Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Journal of Symbolic Computation 42 (2007) 1003–1011

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Gröbner bases with coefficients in rings

Franz Pauer*

Institut für Mathematik, Universität Innsbruck, Technikerstr. 13, A-6020 Innsbruck, Austria

Received 11 January 2006; accepted 12 June 2007
Available online 1 September 2007

Abstract

This article gives a short introduction to the theory of Gröbner bases in a class of rings, which includes rings of differential operators and polynomial rings over commutative noetherian rings. A definition of reduced Gröbner bases for these rings is proposed.

Keywords: Gröbner basis; Reduced Gröbner basis; Rings of differential operators; Polynomial rings

1. Introduction

Some years after the publication of B. Buchberger's fundamental paper on Gröbner bases for ideals in commutative polynomial rings over fields (Buchberger, 1970) W. Trinks published a natural generalization to polynomial rings over commutative noetherian rings (Trinks, 1978). He translated in a natural way the notions of S-polynomial and of reduction from the field case to the ring case. This approach is very near to the case of coefficient fields if one considers only principal ideal domains instead of general noetherian rings (Pauer and Pfeifhofer, 1988). Another access to Gröbner bases over rings was proposed in Buchberger (1984), Kandri-Rody and Kapur (1988), Möller (1988) and Pan (1988). The difference between these two approaches can be well-illustrated by the following example: a Gröbner basis of the ideal generated by $2x_1$ and $3x_2$ in $\mathbb{Z}[x_1, x_2]$ is $\{2x_1, 3x_2\}$ according to Trinks (1978) and $\{2x_1, 3x_2, x_1x_2\}$ according to Buchberger (1984). Since then a lot of results on Gröbner bases over rings have been obtained and good presentations in text books are available (e.g. in Adams and Loustaunau (1994), Chapter 4). There are many reasons to study Gröbner bases in polynomial rings over a ring, here is one of

* Tel.: +43 0 512 507 6082; fax: +43 0 512 507 2920.
E-mail address: Franz.Pauer@uibk.ac.at.

0747-7171/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2007.06.006

them: In order to speed up the computation of Gröbner bases over the field of rational numbers, one can try to use residue-class methods and thus one has to study Gröbner bases over $\mathbb{Z}$, $\mathbb{Z}_p$, and $\mathbb{Z}_{p^\ell}$ (see e.g. Pauer (1992)).

Gröbner bases in (non-commutative) rings of differential operators (e.g. the Weyl-algebra) were introduced in Galligo (1985) and Castro (1987). Motivated by problems of system theory, in Insa and Pauer (1998) the approach of Trinks was used to define and compute Gröbner bases for a larger class of rings of differential operators. As an application a method is given to check whether a finitely presented left-module over a certain ring of differential operators is a torsion module or not (cf. Insa and Pauer (1998), Chapter 4). Improvements of the algorithm to compute these Gröbner bases have recently been made in Winkler and Zhou (2005).

This (mainly tutorial) paper presents a unified approach to Gröbner bases of left-ideals in a class of rings which includes rings of differential operators and polynomial rings with coefficients in noetherian rings. In Section 1 a division algorithm and Gröbner bases are introduced. In Section 2 Buchberger's algorithm is presented and in Section 3 a definition of reduced Gröbner bases is proposed. Several remarks point out the problems arising from the non-commutativity or the existence of zero-divisors of the considered rings.

2. Division algorithm and Gröbner bases

Let R be a commutative noetherian ring such that we can solve linear equations over R, i.e.

- for all $z \in R$ and for all finite subsets $S \subseteq R$, we can decide, whether z is an element of the ideal in R generated by S and – if yes – we can compute a family $(d_s)_{s\in S}$ in R such that $z = \sum_{s\in S} d_s s$, and generalised common left multiples
- for all finite subsets $S \subseteq R$ we can compute a finite system of generators of the R-module

$$\left\{ (c_s)_{s\in S} \in R^S \;\middle|\; \sum_{s\in S} c_s s = 0 \right\}$$

of its syzygies.

