring

The following lemma provides a necessary and sufficient condition for a term to belong to a module generated by terms over a coherent strict Bézout ring with a divisibility test.

Lemma 4.1 (Term modules, see [19, Lemma 227])**.** *Let $\mathbf{R}$ be a coherent strict Bézout ring with a divisibility test. Let U be a submodule of $\mathbf{H}_m$ generated by a finite collection of terms $a_\alpha \underline{X}^\alpha e_{i_\alpha}$ with $\alpha \in A$. A term $b\underline{X}^\beta e_r$ lies in U iff there is a nonempty subset A' of A such that $\underline{X}^\alpha e_{i_\alpha}$ divides $\underline{X}^\beta e_r$ for every $\alpha \in A'$ (i.e. $i_\alpha = r$ and $\underline{X}^\alpha \mid \underline{X}^\beta$) and $\gcd_{\alpha\in A'}(a_\alpha)$ divides b. In the local case, there hence is an a_α with $\alpha \in A'$ that divides b.*

Proof. The condition is clearly sufficient. For the necessity, write

$$b\underline{X}^\beta e_r = \sum\nolimits_{\alpha\in\tilde{A}} c_\alpha a_\alpha \underline{X}^{\gamma_\alpha}\underline{X}^\alpha e_{i_\alpha}$$

with $\tilde{A} \subseteq A$, $c_\alpha \in \mathbf{R}\setminus\{0\}$, and $\underline{X}^{\gamma_\alpha} \in \mathbb{M}_n$. Then $b = \sum_{\alpha\in A'} c_\alpha a_\alpha$, where A' is the set of those α such that $\gamma_\alpha + \alpha = \beta$ and $i_\alpha = r$. For each $\alpha \in A'$, $\underline{X}^\alpha$

divides $\underline{X}^{\beta}$. Since the gcd of the a_α's with $\alpha \in A'$ divides every a_α, it also divides b. □

The following lemma is a key result for the characterisation of Gröbner bases by means of S-polynomials: see [6, Chapter 2, §6, Lemma 5] and, for valuation rings, [19, Lemma 233, adding the hypothesis of coherence].

Lemma 4.2. *Let* $\mathbf{R}$ *be a coherent strict Bézout ring and* $f_1, \dots, f_p \in \mathbf{H}_m \setminus \{0\}$ *with the same leading monomial* M*. Let* $c_1, \dots, c_p \in \mathbf{R}$*. If* $c_1 f_1 + \cdots + c_p f_p$ *vanishes or has leading monomial* $< M$*, then* $c_1 f_1 + \cdots + c_p f_p$ *is a linear combination with coefficients in* $\mathbf{R}$ *of the S-polynomials* $\mathrm{S}(f_i, f_j)$ *with* $1 \le i \le j \le p$*.*

Proof. Let us write, for $j \neq i$, $\mathrm{LC}(f_j) = d_{i,j} a_{i,j}$ with $d_{i,j} = \gcd(\mathrm{LC}(f_i), \mathrm{LC}(f_j))$, so that $\gcd(a_{i,j}, a_{j,i}) = 1$ and $\mathrm{S}(f_i, f_j) = a_{i,j} f_i - a_{j,i} f_j$. For each permutation $i_1, \dots, i_p$ of $1, \dots, p$, we shall transform the sum $a_{i_1,i_2} \cdots a_{i_{p-1},i_p}(c_1 f_1 + \cdots + c_p f_p)$ by replacing successively

$$\begin{aligned} a_{i_1,i_2} f_{i_1} \quad & \text{by } \mathrm{S}(f_{i_1}, f_{i_2}) + a_{i_2,i_1} f_{i_2}, \\ \vdots \quad & \qquad \vdots \\ a_{i_{p-1},i_p} f_{i_{p-1}} \quad & \text{by } \mathrm{S}(f_{i_{p-1}}, f_{i_p}) + a_{i_p,i_{p-1}} f_{i_p}. \end{aligned}$$

At the end, the sum will be a linear combination of $\mathrm{S}(f_{i_1}, f_{i_2})$, $\mathrm{S}(f_{i_2}, f_{i_3})$, …, $\mathrm{S}(f_{i_{p-1}}, f_{i_p})$, and f_{i_p}; let z be the coefficient of f_{i_p} in this combination. The sum as well as each of the S-polynomials vanish or have leading monomial $< M$, so that the hypothesis yields $z\,\mathrm{LC}(f_{i_p}) = 0$; therefore $z f_{i_p}$ is a multiple of $\mathrm{S}(f_{i_p}, f_{i_p})$.

It remains to obtain a Bézout identity w.r.t. the products $a_{i_1,i_2} \cdots a_{i_{p-1},i_p}$, because it yields an expression of $c_1 f_1 + \cdots + c_p f_p$ as a linear combination of the required form. For this, it is enough to develop the product of the $\binom{s}{2}$ Bézout identities w.r.t. $a_{i,j}$ and $a_{j,i}$, $1 \le i < j \le p$: this yields a sum of products of $\binom{s}{2}$ terms, each of which is either $a_{i,j}$ or $a_{j,i}$, $1 \le i < j \le p$, so that it is indexed by the tournaments on the vertices $1, \dots, p$; every such product contains a product of the above form $a_{i_1,i_2} \cdots a_{i_{p-1},i_p}$ because every tournament contains a hamiltonian path (see [14]). □

Remark 4.3. The above proof results from an analysis of the following proof in the case where $\mathbf{R}$ is local and $m = 1$, which entails in fact the general case. Since $\mathbf{R}$ is a valuation ring, we may consider a permutation $i_1, \dots, i_p$ of $1, \dots, p$ such that $\mathrm{LC}(f_{i_p}) \mid \mathrm{LC}(f_{i_{p-1}}) \mid \cdots \mid \mathrm{LC}(f_{i_1})$. Thus $\mathrm{S}(f_{i_1}, f_{i_2}) = f_{i_1} - a_{i_2,i_1} f_{i_2}, \dots, \mathrm{S}(f_{i_{p-1}}, f_{i_p}) = f_{i_{p-1}} - a_{i_p,i_{p-1}} f_{i_p}$ for some $a_{i_2,i_1}, \dots, a_{i_p,i_{p-1}}$. Then, by replacing successively f_{i_k} by $\mathrm{S}(f_{i_k}, f_{i_{k+1}}) + a_{i_{k+1},i_k} f_{i_{k+1}}$, the linear

combination $c_1 f_1 + \cdots + c_p f_p$ may be rewritten as a linear combination of $\mathrm{S}(f_{i_1}, f_{i_2})$, …, $\mathrm{S}(f_{i_{p-1}}, f_{i_p})$, and f_{i_p}, with the coefficient of f_{i_p} turning out to lie in $\mathrm{Ann}(\mathrm{LC}(f_{i_p}))$.

Lemma 4.2 enables us to generalise some classical results on the existence and characterisation of Gröbner bases to the case of coherent strict Bézout rings with a divisibility test. See [19, Theorem 234] for the case of valuation rings and ideals.

Theorem 4.4 (Buchberger's criterion for Gröbner bases)**.** *Let* $\mathbf{R}$ *be a coherent strict Bézout ring with a divisibility test and* $U = \langle g_1, \ldots, g_p \rangle$ *a nonzero submodule of* $\mathbf{H}_m$*. Then* $G = (g_1, \ldots, g_p)$ *is a Gröbner basis for* U *iff the remainder of* $\mathrm{S}(g_i, g_j)$ *on division by* G *vanishes for all pairs* $i \leq j$*.*

Theorem 4.4 entails that Buchberger's algorithm 2.5 constructs a Gröbner basis for finitely generated ideals of coherent valuation rings with a divisibility test when such a basis exists (compare [19, Algorithm 235]). The two following theorems provide a general explanation for the termination of Buchberger's algorithm and are therefore pivotal.

Theorem 4.5 (Termination of Buchberger's algorithm, case $m = 1$)**.** *Let* $\mathbf{R}$ *be a coherent valuation ring with a divisibility test,* I *a nonzero finitely generated ideal of* $\mathbf{R}[\underline{X}]$*, and* $>$ *a monomial order on* $\mathbf{R}[\underline{X}]$*. If* $\mathrm{LT}(I)$ *is finitely generated, then Buchberger's algorithm 2.5 computes a finite Gröbner basis for* I*.*

Proof. Let $f_1, \ldots, f_p \in \mathbf{R}[\underline{X}] \setminus \{0\}$ be generators of I. Let $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r) \rangle$ with $g_i \in I \setminus \{0\}$. Let $1 \leq k \leq r$. As $g_k \in I$, there exist $E \subseteq \{1, \ldots, p\}$ and $h_i \in \mathbf{R}[\underline{X}] \setminus \{0\}$, $i \in E$, such that

$$g_k = \sum\nolimits_{i \in E} h_i f_i \tag{4.1}$$

with $\mathrm{mdeg}(g_k) \leq \sup_{i \in E}(\mathrm{mdeg}(M_i N_i)) =: \gamma$ (we call it the *multidegree of the expression* (4.1) for g_k w.r.t. the generating set $\{f_1, \ldots, f_p\}$ of I), where $M_i = \mathrm{LM}(h_i)$ and $N_i = \mathrm{LM}(f_i)$. Let $F = \{\, i \in E \,;\, \mathrm{mdeg}(M_i N_i) = \gamma \,\}$.

Case 1: $\mathrm{mdeg}(g_k) = \gamma$, say $\mathrm{mdeg}(g_k) = \mathrm{mdeg}(M_{i_0} N_{i_0})$ for some $i_0 \in F$. As the leading coefficients of the $h_i f_i$'s with $i \in F$ are comparable w.r.t. division, we can suppose that all of them are divisible by the leading coefficient of $h_{i_0} f_{i_0}$. It follows that $\mathrm{LT}(g_k) \in \langle \mathrm{LT}(f_{i_0}) \rangle \subseteq \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_p) \rangle$.

