UNIVERSITÄT KAISERSLAUTERN
Zentrum für Computeralgebra

REPORTS ON COMPUTER ALGEBRA
NO. 09

ZENTRUM FÜR COMPUTERALGEBRA DER UNIVERSITÄT KAISERSLAUTERN

Z A C

Introducing reduction to polycyclic group rings – a comparison of methods

by

B. Reinert

October 1996

The Zentrum für Computeralgebra (Centre for Computer Algebra) at the University of Kaiserslautern was founded in June 1993 by the Ministerium für Wissenschaft und Weiterbildung in Rheinland-Pfalz (Ministry of Science and Education of the state of Rheinland-Pfalz). The centre is a scientific institution of the departments of **Mathematics, Computer Science, and Electrical Engineering** at the University of Kaiserslautern.
The goals of the centre are to advance and to support the use of Computer Algebra in industry, research, and teaching. More concrete goals of the centre include

- the development, integration, and use of software for Computer Algebra
- the development of curricula in Computer Algebra under special consideration of interdisciplinary aspects
- the realisation of seminars about Computer Algebra
- the cooperation with other centres and institutions which have similar goals

The present coordinator of the Reports on Computer Algebra is:
Olaf Bachmann (email: `obachman@mathematik.uni-kl.de`)

Zentrum für Computeralgebra
c/o Prof. Dr. G.-M. Greuel, FB Mathematik
Erwin-Schrödinger-Strasse
D-67663 Kaiserslautern; Germany
Phone: 49 - 631/205-2850   Fax: 49 - 631/205-5052
email: `greuel@mathematik.uni-kl.de`
URL: `http://www.mathematik.uni-kl.de/~zca/`

Introducing Reduction to Polycyclic Group Rings - A Comparison of Methods

Birgit Reinert*
Fachbereich Informatik
Universität Kaiserslautern
67663 Kaiserslautern
Germany
reinert@informatik.uni-kl.de

October 1996

Abstract

It is well-known that for the integral group ring of a polycyclic group several decision problems are decidable. In this paper a technique to solve the membership problem for right ideals originating from Baumslag, Cannonito and Miller and studied by Sims is outlined. We want to analyze, how these decision methods are related to Gröbner bases. Therefore, we define effective reduction for group rings over Abelian groups, nilpotent groups and more general polycyclic groups. Using these reductions we present generalizations of Buchberger's Gröbner basis method by giving an appropriate definition of "Gröbner bases" in the respective setting and by characterizing them using concepts of saturation and s-polynomials.

Keywords: Gröbner bases, polycyclic group rings, rewriting

1 Introduction

By introducing the theory of Gröbner bases for polynomial ideals in commutative polynomial rings over fields, Buchberger established a rewriting approach to the theory of polynomial ideals (see [Bu65]). He used polynomials as rules by giving an admissible term ordering on the terms and using the largest monomial according to this ordering as a left hand side of a rule. "Reduction" defined in this way can be compared to division of one polynomial by a set of finitely many polynomials. A Gröbner basis now is 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 (especially the polynomials in the ideal generated by G reduce to zero using G). Hence in case they can be computed such bases enable

*The author was supported by the Deutsche Forschungsgemeinschaft (DFG).

to solve many problems related to ideals. For the polynomial ring Buchberger developed a terminating procedure to transform a finite generating set of a polynomial ideal into a finite Gröbner basis of the same ideal.

Since the theory of Gröbner bases turned out to be of outstanding importance for polynomial rings, extensions of Buchberger's ideas to other algebras followed, for example to free algebras ([Mo85, Mo94]), Weyl algebras ([La85]), enveloping fields of Lie algebras ([ApLa88]), solvable rings ([KaWe90, Kr93]), skew polynomial rings ([We92]), free group rings ([Ro93]) and monoid and group rings ([MaRe93b]).

Especially group rings are subject of extensive studies in mathematics. In 1981 Baumslag, Cannonito and Miller showed that for the integral group ring of a polycyclic group several decision problems including the membership problem for submodules are computable [BaCaMi81]. In [Si94] Sims studies these ideas and shows connections between special submodule bases which allow to solve the membership problem and Gröbner bases.

In this paper we want to present our results on generalizing reduction and Gröbner bases to polycyclic group rings and especially to the subclasses of Abelian groups and nilpotent groups. We want to point out that instead of using the fact that every group ring over a polycyclic group is Noetherian, we give a rewriting oriented approach which leads to a syntactical characterization of Gröbner bases in terms of s-polynomials and a completion based algorithm to compute them. In order to do this we have to give conditions when a polynomial can be used to reduce another polynomial. Due to the presentation of the group elements by ordered group words we can define a concept of "syntactical divisors" or "commutative prefixes" on the 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. But we will see that this property alone in general will not be sufficient to ensure that reduction based on commutative prefixes is Noetherian. Hence additional conditions concerning the presentation chosen for the group and whether left or right multiples are used for reduction will be important. This leads to different instances of reduction for groups depending on their presentation. Notice that, since for finitely generated groups we have that Abelian implies nilpotent which again implies polycyclic, reduction in polycyclic group rings will also work for nilpotent group rings and again reduction specialized for nilpotent group rings can be used for Abelian group rings. We will also see why the reverse does not hold.

In section 2 the basic notions of this paper are presented. It is well known that a polycyclic group $\mathcal{G}$ can be presented by a confluent semi-Thue system of a special form. Such presentations are given and both - the vocabulary of Wißmann in [Wi89] and of Sims in [Si94] - are presented. In order to keep the paper self-contained, section 3 cites the results on the Baumslag, Cannonito, Miller approach to solve the submodule problem in polycyclic group rings as given in chapter 10 of Sims' book [Si94]. It also includes a possible way of deducing reduction in this setting, and problems related to this reduction. Furthermore, we sketch Sims' generalization of Gröbner bases to finitely generated free Abelian group rings — so called rings of Laurent polynomials. Section 4 relates special Gröbner bases to solutions of the subgroup problem by rewriting techniques. It is outlined how Wißmann's approach [Wi89] to the subgroup problem in nilpotent and polycyclic groups can be seen in our setting. Section 5 states how Gröbner bases can be generalized for right and two-sided ideals in finitely generated nilpotent group rings. A comparison with Sims' approach for

Laurent polynomials is done for the special case of free Abelian groups. Finally section 6 outlines how a generalization for left and two-sided ideals works for arbitrary polycyclic groups (hence especially for finitely generated nilpotent groups) and which problems arise for right ideals.

2 Basic Definitions

Let $\mathcal{G}$ be a group with binary operation $\circ$ and identity λ. The elements of a group ring $\mathbf{K}[\mathcal{G}]$ over a field $\mathbf{K}$ 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 $\gamma_g = \sum_{x \circ y = g \in \mathcal{G}} \alpha_x \cdot \beta_y$. Polynomials will be written as finite sums $\sum_{i=1}^{k} \alpha_i \cdot t_i$ with $\alpha_i \in \mathbf{K}$ and $t_i \in \mathcal{G}$.

For a subset F of $\mathbf{K}[\mathcal{G}]$ we can specify special subsets of $\mathbf{K}[\mathcal{G}]$ as follows: We call the set $\mathsf{ideal}_r(F) = \{\sum_{i=1}^{n} \alpha_i \cdot f_i * w_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, w_i \in \mathcal{G}\}$ the **right ideal**[1], $\mathsf{ideal}_l(F) = \{\sum_{i=1}^{n} \alpha_i \cdot w_i * f_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, w_i \in \mathcal{G}\}$ the **left ideal**, and $\mathsf{ideal}(F) = \{\sum_{i=1}^{n} \alpha_i \cdot u_i * f_i * w_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, u_i, w_i \in \mathcal{G}\}$ the **two-sided ideal** generated by F.