Important examples for R are $\mathbb{Z}$, $\mathbb{Z}_k$, polynomial rings with coefficients in a field, and certain subrings of the field of rational functions with coefficients in a field K, for instance

$$\left\{ \frac{p}{q} \;\middle|\; p, q \in K[y_1, \ldots, y_n], q(a) \neq 0 \right\}, \quad \text{where } a \in K^n.$$

Let A be a (left-)noetherian associative ring with unity containing R as a subring and elements $x_1, \ldots, x_n$ such that

- the elements $x_1, \ldots, x_n$ commute, i.e. $x_i x_j = x_j x_i$, $1 \le i, j \le n$,
- A is a free (left-)R-module and the family $(x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n})_{\alpha\in\mathbb{N}^n}$ is an R-basis of the R-module A, i.e. every element of A can uniquely be written as $\sum_{\alpha\in\mathbb{N}^n} c_\alpha x^\alpha$, where only finitely many x^α are not zero.

Well-known examples for A are

- commutative polynomial rings $R[x_1, \ldots, x_n]$ over the ring R and

- rings of differential operators with coefficients in certain rings R:
  Let K be a field and $K(y) := K(y_1, \ldots, y_n)$ the field of rational functions in n variables over K. Let $\frac{\partial}{\partial y_i}\colon K(y) \to K(y)$ be the partial derivate by y_i, $1 \le i \le n$. Let R be a noetherian K-subalgebra of $K(y_1, \ldots, y_n)$ which is stable by $\frac{\partial}{\partial y_i}$, $1 \le i \le n$ (i.e. $\frac{\partial}{\partial y_i}(z) \in R$, for all $z \in R, 1 \le i \le n$) and such that we can solve linear equations over R. We denote by D_i the restriction of $\frac{\partial}{\partial y_i}$ to $R, 1 \le i \le n$. Then $D_1, \ldots, D_n \in \mathrm{End}_K(R)$. Let $A := R[D] := R[D_1, \ldots, D_n]$ be the subring of $\mathrm{End}_K(R)$ generated by $R \cdot id_R = R$ and $x_1 := D_1, \ldots, x_n := D_n$. If $R = K[y]$, then A is the Weyl-algebra.

Definition 1. Let $<$ be a term order on $\mathbb{N}^n$ (i.e. a total order on $\mathbb{N}^n$ such that $0 \in \mathbb{N}^n$ is the least element and $\alpha < \beta$ implies $\alpha + \gamma < \beta + \gamma$, for all $\alpha, \beta, \gamma \in \mathbb{N}^n$). For an element $0 \neq f = \sum_{\alpha\in\mathbb{N}^n} c_\alpha x^\alpha \in A$ we define

- $\deg(f) := \max_<\{\alpha |\, c_\alpha \neq 0\} \in \mathbb{N}^n$ ("degree of f"),
- $\mathrm{lc}(f) := c_{\deg(f)}$ ("leading coefficient of f"),
- $\mathrm{lm}(f) := \mathrm{lc}(f)x^{\deg(f)}$ ("leading monomial of f").

For a subset F of A we define

- $\deg(F) := \{\deg(f) |\, f \in F, f \neq 0\}$,
- $\mathrm{lc}(F) := \{\mathrm{lc}(f) \mid f \in F, f \neq 0\}$,
- $\mathrm{lm}(F) := \{\mathrm{lm}(f) |\, f \in F, f \neq 0\}$.

We make the following assumptions on A and $<$:
For all $\alpha \in \mathbb{N}^n$ and $f, g \in A$ such that $f \cdot g \neq 0$

(1) $\deg(f \cdot g) \le \deg(f) + \deg(g)$
(2) $\deg(x^\alpha f) = \alpha + \deg(f)$
(3) $\mathrm{lc}(x^\alpha f) = \mathrm{lc}(f)$.

Remark. It is easy to verify that these conditions hold for all term orders and all rings of differential operators or commutative rings of polynomials. In commutative polynomial rings we even have $\mathrm{lm}(x^\alpha f) = x^\alpha \mathrm{lm}(f)$, but in rings of differential operators this is not true in general. Consider for example $\mathrm{lm}(D_1(y_1D_1)) = y_1{D_1}^2 \neq D_1(y_1D_1) = D_1 + y_1{D_1}^2$.

