International Journal of Algebra, Vol. 7, 2013, no. 11, 539 - 548
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ija.2013.3550

Gröbner Bases over a Dual Valuation Domain

André Saint Eudes Mialébama Bouesso

Université Cheikh Anta Diop
Département de Mathématiques et Informatique
Laboratoire d'Algèbre, de Cryptographie, de Géométrie algébrique et applications
BP 5005 Dakar Fann, Sénégal
sainteudes@gmail.com

Abstract

Buchberger's algorithm was already studied over many kinds of rings such as principal ideal rings, noetherian valuation rings with zero divisors, Dedekind rings with zero divisors, Gaussian rings, ... In this paper, we propose the Buchberger's algorithm over $\mathcal{V}[\varepsilon]$ satisfying to $\varepsilon^2 = 0$ where $\mathcal{V}$ is any noetherian valuation domain and we give some applications in $\mathbb{Z}_{p\mathbb{Z}}[\varepsilon]$ where p is a prime number and $\mathbb{Z}_{p\mathbb{Z}} = \{\frac{a}{b} \mid a \in \mathbb{Z},\ b \notin p\mathbb{Z}\}$.

Keywords: Gröbner bases, dual noetherian valuation domain, S-polynomials, Buchberger's algorithm

1 Introduction

In 1965 Bruno Buchberger introduced the theory of Gröbner bases in polynomials ring over a field in order to solve the ideal membership problem (see [1, 2]). This theory was generalized by many authors in different ways such as [5, 8, 9], ... for the noncommutative case and [4, 6, 7, 10, 11] for the commutative case.

In [6, 10, 11] authors presented Buchberger's algorithm over noetherian valuation rings with zero divisors and over Dedekind rings with zero divisors.

Both methods don't cover the ring $\mathcal{V}[\varepsilon]$ since this ring is neither a valuation ring nor a Dedekind ring.

It is also proposed in [4] an interesting method for computing a Gröbner basis over many kinds of rings with zero divisors, such rings cover $\mathbb{Z}_n$ where n is not a prime number as well as $\mathbb{Z}_n[i]$ satisfying to $i^2+1=0$, this method cover many others rings with zero divisors but does not cover the ring of dual valuation domain $\mathcal{V}[\varepsilon]$ satisfying to $\varepsilon^2=0$ where $\mathcal{V}$ is a valuation domain.

In this paper we propose a method for computing a Gröbner basis over the ring of dual noetherian valuation domain $\mathcal{V}[\varepsilon]$ and we present some applications in $\mathbb{Z}_{p\mathbb{Z}}[\varepsilon]$ where p is a prime number.

This paper is organized as follows:

Section 1: We study some elementary properties of the ring $\mathcal{V}[\varepsilon]$ and we recall some necessary tools for computing a Gröbner basis.

Section 2: We adapt the Buchberger's algorithm in $\mathcal{V}[\varepsilon]$.

2 Basic notions

Throughout this paper, we denote by $\mathcal{V}$ a noetherian valuation domain, $\mathcal{V}[\varepsilon]$ the ring of dual valuation domain satisfying to $\varepsilon^2=0$, whose elements are of the form $a+\varepsilon b$ with $a,b\in\mathcal{V}$ and $J_\varepsilon=\varepsilon\cdot\mathcal{V}[\varepsilon]=\{\varepsilon a/a\in\mathcal{V}\}$ the set of zero divisors of $\mathcal{V}[\varepsilon]$. If R is a ring and E a subset of R, we denote by $\langle E\rangle$ the ideal generated by E.

1. **Division in $\mathcal{V}[\varepsilon]$**: An element $z_1=a_1+\varepsilon b_1$ divides $z_2=a_2+\varepsilon b_2$ in $\mathcal{V}[\varepsilon]$ if and only if a_1 divides a_2 in $\mathcal{V}$ and a_1 divides $b_2-b_1\dfrac{a_2}{a_1}$ in $\mathcal{V}$.

2. Let $R=\mathcal{V}[\varepsilon][X_1,\dots,X_m]$ be the free associative algebra with commuting variables $X_1,\dots,X_m$, defined over the ring $\mathcal{V}[\varepsilon]$.