As we are interested in constructing Gröbner bases for ideals in $\mathbf{K}[\mathcal{G}]$, we need an appropriate presentation of the group $\mathcal{G}$ in order to do computations. Structures which can be used to present groups are **semi-Thue systems** (also called **string-rewriting systems**). Let us start with some basic definitions. For a finite alphabet Σ, Σ^* will denote the set of all **words** over the alphabet Σ where λ presents the **empty word**, i.e., the word of length zero. $\equiv$ will denote the **identity** on Σ^*. A **semi-Thue system** T over Σ is a subset of $\Sigma^* \times \Sigma^*$. The elements (l, r) of T are called **rules** and will often be written as $l \longrightarrow r$. The **single-step reduction relation** on Σ^* induced by a semi-Thue system T is defined as follows: For any u, v in Σ^*, $u \longrightarrow_T v$ if and only if there exist x, y in Σ^* and (l, r) in T such that $u \equiv xly$ and $v \equiv xry$. The **reduction relation** on Σ^* induced by T is the reflexive transitive closure of $\longrightarrow_T$ and is denoted by $\xrightarrow{*}_T$. The reflexive transitive symmetric closure is denoted by $\xleftrightarrow{*}_T$. If $u \xrightarrow{*}_T v$ holds then one says that u reduces to v. In case u has no descendant except itself it is called **irreducible**. The reduction is called **Noetherian** if and only if there is no infinite chain $u \longrightarrow_T v_1 \longrightarrow_T v_2 \longrightarrow_T \ldots$. We speak of **confluence** if for all u, v, w in Σ^*, $u \xrightarrow{*}_T$ and $u \xrightarrow{*}_T w$ imply the existence of z in Σ^* such that $v \xrightarrow{*}_T z$ and $w \xrightarrow{*}_T z$. A semi-Thue system is called **convergent** if it is both, Noetherian and confluent, i.e., unique normal forms exist for the irreducible elements.

Definition 1
Let Σ be an alphabet. A mapping $\imath : \Sigma \longrightarrow \Sigma$ is called an **involution** if $\imath(\imath(a)) = a$ for all $a \in \Sigma$. A semi-Thue system is called a **group system** if there exists an involution $\imath$ such that for all $a \in \Sigma$ the rules $(\imath(a)a, \lambda)$ and $(a\imath(a), \lambda)$ are included in T. ⋄

Note that sometimes we will assume that $\Sigma = \Gamma \cup \Gamma^{-1}$ where $\Gamma^{-1} = \{a^{-1} \mid a \in \Gamma\}$ contains

[1] Notice that the linear combinations in these definitions of ideals in fact describe elements of $\mathbf{K}[\mathcal{G}]$. Since the elements $\alpha_i \in \mathbf{K}$ and $w_i \in \mathcal{G}$ can be interpreted as elements of $\mathbf{K}[\mathcal{G}]$ the multiplication $f_i * w_i$ is well-defined and gives us an element say h_i in $\mathbf{K}[\mathcal{G}]$, as does again the multiplcation $\alpha_i \cdot h_i$.

the formal inverses of Γ and T contains the rules corresponding to the trivial relations in a group, namely $\{(aa^{-1}, \lambda), (a^{-1}a, \lambda) \mid a \in \Gamma\}$.

An equivalence relation on Σ^* is said to be a congruence relation in case it is admissible, i.e., compatible with concatenation. Since this is obviously true for the reduction relation induced by a semi-Thue system T, the reflexive transitive symmetric closure $\overset{*}{\longleftrightarrow}_T$ is a congruence relation on the set Σ^*, the **Thue congruence**. The congruence classes are denoted by $[w]_T = \{v \in \Sigma^* \mid v \overset{*}{\longleftrightarrow}_T w\}$ and we can set $\mathbf{M}_T = \{[w]_T \mid w \in \Sigma^*\}$. In fact $\mathbf{M}_T$ is the factor monoid of the free monoid Σ^* modulo the congruence induced by T as the following lemma establishes.

Lemma 1
Let (Σ, T) be a semi-Thue system.

1. *The set $\mathbf{M}_T$ together with the binary operation $\circ : \mathbf{M}_T \times \mathbf{M}_T \longrightarrow \mathbf{M}_T$ defined by $[u]_T \circ [v]_T = [uv]_T$ and the identity $[\lambda]_T$ is a monoid, called the* **factor monoid** *of Σ^* and $\overset{*}{\longleftrightarrow}_T$.*

2. *In case T is a group system, the set $\mathbf{M}_T$ together with $\circ$, $[\lambda]_T$ and inv is a group, where $\mathsf{inv}([w]_T) = [\mathrm{inv}(w)]_T$, and $\mathrm{inv}(\lambda) = \lambda$, $\mathrm{inv}(wa) = \imath(a)\mathrm{inv}(w)$ for all $w \in \Sigma^*$, $a \in \Sigma$.*

Hence, semi-Thue systems are means for presenting monoids and groups. The following definitions are closely related to describing monoids and groups in terms of generators and defining relations. We call a pair (Σ, T) a **presentation** of a monoid (group) $\mathcal{M}$ if $\mathcal{M} \cong \mathbf{M}_T$. Note that every monoid can be presented by a (even convergent) semi-Thue system. Just let Σ be the (possibly infinite) set of all elements and T the multiplication table. The problem is that this presentation in general is neither finite nor recursive. We call a monoid (group) $\mathcal{M}$ **finitely generated**, if $\mathcal{M}$ has a presentation (Σ, T) such that Σ is finite. $\mathcal{M}$ is said to be **finitely presented**, if additionally T is finite. In order to do effective computations in our monoid or group we have to be able to compute representatives for the congruence classes of the elements. A very nice solution occurs in case we are able to give convergent finite semi-Thue systems as presentations, since then every congruence class has a unique representative and many problems, e.g. the word problem, are algorithmically solvable. The class of polycyclic groups, which include the Abelian and nilpotent groups, allow convergent presentations[2]. The following notations are taken from [Wi89].

Let $\Sigma = \{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$ be a finite alphabet and for $1 \leq k \leq n$ we define the subsets $\Sigma_k = \{a_i, a_i^{-1} \mid k \leq i \leq n\}$, $\Sigma_{n+1} = \emptyset$. We first distinguish several particular classes of rules over Σ.

Definition 2
Let $i, j \in \{1, \ldots, n\}$, $j > i$ and $\delta, \delta' \in \{1, -1\}$.

1. A rule $a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} a_j^{\delta}$ is called a **CAB-rule** (Abelian).

2. A rule $a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} a_j^{\delta} z$, $z \in \Sigma_{j+1}^*$ is called a **CNI-rule** (nilpotent).

[2] A survey on groups allowing convergent presentations can be found in [MaOt89].

3. A rule $a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} z$, $z \in \Sigma_{i+1}^*$ is called a **CP-rule** (polycyclic). ◇

Definition 3
For X ∈ {AB, NI, P} a subset C of $\Sigma^* \times \Sigma^*$ is called a **commutation system** if

1. C contains only CX-rules, and
2. for all $1 \leq i < j \leq n$ and for all $\delta, \delta' \in \{1, -1\}$ there is exactly one rule $a_j^{\delta} a_i^{\delta'} \longrightarrow r$ in C. ◇

Definition 4
For $1 \leq i \leq n$ a rule $a_i^m \longrightarrow r$ where $m \geq 1$, $r \in \Sigma_{i+1}^*$ is called a **positive P-rule** and a rule $a_i^{-1} \longrightarrow uv$ where $u \in \{a_i\}^*$ and $v \in \Sigma_{i+1}^*$ is called a **negative P-rule**. Then a subset P of $\Sigma^* \times \Sigma^*$ is called a **power system** if

1. P contains only positive and negative P-rules.
2. For all $1 \leq i \leq n$ there is a negative P-rule $a_i^{-1} \longrightarrow uv$ in P if and only if there also is a positive P-rule of the form $a_i^m \longrightarrow r$ with $m \geq 1$ in P.
3. For all $1 \leq i \leq n$ there is at most one negative P-rule $a_i^{-1} \longrightarrow uv$ and at most one positive P-rule $a_i^m \longrightarrow r$ in P. ◇

In combining these rule systems we can characterize special group presentations. For X in {AB, NI, P}, a presentation (Σ, T) is called a **CX-string-rewriting system** (CX-system) if $T = C \cup I$ where C is a commutation system and I contains the trivial rules, i.e., $I = \{a_i a_i^{-1} \longrightarrow \lambda, a_i^{-1} a_i \longrightarrow \lambda | 1 \leq i \leq n\}$. It is called a **PCX-string-rewriting system** (PCX-system) if $T = C \cup P \cup I$ where T additionally includes a power system P. The motivation for such presentations stems from the fact that they can be used to characterize special classes of groups.

