Non-Commutative Gröbner Bases in Poincaré-Birkhoff-Witt Extensions

Mark Giesbrecht[1], Greg Reid[2], and Yang Zang[2]

[1] School of Computer Science,
University of Waterloo, Waterloo, Canada
mwg@uwaterloo.ca
[2] Department of Applied Mathematics,
University of Western Ontario, London, Canada
{reid,yzhang26}@uwo.ca

Abstract. Commutative Gröbner Bases are a well established technique with many applications, including polynomial solving and constructive approaches to commutative algebra and algebraic geometry. Noncommutative Gröbner Bases are a focus of much recent research activity. For example, combining invariant theory and elimination theory, or elimination in moving frames of partial differential operators invariant under an equivalence group, requires the use of noncommutative Gröbner bases. This paper presents theory and algorithms for noncommutative Gröbner bases in Poincaré-Birkhoff-Witt extensions. These extension rings generalize the previous domains over which noncommutative Gröbner bases have been applied. Our approach to noncommutative Gröbner bases differs from previous work which assumes that the coefficients are from a field or commutative ring. In applications such as Cartan's method of moving frames, this is not the case, and the theory that we present can be applied.

1 Introduction

Since the mid-1980's, noncommutative Gröbner bases have developed as an active research area in Computer Algebra, with many applications. See, for example, Chyzak and Salvy [6] for Ore algebras, Green [10] for path algebras, Kandri-Rody and Weispfenning [12] for algebras of solvable type, Mora [17] for free algebras over fields. Generally speaking, there are two streams in these studies. One is free algebras, which preserve properties of semigroups. The other is algebras of solvable type (including rings of differential operators) which preserve Dickson's lemma. In most of the above papers, the authors assume that the coefficients are from a field or commutative ring, and that these commute with the indeterminates (although the indeterminates may not commute with each other).

There are many interesting and useful rings which the above papers do not address. Examples include some kinds of homogenous partial differential equations with non-constant coefficients (see Adams et al. [2]). The method of choosing coordinates which are invariant under a given symmetry group (e.g. polar coordinates), in its most general form requires the introduction of a moving frame of non-commuting partial differential operators (Cartan's famous equivalence method). Elimination theories for such systems, by necessity, require a non-commutative Gröbner Basis method of the type presented in this paper (see Lisle & Reid [14], and Mansfield [15]). Another example is the skew enveloping algebra $R\#U(L)$ (see McConnell and Robson [16]), which is important in associative ring theory. This motivates us to define Gröbner bases in Poincaré-Birkhoff-Witt (PBW) extensions. We prove the left division rule and many fundamental properties of such Gröbner bases, and give an algorithm to construct them. As a special case, we consider the graded lexicographic ordering, and reduce computing Gröbner bases of PBW extensions to the commutative case. Finally we apply this theory to the moving frame approach in Section 4.

Differential elimination algorithms have been effective in pre-processing and simplifying systems for the subsequent application of the methods of scientific computation. Such methods include numerical integration techniques and symmetry techniques.

A popular new research area is the area of Geometric Integration [18]. The general philosophy of that area is to include as many qualitative features of the physical system being studied as possible in the tools used to study the system. For example numerical integrators, which are invariant under the symplectic group (*geometric integrators*) are used to numerically solve Hamilton's equations, which are also symplectically invariant. This paper represents progress in this direction for differential elimination algorithms by, for example, enabling the differentiations and eliminations of such algorithms to be executed in a moving frame, invariant under a group admitted by the given problem. Our extension of such algorithms

Appears in Proceedings of the Fifth International Workshop on Computer Algebra in Scientific Computing, September 22-27, 2002, Yalta, Ukraine. pp. 97-106.

to coefficients which do not come from a field (and are not necessarily invertible) are potentially relevant for matrix formulations arising in non-commutative field theories. In such instances it is helpful to be able to perform such calculations, as physicists would, in the non-commutative matrix formalism, instead of breaking it down to components and using commutative differential algebra, as is the current practice. This is an area which we are investigating.