Case 2: $\mathrm{mdeg}(g_k) < \gamma$. We have

$$\begin{aligned} g_k &= \sum\nolimits_{i \notin F} h_i f_i + \sum\nolimits_{i \in F} h_i f_i \\ &= \sum\nolimits_{i \notin F} h_i f_i + \sum\nolimits_{i \in F} (h_i - \mathrm{LT}(h_i)) f_i + \sum\nolimits_{i \in F} \mathrm{LT}(h_i) f_i. \end{aligned}$$

Letting $c_i = \mathrm{LC}(h_i)$, we get

$$\mathrm{mdeg}\big(\sum\nolimits_{i\in F} c_i M_i f_i\big) < \gamma.$$

By virtue of Lemma 4.2, there exists a finite family $(a_{i,j})$ of elements of $\mathbf{R}$ such that

$$\sum\nolimits_{i\in F} c_i M_i f_i = \sum\nolimits_{i\le j\in F} a_{i,j}\mathrm{S}(M_i f_i, M_j f_j).$$

But, for $i \le j \in F$, letting $N_{i,j} = \mathrm{lcm}(N_i, N_j)$ and writing $\mathrm{S}(f_i, f_j) = a\frac{N_{i,j}}{N_i} f_i + b\frac{N_{i,j}}{N_j} f_j$ for some a, $b \in \mathbf{R}$, we have $\mathrm{S}(M_i f_i, M_j f_j) = a\frac{X^\gamma}{M_i N_i} M_i f_i + b\frac{X^\gamma}{M_j N_j} M_j f_j = \frac{X^\gamma}{N_{i,j}}\mathrm{S}(f_i, f_j)$. It follows that

$$\sum\nolimits_{i\in F} c_i M_i f_i = \sum\nolimits_{i\le j\in F} a_{i,j} m_{i,j}\mathrm{S}(f_i, f_j),$$

where the $m_{i,j}$'s are monomials. Thus we obtain another expression for g_k,

$$g_k = \sum\nolimits_{i\notin F} h_i f_i + \sum\nolimits_{i\in F}(h_i - \mathrm{LT}(h_i)) f_i + \sum\nolimits_{i\le j\in F} a_{i,j} m_{i,j}\mathrm{S}(f_i, f_j),$$

and the multidegree of this expression, now w.r.t. the generating set of I obtained by adding the elements $\mathrm{S}(f_i, f_j)$, $i \le j \in F$, to the $f_1, \dots, f_p$, is $< \gamma$. Reiterating this, we end up with a situation like that of Case 1 for all the g_k's because the set of monomials is well-ordered. So we reach the termination condition in Algorithm 2.5 after a finite number of steps. □

Theorem 4.6 (Termination of Buchberger's algorithm)**.** *Let* $\mathbf{R}$ *be a coherent strict Bézout ring with a divisibility test and* U *a nonzero finitely generated submodule of* $\mathbf{H}_m$*. If* $\mathrm{LT}(U)$ *is finitely generated, then Buchberger's algorithm 2.5 computes a Gröbner basis for* U*.*

Proof. It suffices to prove the result when $\mathbf{R}$ is local and $m = 1$, in which case this is Theorem 4.5. Let us explain in a few words how to pass from the local to the global case (compare [19, Section 3.3.11] and [9]). Suppose that we are computing $\mathrm{S}(f, g)$ and that the leading coefficients a and b of f and g are uncomparable under division. A key fact is that if we write $a = \gcd(a, b)\, a'$, $b = \gcd(a, b)\, b'$ with $\gcd(a', b') = 1$, then a divides b in $\mathbf{R}[\frac{1}{a'}]$, b divides a in $\mathbf{R}[\frac{1}{b'}]$, and the two multiplicative subsets $a'^{\mathbb{N}}$ and $b'^{\mathbb{N}}$ are comaximal because $1 \in \langle a', b'\rangle$. Then $\mathbf{R}$ splits into $\mathbf{R}[\frac{1}{a'}]$ and $\mathbf{R}[\frac{1}{b'}]$, and we can continue as if $\mathbf{R}$ were a valuation ring. If $\mathrm{mdeg}(f) = \mu$ and $\mathrm{mdeg}(g) = \nu$, then $\mathrm{S}(f, g)$ is being computed as follows:

- in the ring $\mathbf{R}[\frac{1}{b'}]$, $\mathrm{S}(f, g) = X^{(\nu-\mu)^+} f - \frac{a'}{b'} X^{(\mu-\nu)^+} g =: S_1$;

- in the ring $\mathbf{R}[\frac{1}{a'}]$, $\mathrm{S}(f,g) = \frac{b'}{a'}X^{(\nu-\mu)^+}f - X^{(\mu-\nu)^+}g =: S_2$.

But, letting $\mathrm{S} := b'X^{(\nu-\mu)^+}f - a'X^{(\mu-\nu)^+}g$, we have

$$\mathrm{S} = b'S_1 = a'S_2.$$

As S is equal to S_1 up to a unit in $\mathbf{R}[\frac{1}{b'}]$, and to S_2 in $\mathbf{R}[\frac{1}{a'}]$, it can replace both of them, and thus there was no need to open the two branches $\mathbf{R}[\frac{1}{a'}]$ and $\mathbf{R}[\frac{1}{b'}]$. □

When is a valuation ring a Gröbner ring?

We recall here some results given in [19] on the interplay between the concepts of Gröbner ring, Krull dimension, and archimedeanity; here are the relevant definitions.

Definition 4.7.

- The (Jacobson) *radical* $\mathrm{Rad}(\mathbf{R})$ of an arbitrary ring $\mathbf{R}$ is the ideal $\{\, a \in \mathbf{R} \,;\, 1 + a\mathbf{R} \subseteq \mathbf{R}^\times \,\}$, where $\mathbf{R}^\times$ is the unit group of $\mathbf{R}$.

- The *residual field* of a local ring $\mathbf{R}$ is the quotient $\mathbf{R}/\mathrm{Rad}(\mathbf{R})$. The local ring $\mathbf{R}$ is *residually discrete* if its residual field is discrete: this means that $x \in \mathbf{R}^\times$ is decidable. A nontrivial local ring $\mathbf{R}$ is residually discrete iff it is the disjoint union of $\mathbf{R}^\times$ and $\mathrm{Rad}(\mathbf{R})$.

- A residually discrete valuation ring $\mathbf{R}$ is *archimedean* if

$$\forall a, b \in \mathrm{Rad}(\mathbf{R}) \setminus \{0\} \;\; \exists k \in \mathbb{N} \;\; a \mid b^k.$$

- A strongly discrete ring $\mathbf{R}$ is a *Gröbner ring* if for every $n \in \mathbb{N}$ and every finitely generated ideal I of $\mathbf{R}[\underline{X}]$ endowed with the lexicographic monomial order, the module $\mathrm{LT}(I)$ is finitely generated as well.

One sees easily that a Gröbner ring is coherent ([19, Proposition 224]). Moreover if $\mathbf{R}$ is Gröbner, then so is $\mathbf{R}[Y]$.

For a coherent valuation ring with a divisibility test, it is proved in [19] that archimedeanity is equivalent to being a Gröbner ring (at least when we assume that there is no nonzero zerodivisor or there exists a nonzero zerodivisor, see [19, Theorem 272]). For a valuation domain with a divisibility test, it is proved that the condition is equivalent to having Krull dimension ≤ 1 ([19, Theorem 256]). This implies that a strongly discrete Prüfer domain is Gröbner iff it has Krull dimension ≤ 1 ([18, Corollary 6]). This applies to Bézout domains with a divisibility test. When a coherent valuation ring with

a divisibility test has a nonzero zerodivisor, it is proved that archimedeanity is equivalent to being zero-dimensional ([19, Proposition 265]).

Let us now, for the comfort of the reader, provide simple arguments for some of these results. Recall that a ring $\mathbf{R}$ has Krull dimension ≤ 1 if, given $a, b \in \mathbf{R}$,

$$\exists k, \ell \in \mathbb{N}\ \exists x, y \in \mathbf{R}\quad b^\ell(a^k(ax-1)+by)=0; \tag{4.2}$$

when b is regular and $a \in \mathrm{Rad}(\mathbf{R})$, we get that $a^k = zb$ for some k and some z. This shows that a valuation domain of Krull dimension ≤ 1 is archimedean. Conversely, an equality $a^k = zb$ is a particularly simple case of (4.2) (take $x = 0$). Also, when a is invertible, one has $ax - 1 = 0$ for some x, which is also a form of (4.2). So, if in a local ring the disjunction "x is invertible or $x \in \mathrm{Rad}(\mathbf{R})$" is explicit (i.e. if the residual field is discrete), then archimedeanity implies Krull dimension ≤ 1. Summing up, an archimedean valuation ring with a divisibility test has Krull dimension ≤ 1, and a valuation domain with Krull dimension ≤ 1 is archimedean: so a valuation domain is archimedean iff it has Krull dimension ≤ 1.

Recall now that for a local ring, being zero-dimensional means that every element is invertible or nilpotent. Let us consider a valuation ring with a divisibility test containing a nonzero zerodivisor x. We have $xy = 0$ with $y \neq 0$. If $x = yz$, then $y^2z = 0$, so that $x^2 = 0$. If $y = xz$, then $y^2 = 0$. So we have a nonzero nilpotent element u. In this case archimedeanity is equivalent to being zero-dimensional. Indeed, assume first archimedeanity. For an $a \in \mathrm{Rad}(\mathbf{R})$, we have $u \mid a^k$, so $a^{2k} = 0$. Then assume zero-dimensionality. For any $a, b \in \mathrm{Rad}(\mathbf{R})$, we have a k such that $a^k = 0$, so $b \mid a^k$.

So, for a coherent valuation ring with a divisibility test, if 0 is the unique zerodivisor, archimedeanity is equivalent to having dimension ≤ 1, and if $\mathbf{R}$ has a nonzero zerodivisor, archimedeanity is equivalent to being zero-dimensional.

