J. Symbolic Computation (1998) **25**, 23–43

A Generalization of Gröbner Basis Algorithms to Polycyclic Group Rings

KLAUS MADLENER[†] AND BIRGIT REINERT[‡]

Fachbereich Informatik, Universität Kaiserslautern,
67663 Kaiserslautern, Germany

It is well-known that for the integral group ring of a polycyclic group several decision problems are decidable, in particular the ideal membership problem. In this paper we define an effective reduction relation for group rings over polycyclic groups. This reduction is based on left multiplication and hence corresponds to left ideals. Using this reduction we present a generalization of Buchberger's Gröbner basis method by giving an appropriate definition of "Gröbner bases" in this setting and by characterizing them using the concepts of saturation and s-polynomials. The approach is extended to two-sided ideals and a discussion on a Gröbner bases approach for right ideals is included.

1. Introduction

By introducing Gröbner basis theory for polynomial ideals into the theory of commutative polynomial rings over fields, Buchberger (1965) established a rewriting approach to the theory of polynomial ideals. He used polynomials as rules by giving an admissible term ordering for the terms and using the largest monomial according to this ordering as the left-hand side of the rule. "Reduction" defined in this way can be compared to division of one polynomial by a set of finitely many polynomials or to special forms of Gaussian elimination. A Gröbner basis is now a set of polynomials G such that every polynomial in the polynomial ring has a unique normal form with respect to reduction using the polynomials in G as rules (in particular the polynomials in the ideal generated by G reduce to zero using G). Hence such bases enable many problems related to ideals (when they can be computed) to be solved. For the polynomial ring Buchberger developed a terminating procedure to transform the finite generating set of a polynomial ideal into a finite Gröbner basis of the same ideal.

Since Gröbner basis theory turned out to be so important for polynomial rings, Buchberger's ideas were extended to other algebras, for example free algebras (Mora, 1985, 1994), Weyl algebras (Lassner, 1985), enveloping fields of Lie algebras (Apel and Lassner, 1988), solvable rings (Kandri-Rody and Weispfenning, 1990; Kredel, 1993), skew polynomial rings (Weispfenning, 1992), free group rings (Rosenmann, 1993) and monoid and

[†] Email: {madlener,reinert}@informatik.uni-kl.de

[‡] The second author was supported by the Deutsche Forschungsgemeinschaft (DFG).

0747–7171/98/010023 + 21 $25.00/0 sy970165

group rings (Madlener and Reinert, 1993b). The results of this paper now complete our claim that Gröbner basis methods can be successfully adapted to all group rings in which the subgroup problem of the group is solvable using rewriting techniques (free groups, plain groups, context-free groups, Abelian groups and nilpotent groups are discussed in Reinert (1995)).

Group rings, in particular, are the subject of extensive studies in mathematics. In 1981 Baumslag, Cannonito and Miller showed that for an integral group ring of a polycyclic group, i.e., a group with a finite subnormal series with cyclic factors, several decision problems including the membership problem for submodules are computable (Baumslag *et al.*, 1981). Studying these ideas Sims (1994) described how the connections between special submodule bases enable the membership problem and conventional Gröbner bases to be solved.

In this paper we present our results which generalize reduction and Gröbner bases to polycyclic group rings. We want to point out that instead of using the fact that every group ring over a polycyclic group is Noetherian, our approach is oriented towards rewriting which leads to a syntactical characterization of Gröbner bases in terms of s-polynomials and a completion-based algorithm with which to compute them.

It is well-known that a polycyclic group $\mathcal{G}$ can be represented by a special form of the confluent semi-Thue system (Wißmann, 1989; Sims, 1994). This type of presentations includes the usual confluent presentations for finitely generated Abelian and nilpotent groups. Due to this presentation we can define the concept of "commutative prefixes" for group elements which captures the known fact that in the commutative polynomial ring a divisor of a term is also a commutative prefix of this term. This concept was used to define a Noetherian reduction in group rings over finitely generated nilpotent rings in Madlener and Reinert (1996) and to generalize Gröbner basis algorithms for right and two-sided ideals in this setting. Due to the fact that polycyclic groups represented by convergent polycyclic power commutation systems have crucially different collection properties from those of nilpotent groups represented by convergent nilpotent power commutation systems, these generalizations no longer work. Nevertheless, they can be applied when studying a special form of left reduction (called here left polycyclic reduction (*lpc-reduction*)) and, at first, left ideals. Later on we show how Gröbner bases of two-sided ideals can be characterized using left Gröbner bases if, in addition, we require that the generated left ideal coincides with the generated ideal. For Abelian groups the latter is obvious and for polycyclic groups we can give additional conditions for when this holds. Since we have no admissible ordering on the group elements, reduction steps are not preserved under multiplication with group elements, i.e., if a polynomial p is reducible using a polynomial f, a multiple $w * p$ for some group element w no longer needs to be reducible using f. Remember that this was essential in Buchberger's approach as it implies that when $p \overset{*}{\longrightarrow}_F 0$ we can conclude $w * p \overset{*}{\longrightarrow}_F 0$. Furthermore, lpc-reduction does not capture left ideal congruence. To repair these defects we use a technique known as saturation: F is said to be saturated if, for all $f \in F$, $w \in \mathcal{G}$, the left-multiple $w * f$ is lpc-reducible in *one* step to zero using F. Using this concept we give a characterization of a left Gröbner basis using s-polynomials and present an algorithm to compute finite left Gröbner bases. Then the approach is extended to compute Gröbner bases with two-sided ideals. Contrary to expectation it is shown that right ideals cannot be treated in the same fashion. Nevertheless by choosing the appropriate presentation of the polycyclic group a similar result for right ideals can be presented.

The proofs of the lemmata and theorems stated in this paper can be found in the appendix unless they have been published elsewhere.

2. Basic Definitions

Let $\mathcal{G}$ be a group with binary operation $\circ$ and identity λ. The elements of a group ring $\mathbb{K}[\mathcal{G}]$ over a field $\mathbb{K}$ can be presented as polynomials $f = \sum_{g \in \mathcal{G}} \alpha_g \cdot g$ where only finitely many coefficients are non-zero. Addition and multiplication for two polynomials $f = \sum_{g \in \mathcal{G}} \alpha_g \cdot g$ and $h = \sum_{g \in \mathcal{G}} \beta_g \cdot g$ are defined as $f + h = \sum_{g \in \mathcal{G}} (\alpha_g + \beta_g) \cdot g$ and $f * h = \sum_{g \in \mathcal{G}} \gamma_g \cdot g$ with $\gamma_g = \sum_{x \circ y = g \in \mathcal{G}} \alpha_x \cdot \beta_y$. For a subset F of $\mathbb{K}[\mathcal{G}]$ we call the set $\mathsf{ideal}_l(F) = \{\sum_{i=1}^{n} \alpha_i \cdot w_i * f_i \mid n \in \mathbb{N}, \alpha_i \in \mathbb{K}, f_i \in F, w_i \in \mathcal{G}\}$ the *left ideal* and $\mathsf{ideal}(F) = \{\sum_{i=1}^{n} \alpha_i \cdot u_i * f_i * w_i \mid n \in \mathbb{N}, \alpha_i \in \mathbb{K}, f_i \in F, u_i, w_i \in \mathcal{G}\}$ the *two-sided ideal* generated by F.

As we are interested in constructing Gröbner bases for ideals in $\mathbb{K}[\mathcal{G}]$, we need an appropriate presentation of the group $\mathcal{G}$ in order to do the computations. Since $\mathcal{G}$ is a polycyclic group, we have special group presentations using finite convergent semi-Thue systems (e.g. see Wißmann (1989) and Sims (1994) for more information on this subject). The generators of these presentations are directly related to the cyclic factors of the polycyclic series. Next we give the technical details of such presentations which are necessary to understand the proofs of the lemmata and theorems. It is important that these presentations allow us to treat the elements of $\mathcal{G}$ as ordered group words and to define a tuple ordering on these representatives which can be used to define particular representations for polynomials and a Noetherian reduction.

Let $\Sigma = \{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$ be a finite alphabet where a_i^{-1} is called the formal inverse of the letter a_i. For $1 \leq k \leq n$ we define the subsets $\Sigma_k = \{a_i, a_i^{-1} \mid k \leq i \leq n\}$, $\Sigma_{n+1} = \emptyset$ and the set of *ordered group words* $\mathsf{ORD}(\Sigma) = \mathsf{ORD}(\Sigma_1)$ recursively by $\mathsf{ORD}(\Sigma_{n+1}) = \{\lambda\}$, and $\mathsf{ORD}(\Sigma_i) = \{w \in \Sigma_i^* \mid w \equiv uv$ for some $u \in \{a_i\}^* \cup \{a_i^{-1}\}^*, v \in \mathsf{ORD}(\Sigma_{i+1})\}$. Note that $\equiv$ will be used to denote identity of elements as words.

Furthermore let the set P include those letters a_i whose exponents are bounded by natural numbers m_i, corresponding to the generators of the finite cyclic factors. The semi-Thue system $T = T_P \cup T_C \cup T_I$ over Σ where $T_P = \{a_i^{m_i} \longrightarrow z, a_i^{-1} \longrightarrow a_i^{m_i - 1} v \mid a_i \in P, z, v \in \mathsf{ORD}(\Sigma_{i+1}),\}$, $T_C = \{a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} z \mid j > i, \delta, \delta' \in \{1, -1\}, z \in \mathsf{ORD}(\Sigma_{i+1})\}$, $T_I = \{a_i a_i^{-1} \longrightarrow \lambda, a_i^{-1} a_i \longrightarrow \lambda \mid 1 \leq i \leq n\}$ is a polycyclic power commutation (PCP) presentation of a group $\mathcal{G}$. By Wißmann (1989) there exist such presentations which are convergent with respect to the syllable ordering (with status left) induced by the precedence $a_1^{-1} \succ a_1 \succ \cdots \succ a_i^{-1} \succ a_i \succ \ldots \succ a_n^{-1} \succ a_n$ on Σ as defined below. Multiplication of two elements $u, v \in \mathsf{ORD}(\Sigma)$, i.e., $u \circ v$, then corresponds to computing the normal form of the word uv.

Definition 2.1. *Let Σ be an alphabet and $\succ$ a partial ordering on Σ^*. We define an ordering $\succ^{\text{lex}}$ on tuples over Σ^* as follows: $(u_0, \ldots, u_m) \succ^{\text{lex}} (v_0, \ldots, v_m)$ if and only if there exists $0 \leq k \leq m$ such that $u_i = v_i$ for all $0 \leq i < k$ and $u_k \succ v_k$. Let $a \in \Sigma$. Then every $w \in \Sigma^*$ can be uniquely decomposed with respect to a as $w \equiv w_0 a w_1 \ldots a w_k$, where $|w|_a = k \geq 0$ and $w_i \in (\Sigma \setminus \{a\})^*$. Given a total precedence $\succ$ on Σ we can then define $u >_{\text{syll}(\Sigma)} v$ if and only if $|u|_a > |v|_a$ or $|u|_a = |v|_a$ and $(u_0, \ldots, u_m) >^{\text{lex}}_{\text{syll}(\Sigma \setminus \{a\})} (v_0, \ldots, v_m)$ where a is the largest letter in Σ according to $\succ$*

and $(u_0, \ldots, u_m)$*,* $(v_0, \ldots, v_m)$ *are the decompositions of* u *and* v *with respect to* a *when* $|u|_a = |v|_a = m$*.*

The irreducible elements representing the elements in $\mathcal{G}$ are ordered group words. Restricting the syllable ordering to ordered group words we find that $a_1^{i_1} \ldots a_n^{i_n} <_{\mathrm{syll}} a_1^{j_1} \ldots a_n^{j_n}$ if and only if for some $1 \leq d \leq n$ we have $i_l = j_l$ for all $1 \leq l \leq d-1$ and $i_d <_{\mathbb{Z}} j_d$ with

$$\alpha <_{\mathbb{Z}} \beta \text{ iff } \begin{cases} \alpha \geq 0 \text{ and } \beta < 0 \\ \alpha \geq 0, \beta > 0 \text{ and } \alpha < \beta \\ \alpha < 0, \beta < 0 \text{ and } \alpha > \beta \end{cases}$$

where $\leq$ is the usual ordering on $\mathbb{Z}$. We then call the letter a_d the *distinguishing letter* of the two elements. Now the following lemma from Wißmann (1989) gives some insight into how special multiples influence the representation of the word representing the product.

Lemma 2.1. *Let* $\mathcal{G}$ *have a convergent PCP presentation* (Σ, T)*. Furthermore for some* $1 \leq i < n$ *let* $w \in \mathsf{ORD}(\Sigma_{i+1})$*. Then we have* $w \circ a_i \equiv a_i z$ *for some* $z \in \mathsf{ORD}(\Sigma_{i+1})$*.*

We can define a tuple ordering on $\mathcal{G}$ as follows. For two elements $w \equiv a_1^{i_1} \ldots a_n^{i_n}$, $v \equiv a_1^{j_1} \ldots a_n^{j_n}$, we define $w \geq_{\mathrm{tup}} v$ if for each $1 \leq l \leq n$ we have either $j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ and $|i_l| \geq |j_l|$ where $\mathsf{sgn}(i)$ is the sign of the non-zero integer i. Furthermore we define $w >_{\mathrm{tup}} v$ if $w \geq_{\mathrm{tup}} v$ and $|i_l| > |j_l|$ for some $1 \leq l \leq n$ and $w \geq_{\mathrm{tup}} \lambda$ for all $w \in \mathcal{G}$. According to this ordering we call v a *commutative prefix* of w if $v \leq_{\mathrm{tup}} w$. Notice that this ordering captures the fact that a divisor of a term in the ordinary polynomial ring is also a commutative prefix of the term. The tuple ordering is not total on $\mathcal{G}$ but we find that $v \leq_{\mathrm{tup}} w$ implies $v \preceq w$.