Remark. If R is not a domain (e.g. $R = \mathbb{Z}_6$) then $\deg(f \cdot g)$ may be strictly smaller than $\deg(f) + \deg(g)$. Consider for example $f := \bar{3}x + \bar{1} \in \mathbb{Z}_6[x]$ and $g := \bar{2} \in \mathbb{Z}_6[x]$. Then $f \cdot g = \bar{2}$, hence $\deg(f \cdot g) = 0 < 1 = \deg(f) + \deg(g)$.

Remark. We use the following notation: If B is a subset of R resp. A, we denote by $_R < B >$ resp. $_A < B >$ the ideal resp. left-ideal generated by B in R resp. A.

Proposition 2 (*Division in A, compare Insa and Pauer (1998), Proposition 1*). *Let F be a finite subset of $A \setminus \{0\}$ and let $g \in A$. Then there are an element $r \in A$ and a family $(h_f)_{f\in F}$ in A such that*

- $g = \sum_{f\in F} h_f f + r$ *(r is "a remainder of g after division by F"),*
- *for all $f \in F$, $h_f = 0$ or* $\deg(h_f) + \deg(f) \le \deg(g)$,
- $r = 0$ *or* $\mathrm{lc}(r) \notin _R< \mathrm{lc}(f);\ f \in F$ *and* $\deg(r) \in \deg(f) + \mathbb{N}^n >$.

The elements $r \in A$, $h_f \in A$, $(f \in F)$ can be computed as follows:

First set $r := g$ and $h_f := 0$ $(f \in F)$.

While $r \neq 0$ and $\mathrm{lc}(r) \in_R < \mathrm{lc}(f);\ f \in F$ and $\deg(r) \in \deg(f) + \mathbb{N}^n >$ do the following:

Let $F' := \{f \in F \mid \deg(r) \in \deg(f) + \mathbb{N}^n\}$, compute a family $(c_f)_{f \in F'}$ in R such that

$$\sum_{f \in F'} c_f \mathrm{lc}(f) = \mathrm{lc}(r).$$

Replace

$$r \quad \text{by} \quad r - \sum_{f \in F'} c_f x^{\deg(r) - \deg(f)} f$$

and

$$h_f \quad \text{by} \quad h_f + c_f x^{\deg(r) - \deg(f)} f, \qquad f \in F'.$$

Proof. Since $\deg(r - \sum_{f \in F'} c_f x^{\deg(r) - \deg(f)} f) < \deg(r)$, the algorithm terminates after finitely many steps. □

Remark. We can solve linear equations over R, hence we are able to decide whether the condition

$$\mathrm{lc}(r) \notin < \mathrm{lc}(f);\ f \in F \text{ and } \deg(r) \in \deg(f) + \mathbb{N}^n >$$

is fulfilled or not. If A is a commutative polynomial ring we could replace this condition by

$$\mathrm{lm}(r) \notin_A < \mathrm{lm}(F) > .$$

But in the general case this would not be reasonable since up to now we have no means to decide if this condition is fulfilled or not. The point is that monomial ideals in commutative polynomial rings are "easy" (e.g. ideal membership can easily be verified) while this is not the case e.g. in rings of differential operators.

Example 3. Let $R := \{\frac{p}{q} \mid p, q \in \mathbb{Q}[y_1, y_2],\ q(0,0) \neq 0\}$ and let

$$f_1 := y_2 D_1 + 1,\ \ f_2 := y_1 D_2, \text{ and } g := (y_1 + y_2) D_1 D_2 + y_1 y_2 D_2$$

be differential operators in $A = R[D_1, D_2]$. Then division of g by $\{f_1, f_2\}$ yields

$$\begin{aligned} r &:= g - (D_2 f_1 + D_1 f_2) = (y_1 + y_2) D_1 D_2 + y_1 y_2 D_2 - (y_1 + y_2) D_1 D_2 - D_1 - 2D_2 \\ &= y_1 y_2 D_2 - D_1 - 2D_2 = (y_1 y_2 - 2) D_2 - D_1 \end{aligned}$$

and

$$h_1 := D_2, \qquad h_2 := D_1.$$

Definition 4. Let I be a left-ideal in A and let G be a finite subset of $I \setminus \{0\}$. For $\alpha \in \mathbb{N}^n$ let

$$\mathrm{lc}(\alpha, I) :=_R < \mathrm{lc}(f);\ f \in I, \deg(f) = \alpha > .$$

Then G is a Gröbner basis of I (with respect to $<$) if and only if for all $\alpha \in \mathbb{N}^n$ the ideal $\mathrm{lc}(\alpha, I)$ is generated by

$$\{\mathrm{lc}(g);\ g \in G,\ \alpha \in \deg(g) + \mathbb{N}^n\}.$$

Remark. If A is a commutative polynomial ring, G is a Gröbner basis of I if and only if $\mathrm{lm}(G)$ generates in A the same ideal as $\mathrm{lm}(I)$. In general this is not true (see Example 6).