Now assume that $\mathbf{R}$ is a coherent valuation ring with a divisibility test. We first compute $(c : d)$ when $c, d \neq 0$. We note that $(c : d) = \langle u \rangle$ for some u (since it is finitely generated). If $c \mid d$, then $(c : d) = \langle 1 \rangle$. If $d \mid c$, then we have a y with $c = dy$. So $y \in \langle u \rangle$, say $y = tu$. Since $u \in (c : d)$, we have a z with $du = cz = dyz = dutz$. So $du(1 - tz) = 0$. If $1 - tz$ is invertible, then $du = 0$, so that $c = dy = dut = 0$, which is impossible. So tz is invertible and $\langle u \rangle = \langle y \rangle$: more precisely $u = yt'$ with t' invertible.

Now let $a, b \in \mathrm{Rad}(\mathbf{R}) \setminus \{0\}$. We show that $(b : a^\infty)$ is finitely generated iff $b \mid a^k$ for some k. If $a^k = bx$ then $(b : a^k) = \langle 1 \rangle$, so $(b : a^\infty) = \langle 1 \rangle$. If $(b : a^\infty)$ is finitely generated, then we have a k such that $(b : a^k) = (b : a^{k+1})$. If $b \mid a^k$ or $b \mid a^{k+1}$, then we are done. The other case ($a^k \mid b$ and $a^{k+1} \mid b$) is

impossible, for if we have x, y such that $b = a^k x = a^{k+1} y = a^k(ay)$, then

$$\langle y \rangle = (b : a^{k+1}) = (b : a^k) = \langle x \rangle = \langle ay \rangle,$$

so that $y = uay$ and $(1 - ua)y = 0$ for some u; since $a \in \mathrm{Rad}(\mathbf{R})$, $1 - ua$ is invertible, so that $y = 0$, which implies $b = 0$, a contradiction.

We have shown that $\mathbf{R}$ is archimedean iff $(b : a^\infty)$ is finitely generated for all $a, b \in \mathrm{Rad}(\mathbf{R}) \setminus \{0\}$.

We note also that for an arbitrary commutative ring $\mathbf{R}$, one has

$$\forall a, b \in \mathbf{R}\ \langle 1 + bY, a \rangle \cap \mathbf{R} = (b : a^\infty).$$

So a coherent valuation ring $\mathbf{R}$ with a divisibility test is archimedean iff the ideal $\langle 1 + bY, a \rangle \cap \mathbf{R}$ is finitely generated for all $a, b \in \mathbf{R}$. This condition is fulfilled as soon as $\mathbf{R}$ is 1-Gröbner (i.e. satisfies the definition of Gröbner rings with $n = 1$).

For other details on this topic see [19, Exercise 372 p. 207, solution p. 221, Exercise 387 p. 218, solution p. 251].

5 The syzygy theorem and Schreyer's algorithm for a valuation ring

In the book *Gröbner bases in commutative algebra*, Ene and Herzog propose the following exercise.

Problem ([8, Problem 4.11, p. 81])**.** Let $>$ be a monomial order on the free S-module $F = \bigoplus_{j=1}^m Se_j$ [where $S = \mathbf{K}[\underline{X}]$ with $\mathbf{K}$ a discrete field], let $U \subset F$ be a submodule of F, and suppose that $\mathrm{LT}(U) = \bigoplus_{j=1}^m I_j e_j$. Show that U is a free S-module iff I_j is a principal ideal for $j = 1, \ldots, m$.

It is obvious that this condition is sufficient. Unfortunately, it is not necessary as shows the following example, so that the statement of [8, Problem 4.11] is not correct.

Example 5.1. Let $>$ be a TOP monomial order on $\mathbf{K}[X, Y]^2$ for which $Y > X$, $\mathbf{K}$ being a field, let $e_1 = (1, 0)$ and $e_2 = (0, 1)$, and consider the free submodule U of $\mathbf{K}[X, Y]^2$ generated by $u_1 = (Y, X)$ and $u_2 = (X, 0)$. Then $\mathrm{LT}(u_1) = Ye_1$, $\mathrm{LT}(u_2) = Xe_1$, $\mathrm{S}(u_1, u_2) = Xu_1 - Yu_2 = X^2 e_2 =: u_3$, and $\mathrm{S}(u_1, u_3) = \mathrm{S}(u_2, u_3) = 0$. It follows that (u_1, u_2, u_3) is a Gröbner basis for U, and $\mathrm{LT}(U) = \langle Y, X \rangle e_1 \oplus \langle X^2 \rangle e_2$. One can see that $\langle Y, X \rangle$ is not principal and $\mathrm{LT}(U)$ is not free, while U is free.

So we content ourselves with the following observation.

Remark 5.2. Let $>$ be a monomial order on the free S-module $F = \bigoplus_{j=1}^m Se_j$, where $S = \mathbf{R}[\underline{X}]$ and $\mathbf{R}$ is a valuation domain. Let U be a submodule of F and suppose that $\mathrm{LT}(U) = \bigoplus_{j=1}^m I_j e_j$, where I_j is a principal ideal for $j = 1, \ldots, m$. Then $\mathrm{LT}(U)$ and U are free S-modules. (Of course, this is not true anymore if $\mathbf{R}$ is a valuation ring with nonzero zerodivisors. Consider e.g. the ideal $U = \langle 8X + 2\rangle$ in $(\mathbb{Z}/16\mathbb{Z})[X]$: we have $\mathrm{LT}(U) = \langle 2\rangle$ (so that it is principal), but U is not free since $8U = \langle 0\rangle$.)

We shall need the following proposition, which generalises [19, Theorem 291] to the case of modules.

Proposition 5.3 (Generating set for the syzygy module of a list of terms for a coherent valuation ring)**.** *Let* $\mathbf{R}$ *be a coherent valuation ring,* $\mathbf{H}_m$ *a free* $\mathbf{R}[\underline{X}]$*-module with basis* $(e_1, \ldots, e_m)$*, and terms* $T_1, \ldots, T_p$ *in* $\mathbf{H}_m$*. Considering the canonical basis* $(\epsilon_1, \ldots, \epsilon_p)$ *of* $\mathbf{R}[\underline{X}]^p$*, the syzygy module* $\mathrm{Syz}(T_1, \ldots, T_p)$ *is generated by the*

$$\mathrm{S}_{i,j} \in \mathbf{R}[\underline{X}]^p \text{ with } 1 \le i \le j \le p \text{ and } \mathrm{LPos}(T_i) = \mathrm{LPos}(T_j),$$

as computed by the Syzygy algorithm for terms 2.7.

Note that in the Syzygy algorithm for terms 2.7, the a, b will be found as in the S-polynomial algorithm 3.2, so that we get

$$\mathrm{S}_{i,j} = \begin{cases} b\epsilon_i & \text{if } i = j, \text{ where } \langle b\rangle = \mathrm{Ann}(\mathrm{LC}(T_i)), \\ \underline{X}^{\beta}\epsilon_i - a\underline{X}^{\alpha}\epsilon_j & \text{if } i < j \text{ and } \mathrm{LC}(T_i) = a\,\mathrm{LC}(T_j), \text{ else} \\ b\underline{X}^{\beta}\epsilon_i - \underline{X}^{\alpha}\epsilon_j & \text{if } i < j \text{ and } b\,\mathrm{LC}(T_i) = \mathrm{LC}(T_j). \end{cases} \tag{5.1}$$

Here $\beta = (\mathrm{mdeg}(T_j) - \mathrm{mdeg}(T_i))^+$ and $\alpha = (\mathrm{mdeg}(T_i) - \mathrm{mdeg}(T_j))^+$.

Now we shall follow closely Schreyer's ingenious proof [15] of Hilbert's syzygy theorem via Gröbner bases, but with a valuation ring instead of a field. Schreyer's proof is very well explained in [8, §§ 4.4.1–4.4.3].

Theorem 5.4 (Schreyer's algorithm for a coherent valuation ring with a divisibility test)**.** *Let* $\mathbf{R}$ *be a coherent valuation ring with a divisibility test. Let* U *be a submodule of* $\mathbf{H}_m$ *with Gröbner basis* $(g_1, \ldots, g_p)$*. Then the relations* $u_{i,j}$ *computed by Schreyer's syzygy algorithm 2.8 form a Gröbner basis for the syzygy module* $\mathrm{Syz}(g_1, \ldots, g_p)$ *w.r.t. Schreyer's monomial order induced by* $>$ *and* $(g_1, \ldots, g_p)$*. Moreover, for* $1 \le i \le j \le p$ *such that* $\mathrm{LPos}(g_i) = \mathrm{LPos}(g_j)$*,*

$$\mathrm{LT}(u_{i,j}) = \begin{cases} b\epsilon_i & \text{if } i = j, \text{ with } \langle b\rangle = \mathrm{Ann}(\mathrm{LC}(g_i)), \\ \underline{X}^{\beta}\epsilon_i & \text{if } i < j \text{ and } \mathrm{LC}(g_j) \mid \mathrm{LC}(g_i), \text{ else} \\ b\underline{X}^{\beta}\epsilon_i & \text{if } i < j \text{ and } b\,\mathrm{LC}(g_i) = \mathrm{LC}(g_j), \end{cases} \tag{5.2}$$

with $\beta = (\mathrm{mdeg}(g_j) - \mathrm{mdeg}(g_i))^+$.

Proof (a slight modification of the proof of [8, Theorem 4.16]). Let us use the notation of Schreyer's syzygy algorithm 2.8. Let $1 \leq i = j \leq p$. As $\mathrm{LM}(q_\ell)\,\mathrm{LM}(g_\ell) \leq \mathrm{LM}(\mathrm{S}(g_i, g_i)) < \mathrm{LM}(g_i)$ whenever $q_\ell \neq 0$, we infer that $\mathrm{LT}(u_{i,i}) = b\epsilon_i$ with $\langle b \rangle = \mathrm{Ann}(\mathrm{LC}(g_i))$.