In Madlener and Reinert (1996) this ordering is used to define so called quasi-commutative reduction with respect to right ideals. A polynomial p is quasi-commutatively reducible at one of its monomials $\alpha \cdot t$ by another polynomial f when $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$. Then the result of this reduction is $p - (\alpha \cdot \mathsf{HC}(f)^{-1}) \cdot f * (\mathsf{inv}(\mathsf{HT}(f)) \circ t$ and the term t is replaced by smaller terms due to the following lemma:

Lemma 2.2. *Let* $\mathcal{G}$ *be a group represented by a convergent nilpotent power commutation system and* $w, v, \tilde{v} \in \mathcal{G}$ *with* $w \geq_{\mathrm{tup}} v$ *and* $v \succ \tilde{v}$*. Then for* $u \in \mathcal{G}$ *such that* $w = v \circ u$*, we get* $w \succ \tilde{v} \circ u$*. Notice that since* $\mathcal{G}$ *is a group,* u *always exists and is unique, namely* $u = \mathsf{inv}(v) \circ w$*.*

Hence we have established some restricted kind of stability for special right multiples. Unfortunately, the next example shows that for PCP presentations of groups this in general no longer holds.

Example 2.1. *Let* $\Sigma = \{a, a^{-1}, b, b^{-1}, c, c^{-1}\}$ *and* $T = \{ca \longrightarrow abc,\ ca^{-1} \longrightarrow a^{-1}b^{-1}c,\ c^{-1}a \longrightarrow ab^{-1}c^{-1},\ c^{-1}a^{-1} \longrightarrow a^{-1}bc^{-1},\ c^{\delta}b^{\delta'} \longrightarrow b^{\delta'}c^{\delta},\ b^{\delta}a^{\delta'} \longrightarrow a^{\delta'}b^{\delta} \mid \delta,\ \delta' \in \{1, -1\}\} \cup T_I$ *be a PCP presentation of the free nilpotent group with two generators. Then for* $w \equiv a^2b$*,* $v \equiv ab$ *and* $\tilde{v} \equiv ac$ *we have* $w \geq_{\mathrm{tup}} v$*,* $v \succ \tilde{v}$*. Now for* $u \equiv a$ *we find* $v \circ u = ab \circ a \equiv a^2b$*, but* $\tilde{v} \circ u = ac \circ a = a^2bc$ *and hence* $\tilde{v} \circ u \succ w$*.*

This example also stresses the importance of the presentation chosen for the group, as the group is nilpotent. The ideas presented in Madlener and Reinert (1996) are applicable when using the presentation $\Sigma = \{a, a^{-1}, b, b^{-1}, c, c^{-1}\}$ and $T = \{ba \longrightarrow abc, b^{-1}a^{-1} \longrightarrow a^{-1}b^{-1}c, b^{-1}a \longrightarrow ab^{-1}c^{-1}, ba^{-1} \longrightarrow a^{-1}bc^{-1}, c^{\delta}b^{\delta'} \longrightarrow b^{\delta'}c^{\delta}, c^{\delta}a^{\delta'} \longrightarrow a^{\delta'}c^{\delta} \mid \delta, \delta' \in \{1, -1\}\}$.

However, a similar lemma can be proved if we restrict our attention to left-multiples and hence left ideals.

Lemma 2.3. *Let $\mathcal{G}$ be a group represented by a convergent PCP system and $w, v, \tilde{v} \in \mathcal{G}$ with $w \geq_{\mathrm{tup}} v$ and $v \succ \tilde{v}$. Then for $u \in \mathcal{G}$ such that $w = u \circ v$, we get $w \succ u \circ \tilde{v}$. Notice that since $\mathcal{G}$ is a group, u always exists and is unique, namely $u = w \circ \mathsf{inv}(v)$.*

This property motivates the following definition of special representations of polynomials, which will later give rise to the definition of a special reduction called left polycyclic reduction.

Definition 2.2. *Let F be a set of polynomials and p a non-zero polynomial in $\mathbb{K}[\mathcal{G}]$. A representation*

$$p = \sum_{i=1}^{n} \alpha_i \cdot w_i * f_i, \quad \text{with } \alpha_i \in \mathbb{K}^*, f_i \in F, w_i \in \mathcal{G}$$

is called an lpc-standard representation *when for the respective head terms we have $\mathsf{HT}(p) \succeq w_i \circ \mathsf{HT}(f_i) = \mathsf{HT}(w_i * f_i)$ and $\mathsf{HT}(w_i * f_i) \geq_{\mathrm{tup}} \mathsf{HT}(f_i)$ for all $1 \leq i \leq n$. A set $F \subseteq \mathbb{K}[\mathcal{G}]$ is called an* lpc-standard basis *if every non-zero polynomial in $\mathsf{ideal}_l(F)$ has an lpc-standard representation with respect to F.*

A possible approach for right ideals which requires different representations of the polycyclic group can be found in Section 4.

3. Reduction in Polycyclic Group Rings

Let $\mathcal{G}$ be a polycyclic group presented by a convergent PCP system as described in the previous section. Given a non-zero polynomial p in $\mathbb{K}[\mathcal{G}]$, the so called head term $\mathsf{HT}(p)$ is the largest term in p with respect to $\succ$, $\mathsf{HC}(p)$ is the coefficient of this term and the head monomial is $\mathsf{HM}(p) = \mathsf{HC}(p) \cdot \mathsf{HT}(p)$. $\mathsf{T}(p)$ is the set of terms occurring in p. The total ordering $\succeq$ on $\mathcal{G}$ as introduced in the previous section can be extended to a partial ordering on $\mathbb{K}[\mathcal{G}]$ by setting $p > q$ if and only if $\mathsf{HT}(p) \succ \mathsf{HT}(q)$ or ($\mathsf{HM}(p) = \mathsf{HM}(q)$ and $p - \mathsf{HM}(p) > q - \mathsf{HM}(q)$). Now using the head monomial of a polynomial as the left-hand side of a rule, we can define reduction. Frequently in polynomial rings reduction is defined when the head term of the polynomial is a divisor of the term of the monomial to be reduced. Now in groups every element t is a divisor of every other element s since $t \circ (\mathsf{inv}(t) \circ s) = (s \circ \mathsf{inv}(t)) \circ t = s$ holds. But defining reduction as requiring only the divisibility of the term to be reduced by the respective head term would not be Noetherian as the following example shows.

Example 3.1. *Let $\Sigma = \{a, a^{-1}\}$ and $T = \{aa^{-1} \longrightarrow \lambda, a^{-1}a \longrightarrow \lambda\}$ be a presentation of a group $\mathcal{G}$. Let $\mathbb{Q}$ denote the rational numbers. Suppose we simply require divisibility of the head term to allow reduction. Then we could reduce the polynomial $a^2 + 1 \in \mathbb{Q}[\mathcal{G}]$*

at the monomial a^2 by the polynomial $a^{-1}+a$ as $a^2 = a^{-1} \circ a^3$. This would give

$$a^2 + 1 \longrightarrow_{a^{-1}+a} a^2 + 1 - (a^{-1} + a) * a^3 = -a^4 + 1$$

and the polynomial $-a^4 + 1$ likewise would be reducible by $a^{-1} + a$ at the monomial $-a^4$ causing an infinite reduction sequence.

Hence we will give additional restrictions on the divisibility property necessary to allow reduction in order to avoid a monomial being replaced by something larger. Since $\mathcal{G}$, in general, is not commutative, we will restrict ourselves to left-multiples to define reduction.

Definition 3.1. *Let p, f be two non-zero polynomials in $\mathbb{K}[\mathcal{G}]$. We say that f* lpc-reduces *p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow_{f}^{\mathrm{lpc}} q$, if*

(a) $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$ and
(b) $q = p - \alpha \cdot \mathsf{HC}(f)^{-1} \cdot (t \circ \mathsf{inv}(\mathsf{HT}(f))) * f$.

Lpc-reduction by a set $F \subseteq \mathbb{K}[\mathcal{G}]$ is denoted by $p \longrightarrow_{F}^{\mathrm{lpc}} q$ and is abbreviated to $p \longrightarrow_{f}^{\mathrm{lpc}} q$ for some $f \in F$.

Notice that if f lpc-reduces p at $\alpha \cdot t$ to q, then t is no longer a term in q and by Lemma 2.3, $p > q$ holds. This reduction is effective, as it is possible to decide whether we have $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$. Furthermore it is Noetherian and the translation lemma holds.

Lemma 3.1. *Let F be a set of polynomials in $\mathbb{K}[\mathcal{G}]$ and $p, q, h \in \mathbb{K}[\mathcal{G}]$ some polynomials.*

1. *Let $p - q \longrightarrow_{F}^{\mathrm{lpc}} h$. Then there are $p', q' \in \mathbb{K}[\mathcal{G}]$ such that $p \overset{*}{\longrightarrow}_{F}^{\mathrm{lpc}} p'$, $q \overset{*}{\longrightarrow}_{F}^{\mathrm{lpc}} q'$ and $h = p' - q'$.*
2. *Let 0 be a normal form of $p - q$ with respect to $\longrightarrow_{F}^{\mathrm{lpc}}$. Then there exists a polynomial $g \in \mathbb{K}[\mathcal{G}]$ such that $p \overset{*}{\longrightarrow}_{F}^{\mathrm{lpc}} g$ and $q \overset{*}{\longrightarrow}_{F}^{\mathrm{lpc}} g$.*

Gröbner bases as defined by Buchberger (1965) can now be specified for left ideals in this setting as follows.

Definition 3.2. *A set $G \subseteq \mathbb{K}[\mathcal{G}]$ is said to be a* left Gröbner basis*, if $\overset{*}{\longleftrightarrow}_{G}^{\mathrm{lpc}} = \equiv_{\mathsf{ideal}_l(G)}$, and $\longrightarrow_{G}^{\mathrm{lpc}}$ is confluent.*

Since for Buchberger's reduction $\overset{*}{\longleftrightarrow}_{G} = \equiv_{\mathsf{ideal}(G)}$ holds, in order to characterize a Gröbner basis he only had to give a confluence criterion. However, we find that in our setting we have to be more careful, as for lpc-reduction in general we have the situation $\overset{*}{\longleftrightarrow}_{G}^{\mathrm{lpc}} \neq \equiv_{\mathsf{ideal}_l(G)}$. One reason for this phenomenon is that a reduction step is not preserved under left multiplication with elements of $\mathcal{G}$.

Example 3.2. *Let $\mathbb{Q}[\mathcal{G}]$ be the group ring given in Example 3.1. Then for the polynomials $p = a^2 + a$ and $f = a + \lambda$ we find that p is lpc-reducible by f. This is no longer true for the multiple $a^{-2} * p = a^{-2} * (a^2 + a) = \lambda + a^{-1}$. Notice that since $a^{-1} + \lambda \in \mathsf{ideal}_l(p)$ we have $a^{-1} + \lambda \equiv_{\mathsf{ideal}_l(p)} 0$, but $a^{-1} + \lambda \overset{*}{\longleftrightarrow}_{p}^{\mathrm{lpc}} 0$ does not hold.*

We will now demonstrate how we can extend the expressiveness of lpc-reduction. We start by enabling the reducibility of the monomial multiples of a polynomial by using not only the polynomial itself but also a special set of multiples for lpc-reduction. First let us take a look at which multiples will be appropriate for use later on to enable an effective characterization of a left Gröbner basis. As our example shows, we have to pay attention to the problem that different terms of a polynomial can come to the head position by left multiplication with group elements. This is due to the fact that the well-founded ordering on $\mathcal{G}$ is not compatible with left multiplication[†]. The next lemma is a basis for finding left-multiples which bring other terms to the head position when they exist.

Lemma 3.2. *Let p be a non-zero polynomial in $\mathbb{K}[\mathcal{G}]$. Then it is decidable whether for $t \in \mathsf{T}(p)$ there exists an element $w \in \mathcal{G}$ such that $\mathsf{HT}(w * p) = w \circ t$.*

Notice that the proof of this lemma gives details on the form of a possible candidate for w. Now we can enrich a polynomial by the set of those multiples which bring other terms of the polynomial to the head position. However, cases of multiples which are not lpc-reducible by this set of polynomials still remain due to the fact that the "divisibility" criterion for the head term does not hold. Just take a look at the polynomial $p = a^2 + a$ in our example. Then the head term of the multiple $a^{-1} * p = a + \lambda$ results from the head term a^2 of p, but still $a + \lambda$ is not lpc-reducible by p. Therefore, we have to consider further multiples and, in fact, a minimal polynomial among all multiples which bring the same term to the head position exists. For a polynomial p and a term $t \in \mathsf{T}(p)$ we call the term s in a multiple $w * p$ the *t-term* if $s = w \circ t$. The following lemma states that if in two left-multiples of a polynomial the head terms result from the same term t, then there is also a left-multiple of the polynomial with a t-term as head term which is, in some sense, a common commutative prefix of the head terms of the original two multiples. In Example 3.2 for $\lambda * p = a^2 + a$ and $a^{-1} * p = a + \lambda$, both head terms result from the same term a^2 and the head term a of $a^{-1} * p$ is a commutative prefix of the head term a^2 of $\lambda * p$.