Theorem 1 (Theorem 2.5.1. in [Wi89])
For a finitely presented group $\mathcal{G}$ the following statements hold:

1. *$\mathcal{G}$ is Abelian if and only if there is a PCAB-system presenting $\mathcal{G}$.*
2. *$\mathcal{G}$ is nilpotent if and only if there is a PCNI-system presenting $\mathcal{G}$.*
3. *$\mathcal{G}$ is polycyclic if and only if there is a PCP-system presenting $\mathcal{G}$.*

Notice that this theorem is a syntactical illustration of the fact that for finitely generated groups Abelian implies nilpotent which again implies polycyclic.

Using a **syllable ordering** Wißmann has shown that a PCX-system (Σ, T) is a Noetherian string-rewriting system and he gave a completion procedure for such systems which terminates with an output that is again a PCX-system of the same type.

Definition 5
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:

$$(u_0, \ldots, u_m) \succ^{\text{lex}} (v_0, \ldots, v_m)$$

$$\text{if and only if}$$

$$\text{there exists } 0 \leq k \leq m \text{ such that } u_i = v_i \text{ for all } 0 \leq i < k \text{ and } u_k \succ v_k.$$

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 $w_i \in (\Sigma \backslash \{a\})^*$. Given a total precedence[3] $\rhd$ on Σ we can define a **syllable ordering with status left** by

$$u >_{\text{syll}(\Sigma)} v$$

$$\text{if and only if}$$

$$|u|_a > |v|_a \text{ or}$$

$$|u|_a = |v|_a \text{ and } (u_0, \ldots, u_m) >^{\text{lex}}_{\text{syll}(\Sigma \backslash \{a\})} (v_0, \ldots, v_m)$$

where a is the largest letter in Σ according to $\rhd$ and $(u_0, \ldots, u_m)$, $(v_0, \ldots, v_m)$ are the decompositions of u and v with respect to a in case $|u|_a = |v|_a = m$. $\diamond$

The total precedence used on an alphabet $\Sigma = \{a_i, a_i^{-1} \mid 1 \leq i \leq n\}$ in our setting is $a_1^{-1} \succ a_1 \succ \ldots a_i^{-1} \succ a_i \succ \ldots \succ a_n^{-1} \succ a_n$. Using the syllable ordering induced by this precedence we can give a characterization of the elements of our group as a subset of the set of **ordered group words** $\mathsf{ORD}(\Sigma) = \mathsf{ORD}(\Sigma_1)$, where we define $\mathsf{ORD}(\Sigma_i)$ recursively by $\mathsf{ORD}(\Sigma_{n+1}) = \{\lambda\}$, and $\mathsf{ORD}(\Sigma_i) = \{w \in \Sigma_i^* \mid w \equiv uv \text{ for some } u \in \{a_i\}^* \cup \{a_i^{-1}\}^*, v \in \mathsf{ORD}(\Sigma_{i+1})\}$. Further with respect to T we define the constants $\epsilon_T(i)$ for $1 \leq i \leq n$ by setting

$$\epsilon_T(i) = \begin{cases} \infty & \text{if } T \text{ contains no P-rules for } a_i \\ m & \text{if } T \text{ contains a P-rule } a_i^m \longrightarrow r \text{ for some unique } m > 0. \end{cases}$$

One can show that using the syllable ordering for orienting T we get

$$\text{IRR}(T) = \{a_1^{i_1} \ldots a_n^{i_n} | i_1, \ldots, i_n \in \mathbf{Z}, \text{ and if } \epsilon_R(j) \neq \infty \text{ then } 0 \leq i_j \leq \epsilon_T(j)\}.$$

For example the semi-Thue system (Σ, T) where $T = C \cup I$ such that we have $C = \{a_j^{\delta} a_i^{\delta'} \longrightarrow a_i^{\delta'} a_j^{\delta} \mid 1 \leq i < j \leq n, \delta, \delta' \in \{1, -1\}\}$ and $I = \{a_i a_i^{-1} \longrightarrow \lambda, a_i^{-1} a_i \longrightarrow \lambda \mid 1 \leq i \leq n\}$ is a presentation of the free commutative group generated by $\{a_1, \ldots, a_n\}$ and we have $\text{IRR}(T) = \mathsf{ORD}(\Sigma)$.

In restricting the syllable ordering introduced in definition 5 to ordered group words this gives us $a_1^{i_1} \ldots a_n^{i_n} >_{\text{syll}} a_1^{j_1} \ldots a_n^{j_n}$ 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 $i_d >_{\mathbf{Z}} j_d$ with $\alpha >_{\mathbf{Z}} \beta$ if and only if $\beta = 0$ or $(\mathsf{sgn}(\alpha) = -1$ and $\mathsf{sgn}(\beta) = 1)$ or $(\mathsf{sgn}(\alpha) = \mathsf{sgn}(\beta)$ and $|\alpha| > |\beta|)$. where $>$ is the usual ordering[4] on $\mathbf{Z}$ and for $\alpha \in \mathbf{Z}$, $\mathsf{sgn}(\alpha) = 0$ if $\alpha = 0$, $\mathsf{sgn}(\alpha) = 1$ if $\alpha > 0$ and $\mathsf{sgn}(\alpha) = -1$ if $\alpha < 0$. We then call a_d the **distinguishing letter** between the two ordered group words.

The next two technical lemmata are related to some properties of the wellfounded ordering $>_{\mathbf{Z}}$ and will be useful in the proofs later on.

[3] By a precedence on an alphabet we mean a partial ordering on its letters.

[4] By the usual ordering on $\mathbf{Z}$ we mean $\ldots - 3 < -2 < -1 < 0 < 1 < 2 < 3 < \ldots$.

Lemma 2
Let $a, b, c \in \mathbf{Z}$. Then $a >_{\mathbf{Z}} b$ and $a \cdot c \geq 0$ imply $a + c >_{\mathbf{Z}} b + c$.

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

q.e.d.

Lemma 3
Let $a, b, c \in \mathbf{Z}$. Then $a >_{\mathbf{Z}} b$, $a \geq_{\mathbf{Z}} c$, and the existence of an element $x \in \mathbf{Z}$ such that $a + x <_{\mathbf{Z}} b + x$ and $c + x \leq_{\mathbf{Z}} b + x$ imply $b - a \geq_{\mathbf{Z}} c - a$. In case $c + x <_{\mathbf{Z}} b + x$ holds we get $b - a >_{\mathbf{Z}} c - a$.

Proof :
First let us look at the case $b - a = c - a$. This implies $b = c$ and hence $b + y = c + y$ for all $y \in \mathbf{Z}$. Therefore the existence of an $x \in \mathbf{Z}$ such that $c + x <_{\mathbf{Z}} b + x$ implies $b - a \neq_{\mathbf{Z}} c - a$. Now it remains to prove that the case $b - a <_{\mathbf{Z}} c - a$ 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 $a \geq_{\mathbf{Z}} c$) and $a > b \geq 0$ (as $a >_{\mathbf{Z}} b$). Since then $b - a \geq 0$ is not possible, $b - a <_{\mathbf{Z}} c - a$ 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 $b + y <_{\mathbf{Z}} a + y$ and for all $y < -b$ we have $b + y >_{\mathbf{Z}} a + y$. Similarly, for $b \geq c \geq 0$ we find that for all $z \geq -c$ we have $c + z \leq_{\mathbf{Z}} b + z$ and for all $z < -c$, $c + z \geq_{\mathbf{Z}} b + z$ holds. Hence for x such that $a + x <_{\mathbf{Z}} b + x$ and $c + x \leq_{\mathbf{Z}} b + x$ 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 $a \geq_{\mathbf{Z}} c$ 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 $a >_{\mathbf{Z}} c$ must hold as $a \neq c$). Furthermore, $a >_{\mathbf{Z}} b$ implies $a < 0$. Let us analyze the remaining cases. If $c \leq 0$ we find $b < 0$ as well (since $c > b \geq a$). Since the equation $a + x <_{\mathbf{Z}} b + x$ holds for $x \geq -a > 0$ only and $c + x \leq_{\mathbf{Z}} b + x$ for $0 \leq x < -b < -a$ only, no x as required can exist. Hence suppose $c > 0$. Then depending on b the equation $c + x \leq_{\mathbf{Z}} b + x$ holds either for $0 \leq x < -b < -a$ (in case $b < 0$) only or for $x < -b \leq 0$ (in case $b \geq 0$), and as further $x \geq -a > 0$ must hold again no such x can exist.

q.e.d.

The following lemma is an easy observation on the results of multiplying a letter by special ordered group words.