Example 5. If R is a domain and I is generated by one element $f \in A$, then any finite subset of $I \setminus \{0\}$ containing f is a Gröbner basis of I. In $A := \mathbb{Z}_6[x]$ however, $f := \bar{3}x + \bar{1}$ is not a Gröbner basis of the ideal I generated by f, since $\bar{2}f = \bar{2} \notin_A < \mathrm{lm}(f) >$.

Example 6. Let $R \subseteq \mathbb{Q}(y_1, y_2)$ be such that y_1 and y_2 are not invertible in R (e.g. $R = \mathbb{Q}[y_1, y_2]$ or $R = \{\frac{f}{g} \in \mathbb{Q}(y_1, y_2) \mid f, g \in \mathbb{Q}[y_1, y_2],\ g(0, 0) \neq 0\}$). Let $<$ be a term order such that $(1, 0) < (0, 1)$. Then $\{y_1 D_2, y_2 D_1\}$ is not a Gröbner basis of $I :=_A < y_1 D_2, y_2 D_1 >$.

For: I contains $(y_2 D_1) y_1 D_2 - (y_1 D_2) y_2 D_1 = y_2 D_2 - y_1 D_1$ and $\deg(y_2 D_2 - y_1 D_1) = (0, 1)$. Hence $< y_2 > \subseteq \mathrm{lc}((0, 1), I)$ and $\mathrm{lc}((0, 1), I)$ is not generated by $y_1 = \mathrm{lc}(y_1 D_2)$.

Proposition 7. *Let I be a left-ideal in A, let G be a Gröbner basis of I and let $f \in A$. Then $f \in I$ if and only if a remainder of f after division by g is zero.*

Proof. Follows from Proposition 2. □

3. Buchberger's algorithm

Definition 8. Let E be a finite subset of $A \setminus \{0\}$. Then

$$m(E) := \left(\max_{e \in E} \deg(e)_1, \ldots, \max_{e \in E} \deg(e)_n \right) \in \mathbb{N}^n.$$

Proposition 9 (*Compare Insa and Pauer (1998), Proposition 3*). *Let G be a finite subset of $A \setminus \{0\}$ and let I be the left-ideal generated by G. For any non-empty subset $E \subseteq G$ let S_E be a finite set of generators of the R-module*

$$\left\{ (c_e)_{e \in E} \,\middle|\, \sum_{e \in E} c_e \mathrm{lc}(e) = 0 \right\} \leq \ _R(R^E)$$

of syzygies of the family $(\mathrm{lc}(e))_{e \in E}$. Then the following assertions are equivalent:

(1) *G is a Gröbner basis of I.*

(2) *For all $E \subseteq G$ and for all $(c_e)_{e \in E} \in S_E$ a remainder of*

$$\sum_{e \in E} c_e x^{m(E) - \deg(e)} e$$

after division by G is zero.

Proof. (1) ⇒ (2): follows from Proposition 7.
(2) ⇒ (1): Let h $\in I$. We have to show:

$$\mathrm{lc}(h) \in \ _R < \mathrm{lc}(g);\ g \in G, \deg(h) \in \deg(g) + \mathbb{N}^n > .$$

For a family $(f_g)_{g \in G}$ in A we define

$$\delta((f_g)_{g \in G}) := \max_{<} \{\deg(f_g) + \deg(g);\ g \in G\}.$$

Since $h \in I$ there is a family $(h_g)_{g \in G}$ in A such that $h = \sum_{g \in G} h_g g$. We may choose $(h_g)_{g \in G}$ such that

$$\delta := \delta((h_g)_{g \in G}) \quad \text{is minimal}$$

(i.e. if $(h'_g)_{g \in G}$ is such that $h = \sum_{g \in G} h'_g g$, then $\delta((h'_g)_{g \in G}) \geq \delta$).
Let $E := \{g \in G \mid \deg(h_g) + \deg(g) = \delta\} \subseteq G$.