Lemma 3.3. *For $u, v \in \mathcal{G}$, let $u * p$ and $v * p$ be two left-multiples of a non-zero polynomial $p \in \mathbb{K}[\mathcal{G}]$ such that for some term $t \in \mathsf{T}(p)$ the head terms are t-terms, i.e., $\mathsf{HT}(u * p) = u \circ t \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(v * p) = v \circ t \equiv a_1^{j_1} \ldots a_n^{j_n}$. Then there exists a term $\tilde{t} \leq_{\text{tup}} a_1^{\rho_1} \ldots a_n^{\rho_n}$ where*

$$\rho_l = \begin{cases} \mathsf{sgn}(i_l) \cdot \min\{|i_l|, |j_l|\} & \mathsf{sgn}(i_l) = \mathsf{sgn}(j_l) \\ 0 & \textit{otherwise} \end{cases}$$

and an element $\tilde{z} \in \mathcal{G}$ such that $\mathsf{HT}(\tilde{z} * p) = \tilde{z} \circ t = \tilde{t}$. In particular, we have $u * p \xrightarrow{\text{lpc}}_{\tilde{z} * p} 0$ and $v * p \xrightarrow{\text{lpc}}_{\tilde{z} * p} 0$.

These two lemmata now state that given a polynomial, we can construct additional polynomials, which are in fact left-multiples of the original polynomial, such that every left-multiple of the polynomial is lpc-reducible to zero in one step by one of them. Such a property of a set of polynomials is called being (lpc-)saturated. In Example 3.2 the multiples $a^{-1} * p = a + \lambda$ and $a^{-2} * p = a^{-1} + \lambda$ give us a saturating set for $p = a^2 + a$.

[†] Notice that no total, well-founded ordering with this property can exist for a non-trivial group due to the existence of inverses.

Definition 3.3. *A set $S \subseteq \{w * p \mid w \in \mathcal{G}\}$ is called an* (lpc-)saturating set *for a non-zero polynomial p in $\mathbb{K}[\mathcal{G}]$ if, for all $w \in \mathcal{G}$, $w * p \longrightarrow^{\rm lpc}_{S} 0$. A set of polynomials $F \subseteq \mathbb{K}[\mathcal{G}]$ is called* (lpc-)saturated *if, for all $f \in F$ and for all $w \in \mathcal{G}$, $w * f \longrightarrow^{\rm lpc}_{F} 0$.*

A further consequence of the previous lemmata is that finite saturating sets exist and they can be computed as follows.

Procedure Saturation

Given: A non-zero polynomial $p \in \mathbb{K}[\mathcal{G}]$.
Find: $\textsc{Sat}(p)$, a saturating set for p.

```
for all $t \in \mathsf{T}(p)$ do
    $S_t := \emptyset$;
    if $t$ can be brought to head position
        then compute $q = w * p$ with $\mathsf{HT}(w * p) = w \circ t$
             $H_t := \{s \in \mathcal{G} \mid \mathsf{HT}(q) \geq_{\rm tup} s\}$;
             % These are candidates for "smaller" polynomials with $t$-head terms
             $q := \min\{(s \circ \mathsf{inv}(t)) * p \mid s \in H_t, \mathsf{HT}((s \circ \mathsf{inv}(t)) * p)) = s\}$;
             $S_t := \{q\}$;
    endif
endfor
$\textsc{Sat}(p) := \bigcup_{t \in \mathsf{T}(p)} S_t$    % $S$ contains at most $|\mathsf{T}(p)|$ polynomials
```

Notice that this is only a naive procedure and for implementation more structural information should be used, e.g. to rule out unnecessary candidates from the sets H_t.

Lemma 3.4. *For a saturated set F of polynomials in $\mathbb{K}[\mathcal{G}]$, $\overset{*}{\longleftrightarrow}^{\rm lpc}_{F} \; = \; \equiv_{\mathsf{ideal}_l(F)}$ holds.*

Let us now proceed to characterize left Gröbner bases by so-called s-polynomials corresponding to lpc-reduction.

Definition 3.4. *For $p_1, p_2 \in \mathbb{K}[\mathcal{G}]$ such that $\mathsf{HT}(p_1) \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(p_2) \equiv a_1^{j_1} \dots a_n^{j_n}$ with either $i_l = 0$ or $j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ for $1 \leq l \leq n$ we can define an* s-polynomial*, and setting*

$$\rho_l = \begin{cases} \mathsf{sgn}(j_l) & i_l = 0 \\ \mathsf{sgn}(i_l) & \textit{otherwise} \end{cases}$$

the situation $a_1^{\rho_1 \cdot \max\{|i_1|, |j_1|\}} \dots a_n^{\rho_n \cdot \max\{|i_n|, |j_n|\}} = w_1 \circ \mathsf{HT}(p_1) = w_2 \circ \mathsf{HT}(p_2)$ for some $w_1, w_2 \in \mathcal{G}$ gives us

$$\mathsf{spol}(p_1, p_2) = \mathsf{HC}(p_1)^{-1} \cdot w_1 * p_1 - \mathsf{HC}(p_2)^{-1} \cdot w_2 * p_2.$$

Notice that $\mathsf{HT}(p_i) \leq_{\rm tup} a_1^{\rho_1 \cdot \max\{|i_1|, |j_1|\}} \dots a_n^{\rho_n \cdot \max\{|i_n|, |j_n|\}}$ for $i \in \{1, 2\}$ holds when such an s-polynomial exists. Furthermore, if there exists a term t such that $t \geq_{\rm tup} \mathsf{HT}(p_1) \equiv a_1^{i_1} \dots a_n^{i_n}$ and $t \geq_{\rm tup} \mathsf{HT}(p_2) \equiv a_1^{j_1} \dots a_n^{j_n}$, an s-polynomial always exists since then the condition for the existence of an s-polynomial is fulfilled as the tuple-ordering requires that the exponent of a letter a_i in the tuple-smaller term is either zero or has the same sign as the exponent of a_i in the tuple-larger term. We even have $t \geq_{\mathrm{tup}} a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$.

We now can give a characterization of a left Gröbner basis in a familiar way using the concept of saturation.

Theorem 3.1. *For a saturated set $G \subseteq \mathbb{K}[\mathcal{G}]$ the following statements are equivalent:*

1. *For all polynomials $g \in \mathsf{ideal}_l(G)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} 0$.*
2. *For all polynomials $f_k, f_l \in G$ we have $\mathsf{spol}(f_k, f_l) \overset{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} 0$.*

It is also possible to give a characterization of left Gröbner bases in terms of standard representations.

Corollary 3.1. *For a set $G \subseteq \mathbb{K}[\mathcal{G}]$ the following statements are equivalent:*

1. *For all polynomials $g \in \mathsf{ideal}_l(G)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} 0$.*
2. *Every $g \in \mathsf{ideal}_l(G)$ has an lpc-standard representation.*
3. *G is an lpc-standard basis.*
4. *G is a left Gröbner basis.*

Now, using the characterization given in Theorem 3.1 we can state a procedure which enumerates left Gröbner bases in polycyclic group rings.

Procedure Left Gröbner Bases in Polycyclic Group Rings

Given: A finite set of polynomials $F \subseteq \mathbb{K}[\mathcal{G}]$.
Find: $\mathrm{GB}_l(F)$, a left Gröbner basis of $\mathsf{ideal}_l(F)$.

```
$G := \bigcup_{g \in G} \mathrm{SAT}(g)$;   % $G$ is saturated and $\mathsf{ideal}_l(F) = \mathsf{ideal}_l(G)$
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ do   % Test if statement 2 of Theorem 3.1 is valid
    $(q_1, q_2)$ := remove($B$);   % Remove an element using a fair strategy
    if  $h := \mathsf{spol}(q_1, q_2)$ exists
        then  $h'$ := normalform($h$, $\longrightarrow^{\mathrm{lpc}}_{G}$);   % Compute a normal form
              if  $h' \neq 0$   % The s-polynomial does not reduce to zero
                  then  $G := G \cup \mathrm{SAT}(h')$;
                        % $G$ is saturated and $\mathsf{ideal}_l(F) = \mathsf{ideal}_l(G)$
                        $B := B \cup \{(f, g) \mid f \in G, g \in \mathrm{SAT}(h')\}$;
              endif
    endif
endwhile
$\mathrm{GB}_l(F) := G$
```

The set G enumerated by this naive procedure fulfils the requirements of Theorem 3.1, i.e., the set G at each stage generates $\mathsf{ideal}_l(F)$ and is saturated. Using a fair strategy to remove elements from the test set B ensures that for all polynomials entered into G the s-polynomials are considered when they exist. Hence, when the procedure terminates, it computes a left Gröbner basis. The next theorem states that every left Gröbner basis contains a finite one and hence this procedure must terminate since as soon as all the polynomials in the contained Gröbner basis have been added to G all further s-polynomials will reduce to zero and hence nothing more will be added to the set B.

Theorem 3.2. *Every left Gröbner basis contains a finite one.*

Notice that although polycyclic group rings are Noetherian, this does not imply the existence of finite Gröbner bases. In the proof finiteness can be shown using Dickson's lemma (as in the ordinary polynomial ring), as lpc-reduction is related to "commutative prefixes". Let us now continue to show how (as in the case of solvable polynomial rings or skew polynomial rings in Kredel (1993) and Weispfenning, (1992)), Gröbner bases of two-sided ideals can be characterized by left Gröbner bases which have additional properties. We will call a set of polynomials a *Gröbner basis* of the two-sided ideal it generates, if it fulfils one of the equivalent statements in the next theorem.

Theorem 3.3. *For a set of polynomials $G \subseteq \mathbb{K}[\mathcal{G}]$, assuming that $\mathcal{G}$ is presented by (Σ, T) as described above, the following properties are equivalent:*

1. *G is a left Gröbner basis and $\mathsf{ideal}_l(G) = \mathsf{ideal}(G)$.*
2. *For all $g \in \mathsf{ideal}(G)$ we have $g \xrightarrow[G]{*}{}^{\text{lpc}} 0$.*
3. *G is a left Gröbner basis and for all $w \in \mathcal{G}$, $g \in G$ we have $g * w \in \mathsf{ideal}_l(G)$.*
4. *G is a left Gröbner basis and for all $a \in \Sigma$, $g \in G$ we have $g * a \in \mathsf{ideal}_l(G)$.*

Statement 4 provides a constructive approach to using the procedure Left Gröbner Bases in Polycyclic Group Rings in order to compute Gröbner bases of two-sided ideals and Statement 2 states that such bases can be used to decide the membership problem for the two-sided ideal by using lpc-reduction. The following corollary, similar to Theorem 3.1, can be used as the foundation of a procedure to compute two-sided Gröbner bases.

Corollary 3.2. *For a saturated set $G \subseteq \mathbb{K}[\mathcal{G}]$ the following statements are equivalent:*

1. *For all polynomials $g \in \mathsf{ideal}(G)$ we have $g \xrightarrow[G]{*}{}^{\text{lpc}} 0$.*
2. *(a) For all polynomials $f_k, f_l \in G$ we have $\mathsf{spol}(f_k, f_l) \xrightarrow[G]{*}{}^{\text{lpc}} 0$.*
   (b) For all $a \in \Sigma$, $g \in G$ we have $g * a \xrightarrow[G]{*}{}^{\text{lpc}} 0$.

Again the existence of finite Gröbner bases is a consequence of Dickson's lemma.

Corollary 3.3. *Every Gröbner basis contains a finite one.*

Notice that so far we have only characterized lpc-saturated Gröbner bases. Of course Gröbner bases which are not lpc-saturated also exist. It is even possible to introduce inter-reduction for lpc-reduction and to compute reduced Gröbner bases which are unique if we demand that the polynomials are monic, i.e. they have head coefficient 1.

Definition 3.5. *We call a set of polynomials $F \subseteq \mathbb{K}[\mathcal{G}]$* inter-reduced *or* reduced *with respect to $\longrightarrow^{\text{lpc}}$, if no polynomial f in F is lpc-reducible by the other polynomials in $F \setminus \{f\}$.*

Theorem 3.4. *Every (left) ideal in $\mathbb{K}[\mathcal{G}]$ contains a unique monic finite reduced (left) Gröbner basis.*

Such reduced Gröbner bases can be computed by incorporating inter-reduction into the respective procedures.

4. Concluding Remarks

Let us close this paper with some remarks on right ideals in polycyclic group rings. It is known from the work of Baumslag *et al.* (1981) and Sims (1994) that the membership problem for right submodules of a polycyclic group ring is decidable. Using a consistent polycyclic presentation of the group in terms of a polycyclic sequence of generators, the proofs give an inductive argument to lift the property of having a decidable submodule problem. This process, however, is no procedure on its own. Solving membership problems using Gröbner bases provides a direct concept for implementation. So far in this paper we have shown how Gröbner bases can be introduced for left and two-sided ideals and we have provided descriptions of procedures which—after adding knowledge and strategies for more efficiency—are a good basis for an implementation. We have used convergent PCP systems to represent polycyclic groups and one has to keep in mind that the respective collection processes will have great influence on the efficiency when group multiplication is implemented.