   - A monomial in R is a multivariate polynomial of the form $g=X_1^{\alpha_1}\cdots X_m^{\alpha_m}$ where $\alpha_i\in\mathbb{N}$. We denote $X^\alpha=X_1^{\alpha_1}\cdots X_m^{\alpha_m}$ where $\alpha=(\alpha_1,\dots,\alpha_m)$ and by $\mathbb{M}$ the set of all monomials in R.
   - An element of the form zX^α where $z\in\mathcal{V}[\varepsilon][X_1,\dots,X_m]$ is called a term.
   - A term zX^α divides $z'X^\beta$ in R if and only if z divides z' in $\mathcal{V}[\varepsilon]$ and X^α divides X^β in R.

3. **Monomials order:** A total order $<$ in $\mathbb{M}$ is said to be a monomial order if it is a well ordering and If $X^\alpha<X^\beta$ then $X^{\alpha+\gamma}<X^{\beta+\gamma}$ for all $\alpha,\beta,\gamma\in\mathbb{N}^n$.

- **Lexicographic order**: we say that $X^\alpha >_{\text{lex}} X^\beta$ if the first left non zero component of $\alpha - \beta$ is > 0.
- **Graded lexicographic order**: We say that $X^\alpha >_{\text{grlex}} X^\beta$ if $|\alpha| > |\beta|$ or if $|\alpha| = \sum_{i=1}^{s} \alpha_i = |\beta| = \sum_{i=1}^{s} \beta_i$ and $X^\alpha >_{\text{lex}} X^\beta$ for $\alpha = (\alpha_1, \ldots, \alpha_n),\ \beta = (\beta_1, \ldots, \beta_n)$.

4. Let $f = \sum_{\alpha} z_\alpha X^\alpha$ be a nonzero polynomial in R. Let $I = \langle f_1, \ldots, f_s \rangle$ be a finitely generated ideal of R and let us fix a monomial order $<$ in $\mathbb{M}$, then:

   - The multidegree of f is $\text{mdeg}(f) := \max\{\alpha / z_\alpha \neq 0\}$.
   - The leading coefficient of f is $Lc(f) := z_{\text{mdeg}(f)}$.
   - The leading monomial of f is $Lm(f) := X^{\text{mdeg}(f)}$.
   - The leading term of f is $Lt(f) := Lc(f) \cdot Lm(f)$.
   - $\langle Lt(I) \rangle := \langle Lt(g) / g \in I \setminus \{0\} \rangle$.

5. **Division algorithm** (see [3, 10])

   We recall the division algorithm in R. Let $<$ be a monomial order and $f_1, \ldots, f_s \in R$. Then there exists $q_1, \ldots, q_s, r \in R$ such that $f = \sum_{i=1}^{s} q_i f_i + r$ with $\text{mdeg} f \geq \text{mdeg}(q_i f_i)$ for $q_i f_i \neq 0$ and $r = 0$ or each term occurring in r is not divisible by any of $Lt(f_i)\ \forall\ 1 \leq i \leq s$.

   Input: $f_1, \ldots, f_s, f$ and $<$.

   Output: $q_1, \ldots, q_s, r$.

   Initialization: $q_1 := 0, \ldots, q_s := 0;\ r := 0$ and $p := f$.

   While $p \neq 0$ do:

   $i := 1$

   DIVOCCUR:=False

   while $i \leq s$ and DIVOCCUR:=False do

   If $Lt(f_i)$ divides $Lt(p)$ then

   $$q_i := q_i + \frac{Lt(p)}{Lt(f_i)}$$

$$p := q_i - \frac{Lt(p)}{Lt(f_i)} \cdot f_i$$

DIVOCCUR:=True

Else

$i := i + 1$

If DIVOCCUR:=False then

$r := r + Lt(p);\ p := p - Lt(p)$

Example 2.1. *In $\mathbb{Z}_{2\mathbb{Z}}[\varepsilon][x, y]$ with $x <_{lex} y$, let us divide $f = (3 + 5\varepsilon)xy^2 + 3\varepsilon y$ by $f_1 = (5 - 2\varepsilon)x - \varepsilon y^2$ and $f_2 = (7 - 3\varepsilon)xy$. We find:*

- $f = (\frac{3}{5} + \frac{31}{25}\varepsilon) \cdot f_1 + (\frac{3}{5}\varepsilon y^4 + 3\varepsilon y)$ *if we start the division by f_1.*
- $f = (\frac{3}{7} + \frac{44}{49}\varepsilon)y \cdot f_2 + (3\varepsilon y)$ *if we start the division by f_2.*

6. **Gröbner basis**: A subset $G = \{g_1, \ldots, g_t\}$ of an ideal $I \subset R$ is called Gröbner basis for I with respect to a monomial order $<$ if $I = \langle G\rangle$ and $\langle Lt(I)\rangle = \langle Lt(G)\rangle$.