- Case 1: $\deg(h) = \delta$. Then there is a non-empty subset $E' \subseteq E$ such that

  $$\operatorname{lm}(h) = \sum_{g \in E'} \operatorname{lm}(h_g g) \quad \text{and} \quad \operatorname{lc}(h) = \sum_{g \in E} \operatorname{lc}(h_g)\operatorname{lc}(g) \in_R < \operatorname{lc}(g);\, g \in E' > .$$

  (Note that assumptions (1)–(3) on A imply $\operatorname{lc}(h_g)\operatorname{lc}(g) = 0$ or $\operatorname{lc}(h_g g) = \operatorname{lc}(h_g)\operatorname{lc}(g)$). If $g \in E$, then $\deg(h) = \delta = \deg(h_g) + \deg(g)$, hence $\deg(h) \in \deg(g) + \mathbb{N}^n$. Therefore $\operatorname{lc}(h) \in_R < \operatorname{lc}(g);\, g \in G, \deg(h) \in \deg(g) + \mathbb{N}^n >$.
- Case 2: $\deg(h) < \delta$. Then $\sum_{g \in E} \operatorname{lc}(h_g)\operatorname{lc}(g) = 0$, hence

  $$(\operatorname{lc}(h_g))_{g \in E} \in \left\{ (c_g)_{g \in E} \;\middle|\; \sum_{g \in E} c_g \operatorname{lc}(g) = 0 \right\}.$$

  Thus there are $r_c \in R$ such that $(\operatorname{lc}(h_g))_{g \in E} = \sum_{c \in S_E} r_c c$, i.e.:

  $$\operatorname{lc}(h_g) = \sum_{c \in S_E} r_c c_g, \quad \text{for all } g \in G.$$

  Now

  $$\begin{aligned} h &= \sum_{g \in G} h_g g = \sum_{g \in E} h_g g + \sum_{g \in G \setminus E} h_g g \\ &= \sum_{g \in E} \left(h_g - \sum_{c \in S_E} r_c c_g x^{\deg(h_g)} \right) g + \sum_{g \in E} \sum_{c \in S_E} r_c c_g x^{\deg(h_g)} g + \sum_{g \in G \setminus E} h_g g. \end{aligned}$$

  For all $g \in E$ we have $\deg(h_g) + \deg(g) = \delta$, hence there is an element $u \in \mathbb{N}^n$ such that $\delta = m(E) + u$. Thus

  $$\begin{aligned} \sum_{g \in E} \sum_{c \in S_E} r_c c_g x^{\deg(h_g)} g &= \sum_{c \in S_E} r_c x^u \left(\sum_{g \in E} c_g x^{m(E) - \deg(g)} g \right) \\ &\quad + \sum_{c \in S_E} r_c \left(\sum_{g \in E} c_g x^{\deg(h_g)} - x^u c_g x^{m(E) - \deg(g)} \right) g. \end{aligned}$$

  By (ii) there are families $(h_g(c))_{g \in G}$ in A, for all $c \in S_E$, such that

  $$\sum_{g \in E} c_g x^{m(E) - \deg(g)} g = \sum_{g \in G} h_g(c) g$$

  and $\deg(h_g(c)g) < \delta - u$, for all $g \in G$. Therefore there is a family $(h''_g)_{g \in G}$ such that $\delta((h''_g))_{g \in G} < \delta$ and

  $$\sum_{c \in S_E} r_c x^u \left(\sum_{g \in E} c_g x^{m(E) - \deg(g)} g \right) = \sum_{g \in G} h''_g g\, .$$

  Let

  $$\begin{aligned} h'_g &:= \left(h_g - \sum_{c \in S_E} r_c c_g x^{\deg(h_g)} \right) + h''_g \\ &\quad + \sum_{c \in S_E} r_c (c_g x^{\deg(h_g)} - x^u c_g x^{m(E) - \deg(g)}), \quad \text{if } g \in E \end{aligned}$$

and let $h'_g := h_g + h''_g$, if $g \in G \setminus E$. Then it is easy to verify that $h = \sum_{g\in G} h'_g g$ and $\delta((h'_g)_{g\in G}) < \delta$, which is a contradiction to the minimality of δ. Hence case 2 cannot occur. □

Analogous to the case of commutative polynomial rings with coefficients in a field the proposition above implies an algorithm to compute Gröbner bases.