Let $1 \leq i < j \leq p$ such that $\mathrm{LPos}(g_i) = \mathrm{LPos}(g_j)$. Suppose that $\mathrm{LC}(g_i) = a\,\mathrm{LC}(g_j)$ for an a: as $\mathrm{LM}(\underline{X}^\beta g_i) = \mathrm{LM}(a\underline{X}^\alpha g_j)$ and $i < j$, $\mathrm{LT}(\underline{X}^\beta \epsilon_i - a\underline{X}^\alpha \epsilon_j) = \underline{X}^\beta \epsilon_i$ w.r.t. Schreyer's monomial order induced by $>$, and because $\mathrm{LM}(q_\ell)\,\mathrm{LM}(g_\ell) \leq \mathrm{LM}(\mathrm{S}(g_i, g_j)) < \mathrm{LM}(\underline{X}^\beta g_i)$ whenever $q_\ell \neq 0$, we infer that $\mathrm{LT}(u_{i,j}) = \underline{X}^\beta \epsilon_i$; otherwise, with b such that $b\,\mathrm{LC}(g_i) = \mathrm{LC}(g_j)$, we obtain similarly $\mathrm{LT}(u_{i,j}) = b\underline{X}^\beta \epsilon_i$.

Let Equation (5.1) hold with $T_\ell = \mathrm{LT}(g_\ell)$: then $\mathrm{LT}(u_{i,j}) = \mathrm{LT}(\mathrm{S}_{i,j})$ holds for all $1 \leq i \leq j \leq p$.

Let us show now that the relations $u_{i,j}$ form a Gröbner basis for the syzygy module $\mathrm{Syz}(g_1, \ldots, g_p)$. For this, let $v = \sum_{\ell=1}^{p} v_\ell \epsilon_\ell \in \mathrm{Syz}(g_1, \ldots, g_p)$ and let us show that there exist $1 \leq i \leq j \leq p$ with $\mathrm{LPos}(g_i) = \mathrm{LPos}(g_j)$ such that $\mathrm{LT}(u_{i,j})$ divides $\mathrm{LT}(v)$. Let us write $\mathrm{LM}(v_\ell \epsilon_\ell) = N_\ell \epsilon_\ell$ and $\mathrm{LC}(v_\ell \epsilon_\ell) = c_\ell$ for $1 \leq \ell \leq p$. Then $\mathrm{LM}(v) = N_i \epsilon_i$ for some $1 \leq i \leq p$. Now let $v' = \sum_{\ell \in \mathcal{S}} c_\ell N_\ell \epsilon_\ell$, where $\mathcal{S}$ is the set of those ℓ for which $N_\ell\,\mathrm{LM}(g_\ell) = N_i\,\mathrm{LM}(g_i)$. By definition of Schreyer's monomial order, we have $\ell \geq i$ for all $\ell \in \mathcal{S}$. Substituting each ϵ_ℓ in v' by T_ℓ, the sum becomes zero. Therefore v' is a relation of the terms T_ℓ with $\ell \in \mathcal{S}$. By virtue of Proposition 5.3, v' is an $\mathbf{R}[\underline{X}]$-linear combination of the $\mathrm{S}_{\ell,j}$ with $\ell \leq j$ in $\mathcal{S}$. Taking into consideration Equation (5.1), we infer, by virtue of Lemma 4.1, that $\mathrm{LT}(v')$ is a multiple of $\mathrm{LT}(\mathrm{S}_{i,j})$ for some $j \in \mathcal{S}$. The desired result follows since $\mathrm{LT}(v) = \mathrm{LT}(v')$. □

As a consequence of Theorem 5.4, we obtain the following constructive versions of Hilbert's syzygy theorem for a valuation domain.

Theorem 5.5 (Syzygy theorem for a valuation domain with a divisibility test)**.** *Let $M = \mathbf{H}_m/U$ be a finitely presented $\mathbf{R}[\underline{X}]$-module, where $\mathbf{R}$ is a valuation domain with a divisibility test. Assume that, w.r.t. the TOP lexicographic monomial order, $\mathrm{LT}(U)$ is finitely generated. Then M admits a finite free $\mathbf{R}[\underline{X}]$-resolution*

$$0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

of length $p \leq n + 1$.

Proof. It suffices to prove that U has a free $\mathbf{R}[\underline{X}]$-resolution of length $p \leq n$. Let us use the lexicographic monomial order with $X_n > X_{n-1} > \cdots > X_1$ on $\mathbf{R}[\underline{X}]$. Let $(g_1, \ldots, g_p)$ be a Gröbner basis for U w.r.t. the corresponding TOP order. We can w.l.o.g. suppose that whenever $\mathrm{LM}(g_i)$ and $\mathrm{LM}(g_j)$ involve the

same basis element for some $i < j$, say $\mathrm{LM}(g_i) = N_i\epsilon_k$ and $\mathrm{LM}(g_j) = N_j\epsilon_k$, then $N_i > N_j$. More precisely, whenever $N_i = N_j$, one of $\mathrm{LC}(g_i)$ and $\mathrm{LC}(g_j)$ divides the other, say $\mathrm{LC}(g_j) = b\,\mathrm{LC}(g_i)$, and the corresponding g_j may be reduced into $g_j - bg_i$. In a nutshell, all the possible reductions between the $\mathrm{LT}(g_k)$'s are being exhausted. Now, since we have used the lexicographic order with $X_n > X_{n-1} > \cdots > X_1$, it turns out that the indeterminate X_n cannot appear in the leading terms of the $u_{i,j}$'s in (5.2). Thus, after at most n computations of the iterated syzygies, we reach a situation where none of the indeterminates $X_n, \ldots, X_1$ appears in the leading terms of the computed Gröbner basis for the iterated syzygy module. This implies that the iterated syzygy module is free (as noted in Remark 5.2). □

Remark 5.6. In the proof of this theorem, we need to work with the TOP lexicographic monomial order. We do not know what happens for other monomial orders. This applies also to Theorems 5.9 and 6.2.

Corollary 5.7 (Syzygy theorem for a valuation domain of Krull dimension ≤ 1 with a divisibility test)**.** *Let $M = \mathbf{H}_m/U$ be a finitely presented $\mathbf{R}[\underline{X}]$-module, where $\mathbf{R}$ is a valuation domain of Krull dimension ≤ 1 with a divisibility test. Then M admits a finite free $\mathbf{R}[\underline{X}]$-resolution*

$$0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

of length $p \leq n+1$.

Example 5.8. Let $g_1 = Y^4 - Y$, $g_2 = 2Y$, $g_3 = X^3 - 1 \in \mathbb{Z}_{2\mathbb{Z}}[X, Y]$, and let us use the lexicographic order $>_1$ for which $Y >_1 X$. We have

$$\begin{aligned}
\mathrm{S}(g_1, g_2) &= 2g_1 - Y^3 g_2 = -2Y = -g_2,\\
\mathrm{S}(g_1, g_3) &= X^3 g_1 - Y^4 g_3 = Y^4 - YX^3 = g_1 - Yg_3,\\
\mathrm{S}(g_2, g_3) &= X^3 g_2 - 2Yg_3 = 2Y = g_2.
\end{aligned}$$

Thus (g_1, g_2, g_3) is a (pseudo-reduced) Gröbner basis for $I = \langle g_1, g_2, g_3\rangle$ and $\mathrm{LT}(I) = \langle Y^4, 2Y, X^3\rangle$. By Theorem 5.4, $u_{1,3} = (X^3 - 1, 0, -Y^4 + Y)$, $u_{1,2} = (2, -Y^3 + 1, 0)$, $u_{2,3} = (0, X^3 - 1, -2Y)$ form a (pseudo-reduced) Gröbner basis for the syzygy module $\mathrm{Syz}(g_1, g_2, g_3)$ w.r.t. Schreyer's monomial order $>_2$ induced by $>_1$ and (g_1, g_2, g_3). In particular,

$$\begin{aligned}
\mathrm{LT}(\mathrm{Syz}(g_1, g_2, g_3)) &= \langle \mathrm{LT}(u_{1,3}), \mathrm{LT}(u_{1,2}), \mathrm{LT}(u_{2,3})\rangle\\
&= \langle X^3\epsilon_1, 2\epsilon_1, X^3\epsilon_2\rangle = \langle 2, X^3\rangle\epsilon_1 \oplus \langle X^3\rangle\epsilon_2,
\end{aligned}$$

where $(\epsilon_1, \epsilon_2, \epsilon_3)$ stands for the canonical basis of $\mathbb{Z}_{2\mathbb{Z}}[X,Y]^3$. We have

$$\begin{aligned}\mathrm{S}(u_{1,3}, u_{1,2}) = 2u_{1,3} - X^3 u_{1,2} &= (-2, Y^3X^3 - X^3, -2Y^4 + 2Y)\\ &= -u_{1,2} + (Y^3 - 1)u_{2,3},\\ \mathrm{S}(u_{1,3}, u_{2,3}) = \mathrm{S}(u_{1,2}, u_{2,3}) &= 0.\end{aligned}$$

We recover that $(u_{1,3}, u_{1,2}, u_{2,3})$ is a Gröbner basis for $\mathrm{Syz}(g_1, g_2, g_3)$. By Theorem 5.4, the element $u_{1,3;1,2} = (2, -X^3 + 1, -Y^3 + 1)$ forms a (pseudo-reduced) Gröbner basis for the syzygy module $\mathrm{Syz}(u_{1,3}, u_{1,2}, u_{2,3})$ w.r.t. Schreyer's monomial order $>_3$ induced by $>_2$ and $(u_{1,3}, u_{1,2}, u_{2,3})$. In particular, $\mathrm{LT}(\mathrm{Syz}(u_{1,3}, u_{1,2}, u_{2,3})) = \langle \mathrm{LT}(u_{1,3;1,2})\rangle = \langle 2\rangle \epsilon'_1$, where $(\epsilon'_1, \epsilon'_2, \epsilon'_3)$ stands for the canonical basis of $\mathbb{Z}_{2\mathbb{Z}}[X,Y]^3$. By Remark 5.2, $\mathrm{Syz}(u_{1,3}, u_{1,2}, u_{2,3})$ is free. We conclude that I admits the following length-2 free $\mathbb{Z}_{2\mathbb{Z}}[X,Y]$-resolution:

$$0 \longrightarrow \mathbb{Z}_{2\mathbb{Z}}[X,Y] \xrightarrow{u_{1,3;1,2}} \mathbb{Z}_{2\mathbb{Z}}[X,Y]^3 \xrightarrow{\begin{pmatrix} u_{1,3}\\ u_{1,2}\\ u_{2,3}\end{pmatrix}} \mathbb{Z}_{2\mathbb{Z}}[X,Y]^3 \xrightarrow{\begin{pmatrix} g_1\\ g_2\\ g_3\end{pmatrix}} I \to 0.$$