2 Poincaré-Birkhoff-Witt Extensions

We first introduce the definition of PBW extensions used in this paper, which is given by Bell and Goodearl [5]. This definition leads to a unified treatment of many polynomial rings currently studied in associative ring theory and Computer Algebra.

Definition 1. *Let R and T be two associative rings with $R \subseteq T$. T is called a (finite) PBW extension of R if there exist $x_1, x_2, \cdots, x_n \in T$ such that*

(1) the monomials $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ form a basis for T as a free left R-module, where $i_1, i_2, \cdots, i_n \in \mathbb{N}$;

(2) $x_i r - r x_i := [x_i, r] \in R$ for each $i = 1, \cdots, n$ and any $r \in R$;

(3) $x_i x_j - x_j x_i := [x_i, x_j] \in R + Rx_1 + \cdots + Rx_n$ for all $i, j = 1, \cdots, n$.

We write $T = R\langle x_1, \cdots, x_n\rangle$.

It is clear that every element of $R\langle x_1, \cdots, x_n\rangle$ can be uniquely represented as a finite sum $\sum r_i x_1^{i_1} \cdots x_n^{i_n}$, where $r_i \in R, i_1, \cdots, i_n \in \mathbb{N}$. We call the monomials of the form $x_1^{i_1} \cdots x_n^{i_n}$ *standard monomials*. Note also that any non-standard monomial $x_{j_1}^{i_1} \cdots x_{j_n}^{i_n}$ can be expressed as a finite sum of standard monomials.

Remark 1. We remind the reader of the differences between PBW extensions and other similar algebraic structures. For example, comparing PBW extensions with algebras of solvable type defined in [12], we note a number of important differences. Algebras of solvable type require coefficients and indeterminates commute, whereas PBW extensions make no such requirement. For example, $R\#U(L)$ is not an algebra of solvable type in general, but is a PBW extension. On the other hand, algebras of solvable type define a "quantum" or "ordering" version of condition (3) above, which states roughly that the commutator is smaller than the product under a term ordering. In an upcoming paper we define skew-PBW extensions which include both algebras of solvable type and PBW extensions. We also suggest that reader should compare PBW extensions with free algebras and note the differences.

Example 1. There are several prototypical examples of PBW extensions:

(1) The usual multivariate polynomial rings over R, Ore algebras and PBW algebras discussed in Computer algebra. The skew enveloping algebra (or smash product) $R\#U(L)$ is an example of PBW extensions. In particular, the universal enveloping algebra $U(L)$, the n-Weyl algebra $A_n(K)$ and skew polynomial ring (derivation type) $R[x, \delta]$ also are examples of PBW extensions (see McConnell and Robson [16]).

(2) Some kinds of PDEs with non-constant coefficients. For example, let $R = K(x_1, \cdots, x_n)$ be a function field over a field K. It is well-known that all partial derivations over R form a (possibly infinite dimensional) Lie algebra under the usual brace product. In the language of PDEs, one partial differential equation is written as:

$$a_n(x_1, \cdots, x_n)\frac{\partial^{i_1}}{\partial x_1^{i_1}} \cdots \frac{\partial^{i_n}}{\partial x_n^{i_n}} + \cdots + a_0(x_1, \cdots, x_n) = 0.$$

Corresponding to the skew enveloping algebra, the above equation is in the ring $K(x_1, \cdots, x_n)\#U(L)$, and can be written as:

$$a_n(x_1, \cdots, x_n)\bar{x}_1^{i_1} \cdots \bar{x}_n^{i_n} + \cdots + a_0(x_1, \cdots, x_n) = 0$$

where the new (non-commuting) indeterminates $\bar{x}_1, \ldots, \bar{x}_n$ represent the operators $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}$ respectively.

(3) Moving frames (see Section 4) and some systems of linear homogeneous partial differential equations with non-constant coefficients (see [2], [14] and [15]).