Proposition 10. *Let I be a left-ideal in A given by a finite set G of generators. We can compute in finitely many steps a Gröbner basis of I as follows:*

While there are a subset $E \subseteq G$ and a family $(c_e)_{e\in E} \in S_E$ such that the remainder r of

$$\sum_{e\in E} c_g x^{m(E)-\deg(e)} e$$

after division by G is not zero, replace G by $G \cup \{r\}$.

Example 11. Let R, I and $A = R[D_1, D_2]$ be as in Example 6. Let

$$f_1 := y_1 D_2 \quad \text{and} \quad f_2 := y_2 D_1,$$

then $I =_A < f_1, f_2 >$.

Let $<$ be the graded lexicographic order with $(0, 1) > (1, 0)$. Then

$$y_2 D_1 f_1 - y_1 D_2 f_2 = y_2(y_1 D_1 D_2 + D_2) - y_1(y_2 D_1 D_2 + D_1) = y_2 D_2 - y_1 D_1 =: f_3$$
$$y_2 f_1 - y_1 f_3 = y_1^2 D_1 =: f_4$$
$$D_2 f_2 - D_1 f_3 = y_2 D_1 D_2 + D_1 - (y_2 D_1 D_2 - y_1 D_1^2 - D_1) = y_1 D_1^2 + 2D_1 =: f_5.$$

A remainder of

$$y_2 D_2 f_4 - {y_1}^2 D_1 f_3 = {y_1}^2 y_2 D_1 D_2 + {y_1}^3 {D_1}^2 + {y_1}^2 D_1 - {y_1}^2 y_2 D_1 D_2 = {y_1}^3 {D_1}^2 + {y_1}^2 D_1$$

after division by $\{f_1, f_2, f_3, f_4, f_5\}$ is $y_1 D_1 =: f_6$.

Now $D_1 f_1 - D_2 f_6 = D_2 =: f_7$ and $D_2 f_2 - y_2 D_1 f_7 = D_1$ imply that $I =_A < D_1, D_2 >$ and $\{D_1, D_2\}$ is a Gröbner basis of I.

Example 12. Let $R := \mathbb{Z}_6$, $A := \mathbb{Z}_6[x]$ and $f := \bar{3}x + \bar{1}$. Then $S_{\{f\}} = \{\bar{2}\}$ and $\bar{2}f = \bar{2}$ is a remainder of $\bar{2}f$ after division by f. Hence $\{f, \bar{2}\}$ is a Gröbner basis of $_A < f >$.

Remark. Let R be a principal ideal domain (e.g. a field) and let $f, g \in A \setminus \{0\}$. Choose $c, d \in R$ such that $c \cdot \mathrm{lc}(f) = d \cdot \mathrm{lc}(g)$ is a least common multiple of $\mathrm{lc}(f)$ and $\mathrm{lc}(g)$. Then define the *S-polynomial* of f and g by

$$S(f, g) := cx^{m(\{f,g\})-\deg(f)} f - dx^{m(\{f,g\})-\deg(g)} g.$$

Syzygies of finite families in a principal ideal domain are generated by families which have only two non-zero components (see for example Adams and Loustaunau (1994), Section 4.5, or Pauer and Pfeifhofer (1988), Lemma 3.4). Hence in this case assertion (2) in Proposition 9 can be replaced by: For all $f, g \in G$ a remainder of $S(f, g)$ after division by G is zero.

Remark. The definition of Gröbner bases for left-ideals in A and the propositions above can easily be extended to A-submodules of finite-dimensional free (left-)A-modules (cf. Insa and Pauer (1998), Remark 3).