It follows that $\mathbb{Z}_{2\mathbb{Z}}[X,Y]/I$ admits the following length-3 free $\mathbb{Z}_{2\mathbb{Z}}[X,Y]$-resolution:

$$0 \to \mathbb{Z}_{2\mathbb{Z}}[X,Y] \to \mathbb{Z}_{2\mathbb{Z}}[X,Y]^3 \to \mathbb{Z}_{2\mathbb{Z}}[X,Y]^3 \to \mathbb{Z}_{2\mathbb{Z}}[X,Y] \xrightarrow{\pi} \mathbb{Z}_{2\mathbb{Z}}[X,Y]/I \to 0.$$

Another consequence of Theorem 5.4 is the following result.

Theorem 5.9 (Syzygy theorem for a coherent valuation ring with nonzero zerodivisors and a divisibility test)**.** *Let $M = \mathbf{H}_m/U$ be a finitely presented $\mathbf{R}[\underline{X}]$-module, where $\mathbf{R}$ is a coherent valuation ring with a divisibility test and nonzero zerodivisors. Assume that, w.r.t. the TOP lexicographic monomial order, $\mathrm{LT}(U)$ is finitely generated. Then M admits a resolution by finite free $\mathbf{R}[\underline{X}]$-modules*

$$\cdots \xrightarrow{\varphi_{p+3}} F_p \xrightarrow{\varphi_{p+2}} F_p \xrightarrow{\varphi_{p+1}} F_p \xrightarrow{\varphi_p} F_{p-1} \xrightarrow{\varphi_{p-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

such that for some $p \le n+1$,

- $\mathrm{LT}(\mathrm{Ker}(\varphi_p)) = \bigoplus_{j=1}^{m_p} \langle b_j\rangle \epsilon_j$ *with $b_1, \ldots, b_{m_p} \in \mathbf{R}$ and $(\epsilon_1, \ldots, \epsilon_{m_p})$ a basis for F_p,*
- $\mathrm{LT}(\mathrm{Ker}(\varphi_{p+2k-1})) = \bigoplus_{j=1}^{m_p} \mathrm{Ann}(b_j)\epsilon_j$ *for $k \ge 1$,*
- $\mathrm{LT}(\mathrm{Ker}(\varphi_{p+2k})) = \bigoplus_{j=1}^{m_p} \mathrm{Ann}(\mathrm{Ann}(b_j))\epsilon_j$ *for $k \ge 1$,*

and at each step where indeterminates remain present, the considered monomial order is Schreyer's monomial order (as in the proof of Theorem 5.5).

Proof. The part

$$F_p \xrightarrow{\varphi_p} F_{p-1} \xrightarrow{\varphi_{p-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

of the free $\mathbf{R}[\underline{X}]$-resolution with $p \leq n+1$ and $\mathrm{LT}(\mathrm{Ker}(\varphi_p)) = \bigoplus_{j=1}^{m_p} \langle b_j \rangle \epsilon_j$ follows from the proof of Theorem 5.5. W.l.o.g., the b_j's are $\neq 0$. Let us denote by $(g_1, \ldots, g_{m_p})$ a Gröbner basis for $\mathrm{Ker}(\varphi_p)$ such that $\mathrm{LT}(g_j) = b_j \epsilon_j$ for $1 \leq j \leq m_p$. So $\mathrm{S}(g_i, g_j) = 0$ for $i < j$. Thus the fact that $\mathrm{LT}(\mathrm{Ker}(\varphi_{p+1})) = \bigoplus_{j=1}^{m_p} \mathrm{Ann}(b_j)\epsilon_j$, $\mathrm{LT}(\mathrm{Ker}(\varphi_{p+2})) = \bigoplus_{j=1}^{m_p} \mathrm{Ann}(\mathrm{Ann}(b_j))\epsilon_j$, etc. follows immediately from Theorem 5.4. Finally, let us recall the equality $\mathrm{Ann}(\mathrm{Ann}(\mathrm{Ann}(I))) = \mathrm{Ann}(I)$ for an ideal I. □

Let us point out that this shows that the free resolution is in general not a finite one.

Corollary 5.10 (Syzygy theorem for a zero-dimensional coherent valuation ring with a divisibility test)**.** *Let $M = \mathbf{H}_m/U$ be a finitely presented $\mathbf{R}[\underline{X}]$-module, where $\mathbf{R}$ is a zero-dimensional coherent valuation ring[3] with a divisibility test. Then M admits a free $\mathbf{R}[\underline{X}]$-resolution as described in Theorem 5.9.*

Example 5.11. Let $g_1 = Y^4 - Y$, $g_2 = 2Y$, $g_3 = X^3 - 1 \in (\mathbb{Z}/4\mathbb{Z})[X, Y]$, and let us use the lexicographic order $>_1$ for which $Y >_1 X$. We have

$$\begin{aligned}
&\mathrm{S}(g_1, g_1) = 0\, g_1 = 0, \quad \mathrm{S}(g_1, g_2) = 2\, g_1 - Y^3 g_2 = -2Y = -g_2,\\
&\mathrm{S}(g_2, g_2) = 2\, g_2 = 0, \quad \mathrm{S}(g_2, g_3) = X^3 g_2 - 2Y g_3 = 2Y = g_2,\\
&\mathrm{S}(g_3, g_3) = 0\, g_3 = 0, \quad \mathrm{S}(g_1, g_3) = X^3 g_1 - Y^4 g_3 = Y^4 - Y X^3 = g_1 - Y g_3.
\end{aligned}$$

Thus (g_1, g_2, g_3) is a (pseudo-reduced) Gröbner basis for $I = \langle g_1, g_2, g_3 \rangle$ and $\mathrm{LT}(I) = \langle Y^4, 2Y, X^3 \rangle$. By Theorem 5.4, $u_{1,3} = (X^3 - 1, 0, -Y^4 + Y)$, $u_{1,2} = (2, -Y^3 + 1, 0)$, $u_{2,3} = (0, X^3 - 1, -2Y)$, $u_{2,2} = (0, 2, 0)$ form a (pseudo-reduced) Gröbner basis for the syzygy module $\mathrm{Syz}(g_1, g_2, g_3)$ w.r.t. Schreyer's monomial order $>_2$ induced by $>_1$ and (g_1, g_2, g_3). In particular,

$$\begin{aligned}
\mathrm{LT}(\mathrm{Syz}(g_1, g_2, g_3)) &= \langle \mathrm{LT}(u_{1,3}), \ldots, \mathrm{LT}(u_{2,2}) \rangle\\
&= \langle X^3\epsilon_1, 2\epsilon_1, X^3\epsilon_2, 2\epsilon_2 \rangle = \langle 2, X^3 \rangle \epsilon_1 \oplus \langle 2, X^3 \rangle \epsilon_2,
\end{aligned}$$

[3] Note that a zero-dimensional ring without nonzero zerodivisors is a discrete field.

where $(\epsilon_1, \epsilon_2, \epsilon_3)$ stands for the canonical basis of $(\mathbb{Z}/4\mathbb{Z})[X,Y]^3$. We have

$$\begin{aligned}
\mathrm{S}(u_{1,3}, u_{1,3}) &= 0u_{1,3} = 0,\\
\mathrm{S}(u_{1,3}, u_{1,2}) &= 2u_{1,3} - X^3u_{1,2}\\
&= (-2, Y^3X^3 - X^3, -2Y^4 + 2Y)\\
&= -u_{1,2} + (Y^3 - 1)u_{2,3},\\
\mathrm{S}(u_{1,3}, u_{2,3}) &= \mathrm{S}(u_{1,3}, u_{2,2}) = 0,\\
\mathrm{S}(u_{1,2}, u_{1,2}) &= 2u_{1,2} = (0, -2Y^3 + 2, 0)\\
&= (-Y^3 + 1)u_{2,2},
\end{aligned}
\qquad
\begin{aligned}
\mathrm{S}(u_{1,2}, u_{2,3}) &= \mathrm{S}(u_{1,2}, u_{2,2}) = 0,\\
\mathrm{S}(u_{2,3}, u_{2,3}) &= 0u_{2,3} = 0,\\
\mathrm{S}(u_{2,3}, u_{2,2}) &= 2u_{2,3} - X^3u_{2,2}\\
&= (0, -2, 0Y)\\
&= (0, -2, 0)\\
&= -u_{2,2},\\
\mathrm{S}(u_{2,2}, u_{2,2}) &= 2u_{2,2} = 0.
\end{aligned}$$