3 Buchberger's algorithm

Definition 3.1. ***S-polynomials:*** *Let $f, g \in R$, and let us consider a monomial order $>$. Denoting by $Lt(f) = (a_1+\varepsilon b_1)\cdot X^\alpha$, $Lt(g) = (a_2+\varepsilon b_2)\cdot X^\beta$ where $a_1, a_2, b_1, b_2 \in \mathcal{V}[\varepsilon]$; $\alpha, \beta \in \mathbb{N}^n$. Let $\gamma \in \mathbb{N}^n$ with $\gamma_i = \max(\alpha_i, \beta_i)$ for each i, the S-polynomial of f and g is given by:*

1. *Suppose that $f \neq g$:*

   - *$Lc(f) \in J_\varepsilon$ and $Lc(g) \in J_\varepsilon$ then:*

$$S(f,g) = \begin{cases} \frac{b_2}{b_1}\frac{X^\gamma}{X^\alpha}f - \frac{X^\gamma}{X^\beta}g \text{ if } b_1/b_2 \\ \frac{X^\gamma}{X^\alpha}f - \frac{b_1}{b_2}\frac{X^\gamma}{X^\beta}g \text{ if } b_2/b_1. \end{cases}$$

   - *If $Lc(f) \in J_\varepsilon$ and $Lc(g) \notin J_\varepsilon$ then:*

$$S(f,g) = \begin{cases} \frac{a_2}{b_1}\frac{X^\gamma}{X^\alpha}f - \frac{X^\gamma}{X^\beta}(\varepsilon g) \text{ if } b_1/a_2 \\ \frac{X^\gamma}{X^\alpha}f - \frac{b_1}{a_2}\frac{X^\gamma}{X^\beta}(\varepsilon g) \text{ if } a_2/b_1. \end{cases}$$

   If $Lc(f) \notin J_\varepsilon$ and $Lc(g) \in J_\varepsilon$ then replace f by g and vice versa.

- *If $Lc(f) \notin J_\varepsilon$ and $Lc(g) \notin J_\varepsilon$ then:*

$$S(f,g) = \begin{cases} \dfrac{a_2}{a_1}\dfrac{X^\gamma}{X^\alpha}(\varepsilon f) - \dfrac{X^\gamma}{X^\beta}(\varepsilon g) \text{ if } a_1/a_2 \\ \dfrac{X^\gamma}{X^\alpha}(\varepsilon f) - \dfrac{a_1}{a_2}\dfrac{X^\gamma}{X^\beta}(\varepsilon g) \text{ if } a_1/a_2. \end{cases}$$

2. Suppose that $f = g$ then:

$$S(f,f) = \begin{cases} \varepsilon f \text{ if } Lc(f) \in J_\varepsilon \\ 0 \text{ if not.} \end{cases}$$

Example 3.2. *Let us compute in $R = \mathbb{Z}_{2\mathbb{Z}}[\varepsilon][x,y]$ the S-polynomials of $f = (3+5\varepsilon)xy^2+3\varepsilon y$, $g = (7-3\varepsilon)xy$, $h_1 = 5\varepsilon x-(1+\varepsilon)y^2$ and $h_2 = 2\varepsilon x^2+(3-2\varepsilon)y$ with respect to $X <_{lex} Y$:*

$S(f,g) = \dfrac{7}{3}(\varepsilon f) - y(\varepsilon g) = 0$

$S(f,h_1) = \dfrac{5}{3}(\varepsilon f) - y^2 h_1 = (1+\varepsilon)y^4$

$S(h_1,h_2) = \dfrac{2}{5}xh_1 - h_2 = -\dfrac{2}{5}xy^2 - (3-2\varepsilon)y$

$S(h_1,h_1) = -\varepsilon y^2.$

Lemma 3.3. *Let $<$ be a monomial order, and $f_1, \ldots, f_s \in R = \mathcal{V}[\varepsilon][X_1, \ldots, X_m]$ such that $mdeg(f_i) = \gamma \in \mathbb{N}^n$ for each $1 \leq i \leq s$. Suppose that $mdeg(\sum_{i=1}^{s} z_i f_i) < \gamma$ for some $z_1, \ldots, z_s \in \mathcal{V}[\varepsilon]$:*