Remark. Our assumption that the "variables" $x_1, \dots, x_n$ commute (but they do not necessarily commute with the coefficients) restricts non-commutative examples essentially to rings of differential operators (where the variables are partial derivatives). If we weaken the assumption $x_j x_i = x_i x_j$ to $x_j x_i = c_{ij} x_i x_j + d_{ij}$, $1 \leq i < j \leq n$, where $c_{ij} \in R$ and $d_{ij} \in A$ such that $\deg(d_{ij}) < \deg(x_i x_j)$, then A is a *G-algebra* (Levandowskyy, 2005) or *PBW-algebra* (Bueso et al., 2003) or *algebra of solvable type* (Kandri-Rody and Weispfenning, 1990). Important examples for these algebras are universal enveloping algebras of finite-dimensional Lie algebras (where the term order is degree-compatible), see Kandri-Rody and Weispfenning (1990), Theorem 1.14. The generalization to G-algebras of the approach presented here should be possible.

4. Reduced Gröbner bases

In this section we need additional data for the coefficient ring R. We assume that

- for any ideal Q in R we have selected a finite system of generators $\mathrm{Gen}(Q)$ of Q and
- for any ideal Q of R and any coset $z + Q \subseteq R$ we have selected an element $r(z, Q) \in z + Q$ such that $r(0, Q) = 0$.

Moreover we assume that if an ideal Q is given by a finite set of generators, then for any $z \in R$ the set $\mathrm{Gen}(Q)$ and the element $r(z, Q)$ can be computed in finitely many steps.

Example 13. Let $R = \mathbb{Z}$. Let $a_1, \dots, a_m$ be integers, Q the ideal generated by them and $a := gcd(a_1, \dots, a_m)$ their greatest common divisor. Let $z \in \mathbb{Z}$. Then we choose $\mathrm{Gen}(Q) := \{a\}$ and $r(z, Q) :=$ the remainder of z after division by a.

Example 14. Let $R = \mathbb{Z}_k$, where $k \geq 2$. Let $a_1, \dots, a_m$ be integers, Q the ideal generated by their residue classes $\bar{a}_1, \dots, \bar{a}_m$ modulo k and $a := gcd(a_1, \dots, a_m)$ their greatest common divisor. Then we choose $\mathrm{Gen}(Q) := \{\bar{a}\}$ and $r(z, Q) :=$ the residue class modulo k of the remainder of z after division by a.

Example 15. Let R be the polynomial ring $K[y_1, \dots, y_m]$ over a field K. Choose a term order $\preccurlyeq$ on $\mathbb{N}^m$. For an ideal $Q \trianglelefteq R$ and an element $z \in R$ we choose $\mathrm{Gen}(Q) :=$ the reduced Gröbner basis of Q with respect to $\preccurlyeq$ and $r(z, Q) :=$ the normal form of z with respect to Q and $\preccurlyeq$.

Definition 16. Let I be a left-ideal in A and $\alpha \in \mathbb{N}^n$. Let

$$\mathrm{lc}(< \alpha, I) :=_R < \mathrm{lc}(f);\ f \in I, \alpha \in \deg(f) + \mathbb{N}^n, \alpha \neq \deg(f) > .$$

Then $\mathrm{lc}(< \alpha, I) \subseteq \mathrm{lc}(\alpha, I)$. Define

$$\mathrm{Gen}(\alpha, I) := \{r(h, \mathrm{lc}(< \alpha, I)) \mid h \in \mathrm{Gen}(\mathrm{lc}(\alpha, I))\} \setminus \{0\}.$$

Definition 17. Let I be a left-ideal in A. A Gröbner basis G of I is a *reduced Gröbner basis* (with respect to $<$) iff

- for all $\alpha \in \deg(I)$ the map $\{g \in G \mid \deg(g) = \alpha\} \to \mathrm{Gen}(\alpha, I)$, $g \mapsto \mathrm{lc}(g)$, is bijective and
- for all $g := \sum_{\beta \in \mathbb{N}^n} c_{\beta,g} x^\beta \in G$ and all $\alpha \in \mathbb{N}^n$ with $\alpha \neq \deg(g)$ and $c_{\alpha,g} \neq 0$ we have $c_{\alpha,g} = r(c_{\alpha,g}, \mathrm{lc}(\alpha, I))$.