We recover that $(u_{1,3}, u_{1,2}, u_{2,3}, u_{2,2})$ is a Gröbner basis for $\mathrm{Syz}(g_1, g_2, g_3)$. By Theorem 5.4, $u_{1,3;1,2} = (2, -X^3 + 1, -Y^3 + 1, 0)$, $u_{1,2;1,2} = (0, 2, 0, Y^3 - 1)$, $u_{2,3;2,2} = (0, 0, 2, -X^3 + 1)$, $u_{2,2;2,2} = (0, 0, 0, 2)$ form a (pseudo-reduced) Gröbner basis for the syzygy module $\mathrm{Syz}(u_{1,3}, u_{1,2}, u_{2,3}, u_{2,2})$ w.r.t. Schreyer's monomial order $>_3$ induced by $>_2$ and $(u_{1,3}, u_{1,2}, u_{2,3}, u_{2,2})$. In particular,

$$\begin{aligned}
\mathrm{LT}(\mathrm{Syz}(u_{1,3}, u_{1,2}, u_{2,3}, u_{2,2})) &= \langle \mathrm{LT}(u_{1,3;1,2}), \dots, \mathrm{LT}(u_{2,2;2,2})\rangle\\
&= \langle 2\epsilon'_1, \dots, 2\epsilon'_4\rangle = \langle 2\rangle\epsilon'_1 \oplus \langle 2\rangle\epsilon'_2 \oplus \langle 2\rangle\epsilon'_3 \oplus \langle 2\rangle\epsilon'_4,
\end{aligned}$$

where $(\epsilon'_1, \dots, \epsilon'_4)$ stands for the canonical basis of $(\mathbb{Z}/4\mathbb{Z})[X,Y]^4$. By Theorem 5.4, we find four vectors $u_{(1,3;1,2),(1,3;1,2)}, \dots, u_{(2,2;2,2),(2,2;2,2)} \in (\mathbb{Z}/4\mathbb{Z})[X,Y]^4$ forming a (pseudo-reduced) Gröbner basis for the syzygy module $\mathrm{Syz}(u_{1,3;1,2}, \dots, u_{2,2;2,2})$ w.r.t. Schreyer's monomial order $>_4$ induced by $>_3$ and $(u_{1,3;1,2}, \dots, u_{2,2;2,2})$. In particular,

$$\begin{aligned}
\mathrm{LT}(\mathrm{Syz}(u_{1,3;1,2}, \dots, u_{2,2;2,2})) &= \langle \mathrm{LT}(u_{(1,3;1,2),(1,3;1,2)}), \dots, \mathrm{LT}(u_{(2,2;2,2),(2,2;2,2)})\rangle\\
&= \langle 2\rangle\epsilon'_1 \oplus \langle 2\rangle\epsilon'_2 \oplus \langle 2\rangle\epsilon'_3 \oplus \langle 2\rangle\epsilon'_4,
\end{aligned}$$

etc. We conclude that I admits the free $(\mathbb{Z}/4\mathbb{Z})[X,Y]$-resolution

$$\cdots \xrightarrow{\varphi_3} (\mathbb{Z}/4\mathbb{Z})[X,Y]^4 \xrightarrow{\varphi_2} (\mathbb{Z}/4\mathbb{Z})[X,Y]^4 \xrightarrow{\varphi_1} (\mathbb{Z}/4\mathbb{Z})[X,Y]^3 \xrightarrow{\varphi_0} I \longrightarrow 0$$

such that $\mathrm{LT}(\mathrm{Ker}(\varphi_i)) = \langle 2\rangle\epsilon'_1 \oplus \langle 2\rangle\epsilon'_2 \oplus \langle 2\rangle\epsilon'_3 \oplus \langle 2\rangle\epsilon'_4$ for $i \geq 1$.

6 The syzygy theorem and Schreyer's algorithm for a Bézout ring

As explained in the proof of Theorem 4.6, one can avoid branching when computing a dynamical Gröbner basis (see [10, 16, 19]) for a Bézout domain

of Krull dimension ≤ 1 (e.g. $\mathbb{Z}$ and the ring of all algebraic integers—note that the last one is not a PID) or a zero-dimensional coherent Bézout ring. Note that this is not possible for Prüfer domains of Krull dimension ≤ 1 which are not Bézout domains (e.g. $\mathbb{Z}[\sqrt{-5}]$, see [10, Section 4]).

Let us now generalise the results of Section 5 to the case of coherent strict Bézout rings.

Theorem 6.1 (Schreyer's algorithm for Bézout rings)**.** *We consider a coherent strict Bézout ring* $\mathbf{R}$ *with a divisibility test. Let* U *be a submodule of* $\mathbf{H}_m$ *with Gröbner basis* $(g_1, \ldots, g_p)$*. Then the relations* $u_{i,j}$ *computed by Algorithm 2.8 form a Gröbner basis for the syzygy module* $\mathrm{Syz}(g_1, \ldots, g_p)$ *w.r.t. Schreyer's monomial order induced by* $>$ *and* $(g_1, \ldots, g_p)$*.*

Proof. This follows directly from the local case given by Theorem 5.4: see the proof of Theorem 4.6 for an explanation. □

Theorem 6.2 (Syzygy theorem for a Bézout domain with a divisibility test)**.** *Let* $M = \mathbf{H}_m/U$ *be a finitely presented* $\mathbf{R}[\underline{X}]$*-module, where* $\mathbf{R}$ *is a Bézout domain with a divisibility test. Assume that, w.r.t. the TOP lexicographic monomial order,* $\mathrm{LT}(U)$ *is finitely generated. Then* M *admits a finite free* $\mathbf{R}[\underline{X}]$*-resolution*

$$0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

of length $p \leq n + 1$*.*

Proof. This follows directly from the local case. □

Corollary 6.3 (Syzygy theorem for a one-dimensional Bézout domain with a divisibility test)**.** *Let* $M = \mathbf{H}_m/U$ *be a finitely presented* $\mathbf{R}[\underline{X}]$*-module, where* $\mathbf{R}$ *is a Bézout domain of Krull dimension* ≤ 1 *with a divisibility test. Then* M *admits a finite free* $\mathbf{R}[\underline{X}]$*-resolution*

$$0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

of length $p \leq n + 1$*.*

Let us now treat the case of zero-dimensional coherent Bézout rings.

Theorem 6.4 (Syzygy theorem for a zero-dimensional Bézout ring with a divisibility test)**.** *Let* $M = \mathbf{H}_m/U$ *be a finitely presented* $\mathbf{R}[\underline{X}]$*-module, where* $\mathbf{R}$ *is a coherent zero-dimensional Bézout ring with a divisibility test. Then* M *admits a free* $\mathbf{R}[\underline{X}]$*-resolution*

$$\cdots \xrightarrow{\varphi_{p+3}} F_p \xrightarrow{\varphi_{p+2}} F_p \xrightarrow{\varphi_{p+1}} F_p \xrightarrow{\varphi_p} F_{p-1} \xrightarrow{\varphi_{p-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

such that for some $p \leq n + 1$*,*

- $\mathrm{LT}(\mathrm{Ker}(\varphi_p)) = \bigoplus_{j=1}^{m_p} \langle b_j \rangle \epsilon_j$ *with* $b_1, \ldots, b_{m_p} \in \mathbf{R}$ *and* $(\epsilon_1, \ldots, \epsilon_{m_p})$ *a basis for* F_p,
- $\mathrm{LT}(\mathrm{Ker}(\varphi_{p+2k-1})) = \bigoplus_{j=1}^{m_p} \mathrm{Ann}(b_j)\epsilon_j$ *for* $k \geq 1$,
- $\mathrm{LT}(\mathrm{Ker}(\varphi_{p+2k})) = \bigoplus_{j=1}^{m_p} \mathrm{Ann}(\mathrm{Ann}(b_j))\epsilon_j$ *for* $k \geq 1$,

and at each step where indeterminates remain present, the considered monomial order is Schreyer's monomial order.

Proof. This follows directly from the local case. □

The case of the integers

The following theorems are particular cases of Theorem 6.1 and Corollary 6.3 for $\mathbf{R} = \mathbb{Z}$.

Theorem 6.5 (Schreyer's algorithm for $\mathbf{R} = \mathbb{Z}$)**.** *Let U be a submodule of $\mathbf{H}_m$ with Gröbner basis $(g_1, \ldots, g_p)$. Then the relations $u_{i,j}$ computed by Algorithm 2.8 form a Gröbner basis for the syzygy module $\mathrm{Syz}(g_1, \ldots, g_p)$ w.r.t. Schreyer's monomial order induced by $>$ and $(g_1, \ldots, g_p)$. Moreover, for $1 \leq i < j \leq p$ such that $\mathrm{LPos}(g_i) = \mathrm{LPos}(g_j)$, we have*

$$\mathrm{LT}(u_{i,j}) = \frac{\mathrm{LC}(g_j)}{\gcd(\mathrm{LC}(g_i), \mathrm{LC}(g_j))} \underline{X}^{(\mathrm{mdeg}(g_j) - \mathrm{mdeg}(g_i))^+} \epsilon_i.$$

Theorem 6.6 (Syzygy theorem for $\mathbf{R} = \mathbb{Z}$)**.** *Let M be a finitely generated $\mathbb{Z}[\underline{X}]$-module. Then M admits a finite free $\mathbb{Z}[\underline{X}]$-resolution*

$$0 \to F_p \to F_{p-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

of length $p \leq n + 1$.