1. *If $Lc(f_i) \in J_\varepsilon \ \forall\ 1 \leq i \leq s$ then $\sum_{i=1}^{s} z_i f_i$ is a linear combination with coefficients in $\mathcal{V}[\varepsilon]$ of S-polynomials $S(f_i,f_j)$ for $1 \leq i \leq j \leq s$.*

2. *If there exists i_0 such that $Lc(f_{i_0}) \notin J_\varepsilon$ then $\varepsilon \sum_{i=1}^{s} z_i f_i$ is a linear combination with coefficients in $\mathcal{V}[\varepsilon]$ of S-polynomials $S(f_i,f_j)$ for $1 \leq i \leq j \leq s$.*

Furthermore, each S-polynomial has multidegree $< \gamma$.

Proof:

1. Suppose that $Lc(f_i) = \varepsilon b_i \in J_\varepsilon \ \forall\ 1 \leq i \leq s$ and we can assume that $b_s/b_{s-1}/\ldots/b_1$ since $\mathcal{V}$ is a valuation domain.

$$\sum_{i=1}^{s} z_i f_i = z_1(f_1 - \frac{b_1}{b_s}f_s) + z_2(f_2 - \frac{b_2}{b_s}f_s) + \ldots + z_{s-1}(f_{s-1} - \frac{b_{s-1}}{b_s}f_s) + (z_1\frac{b_1}{b_s} + z_2\frac{b_2}{b_s} + \ldots + z_{s-1}\frac{b_{s-1}}{b_s} + z_s)f_s.$$

By hypothesis, we have $(z_1\frac{b_1}{b_s} + z_2\frac{b_2}{b_s} + \ldots + z_{s-1}\frac{b_{s-1}}{b_s} + z_s)\cdot \varepsilon b_s = 0$ then, $(z_1\frac{b_1}{b_s} + z_2\frac{b_2}{b_s} + \ldots + z_{s-1}\frac{b_{s-1}}{b_s} + z_s)f_s \in \mathcal{V}[\varepsilon]S(f_s, f_s)$.

We deduce that $\sum_{i=1}^{s} z_i f_i = \sum_{i,j} z_{i,j}S(f_i, f_j)$.

2. Let $Lc(f_i) = a_i + \varepsilon b_i$ and suppose that there exists at least i_0 for which $a_{i_0} \neq 0$ then:

$$\varepsilon\sum_{i=1}^{s} z_i f_i = \sum_{Lc(f_i)\notin J_\varepsilon} z_i(\varepsilon f_i) + \sum_{Lc(f_i)\in J_\varepsilon} (\varepsilon f_i).$$

Without loss of generalities we set: $\sum_{Lc(f_i)\notin J_\varepsilon} z_i(\varepsilon f_i) = \sum_{i=1}^{k} z_i(\varepsilon f_i)$ and $\sum_{Lc(f_i)\in J_\varepsilon} z_i(\varepsilon f_i) = \sum_{i=k+1}^{s} z_i(\varepsilon f_i)$, then:

$$\sum_{i=k+1}^{s} z_i(\varepsilon f_i) = \sum_{i=k+1}^{s} z_i S(f_i, f_i)\ (*).$$

Assume that $Re(Lc(f_k))/Re(Lc(f_{k-1}))/\ldots/Re(Lc(f_1))$ then:

$$\sum_{i=1}^{k} z_i(\varepsilon f_i) = z_1[(\varepsilon f_1) - \frac{Re(Lc(f_1))}{Re(Lc(f_k))}(\varepsilon f_k)] + z_2[(\varepsilon f_2) - \frac{Re(Lc(f_2))}{Re(Lc(f_k))}(\varepsilon f_k)] + \ldots + z_{k-1}[(\varepsilon f_{k-1}) - \frac{Re(Lc(f_{k-1}))}{Re(Lc(f_k))}(\varepsilon f_k)] + (z_1\frac{Re(Lc(f_1))}{Re(Lc(f_k))} + z_2\frac{Re(Lc(f_2))}{Re(Lc(f_k))} + \ldots + z_{k-1}\frac{Re(Lc(f_{k-1}))}{Re(Lc(f_k))} + z_k)(\varepsilon f_k).$$