We denote by $\mathcal{M}(X)$ or $\mathcal{M}(x_1,\ldots,x_n)$ the set $\{x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}\,|\,\alpha_i\in\mathbb{N}\}$ of all standard monomials of $\{x_1,\cdots,x_n\}$. For simplicity, we write $X^\alpha=x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ and $\alpha=(\alpha_1,\alpha_2,\cdots,\alpha_n)\in\mathbb{N}^n$. Given a total order $\prec$ on the set of standard monomials, we define the *leading monomial* $\mathrm{lm}(f)$ of $f\in R\langle x_1,\cdots,x_n\rangle$ to be the largest standard monomial occurring in f with non-zero coefficient, the *leading coefficient* $\mathrm{lc}(f)$ to be the coefficient of $\mathrm{lm}(f)$ and *leading term* $\mathrm{lt}(f)=\mathrm{lc}(f)\cdot\mathrm{lm}(f)$. For a subset $S\subseteq R\langle x_1,\cdots,x_n\rangle$, $\mathrm{lm}(S)=\{\mathrm{lm}(s)|s\in S\}$ while $\mathrm{lc}(S)$ and $\mathrm{lt}(S)$ are similarly defined and $_\ell(S)$ will be the left ideal generated by S in $R\langle x_1,\cdots,x_n\rangle$. The *degree* of $X^\alpha:=x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ is $deg(X^\alpha)=|\alpha|:=\alpha_1+\cdots\alpha_n$.

Definition 2. *An admissible order $\prec$ on $\mathcal{M}(X)$ is a total order of $\mathcal{M}(X)$ which satisfies:*

(1) multiplicative, i.e., $r\prec X^\alpha$ and $X^\alpha\prec X^\beta$ imply that $\mathrm{lm}(X^\eta X^\alpha X^\gamma)\prec\mathrm{lm}(X^\eta X^\beta X^\gamma)$, where $X^\eta,X^\alpha,X^\beta,X^\gamma\in\mathcal{M}(X)$ and $r\in R$.

(2) degree compatible, i.e., $deg(X^\alpha)\prec deg(X^\beta)$ implies $X^\alpha\prec X^\beta$, where $X^\alpha,X^\beta\in\mathcal{M}(X)$.

Remark 2. From condition (2), we get the *descending chain condition*, i.e., there are no infinite strictly descending chains of standard monomials, which is used to prove that the reductions will stop eventually.

Example 2. The typical example of this order is the graded lexicographic ordering. That is, $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}\prec x_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$ if and only if the first nonzero component of $(\sum_{k=1}^n(\alpha_k-\beta_k),\alpha_1-\beta_1,\cdots,\alpha_n-\beta_n)$ is negative.

Before computing Gröbner bases in PBW extensions, we first need a notion of the coefficient ring being computable.

Definition 3. *An associative (though not necessarily commutative) ring R is (left) computable, if in addition to the usual arithmetic operations being computable, the following two conditions hold:*

(1) (left ideal membership) Given $a,a_1,\cdots,a_m\in R$, there is an algorithm which decides whether a is in the left ideal $R(a_1,\cdots,a_m)$ and if so, finds $b_1,b_2,\cdots,b_m\in R$ such that $a=\sum_{i=1}^m b_ia_i$.

(2) (left syzygies) Given $a_1,\cdots,a_m\in R$ there is an algorithm which finds a finite set of generators for the R-module

$$Syz(a_1,\cdots,a_m):=\{(b_1,\cdots,b_m)\in R^m|\sum_{i=1}^m b_ia_i=0\}.$$

If R is a field, the condition "left ideal membership" is trivial. But if R is a ring, it is a useful and necessary condition. The condition "left syzygies" is needed to guarantee that the algorithm `GröbnerPBW` which follows is implementable, since from the noetherian condition we only know that there exist a finite number of generators. In fact these conditions have been used in many papers, for example, Gianni, Trager and Zacharias [9]. It is a common condition when one considers Gröbner theory on rings instead of fields. There are many rings satisfying this condition, for example, the usual polynomial ring over a field and the universal enveloping Lie algebra over a field (see Apel and Lassner [4]).