Lemma 4

1. *Let $\mathcal{G}$ be a nilpotent group with a convergent PCNI-presentation (Σ, T). Further for some $1 \leq j < i \leq n$ let $w_1 \in \mathsf{ORD}(\Sigma \backslash \Sigma_j)$, $w_2 \in \mathsf{ORD}(\Sigma_{i+1})$. Then we have $a_i \circ w_1 \equiv w_1 a_i z_1$ and $w_2 \circ a_i \equiv a_i z_2$ for some $z_1, z_2 \in \mathsf{ORD}(\Sigma_{i+1})$.*

2. *Let $\mathcal{G}$ be a polycyclic group with a convergent PCP-presentation (Σ, T). Further 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 $z \in \mathsf{ORD}(\Sigma_{i+1})$.*

Proof :
This follows immediately from the rules given in the respective presentations.

q.e.d.

We now define a new ordering on $\mathcal{G}$ called a **tuple ordering**, which will be crucial in our definitions of reduction.

Definition 6
For two elements $w \equiv a_1^{i_1} \ldots a_n^{i_n}, v \equiv a_1^{j_1} \ldots a_n^{j_n} \in \mathsf{ORD}(\Sigma)$, we define $w \geq_{\text{tup}} v$ 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. Further we define $w >_{\text{tup}} v$ if $w \geq_{\text{tup}} v$ and $|i_l| > |j_l|$ for some $1 \leq l \leq n$ and $w \geq_{\text{tup}} \lambda$ for all $w \in \mathcal{G}$. According to this ordering we call v a **syntactic divisor** or **commutative prefix** of w if $w >_{\text{tup}} v$. ⋄

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 $w >_{\text{tup}} v$ implies $w \succ v$, where $\succeq$ is the ordering on $\mathcal{G}$ induced by the syllable ordering used as completion ordering for the respective PCX-presentation of $\mathcal{G}$. Given a non-zero polynomial p in $\mathbf{K}[\mathcal{G}]$, 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 $\mathcal{G}$ can be extended to a partial ordering on $\mathbf{K}[\mathcal{G}]$ by setting $p > q$ if and only if $\mathsf{HT}(p) \succ \mathsf{HT}(q)$ or $(\mathsf{HM}(p) = \mathsf{HM}(q)$ and $p - \mathsf{HM}(p) > q - \mathsf{HM}(q))$.

The tuple ordering can be used to specify special representations of right and left ideal elements and special bases of them.

Definition 7
Let F be a set of polynomials and p a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$.

1. A representation

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

   is called a **right commutative prefix standard representation** in case for the respective head terms we have $\mathsf{HT}(p) \succeq \mathsf{HT}(f_i) \circ w_i = \mathsf{HT}(f_i * w_i)$ and $\mathsf{HT}(f_i * w_i) \geq_{\text{tup}} \mathsf{HT}(f_i)$ for all $1 \leq i \leq n$. In our previous work this was also called a **quasi-commutative (qc-) standard representation**.

2. A representation

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

is called a **left commutative prefix standard representation** in case 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 $1 \leq i \leq n$. Again for historical reasons this is sometimes called a **left polycyclic (lpc-) standard representation**.

A set $F \subseteq \mathbf{K}[\mathcal{G}]$ is called a right commutative prefix respectively left commutative prefix **standard basis** if every non-zero polynomial in $\mathsf{ideal}_r(F)$ respectively $\mathsf{ideal}_l(F)$ has a right commutative prefix respectively left commutative prefix standard representation with respect to F. $\diamond$

Notice that in case $\mathcal{G}$ is Abelian these representations coincide and are called commutative standard representations. We will later on see how such representations are related to different reductions, which will be Noetherian because of the following statements, which heavily depend on the presentation of the group.

Lemma 5
Let $\mathcal{G}$ be a nilpotent group with a convergent PCNI-presentation, $w, v, \tilde{v} \in \mathcal{G}$ 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 $u = \mathsf{inv}(v) \circ w$.

Proof :
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 $x \in \mathsf{ORD}(\Sigma \backslash \Sigma_d)$, $y_v, y_{\tilde{v}} \in \mathsf{ORD}(\Sigma_{d+1})$ and $v_d >_{\mathbf{Z}} \tilde{v}_d$. Then for $u \equiv a_1^{u_1} \dots a_n^{u_n}$ we get $v \circ a_1^{u_1} \dots a_d^{u_d} = a_1^{w_1} \dots a_{d-1}^{w_{d-1}} \circ a_d^{u_d+v_d+s_d} \circ (a_{d+1}^{s_{d+1}} \dots a_n^{s_n} \circ y_v)$ and similarly $\tilde{v} \circ a_1^{u_1} \dots a_d^{u_d} = a_1^{w_1} \dots a_{d-1}^{w_{d-1}} \circ a_d^{u_d+v_d+s_d} \circ (a_{d+1}^{s_{d+1}} \dots a_n^{s_n} \circ y_{\tilde{v}})$ and since $(a_{d+1}^{s_{d+1}} \dots a_n^{s_n} \circ y_v)$,$(a_{d+1}^{s_{d+1}} \dots a_n^{s_n} \circ y_{\tilde{v}}) \in \mathsf{ORD}(\Sigma_{d+1})$ and the exponents of the letter a_d are different, in order to decide whether $w \succ \tilde{v} \circ u$ we only have to compare the exponents of a_d in the normal forms of the respective products. Now, $w \geq_{\mathrm{tup}} v$ gives us, for the exponent w_d of the letter a_d in w, $w_d \geq_{\mathbf{Z}} v_d$, $\mathsf{sgn}(w_d) = \mathsf{sgn}(v_d)$ and $u_d + v_d + s_d = w_d$ or $(u_d + v_d + s_d)$ mod $m_d = w_d$ in case a_d is bounded by m_d.

To show that $w \succ \tilde{v} \circ u$ we now have to distinguish two cases. If the letter a_d has unbounded exponents, we can apply lemma 2 since $v_d >_{\mathbf{Z}} \tilde{v}_d$ and $v_d \cdot (u_d + s_d) \geq 0$ 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 $(v_d + u_d + s_d)$ mod $m_d = w_d$. Now in case $v_d + u_d + s_d = w_d$ we are done, as then $u_d + s_d \geq 0$ implies $v_d + u_d + s_d > \tilde{v}_d + u_d + s_d$. Else, as $v_d \leq w_d$, for $y = w_d - v_d$ we know $u_d + s_d = l \cdot m_d + y$ with $0 \leq y < m_d$ and hence $0 \leq (\tilde{v}_d + u_d + s_d)$ mod $m_d = (\tilde{v}_d + l \cdot m_d + y)$ mod $m_d = \tilde{v}_d + y < v_d + y = w_d$ and we are done.

q.e.d.

However, the next example shows that for PCP-presentations of groups this in general no longer holds.

Example 1
Let $\Sigma = \{a_1, a_1^{-1}, a_2, a_2^{-1}, a_3, a_3^{-1}\}$ and $T = \{a_3 a_1 \longrightarrow a_1 a_2 a_3, a_3 a_1^{-1} \longrightarrow$

$a_1^{-1}a_2^{-1}a_3, a_3^{-1}a_1 \longrightarrow a_1a_2^{-1}a_3^{-1}, a_3^{-1}a_1^{-1} \longrightarrow a_1^{-1}a_2a_3^{-1}, a_3^{\delta}a_2^{\delta'} \longrightarrow a_2^{\delta'}a_3^{\delta}, a_2^{\delta}a_1^{\delta'} \longrightarrow a_1^{\delta'}a_2^{\delta} \mid \delta, \delta' \in \{1, -1\}\} \cup T_I$ be a polycyclic presentation of the free nilpotent group with two generators. Then for $w \equiv a_1^2a_2$, $v \equiv a_1a_2$ and $\tilde{v} \equiv a_1a_3$ we have $w \geq_{\text{tup}} v$, $v \succ \tilde{v}$. Now for $u \equiv a_1$ we find $v \circ u = a_1a_2 \circ a_1 \equiv a_1^2a_2$, but $\tilde{v} \circ u = a_1a_3 \circ a_1 = a_1^2a_2a_3$ and hence $\tilde{v} \circ u \succ w$.