Since by hypothesis $0 = z_1Lc(f_1) + \ldots + z_sLc(f_s) = \varepsilon(z_1Lc(f_1) + \ldots + z_kLc(f_k)) = \varepsilon(z_1Re(Lc(f_1)) + \ldots + z_kRe(Lc(f_k)))$ then:

$\sum_{i=1}^{k} z_i(\varepsilon f_i) = \sum_{i,j} z_{i,j}S(f_i, f_j)$ (**). Thus from (*) and (**) we get the desired result.

□

Theorem 3.4. *Let $<$ be a monomial order and $G = \{g_1, \ldots, g_s\}$ be a finite set of polynomials of $R = \mathcal{V}[\varepsilon][X_1, \ldots, X_m]$. Let $I = \langle G \rangle$ be an ideal of R, then G is a Gröbner basis for I if and only if all remainder of S-polynomials $S(g_i, g_j)$ by G is zero for $1 \leq i \leq j \leq s$.*

Proof

(a) $S(g_i, g_j) \in \langle g_i, g_j \rangle \subset \langle G \rangle \Rightarrow \overline{S(g_i, g_j)}^G = 0$ where $\overline{S(g_i, g_j)}^G$ is the remainder of $S(g_i, g_j)$ under the division by G.

(b) Conversely, we need to prove that $\langle Lt(I) \rangle = \langle Lt(G) \rangle$.
Let $f \in I$ then

$$f = \sum_{i=1}^{s} h_i g_i \qquad (1)$$

where $h_i \in R$ and $\mathrm{mdeg}(f) \leq \max_i \{\mathrm{mdeg}(h_i g_i)\} = \gamma$. Let γ be the smallest multidegree satisfying to (1), then $\mathrm{mdeg}(f) \leq \gamma$.

- If $\mathrm{mdeg}(f) < \gamma$, from (1) we have:
  $f = \sum_{i=1}^{s} h_i g_i = \sum_{\mathrm{mdeg}(h_i g_i) = \gamma} h_i g_i + \sum_{\mathrm{mdeg}(h_i g_i) < \gamma} h_i g_i \qquad (2)$
  Notice that:
  $\sum_{\mathrm{mdeg}(h_i g_i) = \gamma} h_i g_i = \sum_{\mathrm{mdeg}(h_i g_i) = \gamma} Lt(h_i) g_i + \sum_{\mathrm{mdeg}(h_i g_i) = \gamma} (h_i - Lt(h_i)) g_i$ (3).
  Let $Lt(h_i) = m_i X^{\alpha_i}$ with $m_i \in \mathcal{V}[\varepsilon]$, then
  $\sum_{\mathrm{mdeg}(h_i g_i) = \gamma} Lt(h_i) g_i = \sum_{\mathrm{mdeg}(h_i g_i) = \gamma} m_i (X^{\alpha_i} g_i)$ (*).
  - Suppose that $Lc(g_i) \in J_\varepsilon \ \forall\ i$ then from the previous lemma (*) become:
    $\sum_{\mathrm{mdeg}(h_i g_i) = \gamma} Lt(h_i) g_i = \sum_{i,j} z_{ij} S(X^{\alpha_i} g_i, X^{\alpha_j} g_j)$ where $z_{ij} \in \mathcal{V}[\varepsilon]$.
    Since $S(X^{\alpha_i} g_i, X^{\alpha_j} g_j) = \dfrac{Im(Lc(g_i))}{Im(Lc(g_j))} \dfrac{X^\gamma}{X^{\alpha_i} Lm(g_i)} (X^{\alpha_i} g_i) - \dfrac{X^\gamma}{X^{\alpha_j} Lm(g_j)} (X^{\alpha_j} g_j) = X^{\gamma - \gamma_{ij}} S(g_i, g_j)$ with $X^{\gamma_{ij}} = \mathrm{lcm}(Lm(g_i), Lm(g_j))$.
    Therefore $\sum_{\mathrm{mdeg}(h_i g_i) = \gamma} Lt(h_i) g_i = \sum_{i,j} z_{ij} X^{\gamma - \gamma_{ij}} S(g_i, g_j)$ (4).
    By hypothesis for $1 \leq i \leq j \leq s$, $S(g_i, g_j) = \sum_k q_{ijk} g_k$
    where $\mathrm{mdeg}(q_{ijk} g_k) \leq \mathrm{mdeg}(S(g_i, g_j))$, then $\sum_{\mathrm{mdeg}(h_i g_i) = \gamma} Lt(h_i) g_i =$