As seen in Section 2, the concept used to describe left ideal congruences by reduction and Gröbner bases cannot be carried over to right ideal congruences. This is due to the fact that when the group is represented by a convergent PCP system (also called a consistent polycyclic presentation in Sims (1994)), Lemma 2.2 no longer holds. It is even true that right ideals cannot be treated using the notions of Gröbner bases presented here unless the representation of the group is changed. This arises from the fact that right ideals in group rings (as well as left ideals) are related to the subgroup problem of the respective group.

Theorem 4.1. (see 5.1.2 in Reinert (1995)) *Let S be a finite subset of $\mathcal{G}$ and $\mathbb{K}[\mathcal{G}]$ the group ring corresponding to $\mathcal{G}$. Further let $P_S = \{s-1 \mid s \in S\}$ be a set of polynomials associated to S. Then the following statements are equivalent:*

1. $w \in \langle S \rangle$.
2. $w - 1 \in \mathsf{ideal}_r(P_S)$.
3. $w - 1 \in \mathsf{ideal}_l(P_S)$.

Wißmann (1989) gives a completion-based approach to solving the subgroup problem for polycyclic groups: Given a convergent polycyclic presentation of a group $\mathcal{G}$ and a finite generating set U, decide whether some $g \in \mathcal{G}$ is in the subgroup $\langle U \rangle = \{u_1 \circ \ldots \circ u_n \mid n \in \mathbb{N}, u_i \in U \cup U^{-1}\}$ generated by U. He solves this problem by introducing a reduction as follows: For $g, h \in \mathcal{G}$, $g \Longrightarrow_U h$ iff there exists $u \in U \cup U^{-1}$ such that $h = u \circ g$ and $h <_{\mathrm{syll}} g$. Then he gives a completion procedure which computes a finite λ-confluent basis B of $\langle U \rangle$, i.e., for all $g \in \langle U \rangle$ we have $g \overset{*}{\Longrightarrow}_B \lambda$. Furthermore, Wißmann (1989) states that for $\Longrightarrow$-reduction no finite confluent basis need exist (cf. Theorem 3.6.9). By Theorem 4.1 we know how a subgroup is related to a right ideal and such a right ideal congruence can be described by reduction. For example this can be done using so called strong reduction:

For $p, f \in \mathbb{K}[\mathcal{G}]$, let $\mathsf{HT}(f * w) = t$ for some $t \in \mathsf{T}(p)$, $w \in \mathcal{G}$, then $p \longrightarrow^{\mathrm{s}}_{f} p - \alpha \cdot f * w = q$, where $\alpha \in \mathbb{K}$ such that $t \notin \mathsf{T}(q)$. Now $\Longrightarrow$-reduction and strong reduction are comparable as follows: For $g, h \in \mathcal{G}$, let $g \Longrightarrow_{U} h$, i.e., $h = u \circ g$ and $h <_{\mathrm{syll}} g$. Then for the polynomials $f = u - 1$ and $p = g$ we get $\mathsf{HT}(f * (\mathsf{inv}(u) \circ g)) = \mathsf{HT}(g - u \circ g) = g$, as $h = u \circ g <_{\mathrm{syll}} g$, and hence $p \longrightarrow^{\mathrm{s}}_{f} g - (g - u \circ g) = u \circ g = h$. Furthermore, the existence of a finite Gröbner basis for the right ideal generated by $P_U = \{u - 1 \mid u \in U\}$ implies the existence of a finite Gröbner basis of the form $G = \{u - v \mid u, v \in \mathcal{G}\}$ and then the set $\{u \circ \mathsf{inv}(v), v \circ \mathsf{inv}(u) \mid u - v \in G\}$ is a finite subgroup basis which is a convergent basis with respect to $\Longrightarrow$-reduction as defined by Wißmann. To see this assume that for the polynomials $f = u - v$ and $p = g$ we have that f strongly reduces p, i.e., there exists x in $\mathcal{G}$ such that $\mathsf{HT}(f * x) = g$. We have to distinguish two possible cases. If $g = \mathsf{HT}(f * x) = u \circ x >_{\mathrm{syll}} v \circ x$ we get $g \Longrightarrow_{v \circ \mathsf{inv}(u)} v \circ x$ as $(v \circ \mathsf{inv}(u)) \circ g = (v \circ \mathsf{inv}(u)) \circ (u \circ x) = v \circ x$ and $u \circ x >_{\mathrm{syll}} v \circ x$. Similarly, $g = \mathsf{HT}(f * x) = v \circ x >_{\mathrm{syll}} u \circ x$ implies $g \Longrightarrow_{u \circ \mathsf{inv}(v)} v \circ x$. Now since as stated above such finite convergent bases of the subgroup do not, in general, exist if $\mathcal{G}$ is represented by a convergent PCP system, Gröbner bases of right ideals will, in general, not be finite. A thorough study of these connections can be found in Reinert (1996).

Notice that the subgroup membership problem can still be solved using Gröbner basis methods related to lpc-reduction, since for the lpc-Gröbner basis B of $\mathsf{ideal}_l(P_U)$ we have $g \in \langle U \rangle$ iff $g \xrightarrow{*}{}^{\mathrm{lpc}}_{B} 0$.

We close this section by outlining how Gröbner basis methods can be introduced to describe right ideals in polycyclic group rings provided that the groups are represented in a slightly different way. So far we have used convergent PCP presentations with a syllable ordering with status *left* as completion ordering. If we now change this ordering into a syllable ordering with status *right*, i.e., the syllables will be compared from the right to the left, completion again will halt with a system containing power and commutation rules with similar properties except that now the ordered group words are of the form $a_n^{i_n} \dots a_1^{i_1}$, since the commutator rules will have the form $a_l^{\delta} a_k^{\delta'} \longrightarrow z a_l^{\delta}$ where $l < k$,$\delta, \delta' \in \{1, -1\}$ and $z \equiv a_n^{i_n} \dots a_{l+1}^{i_{l+1}}$. Then the results of Section 3 are symmetric when using multiplication from the right and we can introduce right polycyclic reduction, i.e., a polynomial p is reducible at a monomial $\alpha \cdot t$ by a polynomial f when $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$ and the result of the reduction will be $p - (\alpha \cdot \mathsf{HC}(f)^{-1}) \cdot f * (\mathsf{inv}(\mathsf{HT}(f)) \circ t$. Gröbner bases can be defined and computed as in the case of left polycyclic reduction.

Acknowledgement: The second author wants to thank Joachim Neubüser for his steady encouragement to continue working on this particular subject.

References

Apel J., Lassner W. (1988). An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras. *J. Symbolic Computation*, **6**, 361–370.

Baumslag G., Cannonito F. and Miller C., III. (1981). Computable algebra and group embeddings. *J. Algebra*, **69**, 186–212.

Becker T. and Weispfenning V. (1992). *Gröbner Bases—A Computational Approach to Commutative Algebra*, Berlin: Springer Verlag.

Book R. and Otto F. (1993). *String-Rewriting Systems*, Berlin: Springer Verlag.

Buchberger B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*, PhD Thesis. Universität Innsbruck.

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

Kargapolov M.I. and Merzljakov Ju.I. (1979). *Fundamentals of the Theory of Groups*, Berlin: Springer Verlag.

Kredel H. (1993). *Solvable Polynomial Rings*, Aachen: Verlag Shaker.

Lassner W. (1985). Symbol representations of noncommutative algebras. EUROCAL'85. Springer LNCS 204, pp. 99–115.

Madlener K. and Reinert B. (1993a). *On Gröbner Bases in Monoid and Group Rings*. SEKI Report SR-93-08, Universität Kaiserslautern.

Madlener K. and Reinert B. (1993b). *Computing Gröbner Bases in Monoid and Group Rings*. Proc. ISSAC'93. pp. 254–263.

Madlener K. and Reinert B. (1996). A generalization of Gröbner bases algorithms to nilpotent group rings. *Applicable Algebra in Engineering, Communications and Computing*, **8**, 103–123.

Mora F. (1985). Gröbner Bases for Non-Commutative Polynomial Rings. Proc. AAECC-3. Springer LNCS 229. pp. 353–362.

Mora T. (1994). An introduction to commutative and non-commutative Gröbner bases. *Theoretical Computer Science*, **134**, 131–173.

Reinert B. (1995). *Gröbner Bases in Monoid and Group Rings* PhD Thesis. Universität Kaiserslautern.

Reinert B. (1996). Introducing Reduction to Polycyclic Group Rings - A Comparison of Methods. Reports on Computer Algebra No. 9. Centre of Computer Algebra. Universität Kaiserslautern.

Rosenmann A. (1993). An Algorithm for Constructing Gröbner and Free Schreier Bases in Free Group Algebras. *J. Symbolic Computation*, **16**, 523–549.

Sims C. (1994). *Computation with Finitely Presented Groups*. Cambridge University Press.

Weispfenning V. (1987). Gröbner bases for polynomial ideals over commutative regular rings. Proc. EUROCAL'87. Springer LNCS 378. pp. 336–347.

Weispfenning V. (1992). Finite Gröbner bases in non-noetherian skew polynomial rings. Proc. ISSAC'92. pp. 329–334.

Wißmann D. (1989). *Anwendung von Rewriting-Techniken in polyzyklischen Gruppen*. PhD Thesis. Universität Kaiserslautern.

A. Appendix

This section contains two auxiliary lemmata and the proofs of the lemmata and theorems presented in this paper.

Lemma A.1. *Let $a, b, c \in \mathbb{Z}$. Then $a >_{\mathbb{Z}} b$ and $a \cdot c \geq 0$ imply $a + c >_{\mathbb{Z}} b + c$.*

Proof. When $a > 0$ we find $b \geq 0$ (since $a >_{\mathbb{Z}} b$) and $c \geq 0$ (as $a \cdot c \geq 0$). This immediately implies $a + c > b + c \geq 0$ and hence $a + c >_{\mathbb{Z}} b + c$.

On the other hand, $a < 0$ gives us $c \leq 0$ (since $a \cdot c \geq 0$) and depending on b either $a + c < b + c < 0$ or $a + c < 0 \leq b + c$, again implying $a + c >_{\mathbb{Z}} b + c$. □

Lemma A.2. *Let $a, b, c \in \mathbb{Z}$. Then $a >_{\mathbb{Z}} b$, $a \geq_{\mathbb{Z}} c$, and the existence of an element $x \in \mathbb{Z}$ such that $a + x <_{\mathbb{Z}} b + x$ and $c + x \leq_{\mathbb{Z}} b + x$ implies $b - a \geq_{\mathbb{Z}} c - a$. When $c + x <_{\mathbb{Z}} b + x$ holds we get $b - a >_{\mathbb{Z}} c - a$.*

Proof. First let us look at the case $b - a = c - a$. This implies $b = c$ and hence $b + y = c + y$ for all $y \in \mathbb{Z}$. Therefore the existence of an $x \in \mathbb{Z}$ such that $c + x <_{\mathbb{Z}} b + x$ implies $b - a \neq_{\mathbb{Z}} c - a$.

Now it remains to prove that the case $b - a <_{\mathbb{Z}} c - a$ is not possible. First suppose $c - a < 0$. Let us distinguish the two possible cases: If $a > 0$ we get $a \geq c \geq 0$ (as $a \geq_{\mathbb{Z}} c$) and $a > b \geq 0$ (as $a >_{\mathbb{Z}} b$). Since then $b - a \geq 0$ is not possible, $b - a <_{\mathbb{Z}} c - a$ implies that we have $c - a < b - a < 0$ and hence $a > b \geq c \geq 0$ must hold. We now show that in this case no x as described in the lemma can be found. For $a > b \geq 0$ we get that for all $y \geq -b$ we have $b + y <_{\mathbb{Z}} a + y$ and for all $y < -b$ we have $b + y >_{\mathbb{Z}} a + y$. Similarly, for $b \geq c \geq 0$ we find that for all $z \geq -c$ we have $c + z \leq_{\mathbb{Z}} b + z$ and for all $z < -c$, $c + z \geq_{\mathbb{Z}} b + z$ holds. Hence for x such that $a + x <_{\mathbb{Z}} b + x$ and $c + x \leq_{\mathbb{Z}} b + x$ to hold, we must have $x < -b$ and $x \geq -c$, contradicting $-b \leq -c$. On the other hand, $a < 0$ leads to a contradiction $c - a \geq 0$ as $a \geq_{\mathbb{Z}} c$ either implies $c \geq 0$ or $a \leq c < 0$. Hence let us suppose $c - a > 0$ and therefore $c - a > b - a \geq 0$ implying $c > b \geq a$ (and hence $a >_{\mathbb{Z}} c$ must hold as $a \neq c$). Furthermore, $a >_{\mathbb{Z}} b$ implies $a < 0$. Let us analyse the remaining cases. If $c \leq 0$ we find $b < 0$ as well (since $c > b \geq a$). Since the equation $a + x <_{\mathbb{Z}} b + x$ holds for $x \geq -a > 0$ only and $c + x \leq_{\mathbb{Z}} b + x$ for $0 \leq x < -b < -a$ only, no x as required can exist. Hence suppose $c > 0$. Then depending on b the equation $c + x \leq_{\mathbb{Z}} b + x$ holds either for $0 \leq x < -b < -a$ (when $b < 0$) only or for $x < -b \leq 0$ (when $b \geq 0$), and as further $x \geq -a > 0$ must hold again no such x can exist. □