◇

This example stresses the importance of the presentation chosen for the group, as the group is nilpotent. Note that lemma 5 holds when using the presentation $\Sigma = \{a_1, a_1^{-1}, a_2, a_2^{-1}, a_3, a_3^{-1}\}$ and $T = \{a_2a_1 \longrightarrow a_1a_2a_3, a_2^{-1}a_1^{-1} \longrightarrow a_1^{-1}a_2^{-1}a_3, a_2^{-1}a_1 \longrightarrow a_1a_2^{-1}a_3^{-1}, a_2a_1^{-1} \longrightarrow a_1^{-1}a_2a_3^{-1}, a_3^{\delta}a_2^{\delta'} \longrightarrow a_2^{\delta'}a_3^{\delta}, a_3^{\delta}a_1^{\delta'} \longrightarrow a_1^{\delta'}a_3^{\delta} \mid \delta, \delta' \in \{1, -1\}\}$. Then for $w \equiv a_1^2a_2$, $v \equiv a_1a_2$ and $\tilde{v} \equiv a_1a_3$ we get $u \equiv a_1a_3^{-1}$ and $\tilde{v} \circ u = a_1a_3 \circ a_1a_3^{-1} \equiv a_1^2 \prec w$.

Still for groups with convergent PCP-presentations a similar stability property holds for left multiples.

Lemma 6

Let $\mathcal{G}$ be a polycyclic group with a convergent PCP-presentation, $w, v, \tilde{v} \in \mathcal{G}$ with $w \geq_{\text{tup}} v$ 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 $u = w \circ \mathsf{inv}(v)$.

Proof :

Let a_d be the distinguishing letter between v and $\tilde{v}$, i.e., $v \equiv xa_d^{v_d}y_v$, $\tilde{v} \equiv xa_d^{\tilde{v}_d}y_{\tilde{v}}$ with $x \in \mathsf{ORD}(\Sigma\backslash\Sigma_d)$, $y_v, y_{\tilde{v}} \in \mathsf{ORD}(\Sigma_{d+1})$ and $v_d >_{\mathbf{Z}} \tilde{v}_d$. Then for $u \equiv a_1^{u_1} \ldots a_n^{u_n}$ we get $u \circ v = a_1^{u_1} \ldots a_n^{u_n} \circ xa_d^{v_d}y_v = a_1^{u_1} \ldots a_{d-1}^{u_{d-1}} \circ x'a_d^{u_d+v_d+z_1}y_v{}' = x'' \circ a_d^{u_d+v_d+z_2} \circ y_v''$ with $x', x'' \in \mathsf{ORD}(\Sigma\backslash\Sigma_d)$, $y_v{}', y_v'' \in \mathsf{ORD}(\Sigma_{d+1})$ 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, $w \geq_{\text{tup}} v$ gives us, for the exponent w_d of the letter a_d in w, $w_d \geq_{\mathbf{Z}} v_d$, $\mathsf{sgn}(w_d) = \mathsf{sgn}(v_d)$ and $u_d + v_d + z_2 = w_d$ or $(u_d + v_d + z_2)$ mod $m_d = w_d$ in case a_d is bounded by m_d. To show that $w \succ u \circ \tilde{v}$ we can proceed as in lemma 5.

q.e.d.

Let us close this section by summarizing Sims' notions for presenting polycyclic groups as given in chapter 9 of [Si94]. Let

$$\mathcal{G} = \mathcal{G}_1 \geq \mathcal{G}_2 \geq \ldots \geq \mathcal{G}_{n+1} = \{\lambda\}$$

be a polycyclic series for $\mathcal{G}$. For $1 \leq i \leq n$ let a_i be an element of $\mathcal{G}_i$ whose image in $\mathcal{G}_i/\mathcal{G}_{i+1}$ generates that group. The letters $a_1, \ldots, a_n$ are called a **polycyclic generating sequence** and we have $\mathcal{G}_i = \langle a_i, \ldots, a_n \rangle$, i.e., $\mathcal{G}_i$ is the subgroup of $\mathcal{G}$ generated by $a_i, \ldots, a_n$. Further let $I = \{i \mid \mathcal{G}_i/\mathcal{G}_{i+1} \text{ is finite}\}$ and for $i \in I$ set $m_i = |\mathcal{G}_i : \mathcal{G}_{i+1}|$. It is assumed that the generating sequence is not redundant in the sense that no a_i is in $\mathcal{G}_{i+1}$. Every element of $\mathcal{G}$ can be expressed in the form $a_1^{i_1} \ldots a_n^{i_n}$, where $i_1, \ldots, i_n \in \mathbf{Z}$, and such a presentation is called a **collected word**, if $0 \leq i_j < m_j$ for $j \in I$. Now $\mathcal{G}$ gives rise to a unique presentation called the **standard polycyclic presentation** with respect to the letters $a_1, \ldots, a_n$, namely

$$\begin{array}{lcll}
a_j a_i & = & a_i a_{i+1}^{\alpha_{ij(i+1)}} \ldots a_n^{\alpha_{ijn}}, & j > i, \\
a_j^{-1} a_i & = & a_i a_{i+1}^{\beta_{ij(i+1)}} \ldots a_n^{\beta_{ijn}}, & j > i,\ j \notin I, \\
a_j a_i^{-1} & = & a_i^{-1} a_{i+1}^{\gamma_{ij(i+1)}} \ldots a_n^{\gamma_{ijn}}, & j > i,\ i \notin I, \\
a_j a_i^{-1} & = & a_i^{-1} a_{i+1}^{\delta_{ij(i+1)}} \ldots a_n^{\delta_{ijn}}, & j > i,\ i, j \notin I, \\
a_i^{m_i} & = & a_{i+1}^{\mu_{i(i+1)}} \ldots a_n^{\mu_{in}} & i \in I, \\
a_i^{-1} & = & a_i^{m_i - 1} a_{i+1}^{\nu_{i(i+1)}} \ldots a_n^{\nu_{in}} & i \in I, \\
a_i a_i^{-1} & = & \lambda, & i \notin I, \\
a_i^{-1} a_i & = & \lambda, & i \notin I,
\end{array}$$

where the right sides are collected words. Every presentation which has this form defines a polycyclic group, but there might be a_i such that $|\mathcal{G}_i : \mathcal{G}_{i+1}| = m$ although there is no relation of the form $a_i^m = \ldots$ or only a relation of the form $a_i^n = \ldots$ with $n > m$. If this is not true, the presentation is called **consistent**, which then is a synonym for confluent.

The relations of such a presentation can be interpreted as rewriting rules over the alphabet $\{a_1, \ldots, a_n\}$ with respect to the syllable ordering - here called wreath ordering - induced by the precedence $a_1^{-1} \succ a_1 \succ \ldots \succ a_n^{-1} \succ a_n$. Then a consistent polycyclic presentation gives rise to a convergent PCP presentation.

3 Solving the Submodule Problem in Polycyclic Group Rings

In [Si94] Sims gives the following discussion for handling finitely generated right modules over the integral group ring of any polycyclic group $\mathcal{G}$, which is based on the work of Baumslag, Cannonito and Miller [BaCaMi81].

Let $a_1, \ldots, a_n$ be a polycyclic generating sequence for $\mathcal{G}$ together with a consistent polycyclic presentation for $\mathcal{G}$.
In case $n = 1$, $\mathcal{G}$ is cyclic and this case is well known.
Hence let us assume that $n > 1$ and set $\mathcal{H} = \langle a_2, \ldots, a_n \rangle$. Then $\mathcal{H}$ is normal in $\mathcal{G}$ and $\mathcal{G}/\mathcal{H}$ is a cyclic group generated by the image of a_1. By induction on n we may assume that we know how to describe submodules in the modules $\mathbf{Z}[\mathcal{H}]^s$, $s \in \mathbf{N}$. In order to show how this information can be lifted to $\mathbf{Z}[\mathcal{G}]^s$ we have to distinguish whether $1 \in I$ or not. In the following we abbreviate a_1 by a.
First suppose $1 \in I$, i.e., $\mathcal{G}/\mathcal{H}$ is finite and w.l.o.g. let $m = |\mathcal{G} : \mathcal{H}|$. Then $\mathbf{Z}[\mathcal{G}]^s$ is isomorphic (as a $\mathbf{Z}[\mathcal{H}]$-module) to $\mathbf{Z}[\mathcal{H}]^{s \cdot m}$, as if $b_1, \ldots, b_s$ is a $\mathbf{Z}[\mathcal{G}]$-basis for $\mathbf{Z}[\mathcal{G}]^s$, then the set $\{b_i a^j \mid 1 \leq i \leq s, 0 \leq j < m\}$ is a $\mathbf{Z}[\mathcal{H}]$-basis of $\mathbf{Z}[\mathcal{G}]^s$. Now, a $\mathbf{Z}[\mathcal{H}]$-submodule M of $\mathbf{Z}[\mathcal{G}]^s$ is a $\mathbf{Z}[\mathcal{G}]$-submodule if and only if M is closed under multiplication by a from the right. If $T \subset \mathbf{Z}[\mathcal{G}]^s$ is a generating set for M as a $\mathbf{Z}[\mathcal{H}]$-module, then M is closed under multiplication by a if and only if $f * a$ is in M for all $f \in T$. Suppose the products $f * a$ do belong to M. A typical element g of M has the form $\sum_{i=1}^{r} \alpha_i \cdot f_i * h_i$, $\alpha_i \in \mathbf{Z}$,$f_i \in T$, $h_i \in \mathcal{H}$. Then $g * a = \sum_{i=1}^{r} \alpha_i \cdot f_i * (h_i \circ a) = \sum_{i=1}^{r} \alpha_i \cdot f_i * (a \circ a^{-1} \circ h_i \circ a)$, and since $a^{-1} \circ h_i \circ a \in \mathcal{H}$ and each $f_i * a \in M$, we get $g * a \in M$. If some $f * a$ is not in M, then we can add it to T and recompute the $\mathbf{Z}[\mathcal{H}]$-submodule generated by T. Because the ascending chain condition holds, this process will terminate[5]. Since we can describe submodules of $\mathbf{Z}[\mathcal{H}]^{sm}$ effectively,