$\sum_{i,j,k} z_{ij} X^{\gamma-\gamma_{ij}} q_{ijk} g_k$.
Since $\mathrm{mdeg}(S(g_i, g_j)) \leq \gamma_{ij}$ then
$\mathrm{mdeg}(X^{\gamma-\gamma_{ij}} q_{ijk} g_k) \leq \mathrm{mdeg}(X^{\gamma-\gamma_{ij}} S(g_i, g_j)) < \gamma$. By minimality of γ, we get a contradiction.

– Suppose that there exists i_0 such that $Lc(g_{i_0}) \notin J_\varepsilon$ then from the previous lemma (*) become:
$$\varepsilon \sum_{\mathrm{mdeg}(h_i g_i)=\gamma} Lt(h_i) g_i = \sum_{\mathrm{mdeg}(h_i(\varepsilon g_i))=\gamma} Lt(h_i)(\varepsilon g_i) + \sum_{\mathrm{mdeg}(h_i(\varepsilon g_i))<\gamma} Lt(h_i)(\varepsilon g_i)$$
$$\sum_{\mathrm{mdeg}(h_i(\varepsilon g_i))=\gamma} Lt(h_i)(\varepsilon g_i) = \sum_i m_i(X^{\alpha_i}(\varepsilon g_i)) = \sum_{i,j} w_{i,j} S(X^{\alpha_i} g_i, X^{\alpha_j} g_j).$$
From the previous item we have seen that $\mathrm{mdeg}(S(X^{\alpha_i} g_i, X^{\alpha_j} g_j)) < \gamma$ and we can easily see that $\mathrm{mdeg}(m_i(X^{\alpha_i}\varepsilon g_i)) = \mathrm{mdeg}(m_i(X^{\alpha_i} g_i))$, we get a contradiction.

– Suppose that $Lc(g_i) \notin J_\varepsilon \ \forall\ i$ then from the previous lemma (*) become
$$(\varepsilon \sum_{\mathrm{mdeg}(h_i g_i)=\gamma} m_i(X^{\alpha_i} g_i)) = \sum_{\mathrm{mdeg}(h_i(\varepsilon g_i))=\gamma} m_i(X^{\alpha_i}\varepsilon g_i) = \sum_{i,j} t_{i,j} S(X^{\alpha_i} g_i, X^{\alpha_j} g_j)$$
where $t_{i,j} \in \mathcal{V}[\varepsilon]$. From the previous item we have seen that $\mathrm{mdeg}(S(X^{\alpha_i} g_i, X^{\alpha_j} g_j)) < \gamma$ thus we get a contradiction.

Since $\mathrm{mdeg}(f) = \gamma$, then there exists j_0 such that $\mathrm{mdeg}(f) = \mathrm{mdeg}(h_{j_0} g_{j_0}) = \gamma$. We have $Lm(f) = Lm(h_{j_0}) Lm(g_{j_0}) = X^\gamma$. Put $\wedge = \{i / Lm(h_i) Lm(g_i) = Lm(h_{j_0}) Lm(g_{j_0})\}$ then $Lc(f) = \sum_{i\in\wedge} Lc(h_i) Lc(g_i)$.

Therefore $Lt(f) = \sum_{i\in\wedge} Lt(h_i) Lt(g_i)$ hence $Lt(f) \in \sum_{i\in\wedge} \langle Lt(g_i)\rangle \subset \langle Lt(G)\rangle$.

□

The previous theorem guaranties that we can compute a Gröbner basis of an ideal of R after a finite number of step. We are now ready to give the algorithm for computing a Gröbner basis.

Buchberger's algorithm.

Input: $g_1, \ldots, g_s \in R$ and $<$ a monomial order.