In the remainder of the paper, we assume that R is a left computable and noetherian (not necessarily commutative) ring with a finite PBW extension $R\langle x_1,\cdots,x_n\rangle$, and $\prec$ is an admissible order on $\mathcal{M}(X)$.

3 Gröbner Bases in PBW Extensions

In [8], Galligo first considered Gröbner bases in the ring of linear differential operators. Later, many authors extended Galligo's idea to various rings. For example, Chyzak and Salvy [6] consider Gröbner bases in Ore algebras, and Insa and Pauer [11] for Gröbner bases in the ring of differential operators, assuming the coefficient form a subring of a function field. In this paper we consider the more general case, PBW extensions.

Definition 4. *For $f,g\in\mathcal{M}(X)$, f is a factor of g if there exist $p,q\in\mathcal{M}(X)$ such that $g=\mathrm{lm}(pfq)$. Also g is said to be divisible by f, denoted by $f|g$.*

It is easy to see that if $f=x_1^{\alpha_1}\cdots x_n^{\alpha_n}$, and $g=x_1^{\beta_1}\cdots x_n^{\beta_n}$, then f is a factor of g if and only if $\alpha_k\leq\beta_k$, for all $1\leq k\leq n$.

In the following definition, we only require that the leading terms are reduced. The conditions involving reduced polynomials (over rings) are no longer required, and so reducing non-leading terms is unnecessary (see [1], p.211).

Definition 5. *Let G be a finite subset of $R\langle x_1,\cdots,x_n\rangle$ and $f,h\in R\langle x_1,\cdots,x_n\rangle$. We say h is a one step reduction of f modulo G, denoted $f\to^G h$, if for the leading term aX^α in f, there exist $g_1,\cdots,g_t\in G$ and $r_1,\cdots,r_t\in R$ such that*
(1) $\mathrm{lm}(g_i)$'s are factors of X^α, say $\mathrm{lm}(X^{\beta_i}g_iX^{\gamma_i})=X^\alpha$, for all $i=1,\cdots,t$;
(2) $a=\sum_{i=1}^t r_i\,\mathrm{lc}(g_i)$ for some $r_i\in R, i=1,\cdots,t$;
(3) $h=f-\sum_{i=1}^t r_iX^{\beta_i}g_iX^{\gamma_i}$.

Furthermore, we say f reduces to h modulo G if and only if there exist $h_1,\cdots,h_s\in R\langle x_1,\cdots,x_n\rangle$ such that $f\to^G h_1\to^G h_2\to^G\cdots\to^G h_s\to^G h$.

Remark 3.
(1) Note that the conditions of (1) and (3) are equivalent to:
(1)' $\mathrm{lm}(g_i)$'s are factors of X^α, say $\mathrm{lm}(X^{\beta_i}g_i)=X^\alpha$, for all $i=1,\cdots,t$;
(3)' $h=f-\sum_{i=1}^t r_iX^{\beta_i}g_i$.
(2) We remind the reader that Gauss reduction does not work in PBW extensions since the elements of R are not necessarily invertible. Therefore we have to use "sum" to cancel some terms. For example, consider the PBW extension $K[y_1,y_2,y_3]\langle x_1,x_2,x_3\rangle$, where $K[y_1,y_2,y_3]$ is the usual polynomial ring over a field K and $\{x_1,x_2,x_3\}$ is the 3-dimensional Lie algebra with $[x_1,x_2]=x_1,[x_1,x_3]=-2x_1$ and $[x_2,x_3]=-2x_3$. Set $G=\{g_1:=y_1x_1,g_2:=y_2x_2\}$ and $f:=(2y_1+3y_2)x_1x_2+x_1+1$. Since $K[y_1,y_2,y_3]$ is just a ring, not a field, we do elimination as follows:

$$\begin{aligned}h&=f-(2g_1x_2+3g_2x_1)=(2y_1+3y_2)x_1x_2+x_1+1-(2(y_1x_1)x_2+3(y_2x_2)x_1)\\&=(2y_1+3y_2)x_1x_2+x_1+1-(2(y_1x_1x_2)+3y_2(x_1x_2-x_3))=x_1-3y_2x_3+1.\end{aligned}$$