Proof. (of Lemma 2.3) Let a_d be the distinguishing letter between v and $\tilde{v}$, i.e., $v \equiv x a_d^{v_d} y_v$, $\tilde{v} \equiv x a_d^{\tilde{v}_d} y_{\tilde{v}}$ with $x \in \mathsf{ORD}(\Sigma \setminus \Sigma_d)$, $y_v, y_{\tilde{v}} \in \mathsf{ORD}(\Sigma_{d+1})$ and $v_d >_{\mathbb{Z}} \tilde{v}_d$. Then for $u \equiv a_1^{u_1} \ldots a_n^{u_n}$ we get $u \circ v = a_1^{u_1} \ldots a_n^{u_n} \circ x a_d^{v_d} y_v = a_1^{u_1} \ldots a_{d-1}^{u_{d-1}} \circ x' \circ a_d^{u_d + v_d + z_1} \circ y_v{}' = x'' \circ a_d^{u_d + v_d + z_2} \circ y_v''$ with $x', x'' \in \mathsf{ORD}(\Sigma \setminus \Sigma_d)$, $y_v{}', y_v'' \in \mathsf{ORD}(\Sigma_{d+1})$ and similarly $u \circ \tilde{v} = x'' \circ a_d^{u_d + \tilde{v}_d + z_2} \circ y_{\tilde{v}}''$ with $y_{\tilde{v}}'' \in \mathsf{ORD}(\Sigma_{d+1})$. Furthermore, $w \geq_{\mathrm{tup}} v$ gives us, for the exponent w_d of the letter a_d in w, $w_d \geq_{\mathbb{Z}} v_d$, $\mathsf{sgn}(w_d) = \mathsf{sgn}(v_d)$ and $u_d + v_d + z_2 = w_d$ or $(u_d + v_d + z_2)$ mod $m_d = w_d$ when a_d is bounded by m_d. To show that $u \circ \tilde{v} \prec w$ we now have to distinguish two cases. If the letter a_d has unbounded exponents, we can apply Lemma A.1 since $v_d >_{\mathbb{Z}} \tilde{v}_d$ and $v_d \cdot (u_d + z_2) \geq 0$ hold (the latter follows as $w \geq_{\mathrm{tup}} v$). Hence let us assume the letter a_d is bounded, i.e., we know $0 \leq \tilde{v}_d < v_d \leq w_d < m_d$, and since $0 \leq u_d < m_d$ must also hold, we get $0 \leq \tilde{v}_d + u_d < v_d + u_d$ and $(v_d + u_d + z_2)$ mod $m_d = w_d$. Now when $v_d + u_d + z_2 = w_d$ we are done, as then $u_d + z_2 \geq 0$ implies $v_d + u_d + z_2 > \tilde{v}_d + u_d + z_2$. Else, as $v_d \leq w_d$, for $y = w_d - v_d$ we know $u_d + z_2 = l \cdot m_d + y$ with $0 \leq y < m_d$ and hence $0 \leq (\tilde{v}_d + u_d + z_2)$ mod $m_d = (\tilde{v}_d + l \cdot m_d + y)$ mod $m_d = \tilde{v}_d + y < v_d + y = w_d$ and the proof is complete. □

Proof. (of Lemma 3.1)

1. Let $p - q \longrightarrow^{\mathrm{lpc}}_{F} h = p - q - \alpha \cdot w * f$, where $\alpha \in \mathbb{K}^*$, $f \in F$, $w \in \mathcal{G}$ and $w \circ \mathsf{HT}(f) = t \geq_{\mathrm{tup}} \mathsf{HT}(f)$, i.e. $\alpha \cdot \mathsf{HC}(f)$ is the coefficient of t in $p - q$. We have to distinguish three cases:
   (a) $t \in \mathsf{T}(p)$ and $t \in \mathsf{T}(q)$: Then we can eliminate the term t in the polynomials p respectively q by lpc-reduction. We then get $p \longrightarrow^{\mathrm{lpc}}_{f} p - \alpha_1 \cdot w * f = p'$ and $q \longrightarrow^{\mathrm{lpc}}_{f} q - \alpha_2 \cdot w * f = q'$, with $\alpha_1 - \alpha_2 = \alpha$, where $\alpha_1 \cdot \mathsf{HC}(f)$ and $\alpha_2 \cdot \mathsf{HC}(f)$ are the coefficients of t in p respectively q.
   (b) $t \in \mathsf{T}(p)$ and $t \notin \mathsf{T}(q)$: Then we can eliminate the term t in the polynomial p by lpc-reduction and get $p \longrightarrow^{\mathrm{lpc}}_{f} p - \alpha \cdot w * f = p'$ and $q = q'$.
   (c) $t \in \mathsf{T}(q)$ and $t \notin \mathsf{T}(p)$: Then we can eliminate the term t in the polynomial q by lpc-reduction and get $q \longrightarrow^{\mathrm{lpc}}_{f} q + \alpha \cdot w * f = q'$ and $p = p'$.

   In all cases we have $p' - q' = p - q - \alpha \cdot w * f = h$.
2. We show our claim by induction on k, where $p - q \stackrel{k}{\longrightarrow}{}^{\mathrm{lpc}}_{F} 0$. In the base case $k = 0$ there is nothing to show. Hence, let $p - q \longrightarrow^{\mathrm{lpc}}_{F} h \stackrel{k}{\longrightarrow}{}^{\mathrm{lpc}}_{F} 0$. Then by (1) there are $p', q' \in \mathbb{K}[\mathcal{G}]$ such that $p \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{F} p'$, $q \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{F} q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \stackrel{k}{\longrightarrow}{}^{\mathrm{lpc}}_{F} 0$ yields the existence of a polynomial $g \in \mathbb{K}[\mathcal{G}]$ such that $p \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{F} p' \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{F} g$ and $q \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{F} q' \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{F} g$.

□

Proof. (of Lemma 3.2) We show that for a finite set of terms $T = \{t_1, \ldots, t_s\}$, where without loss of generality t_1 is the greatest term, the following holds: If there exists $w \in \mathcal{G}$ such that for some $t_i \in T \setminus \{t_1\}$ we have $w \circ t_i \succ w \circ t_j$ for all $t_j \in T \setminus \{t_i\}$, then we can effectively construct $v \in \mathcal{G}$ such that $v \circ t_i \succ v \circ t_j$ for all $t_j \in T \setminus \{t_i\}$ also holds without knowing w. This will be done by induction on k where $T \subseteq \mathsf{ORD}(\Sigma_{n-k})$.

In the base case $k = 0$ we get $T \subseteq \mathsf{ORD}(\Sigma_n)$, hence $t_1 \equiv a_n^{1_n}$, $t_i \equiv a_n^{i_n}$ and $1_n >_{\mathbb{Z}} i_n$. By our assumption there exists $w \in \mathcal{G}$ with $w \equiv w' a_n^{w_n}$, $w' \in \mathsf{ORD}(\Sigma \setminus \Sigma_n)$ such that $w \circ t_i \succ w \circ t_j$ must hold for all $t_j \in T \setminus \{t_i\}$. We have to consider two cases. First let us assume that the letter a_n is not bounded. Then let us set $v \equiv a_n^{-1_n}$. We have to show that for all $t_j \in T \setminus \{t_i\}$ we have $-1_n + i_n >_{\mathbb{Z}} -1_n + j_n$. The case $t_j = t_1$ is trivial and for each $t_j \in T \setminus \{t_1, t_i\}$ the equation is a consequence of Lemma A.2 as we have $1_n >_{\mathbb{Z}} i_n$, $1_n >_{\mathbb{Z}} j_n$ and, as seen above, there exists an element x, namely w_n, such that $1_n + x <_{\mathbb{Z}} i_n + x$ and $j_n + x <_{\mathbb{Z}} i_n + x$. Now when a_n is bounded by $m_n \in \mathbb{N}$ we can set $v \equiv a_n^{m_n - i_n - 1}$. We find that since for all $t_j \in T \setminus \{t_i\}$, we have $i_n \neq j_n$ and $v \circ t_i \equiv a_n^{m_n - 1}$, for all other multiples $v \circ t_j \equiv a_n^{x_j}$, $x_j < m_n - 1$ must hold.

In the induction step let us assume $k > 0$ and again without loss of generality t_1 is the largest term in $T \subseteq \mathsf{ORD}(\Sigma_{n-k})$. By our assumption there exists $w \in \mathcal{G}$ such that $w \circ t_i \succ w \circ t_j$ for all $t_j \in T \setminus \{t_i\}$. Let a_d be the distinguishing letter between $t_1 \equiv a_{n-k}^{1_{n-k}} \ldots a_n^{1_n}$ and $t_i \equiv a_{n-k}^{i_{n-k}} \ldots a_n^{i_n}$, and let $w \equiv w' w'' a_d^{w_d} w'''$ with $w' \in \mathsf{ORD}(\Sigma \setminus \Sigma_{n-k})$, $w'' \in \mathsf{ORD}(\{a_{n-k+1}, \ldots, a_{d-1}\})$, $w''' \in \mathsf{ORD}(\Sigma_{d+1})$. As before let us first consider the case that the letter a_d is not bounded. Then there exist $l_{n-k}, \ldots, l_{d-1}, x \in \mathbb{Z}$, $z_1, z_i \in \mathsf{ORD}(\Sigma_{d+1})$ such that $w \circ t_1 = w' w'' a_d^{w_d} w''' \circ a_{n-k}^{1_{n-k}} \ldots a_n^{1_n} \equiv w' a_{n-k}^{l_{n-k}} \ldots a_{d-1}^{l_{d-1}} a_d^{w_d + 1_d + x} z_1$, $w \circ t_i \equiv w' a_{n-k}^{l_{n-k}} \ldots a_{d-1}^{l_{d-1}} a_d^{w_d + i_d + x} z_i$. Now let us set $v_d = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{-1_d} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}})$. Since $v_d \circ t_1 = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{-1_d} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_{n-k}^{1_{n-k}} \ldots a_n^{1_n} \equiv a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}} y_1$ and $v_d \circ t_i = a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}} a_d^{-1_d + i_d} y_i$ with $y_1, y_i \in \mathsf{ORD}(\Sigma_{d+1})$, $v_d \circ t_i \succ v_d \circ t_1$ holds. It remains to study $v_d \circ t_j$ for all $t_j \in T \setminus \{t_1, t_i\}$. When the distinguishing letter between t_i and t_j has index $s \leq d$ we must have $t_j \prec t_i$, as $t_j \prec t_1$ and therefore $j_s <_{\mathbb{Z}} i_s = 1_s$ respectively $j_d <_{\mathbb{Z}} i_d <_{\mathbb{Z}} 1_d$ must hold. Then $t_i \equiv x_i a_s^{i_s} y_i$ and $t_j \equiv x_i a_s^{j_s} y_j$ with $x_i \in \mathsf{ORD}(\Sigma \setminus \Sigma_s)$, $y_i, y_j \in \mathsf{ORD}(\Sigma_{s+1})$ and $v_d \circ t_j = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{-1_d} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ x_i a_s^{j_s} y_j = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{-1_d} \circ \mathsf{inv}(a_{s+1}^{i_{s+1}} \ldots a_{d-1}^{i_{d-1}}) \circ a_s^{-i_s + j_s} y_j = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_s^{-i_s + j_s} z_j = a_{n-k}^{1_{n-k}} \ldots a_{s-1}^{1_{s-1}} a_s^{i_s - i_s + j_s} \tilde{z}_j \equiv a_{n-k}^{1_{n-k}} \ldots a_{s-1}^{1_{s-1}} a_s^{j_s} \tilde{z}_j$ with $z_j, \tilde{z}_j \in \mathsf{ORD}(\Sigma_{s+1})$ and and similarly $v_d \circ t_i = a_{n-k}^{1_{n-k}} \ldots a_{s-1}^{1_{s-1}} a_s^{i_s - i_s + i_s} \tilde{z}_i \equiv a_{n-k}^{1_{n-k}} \ldots a_{s-1}^{1_{s-1}} a_s^{i_s} \tilde{z}_i$ with $\tilde{z}_i \in \mathsf{ORD}(\Sigma_{s+1})$ thus implying $v_d \circ t_i \succ v_d \circ t_j$. Otherwise let $T' = \{y_j \mid t_j \in T, t_j \equiv a_{n-k}^{i_{n-k}} \ldots a_d^{i_d} y_j, y_j \in \mathsf{ORD}(\Sigma_{d+1})\}$. Then $T' \subseteq \mathsf{ORD}(\Sigma_{d+1}) \subset \mathsf{ORD}(\Sigma_{n-k})$ and still for $w \in \mathcal{G}$ from above we can conclude $(w \circ a_{n-k}^{i_{n-k}} \ldots a_d^{i_d}) \circ y_i \succ (w \circ a_{n-k}^{i_{n-k}} \ldots a_d^{i_d}) \circ y_j$ for the terms $y_j \in T' \setminus \{y_i\}$. Hence by our induction hypothesis $v_{d+1} \in \mathcal{G}$ can be constructed such that $v_{d+1} \circ y_i \succ v_{d+1} \circ y_j$. Now we can combine v_d and v_{d+1} in order to construct v as follows: let us set $v = v_d \circ (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{i_d} \circ v_{d+1} \circ a_d^{-i_d} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{-1_d} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ ((a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{i_d} \circ v_{d+1} \circ a_d^{-i_d} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}})) = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{-1_d + i_d} \circ v_{d+1} \circ a_d^{-i_d} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}})$. Then we get $v \circ t_i \succ v \circ t_j$ for all $t_j \in T \setminus \{t_i\}$ since $v \circ t_j = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{-1_d + i_d} \circ v_{d+1} \circ a_d^{-i_d} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}} a_d^{i_d} y_j = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{-1_d + i_d} \circ v_{d+1} \circ y_j \equiv a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}} a_d^{-1_d + i_d} z_j$ and similarly $v_d \circ t_i \equiv a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}} a_d^{-1_d + i_d} z_i$ with $z_j, z_i \in \mathsf{ORD}(\Sigma_{d+1})$ and by the definition of v_{d+1} we also know $v_{d+1} \circ y_j = z_j \prec z_i = v_{d+1} \circ y_i$ proving our claim.