[5] This can also be seen, since for m we have $a^m \in \mathcal{H}$.

we can describe submodules of $\mathbf{Z}[\mathcal{G}]^s$.
Now let us suppose that $\mathcal{G}/\mathcal{H}$ is infinite. Then $\mathbf{Z}[\mathcal{G}]^s$ is still a free $\mathbf{Z}[\mathcal{H}]$-module, but with an infinite basis $U = \{b_i a^j \mid 1 \leq i \leq s, j \in \mathbf{Z}\}$. Any element $g \in \mathcal{G}$ can be written uniquely in the form $a^j h$, where $h \in \mathcal{H}$. In this way, $b_i \circ g$ can be expressed as $b_i a^j h$. Thus elements of $\mathbf{Z}[\mathcal{G}]^s$ can easily be described as $\mathbf{Z}[\mathcal{H}]$-linear combinations of the elements of U. However, it is also useful to write g in the form la^j where $l = a^j \circ h \circ a^{-j} \in \mathcal{H}$. When this is done, every element of $\mathbf{Z}[\mathcal{G}]^s$ can be described as

$$c_p * a^p + c_{p-1} * a^{p-1} + \ldots + c_q * a^q$$

where $p, q \in \mathbf{Z}$, $p \geq q$ and $c_i \in \mathbf{Z}[\mathcal{H}]^s$, $p \leq i \leq q$. In case $q \geq 0$ the element is called a **polynomial** and p is called the **degree** and c_0 the **constant term** of the polynomial.
Let T be a finite subset of $\mathbf{Z}[\mathcal{G}]^s$ and let M be the $\mathbf{Z}[\mathcal{G}]$-submodule generated by T. Since a is a unit in $\mathbf{Z}[\mathcal{G}]$ we can multiply each element in T by some power of a such that the resulting element is a polynomial, i.e., it has positive exponents in a only, and additionally we assume it has nonzero constant term c_0. Given $k \in \mathbf{N}$, let M_k be the set of polynomials in M with degree at most k, and let C_k be the set of coefficients of the term a^k occurring in the polynomials in M_k. Let $\sum_{i=0}^{k} c_i * a^i \in M_k$ and $h \in \mathcal{H}$. Then since also $l = a^{-k} \circ h \circ a^k \in \mathcal{H}$, we get $\sum_{i=0}^{k} c_i * a^i l = \sum_{i=0}^{k} c_i * (a^i \circ a^{-k} \circ h \circ a^k) = \sum_{i=0}^{k} c_i * (a^{i-k} \circ h \circ a^k) = \sum_{i=0}^{k} c_i * (a^{i-k} \circ h \circ a^{k-i}) * a^i = \sum_{i=0}^{k} c_i * h_i a^i$ with $h_i \in \mathcal{H}$. Therefore, $c_k * h \in C_k$ for $h \in \mathcal{H}$, i.e., C_k is a $\mathbf{Z}[\mathcal{H}]$-submodule of $\mathbf{Z}[\mathcal{H}]^s$. Furthermore, $C_k \subseteq C_{k+1}$ holds.
Let d be the maximal degree of the polynomials in T (assuming that T has been modified to contain only polynomials as described above). Then one can show that $C_k = C_d$ for $k \geq d$. Moreover, knowing M_d alone allows to solve the membership problem in M, as we can multiply every element $g \in \mathbf{Z}[\mathcal{G}]$ by a power of a in order to turn it into a polynomial, say of degree k. Then in case $k > d$ we check whether $c_k \in C_d$. If not we are done, since then $g \notin M$. Else there exists an element $h \in M_d$ with leading coefficient c_k and we can reduce g by subtracting ha^{k-d}. Thus we may assume that $k \leq d$ which leaves us with the decision whether $g \in M_d$. How do we get to know M_d? Let A be the $\mathbf{Z}[\mathcal{H}]$-module generated by T, B respectively C the elements in A with degree at most $d-1$ respectively constant term 0. Then we have $A \subseteq M_d$ and, moreover, $A = M_d$ if and only if $Ba \subseteq A$ and $Ca^{-1} \subseteq A$.

Sims outlines how these membership problems can be treated using matrix methods. In example 8.3. he states how to compute such a basis in the group ring of the free nilpotent group (see example 1 for a presentation of this group on the letters a_1, a_2, and a_3). Then for the right ideal M of $\mathbf{Z}[\mathcal{G}]$ generated by the set $T = \{a_1 + a_2, a_1 + a_3\}$, the membership problem can be solved using the $\mathbf{Z}[\mathcal{H}]$-basis $\{a_1 + 1, a_2 - 1, a_2^{-1} - 1, a_3 - 1, a_3^{-1} - 1\}$ for M_1. In the next section we will see that a Gröbner basis in our sense will contain one more polynomial, namely $a_1^{-1} + 1$.

Notice that the constructive discussion cited above states how a solution for the membership problem for modules in $\mathbf{Z}[\mathcal{G}]^s$ can be given using a solution for the membership problem for $\mathbf{Z}[\mathcal{H}]^s$. Assuming that the solution is given by reduction methods – say given M, a $\mathbf{Z}[\mathcal{H}]$-module, we can compute a basis B of the module such that g in M iff $g \overset{*}{\Longrightarrow}_B 0$ – we can the lift reduction similar to the case of polynomial rings over reduction rings. However, since elements of $\mathbf{Z}[\mathcal{G}]^s$ in order to decide membership have to be turned into polynomials, i.e., occurrences of a with negative exponents have to be made positive by multiplication with an appropriate power of a, for such a lifted reduction the translation lemma no longer holds.

Example 2
Let $\mathbf{Z}[\mathcal{G}]$ be a group ring with $\mathcal{G}$ presented by $\Sigma = \{a, a^{-1}\}$ and $T = \{aa^{-1} \longrightarrow \lambda, a^{-1}a \longrightarrow \lambda\}$. Further let $p = 3 \cdot a^2 + 1$, then p is a basis of the right $\mathbf{Z}[\mathcal{G}]$-module as described by Sims. The polynomials $f = -2 \cdot a$ and $g = a + a^{-1}$ both do not belong to this right module. Now we have $g - f = 3 \cdot a + a^{-1}$ and we find that the "polynomial" $(g - f) * a = 3 \cdot a^2 + 1$ is "reducible" to 0 using p, while neither of the "polynomials" f nor $g * a$ are reducible with respect to p.
Hence we have the situation that g and f are congruent with respect to the $\mathbf{Z}[\mathcal{G}]$-module generated by p, but do not have the same "normal form". $\diamond$

Hence we cannot expect the resulting bases to be Gröbner bases in the strong sense that every element in $\mathbf{Z}[\mathcal{G}]^s$ has a unique normal form with respect to the module. In the following sections we show how for special cases Gröbner bases can be computed when using other definitions of reduction.

Let us close this section by sketching how Sims introduces Gröbner bases for the special case of finitely generated free Abelian groups in section 10.7 of [Si94]. The group ring then is also called the ring of **Laurent polynomials**.