Output: A Gröbner basis G for $I = \langle g_1, \ldots, g_s\rangle$ with $\{g_1, \ldots, g_s\} \subseteq G$

$G := \{g_1, \ldots, g_s\}$

REPEAT

$G' := G$

For each pair g_i, g_j in G' DO

$S := \overline{S(g_i, g_j)}^{G'}$

If $S \neq 0$ THEN $G := G' \cup \{S\}$

UNTIL $G = G'$

Example 3.5. *Let $R = \mathbb{Z}_{3\mathbb{Z}}[x, y]$ and let us fix a monomial order $x <_{lex} y$. Consider the set $F = \{f_1 = (3 + 5\varepsilon)xy^2 + 3\varepsilon y, f_2 = 5\varepsilon x - (1+\varepsilon)y^2\}$. We want to construct a Gröbner basis for $I = \langle F\rangle$ in R with respect to $x <_{lex} y$. Set $G = \{g_1 := f_1, g_2 := f_2\}$*

$S(g_1, g_2) = (\varepsilon g_1) - \frac{3}{5}y^2 f_2 = \frac{3(1+\varepsilon)}{5}y^4$ *and* $\overline{S(g_1, g_2)}^{G} = \frac{3(1+\varepsilon)}{5}y^4 = g_3$, $G = \{g_1, g_2, g_3\}$.

$S(g_2, g_2) = \varepsilon g_2 = -\varepsilon y^2 = \overline{S(g_2, g_2)}^{G} = g_4$, $G = \{g_1, g_2, g_3, g_4\}$.

Notice that $S(g_1, g_4) = S(g_1, g_3) = S(g_4, g_4) = S(g_3, g_4) = 0$ *and* $\overline{S(g_2, g_3)}^{G} = \overline{S(g_2, g_4)}^{G} = 0$.

Thus $G = \{(3 + 5\varepsilon)xy^2 + 3\varepsilon y, 5\varepsilon x - (1 + \varepsilon)y^2, \frac{3(1+\varepsilon)}{5}y^4, -\varepsilon y^2\}$ *is a Grb̈ner basis for* $I = \langle(3 + 5\varepsilon)xy^2 + 3\varepsilon y, 5\varepsilon x - (1 + \varepsilon)y^2\rangle$.

References

[1] B. Buchberger (1965), *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal*, Ph.D. Thesis, Univ. of Innsbruck, Austria, Math., Inst.

[2] B. Buchberger, *Introduction to Gröbner bases.* (B. Buchberger, F. Winkler, eds.) Gröbner bases and Applications, London Mathematical Society Lecture Note Series 251, Cambridge University Press (1998).

[3] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties and Algorithms, 3rd ed.*, Springer-Verlag, New York, (2007).

[4] Deepak Kapur and Yongyang Cai, *An Algorithm for Computing a Gröbner Basis of a Polynomial Ideal over a Ring with Zero Divisors.* Math.comput.sci. 2 (2009), pp 601-634.

[5] E. Green, *Noncommutative Gröbner bases, and projective resolutions. Computational methods for representations of groups and algebras.* Papers from the First Euroconference held at the University of Essen. Basel, (1999), P. Dräxler, G. O. Michler, and C. M. Ringel, Eds., no. 173 in Progress in Math., Birkhäuser Verlag, pp. 29-60.

[6] A. Hadj Kacem and I. Yengui, *Dynamical Gröbner bases over Dedekind rings*, J. Algebra **324** (2010) pp. 12-24.

[7] D. Kapur and K. Madlener, *Construction of Gröbner bases in "special" rings*, in "Manuscript presented at the Gröbner bases workshop (1988)", Cornell.

[8] A.S.E.Mialébama Bouesso and D. Sow, *Noncommutative Gröbner bases over rings*, (preprint), to be published in communications in algebra (2013).

[9] T. Mora, *Groebner bases for non-commutative polynomial rings*, Proc. AAECC3, LNCS 229 (1986) 353-362

[10] Yengui I., *Dynamical Gröbner bases*. J. Algebra **301** (2006) pp. 447-458.

[11] Yengui I., *Corrigendum to "Dynamical Gröbner bases" [J. Algebra 301 (2) (2006) pp. 447-458]* & to *"Dynamical Gröbner bases over Dedekind rings" [J. Algebra 324 (1) (2010) pp. 12-24]*. J. Algebra **339** (2011) pp. 370-375.

Received: May 10, 2013