Now it remains to check the case where a_d is bounded by m_d. We can set $v_d = (a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}}) \circ a_d^{m_d - i_d - 1} \circ \mathsf{inv}(a_{n-k}^{1_{n-k}} \ldots a_{d-1}^{1_{d-1}})$, and, as above, an element v can be constucted such that $v \circ t_i \succ v \circ t_j$ for all $t_j \in T \setminus \{t_i\}$. □

Proof. (of Lemma 3.3) Let p, $p * u$ and $p * v$ be as described in the lemma and let the letters corresponding to our representation be $\Sigma = \{a_1, \ldots, a_n, a_1^{-1}, \ldots, a_n^{-1}\}$.

We show the existence of $\tilde{z}$ by constructing a sequence $z_1, \ldots, z_n \in \mathcal{G}$, such that for $1 \leq l \leq n$ we have $\mathsf{HT}(z_l * p) = z_l \circ t \equiv a_1^{s_1} \ldots a_l^{s_l} r_l$ with $r_l \in \mathsf{ORD}(\Sigma_{l+1})$ and $a_1^{s_1} \ldots a_l^{s_l} \leq_{\text{tup}} a_1^{\rho_1} \ldots a_l^{\rho_l}$. Then for $\tilde{z} = z_n$ our claim holds.

Let us start by constructing an element $z_1 \in \mathcal{G}$ such that $\mathsf{HT}(z_1 * p) = z_1 \circ t \equiv a_1^{s_1} r_1$, $r_1 \in \mathsf{ORD}(\Sigma_2)$ and $a_1^{s_1} \leq_{\text{tup}} a_1^{\rho_1}$. When $i_1 = j_1$ or $j_1 = 0$ we can set $z_1 = v$ and $s_1 = j_1 = \rho_1$ since $\mathsf{HT}(v * p) = v \circ t \equiv a_1^{j_1} \ldots a_n^{j_n}$. Similarly when $i_1 = 0$ we can set $z_1 = u$ and $s_1 = i_1 = 0 = \rho_1$ since $\mathsf{HT}(u * p) = u \circ t \equiv a_2^{i_2} \ldots a_n^{i_n} \in \mathsf{ORD}(\Sigma_2)$. Hence let us assume $i_1 \neq j_1$ and both are non-zero.

First suppose that $\mathsf{sgn}(i_1) = \mathsf{sgn}(j_1)$. Notice that the proof does not depend on whether a_1 is bounded or not. Then if $|i_1| \geq |j_1|$ we again set $z_1 = v$ since for $s_1 = j_1 = \rho_1$ our claim holds. When $|j_1| > |i_1|$ we set $z_1 = u$ because for $s_1 = i_1 = \rho_1$ our claim holds.

Now let us proceed with the case $\mathsf{sgn}(i_1) \neq \mathsf{sgn}(j_1)$, hence a_1 cannot be bounded. We construct $z_1 \in \mathcal{G}$ such that $\mathsf{HT}(z_1 * p) = z_1 \circ t \in \mathsf{ORD}(\Sigma_2)$ as $\rho_1 = 0$. We claim that the letter a_1 has the same exponent for all terms in $\mathsf{T}(p)$, say b. When this holds, no term in the polynomial $a_1^{-b} * p$ will contain the letter a_1 and the distinguishing letter between $\mathsf{HT}(a_1^{-b} * p)$ and the term $a_1^{-b} \circ t$ is at least of index 2. Furthermore we know $\mathsf{HT}((v \circ a_1^b) * (a_1^{-b} * p)) = \mathsf{HT}(v * p) = v \circ t$. Thus by the construction given in the proof of Lemma 3.2 there exists an element $r \in \mathsf{ORD}(\Sigma_2)$ such that $\mathsf{HT}(r * (a_1^{-b} * p)) = r \circ a_1^{-b} \circ t \in \mathsf{ORD}(\Sigma_2)$ and thus we can set $z_1 = r \circ a_1^{-b}$ and $s_1 = 0 = \rho_1$.

Hence it remains to prove that the exponents of a_1 have the desired property. Suppose we have the representatives $s' \equiv a_1^{b_{s'}} x_{s'}$, $b_{s'} \in \mathbb{Z}$, $x_{s'} \in \mathsf{ORD}(\Sigma_2)$ for the terms $s' \in \mathsf{T}(p)$ and $\mathsf{HT}(p) = s \equiv a_1^{b_s} x_s$. Then we know $b_s \geq_{\mathbb{Z}} b_t$ since $t \in \mathsf{T}(p)$.

Hence in showing that the case $b_s >_{\mathbb{Z}} b_t$ is not possible we find that the exponents of a_1 in s and t are equal. To see this, let us study the possible cases. If $b_s > 0$ we have $b_s > b_t \geq 0$ and hence there exists no $x \in \mathbb{Z}$ such that $b_t + x > b_s + x \geq 0$. On the other hand $b_s < 0$ either implies $b_t > 0$ or ($b_t \leq 0$ and $|b_s| > |b_t|$). In both cases there exists no $x \in \mathbb{Z}$ such that $b_t + x < 0$ and $|b_t + x| > |b_s + x|$. Hence $b_t = b_s$ must hold as we know that t can be brought to head position by u, respectively v, such that the exponents of a_1 in $\mathsf{HT}(u * p)$, respectively $\mathsf{HT}(v * p)$, have different signs.

It remains to show that there cannot exist a term $s' \in \mathsf{T}(p)$ with $b_{s'} <_{\mathbb{Z}} b_s = b_t$. Let us assume such an s' exists. Since $\mathsf{HT}(u * p) = u \circ t \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(v * p) = v \circ t \equiv a_1^{j_1} \ldots a_n^{j_n}$ there then must exist $x_1, x_2 \in \mathbb{Z}$ such that $b_{s'} + x_1 <_{\mathbb{Z}} b_t + x_1 = i_1$ and $b_{s'} + x_2 <_{\mathbb{Z}} b_t + x_2 = j_1$. Without loss of generality let us assume $i_1 > 0$ and $j_1 < 0$ (the other case is symmetric). When $b_t < 0$ we get that $b_t + x_1 = i_1 > 0$ implies $x_1 > |b_t| > 0$. Now, as $b_{s'} <_{\mathbb{Z}} b_t$ either implies $b_{s'} > 0$ or ($b_{s'} \leq 0$ and $|b_{s'}| < |b_t|$), we find $b_{s'} + x_1 > b_t + x_1$ contradicting $b_{s'} + x_1 <_{\mathbb{Z}} b_t + x_1$. On the other hand, when $b_t > 0$ we know $b_t > b_{s'} \geq 0$. Furthermore, $b_t + x_2 = j_1 < 0$ implies $x_2 < 0$ and $|x_2| > b_t$. Hence we get $b_{s'} + x_2 < 0$ and $|b_{s'} + x_2| > |b_t + x_2|$ contradicting $b_{s'} + x_2 <_{\mathbb{Z}} b_t + x_2$.

Thus let us assume that for the letter a_{k-1} we have constructed $z_{k-1} \in \mathcal{G}$ such that $\mathsf{HT}(z_{k-1} * p) = z_{k-1} \circ t \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} r_{k-1} \equiv a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ with $r_{k-1} \in \mathsf{ORD}(\Sigma_k)$, $r' \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \ldots a_{k-1}^{s_{k-1}} \leq_{\text{tup}} a_1^{\rho_1} \ldots a_{k-1}^{\rho_{k-1}}$. We now show that we can find

$z_k = \tilde{w} \circ z_{k-1} \in \mathcal{G}$ such that $\mathsf{HT}(z_k * p) = z_k \circ t \equiv a_1^{s_1} \dots a_k^{s_k} r_k$ with $r_k \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \dots a_k^{s_k} \leq_{\text{tup}} a_1^{\rho_1} \dots a_k^{\rho_k}$.

This will be done in two steps. First we show that for the polynomials $u*p$ and $z_{k-1}*p$ with head terms $a_1^{i_1} \dots a_n^{i_n}$ respectively $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ we can find an element $w_1 \in \mathcal{G}$ such that $\mathsf{HT}(w_1 * z_{k-1} * p) = w_1 \circ z_{k-1} \circ t \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$, $\tilde{r} \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{\tilde{s}_k} \leq_{\text{tup}} a_k^{\tilde{\rho}_k}$ with

$$\tilde{\rho}_k = \begin{cases} \mathsf{sgn}(i_k) \cdot \min\{|i_k|, |l_k|\} & \mathsf{sgn}(i_k) = \mathsf{sgn}(l_k) \\ 0 & \text{otherwise.} \end{cases}$$

Then when $a_k^{\tilde{\rho}_k} \leq_{\text{tup}} a_k^{\rho_k}$ we are finished and set $z_k = w_1 \circ z_{k-1}$ and $s_k = \tilde{s}_k$. Otherwise we can similarly proceed for the polynomials $v * p$ and $w_1 * z_{k-1} * p$ with head terms $a_1^{j_1} \dots a_n^{j_n}$ and $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$ respectively and find an element $w_2 \in \mathcal{G}$ such that for $z_k = w_2 \circ w_1 \circ z_{k-1}$ we have $\mathsf{HT}(z_k * p) = z_k \circ t \equiv a_1^{s_1} \dots a_k^{s_k} r_k$, $r_k \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{s_k} \leq_{\text{tup}} a_k^{\tilde{\rho}_k'}$ with

$$\tilde{\rho}_k' = \begin{cases} \mathsf{sgn}(j_k) \cdot \min\{|j_k|, |\tilde{s}_k|\} & \mathsf{sgn}(j_k) = \mathsf{sgn}(\tilde{s}_k) \\ 0 & \text{otherwise.} \end{cases}$$

Then we can conclude $a_k^{s_k} \leq_{\text{tup}} a_k^{\rho_k}$ as in the case $s_k = 0$ the proof is immediately complete and otherwise we get $\mathsf{sgn}(j_k) = \mathsf{sgn}(\tilde{s}_k) = \mathsf{sgn}(\tilde{\rho}_k) = \mathsf{sgn}(i_k)$ and $\min\{|i_k|, |\tilde{s}_k|, |j_k|\} \leq \min\{|i_k|, |j_k|\}$.

Let us hence show how to construct w_1. Remember that $\mathsf{HT}(u*p) = u \circ t \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(z_{k-1} * p) = z_{k-1} \circ t \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ for some $r' \in \mathsf{ORD}(\Sigma_{k+1})$. In the case $i_k = l_k$ or $l_k = 0$ we can set $w_1 = \lambda$ and $\tilde{s}_k = l_k = \tilde{\rho}_k$ as $\mathsf{HT}(z_{k-1} * p) = z_{k-1} * t \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$. Hence let $i_k \neq l_k$ and $l_k \neq 0$.