Let the free Abelian group $\mathcal{G}$ be generated by $\{a_1, a_1^{-1}, \ldots, a_n, a_n^{-1}\}$ and let the Laurent monomials $U = \{a_1^{\alpha_1} \ldots a_n^{\alpha_n} \mid \alpha_i \in \mathbf{Z}\}$, be ordered by a reverse lexicographic ordering (i.e. a lexicographic ordering comparing from the right to the left) in which the exponents are compared with respect to the ordering $0 < 1 < -1 < 2 < -2 < \ldots$[6]. The elements in U represent the group elements. Two elements $a_1^{\alpha_1} \ldots a_n^{\alpha_n}$ and $a_1^{\beta_1} \ldots a_n^{\beta_n}$ are called aligned, if $\alpha_i \cdot \beta_i \geq 0$ for all $1 \leq i \leq n$. Then, although the ordering on the monomials is not consistent with multiplication, one can specify certain multiples for which multiplication is stable which is done in corollary 7.6.

> Suppose that u, v, and $x \in U$ such that $u \succ v$. If x and u are aligned, then $xu \succ xv$.

This corollary is in fact comparable to the lemmata 5 and 6 specialized for free Abelian groups. The property ensures that multiplying a polynomial with a monomial whose term is aligned to the head term leaves the head term in head position. Hence defining reduction based on this property remains stable, but in general will not capture the ideal congruence. This can be repaired because of theorem 7.9.

> Let f be a nonzero element of $\mathbf{Z}[\mathcal{G}]$. There is a unique subset $\mathcal{T}(f)$ of $\mathbf{Z}[\mathcal{G}]$ such that the following hold:
>
> 1. Each element of $\mathcal{T}(f)$ has the form $y * f$ with $y \in U$.
> 2. If x is in U, then $x * f = y * g$ for a unique pair (y, g) such that g is in $\mathcal{T}(f)$, y is in U, and y is aligned with the leading monomial of g.
>
> The cardinality of $\mathcal{T}(f)$ is at most 2^m.

[6] E.g. we get $a_1 \prec a_1^{-1} \prec a_1^3 a_2 \prec a_1 a_2^2 \prec a_1^{-1} a_2^2 \prec a_1 a_2^{-2}$.

Then for a finite set $T \subset \mathbf{Z}[\mathcal{G}]$ one can define the symmetrized set $\mathcal{S}(T)$ as the union of the sets $\mathcal{T}(f)$, $f \in T$, additionally assuming that all polynomials have positive leading coefficient. This in some sense corresponds to the fact that in the above proof of the Baumslag, Cannonito, Miller approach additionally to the condition $Ba \subseteq A$ one also has to ensure $Ca^{-1} \subseteq A$. Symmetrized sets can be computed as follows:

Function Symm

Given: A finite subset T of $\mathbf{Z}[\mathcal{G}]$.
Find: $\mathcal{S}(T)$, the symmetrized set for T.

```
Begin
    $\mathcal{S} := T - \{0\}$;
    For $i := m$ down to 1 do begin
        $\mathcal{T} := \emptyset$;
        For $f$ in $\mathcal{S}$ do begin
            Let $u$ be the leading monomial of $f$;
            Let $\alpha$ and $\beta$ be the algebraically largest and smallest exponents, respectively, on
                $a_i$ occurring in any monomial $v$ of $f$ for which the exponents on $a_{i+1}, \ldots, a_n$
                in $v$ agree with the corresponding exponents in $u_i$;
            If $\alpha = \beta$ then $\mathcal{T} := \mathcal{T} \cup \{a_i^{-\alpha} * f\}$
            Else begin
                Let $\gamma$ be the greatest integer in[7]$(\alpha + \beta - 1)/2$;
                $\mathcal{T} := \mathcal{T} \cup \{a_i^{-\gamma} * f, a_i^{-\gamma-1} * f\}$
            End
        End;
        $\mathcal{S} := \mathcal{T}$
    End;
    For $f$ in $\mathcal{S}$ do
        If $f$ has negative leading coefficient then replace $f$ by $-f$ in $\mathcal{S}$;
    $\mathcal{S}(T) := \mathcal{S}$
End
```

For example the symmetrized set[8] of the polynomial $g = 2 \cdot a_1^{-2}a_2^3 - 4 \cdot a_1^2a_2^3 - a_1a_2^2 + a_1a_2$ is $\mathcal{S}(g) = \{2 \cdot a_1^{-2}a_2^2 - 4 \cdot a_1^2a_2^2 - a_1a_2 + a_1, 4 \cdot a_1^3a_2^2 - 2 \cdot a_1^{-1}a_2^2 + a_1^2a_2 - a_1^2, a_2^{-1} + 2 \cdot a_1^{-3}a_2 - 4 \cdot a_1a_2 - 1\}$.

Now reduction using *sets which are their own symmetrized sets* is specified by the following procedure:

Function Reduce

Given: A finite subset T of $\mathbf{Z}[\mathcal{G}]$ which is its own symmetrized set.
A non-zero polynomial f in $\mathbf{Z}[\mathcal{G}]$.
Find: An element g of $I + f$ is returned, where I is the ideal of $\mathbf{Z}[\mathcal{G}]$ generated by T. The element g is irreducible with respect to the set of products $y * h$, where h is

[7] I.e. $\gamma = \lfloor (\alpha + \beta - 1)/2 \rfloor$.

[8] see [Si94] page 503 for the concrete computation.

in T, y is in U, and y is aligned with the leading monomial of h.

```
Begin
    $i := 1$; $g := f$; % At all times $g = c_1 \cdot u_1 + \ldots + c_s \cdot u_s$. If $g = 0$ then $s = 0$.
    While $i \leq s$ do
        If there is an element $h$ in $T$ such that the leading term $b \cdot v$ of $h$ satisfies $b \leq_{\mathbf{Z}} c_i$
                and $u_i = y \circ v$, where $y$ is in $U$ and $y$ and $v$ are aligned, then begin
            Let $c_i = q \cdot b + r$, where $q$ and $r$ are integers and $0 \leq r < b$;
            $g := g - q \cdot y * h$; % Recompute $s$ and the terms $c_j \cdot u_j$ with $j \geq i$.
        End
        Else $i := i + 1$;
End
```

Hence reduction of a polynomial p at a monomial $c{\cdot}t$ by a polynomial f can be defined in case there exists u in U such that $\mathsf{HT}(f)$ and u are aligned, $t = u \circ \mathsf{HT}(f)$, and $b = \mathsf{HC}(f) \leq_{\mathbf{Z}} c$. Then for $c = q \cdot b + r$, where q and r are integers and $0 \leq r < b$ we get $p \longrightarrow_f p - q \cdot u * f$. Now critical pairs can be specified with respect to this reduction:

> Let f and g be elements of $\mathcal{S}(T)$ with leading term u and v, respectively, and assume that u and v are aligned. Let $w = \mathsf{LCM}(u, v)$, $x = w \circ \mathsf{inv}(u)$, and $y = w \circ \mathsf{inv}(v)$. The leading monomial of $x * f$ and $y * g$ is w. Suppose $x * f \prec y * g$. Then $(x * f, y * g)$ is a critical pair.

For a critical pair (f, g) let $\mathsf{HC}(g) \geq \mathsf{HC}(f)$ and $\mathsf{HC}(g) = q \cdot \mathsf{HC}(f) + r$ where q and r are integers and $0 \leq r < b$. Then we set $t(f, g) = g - q \cdot f$.

Now Gröbner bases can be computed as follows:

Function GRÖBNER

Given: A finite subset T of $\mathbf{Z}[\mathcal{G}]$.
Find: A Gröbner basis for the ideal of $\mathbf{Z}[\mathcal{G}]$ generated by T.

```
Begin
    $B :=$ SYMM$(T)$;
    Let $C$ be the set of critical pairs obtained from $B$;
    While $C$ is not empty do begin
        Remove a critical pair $(f, g)$ from $C$;
        $h :=$ REDUCE$(B, t(f, g))$;
        If $h \neq 0$ then begin
            $S :=$SYMM$(\{h\})$;
            Form all critical pairs obtainable from an element of $S$ and an element of $B$
                and add these pairs to $C$;
            $B := B \cup S$
        End
    End
End
```

The output of this function will be a set which is both – a symmetrized set and a Gröbner basis.