Example 6.7. Let $g_1 = Y^2 - X + 3$, $g_2 = 4X^2 - 4$, $g_3 = 6X + 6 \in \mathbb{Z}[X, Y]$, and let us use the lexicographic order $>_1$ for which $Y >_1 X$. We have:

$$\begin{aligned}
\mathrm{S}(g_1, g_2) &= 4X^2 g_1 - Y^2 g_2 = 4g_1 + (-X + 3)g_2, \\
\mathrm{S}(g_1, g_3) &= 6X g_1 - Y^2 g_3 = -6g_1 + (-X + 3)g_3, \\
\mathrm{S}(g_2, g_3) &= 3g_2 - 2X g_3 = -2g_3.
\end{aligned}$$

Thus (g_1, g_2, g_3) is a Gröbner basis for $I = \langle g_1, g_2, g_3 \rangle$ and $\mathrm{LT}(I) = \langle Y^2, 4X^2, 6X \rangle$. By Theorem 6.5, $u_{1,2} = (4X^2 - 4, -Y^2 + X - 3, 0)$, $u_{1,3} = (6X + 6, 0, -Y^2 + X - 3)$, $u_{2,3} = (0, 3, -2X + 2)$ form a Gröbner basis for the

syzygy module $\mathrm{Syz}(g_1, g_2, g_3)$ w.r.t. Schreyer's monomial order $>_2$ induced by $>_1$ and (g_1, g_2, g_3). In particular,

$$\begin{aligned}\mathrm{LT}(\mathrm{Syz}(g_1, g_2, g_3)) &= \langle \mathrm{LT}(u_{1,2}), \mathrm{LT}(u_{1,3}), \mathrm{LT}(u_{2,3})\rangle = \langle 4X^2\epsilon_1, 6X\epsilon_1, 3\epsilon_2\rangle \\ &= \langle 4X^2, 6X\rangle\epsilon_1 \oplus \langle 3\rangle\epsilon_2 = 2\langle 2X^2, 3X\rangle\epsilon_1 \oplus \langle 3\rangle\epsilon_2 = 2\langle X^2, 3X\rangle\epsilon_1 \oplus \langle 3\rangle\epsilon_2,\end{aligned}$$

where $(\epsilon_1, \epsilon_2, \epsilon_3)$ stands for the canonical basis of $\mathbb{Z}[X, Y]^3$. Thus

$$u'_{1,2} = Xu_{1,3} - u_{1,2} = (2X^2 + 6X + 4, Y^2 - X + 3, -Y^2X + X^2 - 3X), u_{1,3}, u_{2,3}$$

form a reduced Gröbner basis for $\mathrm{Syz}(g_1, g_2, g_3)$. We have:

$$\begin{aligned}\mathrm{S}(u'_{1,2}, u_{1,3}) &= 3u'_{1,2} - Xu_{1,3} = 2u_{1,3} + (Y^2 - X + 3)u_{2,3}, \\ \mathrm{S}(u'_{1,2}, u_{2,3}) &= \mathrm{S}(u_{1,3}, u_{2,3}) = 0.\end{aligned}$$

We recover that $(u'_{1,2}, u_{1,3}, u_{2,3})$ is a Gröbner basis for $\mathrm{Syz}(g_1, g_2, g_3)$. By Theorem 6.5, $u_{1,2;1,3} = (3, -X - 2, -Y^2 + X - 3)$ forms a (pseudo-reduced) Gröbner basis for the syzygy module $\mathrm{Syz}(u'_{1,2}, u_{1,3}, u_{2,3})$ w.r.t. Schreyer's monomial order $>_3$ induced by $>_2$ and $(u'_{1,2}, u_{1,3}, u_{2,3})$. In particular, $\mathrm{LT}(\mathrm{Syz}(u'_{1,2}, u_{1,3}, u_{2,3})) = \langle \mathrm{LT}(u_{1,2;1,3})\rangle = \langle 3\rangle\epsilon'_1$ where $(\epsilon'_1, \epsilon'_2, \epsilon'_3)$ stands for the canonical basis of $\mathbb{Z}[X, Y]^3$. It follows that $\mathrm{Syz}(u'_{1,2}, u_{1,3}, u_{2,3})$ is free. We conclude that I admits the following length-2 free $\mathbb{Z}[X, Y]$-resolution:

$$0 \to \mathbb{Z}[X, Y] \xrightarrow{u_{1,2;1,3}} \mathbb{Z}[X, Y]^3 \xrightarrow{\begin{pmatrix} u_{1,2} \\ u_{1,3} \\ u_{2,3}\end{pmatrix}} \mathbb{Z}[X, Y]^3 \xrightarrow{\begin{pmatrix} g_1 \\ g_2 \\ g_3\end{pmatrix}} I \to 0.$$

The case of $\mathbb{Z}/N\mathbb{Z}$

The elements of $\mathbb{Z}/N\mathbb{Z}$ are simply written as integers (their representatives in $[\![0, N-1]\!]$). When talking about the gcd of two nonzero elements in $\mathbb{Z}/N\mathbb{Z}$ we mean the gcd of their representatives in $[\![1, N-1]\!]$. For a nonzero element a in $\mathbb{Z}/N\mathbb{Z}$, letting $b = \gcd(N, a)$, the class of $\dfrac{N}{b}$ in $\mathbb{Z}/N\mathbb{Z}$ will be denoted by $\mathrm{ann}(a)$; it generates $\mathrm{Ann}(a)$.

- The Division algorithm 2.3 attains its goal: the gcd and the Bézout identity to be found in line 7 will be computed by finding d, b, b_i $(i \in D)$ in $\mathbb{Z}$ such that $d = \gcd(N, \gcd\{\, \mathrm{LC}(h_i)\ ;\ i \in D\,\}) = bN + \sum_{i\in D} b_i \,\mathrm{LC}(h_i)$; the euclidean division in line 7 will be performed in $\mathbb{Z}$;

- The S-polynomial algorithm 2.4 attains its goal: note that in this case, the generator of the annihilator of $\mathrm{LC}(f)$ to be found on line 3 may be taken to be $\mathrm{ann}(\mathrm{LC}(f))$, so that the auto-S-polynomial of f is

$$\mathrm{S}(f, f) = \mathrm{ann}(\mathrm{LC}(f))f;$$

- Buchberger's algorithm 2.5 attains its goal.

The following theorems are particular cases of Theorems 6.1 and 6.4 for $\mathbf{R} = \mathbb{Z}/N\mathbb{Z}$.

Theorem 6.8 (Schreyer's algorithm for $\mathbf{R} = \mathbb{Z}/N\mathbb{Z}$)**.** *Let U be a submodule of $\mathbf{H}_m$ with Gröbner basis $(g_1, \ldots, g_p)$. Then the relations $u_{i,j}$ computed by Algorithm 2.8 form a Gröbner basis for the syzygy module $\mathrm{Syz}(g_1, \ldots, g_p)$ w.r.t. Schreyer's monomial order induced by $>$ and $(g_1, \ldots, g_p)$. Moreover, for all $1 \leq i \leq j \leq p$ such that $\mathrm{LPos}(g_i) = \mathrm{LPos}(g_j)$, we have*

$$\mathrm{LT}(u_{i,j}) = \begin{cases} \mathrm{ann}(\mathrm{LC}(g_i))\epsilon_i & \text{if } i = j, \\ \frac{\mathrm{LC}(g_j)}{\gcd(\mathrm{LC}(g_i),\mathrm{LC}(g_j))} \underline{X}^{(\mathrm{mdeg}(g_j)-\mathrm{mdeg}(g_i))^+}\epsilon_i & \text{otherwise.} \end{cases}$$

Theorem 6.9 (Syzygy theorem for $\mathbf{R} = \mathbb{Z}/N\mathbb{Z}$)**.** *Let M be a finitely presented $(\mathbb{Z}/N\mathbb{Z})[\underline{X}]$-module. Then M admits a free $(\mathbb{Z}/N\mathbb{Z})[\underline{X}]$-resolution*

$$\cdots \xrightarrow{\varphi_{p+3}} F_p \xrightarrow{\varphi_{p+2}} F_p \xrightarrow{\varphi_{p+1}} F_p \xrightarrow{\varphi_p} F_{p-1} \xrightarrow{\varphi_{p-1}} \cdots \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$$

such that for some $p \leq n+1$,

$$\mathrm{LT}(\mathrm{Ker}(\varphi_p)) = \bigoplus_{j=1}^{m_p} \langle b_j \rangle \epsilon_j, \quad \mathrm{LT}(\mathrm{Ker}(\varphi_{p+1})) = \bigoplus_{j=1}^{m_p} \frac{N}{\gcd(N, b_j)} \epsilon_j,$$
$$\mathrm{LT}(\mathrm{Ker}(\varphi_{p+2})) = \bigoplus_{j=1}^{m_p} \langle b_j \rangle \epsilon_j, \quad \mathrm{LT}(\mathrm{Ker}(\varphi_{p+3})) = \bigoplus_{j=1}^{m_p} \frac{N}{\gcd(N, b_j)} \epsilon_j, \text{ etc.},$$

where $(\epsilon_1, \ldots, \epsilon_{m_p})$ is a basis for F_p, $b_1, \ldots, b_{m_p} \in \mathbb{Z}/N\mathbb{Z}$, and the considered monomial order is Schreyer's monomial order.

Example 6.10. Let $g_1 = Y + 1$, $g_2 = X^3 + X^2 + 6$, $g_3 = 3X^2$, $g_4 = 9$ in $(\mathbb{Z}/12\mathbb{Z})[X, Y]$, and let us use the lexicographic order $>_1$ for which $Y >_1 X$. We have

$$\begin{aligned}
&\mathrm{S}(g_1, g_1) = 0g_1 = 0, && \mathrm{S}(g_2, g_3) = 3g_2 - Xg_3 = g_3 + 2g_4, \\
&\mathrm{S}(g_1, g_2) = X^3 g_1 - Y g_2 = (-X^2 - 6)g_1 + g_2, && \mathrm{S}(g_2, g_4) = 9g_2 - X^3 g_3 = (X^2 + 6)g_4, \\
&\mathrm{S}(g_1, g_3) = 3X^2 g_1 - Y g_3 = g_3, && \mathrm{S}(g_3, g_3) = 4g_3 = 0, \\
&\mathrm{S}(g_1, g_4) = 9g_1 - Y g_4 = g_4, && \mathrm{S}(g_3, g_4) = 3g_3 - X^2 g_4 = 0, \\
&\mathrm{S}(g_2, g_2) = 0g_2 = 0, && \mathrm{S}(g_4, g_4) = 4g_4 = 0.
\end{aligned}$$

Thus (g_1, g_2, g_3, g_4) is a (pseudo-reduced) Gröbner basis for $I = \langle g_1, g_2, g_3, g_4 \rangle$ and $\mathrm{LT}(I) = \langle Y, X^3, 3X^2, 9 \rangle$. By Theorem 6.8, $u_{1,2} = (X^3 + X^2 + 6, -Y - 1,$