Definition 6. *An element $f\in R\langle x_1,\cdots,x_n\rangle$ is said to be in reduced form with respect to G if f can not be reduced modulo G. A reduced form of f modulo G is an element $h\in R\langle x_1,\cdots,x_n\rangle$ such that h is in reduced form with respect to G and $f\to^G h$.*

As in the commutative case we have a division rule, but here it is one-sided.

Proposition 1. (Left division rule) *Let $G:=\{g_1,\cdots,g_t\}\subseteq R\langle x_1,\cdots,x_n\rangle$ and $f\in R\langle x_1,\cdots,x_n\rangle$. Then there exist $h_1,\cdots,h_t,\psi\in R\langle x_1,\cdots,x_n\rangle$ such that $f=h_1g_1+\cdots+h_tg_t+\psi$, where ψ is reduced modulo G and $\mathrm{lm}(f)=max\{max\{\mathrm{lm}(\mathrm{lm}(h_i)\,\mathrm{lm}(g_i))\}_{i=1}^t,\mathrm{lm}(\psi)\}$.*

Proof. If f is reduced modulo G, then there is nothing to do. Assume then that there is a reduction chain $f\to\psi_1\to\psi_2\to\cdots$. By the definition of reduction, the leading term is decreased, that is, $\mathrm{lm}(f)\succ\mathrm{lm}(\psi_1)\succ\mathrm{lm}(\psi_2)\succ\cdots$. Since $\succ$ is a well-ordering, the reduction chain has to stop, say, $f\to\psi_1\to\cdots\to\psi_s\to\psi$, where ψ is reduced modulo G. By the remark 3, we have $f-\psi_1=r_{11}X^{\alpha_{11}}g_1+\cdots+r_{1t}X^{\alpha_{1t}}g_t$, where $\{r_{1i}\}\in R$, $\mathrm{lt}(f)=r_{11}\,\mathrm{lt}(X^{\alpha_{11}}g_1)+\cdots+r_{1t}\,\mathrm{lt}(X^{\alpha_{1t}}g_t)$ (some r_{ji} and α_{ji} maybe zero) and $\mathrm{lm}(f)=\mathrm{lm}(X^{\alpha_{1i}}g_i)$ for all i such that $r_{1i}\neq0$ (since R maybe has zero-divisors). Similarly we have the representation for $\psi_1-\psi_2=r_{21}X^{\alpha_{21}}g_1+\cdots+r_{2t}X^{\alpha_{2t}}g_t$. Therefore

$$f-\psi_2=(f-\psi_1)+(\psi_1-\psi_2)=(r_{11}X^{\alpha_{11}}+r_{21}X^{\alpha_{21}})g_1+\cdots+(r_{1t}X^{\alpha_{1t}}+r_{2t}X^{\alpha_{2t}})g_t.$$

Note that the coefficients of $\{g_i\}$ are not all zero if $s>2$. Continuing in this way, we get the representation for $f-\psi$ as required. □

The above proposition gives a method to calculate the reduced form:

Algorithm: `ReducedForm`
Input: ▸ $G=\{g_1,\cdots,g_t\}\subseteq R\langle x_1,\cdots,x_n\rangle$;
▸ $f\in R\langle x_1,\cdots,x_n\rangle$;
Output: ▸ a reduced form of f modulo G: $h_1,\cdots,h_t,\psi\in R\langle x_1,\cdots,x_n\rangle$ such that $f=h_1g_1+\cdots+h_tg_t+\psi$, where ψ is reduced modulo G and $\mathrm{lm}(f)=max\{max\{\mathrm{lm}(\mathrm{lm}(h_i)\,\mathrm{lm}(g_i))\}_{i=1}^t,\mathrm{lm}(\psi)\}$;