First let us assume that $\mathsf{sgn}(i_k) = \mathsf{sgn}(l_k)$. Without loss of generality we can assume that a_k is not bounded[†]. Then in the case $|i_k| \geq |l_k|$ we can complete the proof by setting $w_1 = \lambda$ as again $\mathsf{HT}(z_{k-1} * p) = z_{k-1} \circ t \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ will do with $\tilde{s}_k = l_k = \tilde{\rho}_k$. Therefore, let us assume that $|l_k| > |i_k|$. Then we consider the multiple $y * z_{k-1} * p$, where $y = (a_1^{s_1} \dots a_{k-1}^{s_{k-1}}) \circ a_k^{-l_k + i_k} \circ \mathsf{inv}(a_1^{s_1} \dots a_{k-1}^{s_{k-1}})$, i.e., the exponent of the letter a_k in the term $y \circ z_{k-1} \circ t$ will be i_k. If $\mathsf{HT}(y * z_{k-1} * p) = y \circ z_{k-1} \circ t$ we are done because then $y \circ z_{k-1} \circ t \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} \tilde{r}_k$ for some $\tilde{r}_k \in \mathsf{ORD}(\Sigma_{k+1})$ and we can set $w_1 = y$ and $\tilde{s}_k = i_k = \tilde{\rho}_k$. Otherwise we show that the t-term $y \circ z_{k-1} \circ t$ in this multiple can be brought to the head position using an element $r \in \mathcal{G}$ such that we have $\mathsf{HT}((r \circ y) * z_{k-1} * p) = r \circ y \circ z_{k-1} \circ t = r \circ y \circ a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r' \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} \tilde{r}$, where $\tilde{r} \in \mathsf{ORD}(\Sigma_{k+1})$, thus allowing to set $\tilde{s}_k = i_k = \tilde{\rho}_k$ and $w_1 = r \circ y$. This follows immediately if we can prove that the exponent of a_k in the term $\mathsf{HT}(y * z_{k-1} * p)$ is also i_k. Then we can apply Lemma 3.2 to the polynomial $y * z_{k-1} * p$ and the term $y \circ z_{k-1} \circ t$. Note that $\mathsf{HT}(y * z_{k-1} * p)$ and $y \circ z_{k-1} \circ t$ have then a distinguishing letter of at least index $k+1$ and further $\mathsf{HT}(\mathsf{inv}(y) * (y * z_{k-1} * p)) = \mathsf{HT}(z_{k-1} * p) = z_{k-1} \circ t$. Therefore, we show that the exponent of a_k in the term $\mathsf{HT}(y * z_{k-1} * p)$ is also i_k. Let $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{b_k} r''$ with $r'' \in \mathsf{ORD}(\Sigma_{k+1})$ be the term in $z_{k-1} * p$ that became the head term (note that a candidate in $\mathsf{T}(z_{k-1} * p)$ for the head term in $y * z_{k-1} * p$ must have prefix $a_1^{s_1} \dots a_{k-1}^{s_{k-1}}$ since $\mathsf{HT}(z_{k-1} * p) \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} r_{k-1}$) and multiplication with y gives us $y \circ a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{b_k} r'' \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x \succ a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} w \equiv y \circ z_{k-1} \circ t$ for some $x, w \in \mathsf{ORD}(\Sigma_{k+1})$ and we have

[†] When a_k is bounded we can still use negative powers of a_k in the computations, as from the point of view of the collection process it does not matter at what time the power rules for a_k are applied.

$c_k \geq_{\mathbb{Z}} i_k$. Then there exist $z_1, z_2 \in \mathcal{G}$ such that $z_1 \circ a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} y \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{i_k+f_k} z$ for some $z \in \mathsf{ORD}(\Sigma_{k+1})$ and $z_2 \circ a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{i_k+f_k} z \equiv a_1^{i_1} \dots a_n^{i_n}$ and $z_2 = (a_1^{i_1} \dots a_{k-1}^{i_{k-1}}) \circ a_k^{-f_k} \circ z_2' \circ \mathsf{inv}(a_1^{i_1} \dots a_{k-1}^{i_{k-1}})$ for some $z_2' \in \mathsf{ORD}(\Sigma_{k+1})$. Note that the t-term in $y * z_{k-1} * p$ is brought to head position by multiplication with $z_2 \circ z_1$. Now multiplying $\mathsf{HT}(y * z_{k-1} * p)$ by $z_2 \circ z_1$ we find $z_2 \circ z_1 \circ a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x = a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{c_k+f_k-f_k} \tilde{x} \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{c_k} \tilde{x}$ for some $\tilde{x} \in \mathsf{ORD}(\Sigma_{k+1})$. This gives us $c_k \leq_{\mathbb{Z}} i_k$ and thus $i_k \leq_{\mathbb{Z}} c_k$ yields $c_k = i_k$.

Finally, we have to check the case that $\mathsf{sgn}(i_k) \neq \mathsf{sgn}(l_k)$ and $l_k \neq 0$. Notice that in this case the letter a_k is not bounded. Let us take a look at the polynomial $y * z_{k-1} * p$ where $y = (a_1^{s_1} \dots a_{k-1}^{s_{k-1}}) \circ a_k^{-l_k} \circ \mathsf{inv}(a_1^{s_1} \dots a_{k-1}^{s_{k-1}})$, i.e., the exponent of the letter a_k in the term $y \circ z_{k-1} \circ t$ will be 0. Suppose $\mathsf{HT}(y * z_{k-1} * p) \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x$, for some term $s \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{b_s} x_s \in \mathsf{T}(z_{k-1} * p)$, $x, x_s \in \mathsf{ORD}(\Sigma_{k+1})$, i.e., $c_k = b_s - l_k$. When this head term is already the corresponding t-term $y \circ z_{k-1} \circ t$, the proof follows and we set $w_1 = y$ and $\tilde{s}_k = 0 = \tilde{\rho}_k$. Now if we can show $c_k = 0$, by Lemma 3.2 the t-term $y \circ z_{k-1} \circ t$ can be brought to the head position by using an element such as that constructed in Lemma 3.2 since the distinguishing letter between $\mathsf{HT}(y * z_{k-1} * p)$ and the term $y \circ z_{k-1} \circ t$ then has at least index $k+1$ and we know $\mathsf{HT}(\mathsf{inv}(y) * (y * z_{k-1} * p)) = \mathsf{HT}(z_{k-1} * p) = z_{k-1} \circ t$. Hence, in showing that $c_k = 0$ the proof follows. As before there exist $z_1, z_2 \in \mathcal{G}$ such that $z_1 \circ y \circ z_{k-1} \circ t \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{f_k} z$ for some $z \in \mathsf{ORD}(\Sigma_{k+1})$ and $z_2 \circ a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{f_k} z \equiv a_1^{i_1} \dots a_n^{i_n}$, i.e., $z_2 = (a_1^{i_1} \dots a_{k-1}^{i_{k-1}}) \circ a_k^{-f_k+i_k} z_2' \circ \mathsf{inv}(a_1^{i_1} \dots a_{k-1}^{i_{k-1}})$ for some $z_2' \in \mathsf{ORD}(\Sigma_{k+1})$. Remember that this multiplication brings the t-term in $y * z_{k-1} * p$ to head position. Hence multiplying $\mathsf{HT}(y * z_{k-1} * p)$ by $z_2 \circ z_1$ we find $z_2 \circ z_1 \circ a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{c_k+i_k} \tilde{x}$ for some $\tilde{x} \in \mathsf{ORD}(\Sigma_{k+1})$. Thus we know $c_k + i_k \leq_{\mathbb{Z}} i_k$. To see that this implies $c_k = 0$ we have to distinguish three cases. Remember that $c_k = b_s - l_k$ and since our head term is an s-term $y \circ s$ for some $s \in \mathsf{T}(z_{k-1} * p)$ we know $b_s \leq_{\mathbb{Z}} l_k$. When $i_k = 0$, we have $c_k \leq_{\mathbb{Z}} 0$ implying $c_k = 0$. When $i_k > 0$ then $c_k + i_k = b_s - l_k + i_k \leq_{\mathbb{Z}} i_k$ implies $0 \leq b_s - l_k + i_k \leq i_k$. Furthermore, as $l_k < 0$ we have $-l_k + i_k > i_k$ implying $b_s < 0$ and hence $|b_s| \leq |l_k|$. But then $b_s - l_k \geq 0$ and $0 \leq b_s - l_k + i_k \leq i_k$ yields $c_k = b_s - l_k = 0$. On the other hand, $i_k < 0$ and $l_k > 0$ imply $0 \leq b_s \leq l_k$ and hence $b_s - l_k + i_k < 0$ yielding $|b_s - l_k + i_k| \leq |i_k|$. Since $b_s - l_k \leq 0$ this inequality can only hold when $c_k = b_s - l_k = 0$. □

Proof. (of Lemma 3.4) $\overset{*}{\longleftrightarrow}{}^{\text{lpc}}_{F} \subseteq \equiv_{\mathsf{ideal}_l(F)}$ is an immediate consequence of the definition of lpc-reduction. To show that the converse also holds, let $p - q \in \mathsf{ideal}_l(F)$. Then $p = q + \sum_{i=1}^{m} \alpha_i \cdot u_i * f_i, \alpha_i, \in \mathbb{K}, f_i \in G, u_i \in \mathcal{G}$ and we show that $p \overset{*}{\longleftrightarrow}{}^{\text{lpc}}_{G} q$ by induction on m. Without loss of generality we can assume that for every multiple $u_i * f_i$, $\mathsf{HT}(u_i * f_i) = u_i \circ \mathsf{HT}(f_i) \geq_{\text{tup}} \mathsf{HT}(f_i)$ holds. When $m = 0$ the lemma holds as then $p = q$. Hence let $p = q + \sum_{i=1}^{m} \alpha_i \cdot u_i * f_i + \alpha_{m+1} \cdot u_{m+1} * f_{m+1}$. Then the induction hypothesis yields $p \overset{*}{\longleftrightarrow}{}^{\text{lpc}}_{G} q + \alpha_{m+1} \cdot u_{m+1} * f_{m+1}$. Now let $t = \mathsf{HT}(u_{m+1} * f_{m+1})$ and $t \geq_{\text{tup}} \mathsf{HT}(f_{m+1})$. Furthermore, let β_1, respectively β_2, be the coefficient of t in q, respectively $q + \alpha_{m+1} \cdot u_{m+1} * f_{m+1}$. Then when $t \notin \mathsf{T}(q)$ we get $q + \alpha_{m+1} \cdot u_{m+1} * f_{m+1} \longrightarrow^{\text{lpc}}_{f_{m+1}} p$. When $t \notin \mathsf{T}(p)$ we similarly get $p - \alpha_{m+1} \cdot u_{m+1} * f_{m+1} \longrightarrow^{\text{lpc}}_{f_{m+1}} q$. As $p - \alpha_{m+1} \cdot u_{m+1} * f_{m+1} = q + \sum_{j=1}^{m} \alpha_j \cdot u_j * f_j$ the induction hypothesis yields $p - \alpha_{m+1} \cdot u_{m+1} * f_{m+1} \overset{*}{\longleftrightarrow}{}^{\text{lpc}}_{F} q$ and hence we are done. Otherwise let $\beta_1 \neq 0$ be the coefficient of t in $q + \alpha_{m+1} \cdot u_{m+1} * f_{m+1}$ and $\beta_2 \neq 0$ the coefficient of t in q.

This gives us the lpc-reduction step

$$q + \alpha_{m+1} \cdot u_{m+1} * f_{m+1} \longrightarrow^{\text{lpc}}_{f_{m+1}} q + \alpha_{m+1} \cdot u_{m+1} * f_{m+1}$$

$$\begin{aligned}&-\beta_1 \cdot \mathsf{HC}(f_{m+1})^{-1} \cdot u_{m+1} * f_{m+1}\\ &= q - (\beta_1 \cdot \mathsf{HC}(f_{m+1})^{-1} - \alpha_{m+1}) \cdot u_{m+1} * f_{m+1}\end{aligned}$$

eliminating the occurrence of t in $q + \alpha_{m+1} \cdot u_{m+1} * f_{m+1}$.

Then obviously $\beta_2 = (\beta_1 \cdot \mathsf{HC}(f_{m+1})^{-1} - \alpha_{m+1}) \cdot \mathsf{HC}(f_{m+1})$ and, therefore, we have $q \xrightarrow{\text{lpc}}_{f_{m+1}} q - (\beta_1 \cdot \mathsf{HC}(f_{m+1})^{-1} - \alpha_{m+1}) \cdot u_{m+1} * f_{m+1}$, i.e., q and $q + \alpha_{m+1} \cdot u_{m+1} * f_{m+1}$ are joinable. □

Proof. (of Theorem 3.1)
$1 \Longrightarrow 2$: By Definition 3.4 when for $f_k, f_l \in G$ the s-polynomial exists we get

$$\mathsf{spol}(f_k, f_l) = \mathsf{HC}(f_k)^{-1} \cdot w_1 * f_k - \mathsf{HC}(f_l)^{-1} \cdot w_2 * f_l \ \in \mathsf{ideal}_l(G),$$

and then $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\text{lpc}}_{G} 0$.