$0,0)$, $u_{1,3} = (3X^2, 0, -Y-1, 0)$, $u_{1,4} = (9, 0, 0, -Y-1)$, $u_{2,3} = (0, 3, -X-1, -2)$, $u_{2,4} = (0, 9, -X^3, -X^2-6)$, $u_{3,3} = (0, 0, 4, 0)$, $u_{3,4} = (0, 0, 3, -X^2)$, $u_{4,4} = (0, 0, 0, 4)$ form a Gröbner basis for the syzygy module $\mathrm{Syz}(g_1, g_2, g_3, g_4)$ w.r.t. Schreyer's monomial order $>_2$ induced by $>_1$ and (g_1, g_2, g_3, g_4). In particular,

$$\begin{aligned}\mathrm{LT}(\mathrm{Syz}(g_1, g_2, g_3, g_4)) &= \langle \mathrm{LT}(u_{1,2}), \ldots, \mathrm{LT}(u_{4,4}) \rangle \\ &= \langle X^3, 3X^2, 9 \rangle \epsilon_1 \oplus \langle 3, 9 \rangle \epsilon_2 \oplus \langle 4, 3 \rangle \epsilon_3 \oplus \langle 4 \rangle \epsilon_4 \\ &= \langle X^3, 3 \rangle \epsilon_1 \oplus \langle 3 \rangle \epsilon_2 \oplus \langle 1 \rangle \epsilon_3 \oplus \langle 4 \rangle \epsilon_4,\end{aligned}$$

where $(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$ stands for the canonical basis of $(\mathbb{Z}/12\mathbb{Z})[X, Y]^4$. Thus $u_{1,2}$, $u'_{1,4} = -u_{1,4} = (3, 0, 0, Y+1)$, $u_{2,3}$, $u'_{3,3} = u_{3,3} - u_{3,4} = (0, 0, 1, X^2)$, $u_{4,4}$ form a reduced Gröbner basis for $\mathrm{Syz}(g_1, g_2, g_3, g_4)$. We have

$$\begin{aligned}\mathrm{S}(u_{1,2}, u'_{1,4}) &= 3\,u_{1,2} - X^3 u'_{1,4} \\ &= (X^2+2)u'_{1,4} + (3Y+3)u_{2,3} + (3YX+3Y+3X+3)u'_{3,3} \\ &\qquad + (2YX^3 + 2YX^2 + 2X^3 + 2X^2 + Y + 1)u_{4,4}, \\ \mathrm{S}(u'_{1,4}, u'_{1,4}) &= 4\,u'_{1,4} = (Y+1)u_{4,4}, \\ \mathrm{S}(u_{2,3}, u_{2,3}) &= 4\,u_{2,3} = (8X+8)u'_{3,3} + (X^3 + X^2 + 1)u_{4,4}, \\ \mathrm{S}(u_{4,4}, u_{4,4}) &= 3\,u_{4,4} = 0.\end{aligned}$$

By Theorem 6.8, the elements $u_{1,2;1,4} = (3, -X^3 - X^2 - 2, -3Y - 3, -3YX - 3Y - 3X - 3, -2YX^3 - 2YX^2 - Y - 2X^3 - 2X^2 - 1)$, $u_{1,4;1,4} = (0, 4, 0, 0, -Y-1)$, $u_{2,3;2,3} = (0, 0, 4, -8X-8, -X^3 - X^2 - 1)$, $u_{4,4;4,4} = (0, 0, 0, 0, 3)$ form a (pseudo-reduced) Gröbner basis for the syzygy module $\mathrm{Syz}(u_{1,2}, u'_{1,4}, u_{2,3}, u'_{3,3}, u_{4,4})$ w.r.t. Schreyer's monomial order $>_3$ induced by $>_2$ and $(u_{1,2}, u'_{1,4}, u_{2,3}, u'_{3,3}, u_{4,4})$. In particular, $\mathrm{LT}(\mathrm{Syz}(u_{1,2}, u'_{1,4}, u_{2,3}, u'_{3,3}, u_{4,4})) = \langle 3 \rangle \epsilon'_1 \oplus \langle 4 \rangle \epsilon'_2 \oplus \langle 4 \rangle \epsilon'_3 \oplus \langle 3 \rangle \epsilon'_5$, where $(\epsilon'_1, \ldots, \epsilon'_5)$ stands for the canonical basis of $(\mathbb{Z}/12\mathbb{Z})[X, Y]^5$.

We conclude that I admits the free $\mathbf{R}[X, Y]$-resolution ($\mathbf{R} = \mathbb{Z}/12\mathbb{Z}$)

$$\cdots \xrightarrow{\varphi_4} \mathbf{R}[X, Y]^4 \xrightarrow{\varphi_3} \mathbf{R}[X, Y]^4 \xrightarrow{\varphi_2} \mathbf{R}[X, Y]^5 \xrightarrow{\varphi_1} \mathbf{R}[X, Y]^4 \xrightarrow{\varphi_0} I \to 0$$

with $\mathrm{LT}(\mathrm{Ker}(\varphi_{2i})) = \langle 4 \rangle \epsilon''_1 \oplus \langle 3 \rangle \epsilon''_2 \oplus \langle 3 \rangle \epsilon''_3 \oplus \langle 4 \rangle \epsilon''_4$ and $\mathrm{LT}(\mathrm{Ker}(\varphi_{2i+1})) = \langle 3 \rangle \epsilon''_1 \oplus \langle 4 \rangle \epsilon''_2 \oplus \langle 4 \rangle \epsilon''_3 \oplus \langle 3 \rangle \epsilon''_4$ for $i \geq 1$, where $(\epsilon''_1, \ldots, \epsilon''_4)$ stands for the canonical basis of $\mathbf{R}[X, Y]^4$.

References

[1] William W. Adams and Philippe Loustaunau. *An introduction to Gröbner bases*, *Graduate Studies in Mathematics*, vol. 3. American Mathematical Society, Providence, 1994. doi:10.1090/gsm/003. (p. 4)

[2] Errett Bishop. *Foundations of constructive analysis*. McGraw-Hill, New York, 1967. (p. 2)

[3] Errett Bishop and Douglas Bridges. *Constructive analysis*, *Grundlehren der mathematischen Wissenschaften*, vol. 279. Springer, Berlin, 1985. doi:10.1007/978-3-642-61667-9. (p. 2)

[4] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. Ph.D. thesis, Mathematisches Institut, Universität Innsbruck, 1965. Translation by Michael P. Abramson: An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal, *J. Symbolic Comput.*, 41(3–4):475–511, 2006. . (p. 8)

[5] David A. Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, *Graduate Texts in Mathematics*, vol. 185. Springer, New York, second ed., 2005. doi:10.1007/b138611. (p. 4)

[6] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics, Springer, Cham, fourth ed., 2015. doi:10.1007/978-3-319-16721-3. (p. 14)

[7] Gema-Maria Díaz-Toca, Henri Lombardi, and Claude Quitté. *Modules sur les anneaux commutatifs: cours et exercices*. Calvage & Mounet, Paris, 2014. (p. 4)

[8] Viviana Ene and Jürgen Herzog. *Gröbner bases in commutative algebra*, *Graduate Studies in Mathematics*, vol. 130. American Mathematical Society, Providence, 2012. (pp. 6, 19, 20, and 21)

[9] Maroua Gamanda and Ihsen Yengui. Noether normalization theorem and dynamical Gröbner bases over Bezout domains of Krull dimension 1. *J. Algebra*, 492, 52–56, 2017. doi:10.1016/j.jalgebra.2017.09.002. (p. 16)

[10] Amina Hadj Kacem and Ihsen Yengui. Dynamical Gröbner bases over Dedekind rings. *J. Algebra*, 324(1), 12–24, 2010. doi:10.1016/j.jalgebra.2010.04.014. (pp. 2, 11, 25, and 26)

[11] Henri Lombardi and Claude Quitté. *Commutative algebra: constructive methods. Finite projective modules*, *Algebra and Applications*, vol. 20. Springer, Dordrecht, 2015. doi:10.1007/978-94-017-9944-7. Translated from the French (Calvage & Mounet, Paris, 2011, revised and extended by the authors) by Tania K. Roblot. (pp. 2, 4, and 12)

[12] Ray Mines, Fred Richman, and Wim Ruitenburg. *A course in constructive algebra*. Universitext, Springer, New York, 1988. doi:10.1007/978-1-4419-8640-5. (p. 2)

[13] Samiha Monceur and Ihsen Yengui. On the leading terms ideals of polynomial ideals over a valuation ring. *J. Algebra*, 351, 382–389, 2012. doi:10.1016/j.jalgebra.2011.11.015. (p. 2)

[14] László Rédei. Ein kombinatorischer Satz. *Acta Sci. Math. (Szeged)*, 7, 39–43, 1934–1935. http://acta.bibl.u-szeged.hu/13432. (p. 14)

[15] Frank-Olaf Schreyer. *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstraßschen Divisionssatz und eine Anwendung auf analytische Cohen-Macaulay Stellenalgebren minimaler Multiplizität*. Master's thesis, Universität Hamburg, 1980. (p. 20)

[16] Ihsen Yengui. Dynamical Gröbner bases. *J. Algebra*, 301(2), 447–458, 2006. doi:10.1016/j.jalgebra.2006.01.051. (pp. 2, 11, and 25)

[17] Ihsen Yengui. Corrigendum to "Dynamical Gröbner bases" and to "Dynamical Gröbner bases over Dedekind rings". *J. Algebra*, 339(1), 370–375, 2011. doi:10.1016/j.jalgebra.2011.05.004. (p. 11)

[18] Ihsen Yengui. The Gröbner ring conjecture in the lexicographic order case. *Math. Z.*, 276(1–2), 261–265, 2014. doi:10.1007/s00209-013-1197-y. (pp. 2 and 17)

[19] Ihsen Yengui. *Constructive commutative algebra: projective modules over polynomial rings and dynamical Gröbner bases*, *Lecture Notes in Mathematics*, vol. 2138. Springer, Cham, 2015. doi:10.1007/978-3-319-19494-3. (pp. 2, 4, 7, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, and 25)