Set $\psi:=f$ and $h_1,\ldots,h_t:=0$;
While $\psi\neq0$ and $\mathrm{lc}(\psi)\in{}_\ell(\mathrm{lc}(g):g\in G,\mathrm{lm}(g)|\,\mathrm{lm}(\psi))$ Do
Find $\{r_i\}_1^t\in R$, $\{X^{\alpha_i}\}_1^t$ so $\mathrm{lc}(\psi)=\sum_{i=1}^t r_i\,\mathrm{lc}(g_i)$, $\mathrm{lm}(X^{\alpha_i}g_i)=\mathrm{lm}(\psi)$;
$\psi:=\psi-\sum_{i=1}^t r_iX^{\alpha_i}g_i$.
For $i=1$ to t Do $h_i:=h_i+r_iX^{\alpha_i}$;
End.

Definition 7. *Let I be a left ideal of $R\langle x_1,\cdots,x_n\rangle$ and G a subset of I. Then G is called a (left) Gröbner basis of I if for all $f\in I$, $f\to^G 0$.*

While some of the definitions and theorems in the PBW extensions case are equivalent to those in the commutative case, others do not hold.

Theorem 1. *Let I be a left ideal of $R\langle x_1,\cdots,x_n\rangle$ and let G be a finite subset of I. The following assertions are equivalent:*

(1) G is a left Gröbner basis of I;

(2) For all $0\neq f\in I$, f is reducible modulo G;

(3) For all $0\neq f\in I$, there exist $g_1,\cdots,g_t\in G$ such that $\operatorname{lm}(g_i), i=1,\cdots,t$ are factors of $\operatorname{lm}(f)$ and $\operatorname{lc}(f)\in {}_\ell(\operatorname{lc}(g_1),\cdots,\operatorname{lc}(g_t))$;

(4) For $\alpha\in\mathbb{N}^n$, let ${}_\ell(\alpha,I):={}_\ell(\operatorname{lc}(f):f\in I,\operatorname{lm}(f)=X^\alpha)$. Then for all $\alpha\in\mathbb{N}^n$ the left ideal ${}_\ell(\alpha,I)$ is generated by $\{\operatorname{lc}(g):g\in G,\operatorname{lm}(g)|X^\alpha\}$.

Proof. (1) $\Rightarrow$ (2) follows from the definition of Gröbner bases.

(2) $\Rightarrow$ (1): Let $G:=\{g_1,\cdots,g_t\}$ and $0\neq f\in I$. Since f is reducible, by induction and Proposition 1, there exist $h_1,\cdots h_t,\psi\in R\langle x_1,\cdots,x_n\rangle$ such that $f=h_1g_1+\cdots h_tg_t+\psi$, where ψ is reduced modulo G. This implies that $\psi=f-(h_1g_1+\cdots+h_tg_t)\in I$, and so ψ is reducible by (2), a contradiction. Therefore $\psi=0$, that is, f can be reduced to 0 modulo G.

(2) $\Leftrightarrow$ (3) follows from the definition of reduction.

(3) $\Rightarrow$ (4): For fixed $\alpha\in\mathbb{N}^n$, for any $r\in {}_\ell(\alpha,I)$, since ${}_\ell(\alpha,I)$ is usually not a principal ideal, there exist $f_1,\cdots,f_t\in I$ with $\operatorname{lm}(f_i)=X^\alpha, i=1,\cdots,t$ and $a_1,\cdots,a_t\in R$ such that $r=a_1\operatorname{lc}(f_1)+\cdots+a_t\operatorname{lc}(f_t)$. From (3), for each f_i, we have $\operatorname{lc}(f_i)=b_1\operatorname{lc}(g_{i1})+\cdots+b_s\operatorname{lc}(g_{is})$, where $g_{ij}\in G,\operatorname{lm}(g_{ij})|\operatorname{lm}(f_i), b_j\in R, j=1,\cdots,s$. Thus $r\in {}_\ell(\operatorname{lc}(g):g\in G,\operatorname{lm}(g)|X^\alpha)$.