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}_l(G)$ is $\xrightarrow{\text{lpc}}_{G}$-reducible to zero. Without loss of generality we assume that G contains no constant polynomials, as then the theorem immediately holds. Remember that for $h \in \mathsf{ideal}_l(G)$, $h \xrightarrow{\text{lpc}}_{G} h'$ implies $h' \in \mathsf{ideal}_l(G)$. Thus as $\xrightarrow{\text{lpc}}_{G}$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_l(G) \setminus \{0\}$ is $\xrightarrow{\text{lpc}}_{G}$-reducible. Let $g = \sum_{j=1}^{m} \alpha_j \cdot w_j * f_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbb{K}^*, f_j \in F, w_j \in \mathcal{G}$. Since G is saturated by Definition 3.3 we can assume $g = \sum_{j=1}^{m} \alpha_j \cdot v_j * g_j$, where $\alpha_j \in \mathbb{K}^*, g_j \in G, v_j \in \mathcal{G}$ and $\mathsf{HT}(v_j * g_j) = v_j \circ \mathsf{HT}(g_j) \geq_{\text{tup}} \mathsf{HT}(g_j)$. Depending on this representation of g and our well-founded total ordering on $\mathcal{G}$ we define $t = \max\{\mathsf{HT}(v_j \circ g_j) \mid j \in \{1, \dots m\}\}$ and K is the number of polynomials $v_j * g_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in the case $\mathsf{HT}(g) = t$ this immediately implies that g is $\xrightarrow{\text{lpc}}_{G}$-reducible. Otherwise we show that g has an lpc-standard representation where all terms are bounded by $\mathsf{HT}(g)$, as this implies that g is top-reducible using G. This will be done by induction on (t, K), where $(t', K') < (t, K)$ if and only if $t' \prec t$ or ($t' = t$ and $K' < K$). Note that this ordering is well-founded since $\geq_{\text{syll}}$ is and $K \in \mathbb{N}$. In the case $t \succ \mathsf{HT}(g)$ there are two polynomials g_k, g_l in the corresponding representation such that $t = v_k \circ \mathsf{HT}(g_k) = v_l \circ \mathsf{HT}(g_l)$ and we have $t \geq_{\text{tup}} \mathsf{HT}(g_k)$,$t \geq_{\text{tup}} \mathsf{HT}(g_l)$. Hence by Definition 3.4 there exists an s-polynomial $\mathsf{spol}(g_k, g_l) = \mathsf{HC}(g_k)^{-1} \cdot z_1 * g_k - \mathsf{HC}(g_l)^{-1} \cdot z_2 * g_l$ and $v_k \circ \mathsf{HT}(g_k) = v_l \circ \mathsf{HT}(g_l) = w \circ z_1 \circ \mathsf{HT}(g_k) = w \circ z_2 \circ \mathsf{HT}(g_l) \geq_{\text{tup}} z_1 \circ \mathsf{HT}(g_k) = z_2 \circ \mathsf{HT}(g_l)$ for some $z_1, z_2, w \in \mathcal{G}$. Let us assume $\mathsf{spol}(g_k, g_l) \neq 0$ since when $\mathsf{spol}(g_k, g_l) = 0$, we can just substitute 0 for $\sum_{i=1}^{n} \delta_i \cdot v'_i * h_i$ in the equations below. Hence, $\mathsf{spol}(g_k, g_l) \xrightarrow{*}{}^{\text{lpc}}_{G} 0$ implies $\mathsf{spol}(g_k, g_l) = \sum_{i=1}^{n} \delta_i \cdot v'_i * h_i, \delta_i \in \mathbb{K}^*, h_i \in G, v'_i \in \mathcal{G}$, where the h_i are due to the lpc-reduction of the s-polynomial and all terms occurring in the sum are bounded by $\mathsf{HT}(\mathsf{spol}(g_k, g_l))$. By Lemma 2.3, since $t = w \circ z_1 \circ \mathsf{HT}(g_k) \geq_{\text{tup}} z_1 \circ \mathsf{HT}(g_k)$ and $z_1 \circ \mathsf{HT}(g_k) \succ \mathsf{HT}(\mathsf{spol}(g_k, g_l))$, we can conclude that t is a proper bound for all terms occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot w * v'_i * h_i$. Since $w \in \mathcal{G}$ and G is saturated, without loss of generality we can assume that the representation has the the required form. We now have:

$$\begin{aligned}&\alpha_k \cdot v_k * g_k + \alpha_l \cdot v_l * g_l\\ &= \alpha_k \cdot v_k * g_k + \underbrace{\alpha'_l \cdot \beta_k \cdot v_k * g_k - \alpha'_l \cdot \beta_k \cdot v_k * g_k}_{=0} + \alpha'_l \cdot \beta_l \cdot v_l * g_l\\ &= (\alpha_k + \alpha'_l \cdot \beta_k) \cdot v_k * g_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot v_k * g_k - \beta_l \cdot v_l * g_l)}_{= w * \mathsf{spol}(g_k, g_l)}\end{aligned}$$

$$= (\alpha_k + \alpha'_l \cdot \beta_k) \cdot v_k * g_k - \alpha'_l \cdot \left(\sum_{i=1}^{n} \delta_i \cdot w * v'_i * h_i \right) \tag{A.1}$$

where $\beta_k = \mathsf{HC}(g_k)^{-1}$, $\beta_l = \mathsf{HC}(g_l)^{-1}$ and $\alpha'_l \cdot \beta_l = \alpha_l$. By substituting (A.1) in our representation of g either t disappears or when t remains maximal among the terms occurring in the new representation of g, K is decreased. □

Proof. (of Theorem 3.2 and Corollary 3.3) Let F be a subset of $\mathbb{K}[\mathcal{G}]$ and G a Gröbner basis (the proof for the existence of a finite left Gröbner basis for $\mathsf{ideal}_l(F)$ is similar) of $\mathsf{ideal}(F)$, i.e., $\mathsf{ideal}(F) = \mathsf{ideal}(G) = \mathsf{ideal}_l(G)$ and for all $g \in \mathsf{ideal}(F)$ we have $g \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} 0$. We can assume that G is infinite as otherwise the proof is complete. Furthermore let $H = \{\mathsf{HT}(g) \mid g \in G\} \subseteq \mathcal{G}$. Then for every polynomial $f \in \mathsf{ideal}(F)$ there exists a term $t \in H$ such that $\mathsf{HT}(f) \geq_{\mathrm{tup}} t$. For each element $u \in H$ the element u can then be viewed as an n-tuple over $\mathbb{Z}$ as it is represented by an ordered group word. But we can also view it as a $2n$-tuple over $\mathbb{N}$ by representing each element u by an extended ordered group word $u \equiv a_1^{-i_1} a_1^{j_1} \ldots a_n^{-i_n} a_n^{j_n}$, where $i_l, j_l \in \mathbb{N}$ and is represented by the $2n$-tuple $(i_1, j_1, \ldots, i_n, j_n)$. Notice that at most one of the two exponents i_l and j_l is non-zero. Now H can be seen as a (possibly infinite) subset of a free commutative monoid $\mathcal{T}_{2n}$ with $2 \cdot n$ generators. Thus by Dickson's lemma there exists a finite subset B of H such that for every $w \in H$ there is a $b \in B$ with $w \geq_{\mathrm{tup}} b$. Now we can use the set B to distinguish a finite Gröbner basis in G as follows. To each term $t \in B$ we can assign a polynomial $g_t \in G$ such that $\mathsf{HT}(g_t) = t$. Then the set $G_B = \{g_t \mid t \in B\}$ is again a Gröbner basis since for every polynomial $f \in \mathsf{ideal}(F)$ there still exists a polynomial g_t, now in G_B, such that $\mathsf{HT}(f) \geq_{\mathrm{tup}} \mathsf{HT}(g_t) = t$. Hence all polynomials in $\mathsf{ideal}(F)$ are lpc-reducible to zero using G_B. □

Proof. (of Theorem 3.3)
$1 \Longrightarrow 2$: Since $g \in \mathsf{ideal}(G) = \mathsf{ideal}_l(G)$ and G is a left Gröbner basis, the proof follows.

$2 \Longrightarrow 3$: To show that G is a left Gröbner basis we have to prove $\stackrel{*}{\longleftrightarrow}{}^{\mathrm{lpc}}_{G} \; = \; \equiv_{\mathsf{ideal}_l(G)}$ and for all $g \in \mathsf{ideal}_l(G)$, $g \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} 0$. The latter follows immediately since $\mathsf{ideal}_l(G) \subseteq \mathsf{ideal}(G)$ and hence for all $g \in \mathsf{ideal}_l(G)$ we have $g \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} 0$. The inclusion $\stackrel{*}{\longleftrightarrow}{}^{\mathrm{lpc}}_{G} \; \subseteq \; \equiv_{\mathsf{ideal}_l(G)}$ is obvious. Hence let $f \equiv_{\mathsf{ideal}_l(G)} g$, i.e., $f - g \in \mathsf{ideal}_l(G)$. But then we have $f - g \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} 0$ and hence by Lemma 3.1 there exists a polynomial $h \in \mathbb{K}[\mathcal{G}]$ such that $f \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} h$ and $g \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} h$, yielding $f \stackrel{*}{\longleftrightarrow}{}^{\mathrm{lpc}}_{G} g$. Finally, $f * w \in \mathsf{ideal}(G)$ and $f * w \stackrel{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G} 0$ implies $f * w \in \mathsf{ideal}_l(G)$.

$3 \Longrightarrow 4$: This follows immediately.

$4 \Longrightarrow 1$: Since it is obvious that $\mathsf{ideal}_l(G) \subseteq \mathsf{ideal}(G)$ it remains to show that $\mathsf{ideal}(G) \subseteq \mathsf{ideal}_l(G)$ holds. Let $g \in \mathsf{ideal}(G)$, i.e., $g = \sum_{i=1}^{n} \alpha_i \cdot u_i * g_i * w_i$ for some $\alpha_i \in \mathbb{K}$, $g_i \in G$ and $u_i, w_i \in \mathcal{G}$. We will show by induction on $|w_i|$ that for $w_i \in \mathcal{G}$, $g_i \in G$, $g_i * w_i \in \mathsf{ideal}_l(G)$ holds. Then g also has a representation in terms of left-multiples and hence lies in the left ideal generated by G as well. When $|w_i| = 0$ we are immediately done. Hence let us assume $w_i \equiv aw$ for some $a \in \Sigma$ and by our assumption we know that $g_i * a \in \mathsf{ideal}_l(G)$. Let $g_i * a = \sum_{j=1}^{m} \beta_j \cdot v_j * g'_j$ for some $\beta_j \in \mathbb{K}$, $g'_j \in G$ and $v_j \in \mathcal{G}$. Then we get $g_i * w_i = g_i * aw = (g_i * a) * w = (\sum_{j=1}^{m} \beta_j \cdot v_j * g'_j) * w = \sum_{j=1}^{m} \beta_j \cdot v_j * (g'_i * w)$ and by our induction hypothesis $g'_j * w \in \mathsf{ideal}_l(G)$ holds for every $1 \leq j \leq m$. Therefore, we can conclude $g_i * w_i \in \mathsf{ideal}_l(G)$. □

Proof. (of Theorem 3.4) The theorem can again be proved using standard techniques as in the case of ordinary polynomial rings. Let G be a finite Gröbner basis of the ideal $\imath$ which must exist by Theorem 3.2 (the proof for the existence of a unique reduced left Gröbner basis for $\mathsf{ideal}_l(F)$ is similar). Then similar to a characaterization of Buchberger's Gröbner bases by head terms the following equation holds:

$$\{t \in \mathcal{G} \mid t \geq_{\mathrm{tup}} \mathsf{HT}(g), g \in G\} = \mathsf{HT}(\imath \setminus \{0\}).$$

The sets $\mathsf{HT}(G)$ and $\mathsf{HT}(\imath\backslash\{0\})$ depend on the presentation of the chosen $\mathcal{M}$, especially on the ordering induced on $\mathcal{M}$. As the set $\mathsf{HT}(G)$ is finite, there exists a subset $H \subseteq \mathsf{HT}(G)$ such that

(a) for all $m \in \mathsf{HT}(G)$ there exists an element $m' \in H$ such that $m \geq_{\mathrm{tup}} m'$,
(b) for all $m \in H$ there exists no element $m' \in H \setminus \{m\}$ such that $m' <_{\mathrm{tup}} m$, and
(c) $\{t \in \mathcal{G} \mid t \geq_{\mathrm{tup}} \mathsf{HT}(g), g \in H\} = \{t \in \mathcal{G} \mid t \geq_{\mathrm{tup}} \mathsf{HT}(g), g \in G\} = \mathsf{HT}(\imath \setminus \{0\})$.

Since for each term $t \in H$ there exists at least one polynomial in G with head term t we can choose one of them, say g_t, for every $t \in H$. Then the set $G' = \{g_t \mid t \in H\}$ is a Gröbner basis as we still have that for every $g \in \imath$, $g \overset{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G'} 0$ holds. Furthermore all polynomials in G' have different head terms and no head term is lpc-reducible by the other polynomials in G'. Hence, if we lpc-inter-reduce G' giving us another set of polynomials G'', we know $\mathsf{HT}(G') = \mathsf{HT}(G'')$ and this set is also a Gröbner basis of $\imath$ since for every $g \in \imath$, $g \overset{*}{\longrightarrow}{}^{\mathrm{lpc}}_{G''} 0$ still holds.

It remains to show the uniqueness of the reduced Gröbner basis if we restrict ourselves to sets of monic polynomials. Let us assume S is another monic reduced Gröbner basis of $\imath$. Furthermore let $f \in S \bigtriangleup G'' = (S \setminus G'') \cup (G'' \setminus S)$ be a polynomial such that $\mathsf{HT}(f)$ is minimal in the set of terms $\mathsf{HT}(S \bigtriangleup G'')$. Without loss of generality we can assume that $f \in S \setminus G''$. As G'' is a Gröbner basis and $f \in \imath$ there exists a polynomial $g \in G''$ such that $\mathsf{HT}(f) \geq_{\mathrm{tup}} \mathsf{HT}(g)$. We can even state that $g \in G'' \setminus S$ as otherwise S would not be lpc-inter-reduced. Since f was chosen such that $\mathsf{HT}(f)$ was minimal in $\mathsf{HT}(S \bigtriangleup G'')$, we get $\mathsf{HT}(f) = \mathsf{HT}(g)$. Otherwise $\mathsf{HT}(f) \succ \mathsf{HT}(g)$ would contradict our assumption. As we assume $f \neq g$ this gives us $f - g \neq 0$, $\mathsf{HT}(f - g) \prec \mathsf{HT}(f) = \mathsf{HT}(g)$ and $\mathsf{HT}(f - g) \in \mathsf{T}(f) \cup \mathsf{T}(g)$. But $f - g \in \imath$ implies the existence of a polynomial $h \in S$ such that $\mathsf{HT}(f - g) \geq_{\mathrm{tup}} \mathsf{HT}(h)$, implying that f is not lpc-reduced. Hence we get that S is not lpc-interreduced, contradicting our assumption. □

Originally received 29 July 1996
Accepted 11 March 1997