Example 18. Let $R := \mathbb{Z}$, $A := \mathbb{Z}[x_1, x_2]$ and I resp. J the ideal generated by $\{2x_1, 3x_2\}$ resp. $\{4x_1, 6x_2, 5x_1x_2\}$. We choose $\mathrm{Gen}(Q)$ and $r(z, Q)$ as in Example 13. Then $\mathrm{lc}((1, 0), I) = \mathbb{Z}2$, $\mathrm{lc}((0, 1), I) = \mathbb{Z}3$ and $\mathrm{lc}((1, 1), I) = \mathbb{Z}$, hence $\mathrm{Gen}((1, 0), I) = \{2\}$, $\mathrm{Gen}((0, 1), I) = \{3\}$ and $\mathrm{Gen}((1, 1), I) = \emptyset$. For J we get $\mathrm{lc}((1, 1), J) = \mathbb{Z}$ but $\mathrm{Gen}((1, 1), J) = \{1\}$. The reduced Gröbner basis of I resp. J is $\{2x_1, 3x_2\}$ resp. $\{4x_1, 6x_2, x_1x_2\}$.

Proposition 19. *Every left-ideal in A has a unique reduced Gröbner basis.*

Proof. Exercise. □

Remark. If R is a field and if we choose $\mathrm{Gen}(R) = \{1\}$ then Definition 17 coincides with that of Buchberger (1984).
If R is a principal ideal ring, if we choose a well-ordering on R such that 0 is the least element, and if we choose $\mathrm{Gen}(Q) := \{\text{the least generating element of } Q\}$ and $r(z, Q) =$ the minimal element in $z + Q$, then Definition 17 coincides with that of Pauer (1992), Section 3.

Acknowledgements

This article was stimulated by the Special Semester on Gröbner Bases 2006 in Linz, Austria, organized by RICAM (the Radon Institute for Computational and Applied Mathematics, Austrian Academy of Science, Linz) and RISC (Research Institute for Symbolic Computation, Johannes Kepler University, Linz) under the scientific direction of B. Buchberger.

References

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

Bueso, J., Gómez-Torrecillas, J., Verschoren, A., 2003. Algorithmic Methods in Non-commutative Algebra. Applications to Quantum Groups. Kluwer Academic Publishers, Dordrecht.

Buchberger, B., 1970. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. Aequationes Math. 4, 374–383.

Buchberger, B., 1984. A critical pair/completion algorithm for finitely generated ideals in rings. In: Börger, E., et al. (Eds.), Logic and Machines: Decision Problems and Complexity. In: Springer Lecture Notes in Computer Science, vol. 171. pp. 137–155.

Castro, F., 1987. Calculs effectifs pour les ideaux d'opérateurs differentiels. In: Aroca, J., et al. (Eds.), Géométrie algébrique et applications, vol. III. Hermann, Paris, pp. 1–20.

Galligo, A., 1985. Some algorithmic questions on ideals of differential operators. In: Springer Lecture Notes in Computer Science, vol. 204. pp. 413–421.

Insa, M., Pauer, F., 1998. Gröbner bases in rings of differential operators. In: Buchberger, B., Winkler, F. (Eds.), Gröbner Bases and Applications. Cambridge University Press, Cambridge.

Kandri-Rody, A., Kapur, D., 1988. Computing a Gröbner basis of a polynomial ideal over a Euclidean domain. J. Symbolic Comput. 6, 37–58.

Kandri-Rody, A., Weispfenning, V., 1990. Non-commutative Gröbner bases in algebras of solvable type. J. Symbolic Comput. 9, 1–26.

Levandowskyy, V., 2005. Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation, Dissertation, Universität Kaiserslautern. http://kluedo.ub.uni-kl.de/volltexte/2005/1883/.

Möller, H., 1988. On the construction of Gröbner bases using syzygies. J. Symbolic Comput. 6, 345–359.

Pan, L., 1988. On the D-bases of polynomial ideals over principal ideal domains. J. Symbolic Comput. 7, 55–69.

Pauer, F., Pfeifhofer, M., 1988. The theory of Gröbner bases. L'Enseignement Mathématique 34, 215–232.

Pauer, F., 1992. On lucky ideals for Gröbner basis computations. J. Symbolic Comput. 14, 471–482.

Trinks, W., 1978. Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. J. Number Theory 10, 475–488.

Winkler, F., Zhou, M., 2005. On computing Gröbner bases in rings of differential operators with coefficients in a ring. Technical Report No. 05-04 in RISC Report Series. University of Linz.