Conversely, let $a\in {}_\ell(\operatorname{lc}(g):g\in G,\operatorname{lm}(g)|X^\alpha)$. Then $a=r_1\operatorname{lc}(g_1)+\cdots+r_t\operatorname{lc}(g_t)$ for some $r_i\in R, g_i\in G,\operatorname{lm}(g_i)|X^\alpha, i=1,\cdots,t$. Choose $\{X^{\alpha_i}\}_1^t\in\mathcal{M}(X)$ such that $\operatorname{lm}(X^{\alpha_i}g_i)=X^\alpha$ for $i=1,\cdots,t$. Note that $X^{\alpha_i}g_i\in I$, we get

$$\begin{aligned}a&=r_1\operatorname{lc}(g_1)+\cdots+r_t\operatorname{lc}(g_t)=r_1\operatorname{lc}(X^{\alpha_1}g_1)+\cdots+r_t\operatorname{lc}(X^{\alpha_t}g_t)\\&\in {}_\ell(\operatorname{lc}(f):f\in I,\operatorname{lm}(f)=X^\alpha).\end{aligned}$$

(4) $\Rightarrow$ (3): For any $0\neq f\in I$, let $\operatorname{lm}(f)=X^\alpha$. Then $\operatorname{lc}(f)\in {}_\ell(\alpha,I)$. By (4), $\operatorname{lc}(f)\in {}_\ell(\operatorname{lc}(g):g\in G,\operatorname{lm}(g)|X^\alpha)$. □

Corollary 1.

(1) If G is a Gröbner basis for the left ideal I in $R\langle x_1,\cdots,x_n\rangle$, then $I={}_\ell(G)$.

(2) If G is a Gröbner basis and $f\in {}_\ell(G)$ and $f\to^G h$, where h is reduced, then $h=0$.

(3) Let G be the Gröbner basis of left ideal I and $f\in R\langle x_1,\cdots,x_n\rangle$. Then $f\in I$ if and only if $f=0$ modulo G.

Next we give a method to construct Gröbner bases in PBW extensions. We remind the reader that in general rings the S-pair criteria do not work. A simple example can be found in ([4], p.248).

Theorem 2. *Let I be the left ideal of $R\langle x_1,\cdots,x_n\rangle$ generated by a finite set G. For $F:=\{g_1,\cdots,g_s\}\subseteq G$, let $\operatorname{lcm}(F)$ be the least common multiple of $\{\operatorname{lm}(g_i)\}_{i=1}^s$. Let $\mathcal{B}_F$ be a finite set of generators of $Syz(\operatorname{lc}(g_1),\cdots,\operatorname{lc}(g_s))$. Then the following assertions are equivalent:*

(1) G is a Gröbner basis of I;

(2) For all $F:=\{g_i\}_1^s\subseteq G$ and for all $\{b_1,\ldots,b_s\}\in\mathcal{B}_F$, we have that $\sum_{i=1}^s b_i(X^{\operatorname{lcm}(F)}/\operatorname{lm}(g_i))g_i$ reduces to zero with respect to G.

Proof. (1) $\Rightarrow$ (2) follows from $\sum_{i=1}^s b_i(X^{\operatorname{lcm}(F)}/\operatorname{lm}(g_i))g_i\in {}_\ell(G)$.

(2) $\Rightarrow$ (1): Let $f\in I$. By Theorem 1 we need to show: $\operatorname{lc}(f)\in {}_\ell(\operatorname{lc}(g):g\in G,\operatorname{lm}(g)|\operatorname{lm}(f))$. Let $G:=\{g_1,\cdots,g_t\}$. Then $f\in I$ implies that there exists a representation $f=\sum_{i=1}^t f_ig_i$. Furthermore we may choose $\{f_i\}_1^t$ such that $max_\prec\{\operatorname{lm}(\operatorname{lm}(f_i)\operatorname{lm}(g_i))\}_{i=1}^t$