4 On the Relations between Gröbner bases and the Subgroup Problem

In this section we want to demonstrate the connection between Gröbner bases in certain group rings and solutions of the subgroup problem by rewriting techniques.

Definition 8
Given a subset U of a group $\mathcal{G}$, let $\langle U \rangle = \{u_1 \circ \ldots \circ u_n \mid n \in \mathbf{N}, u_i \in U \cup U^{-1}\}$ denote the subgroup generated by U. The **generalized word problem** or **subgroup problem** is then to determine, given $w \in \mathcal{G}$, whether $w \in \langle U \rangle$. $\diamond$

The following theorem links this group theoretic problem to right respectively left ideals in the respective group ring.

Theorem 2 (see 5.1.2 in [Re95])
Let U be a finite subset of $\mathcal{G}$ and $\mathbf{K}[\mathcal{G}]$ the group ring corresponding to $\mathcal{G}$. Further let $P_U = \{s-1 \mid s \in U\}$ be a set of polynomials associated to U. Then the following statements are equivalent:

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

Proof :
$1 \Longrightarrow 2$: Let $w = u_1 \circ \ldots \circ u_k \in \langle U \rangle$, i.e., $u_1, \ldots, u_k \in U \cup \{\mathsf{inv}(u) | u \in U\}$. We show $w - 1 \in \mathsf{ideal}_r(P_U)$ by induction on k. In the base case $k = 0$ there is nothing to show, as $w = \lambda \in \langle U \rangle$ and $0 \in \mathsf{ideal}_r(P_U)$. Hence, suppose $w = u_1 \circ \ldots \circ u_{k+1}$ and $u_1 \circ \ldots \circ u_k - 1 \in \mathsf{ideal}_r(P_U)$. Then $(u_1 \circ \ldots \circ u_k - 1) * u_{k+1} \in \mathsf{ideal}_r(P_U)$ and, since $u_{k+1} - 1 \in \mathsf{ideal}_r(P_U)$[9], we get $(u_1 \circ \ldots \circ u_k - 1) * u_{k+1} + (u_{k+1} - 1) = w - 1 \in \mathsf{ideal}_r(P_U)$.

$2 \Longrightarrow 1$: We have to show that $w - 1 \in \mathsf{ideal}_r(P_U)$ implies $w \in \langle U \rangle$. We know $w - 1 = \sum_{j=1}^{n} \alpha_j \cdot (u_j - 1) * x_j$, where $\alpha_j \in \mathbf{K}^*$, $u_j \in U \cup \{\mathsf{inv}(u) | u \in U\}$, $x_j \in \mathcal{G}$. Therefore, by showing the following stronger result we are done: A representation $w - 1 = \sum_{j=1}^{m} p_j$ where $p_j = \alpha_j \cdot (w_j - w'_j)$, $\alpha_j \in \mathbf{K}^*$,$w_j \neq w'_j$ and $w_j \circ \mathsf{inv}(w'_j) \in \langle U \rangle$ implies $w \in \langle U \rangle$. Now, let $w - 1 = \sum_{j=1}^{m} p_j$ be such a representation and $\succeq$ be an arbitrary total well-founded ordering on $\mathcal{G}$. Depending on this representation and $\succeq$ we define $t = \max\{w_j, w'_j \mid j = 1, \ldots m\}$ and K is the number of polynomials p_j containing t as a term. We will show our claim by induction on (m, K), where $(m', K') < (m, K)$ if and only if $m' < m$ or ($m' = m$ and $K' < K$). In case $m = 0$, $w - 1 = 0$ implies $w = 1$ and hence $w \in \langle U \rangle$. Thus let us assume

[9] We either have $u_{k+1} - 1 \in P_U$ or $\mathsf{inv}(u_{k+1}) \in U$, i.e., $(\mathsf{inv}(u_{k+1}) - 1) * u_{k+1} = u_{k+1} - 1 \in \mathsf{ideal}(P_U)$.

$m > 0$.

In case $K = 1$, let p_k be the polynomial containing t. As we either have $p_k = \alpha_k \cdot (t - w'_k)$ or $p_k = \alpha_k \cdot (w_k - t)$, where $\alpha_k \in \{1, -1\}$, without loss of generality we can assume $p_k = t - w'_k$. Using p_k we can decrease m by subtracting p_k from $w - 1$ giving us $w'_k - 1 = \sum_{j=1, j\neq k}^{m} p_j$. Since $t \circ \mathsf{inv}(w'_k) \in \langle U \rangle$ and our induction hypothesis yields $w'_k \in \langle U \rangle$, we can conclude $w = t = (t \circ \mathsf{inv}(w'_k)) \circ w'_k \in \langle U \rangle$.

In case $K > 1$ there are two polynomials p_k, p_l in the corresponding representation and without loss of generality we can assume $p_k = \alpha_k \cdot (t - w'_k)$ and $p_l = \alpha_l \cdot (t - w'_l)$. If then $w'_k = w'_l$ we can immediately decrease m by substituting the occurrence of $p_k + p_l$ by $(\alpha_k + \alpha_l) \cdot p_l$. Otherwise we can proceed as follows:

$$\begin{array}{rcl} p_k + p_l & = & p_k \underbrace{- \alpha_k \cdot \alpha_l^{-1} \cdot p_l + \alpha_k \cdot \alpha_l^{-1} \cdot p_l}_{=0} + p_l \\ & = & \underbrace{(-\alpha_k \cdot w'_k + \alpha_k \cdot w'_l)}_{p'_k} + (\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l \end{array}$$

where $p'_k = \alpha_k \cdot (w'_l - w'_k)$, $w'_k \neq w'_l$ and $w'_k \circ \mathsf{inv}(w'_l) \in \langle U \rangle$, since $w'_k \circ \mathsf{inv}(t), t \circ \mathsf{inv}(w'_l) \in \langle U \rangle$ and $w'_k \circ \mathsf{inv}(w'_l) = w'_k \circ \mathsf{inv}(t) \circ t \circ \mathsf{inv}(w'_l)$. In case $\alpha_k \cdot \alpha_l^{-1} + 1 = 0$, i.e., $\alpha_k = -\alpha_l$, m is decreased. On the other hand p'_k does not contain t, i.e., if m is not decreased K is.

$1 \Longrightarrow 3$ and $3 \Longrightarrow 1$ can be shown analogously.

q.e.d.

As in Buchberger's case on can try to describe these right and left ideals using appropriate definitions of reduction. Then, in case the group ring allows to compute finite Gröbner bases for finitely generated right respectively left ideals, the subgroup problem can be solved using reduction methods. In [Re95] we have studied how such a solution in the free group ring compares to the concept of Nielsen reduction and showed that in fact the appropriate Gröbner bases[10] give rise to so called Nielsen reduced bases of the respective subgroups. Here in the setting of nilpotent and polycyclic groups we want to point out connections to Wißmann's approach given in [Wi89].

The subgroup problem can be described using rewriting techniques as follows: Let U be a generating set of a subgroup of a group presented by (Σ, T). We assume that U is closed under inverses, i.e., if $u \in U$ so is $\mathsf{inv}(u)$. Then we can define a right congruence on Σ^* by $w \sim_U v$ if and only if there exists $x \in \langle U \rangle$ such that $w \overset{*}{\longleftrightarrow}_T xv$. Now the key idea is to express this right congruence by a restricted reduction relation. This can for example be done by introducing a reduction $w \Longrightarrow_U v$ for $w, v \in \mathcal{G}$ if and only if there exists $u \in U \cup U^{-1}$ such that $v = u \circ w$ and $w \succ v$. Moreover, since $\langle U \rangle$ is the coset of λ, a λ-confluent basis B of $\langle U \rangle$ for this reduction then is sufficient to decide the subgroup problem.

We now want to demonstrate how strong reduction[11] in group rings is related to Wißmann's reduction. Strong reduction in a group ring is defined as follows: For $p, f \in \mathbf{K}[\mathcal{G}]$, let $\mathsf{HT}(f * w) = t$ for some $t \in \mathsf{T}(p)$, $w \in \mathcal{G}$, then $p \longrightarrow^{s}_{f} p - \alpha \cdot f * w = q$, where $\alpha \in \mathbf{K}$ such that $t \notin \mathsf{T}(q)$. First we take a closer look at the outcome of using only restricted polynomials

[10] Prefix reduction was used to treat right ideals in free group rings.

[11] A thorough study of the properties of strong reduction can be found in [Re95].

of the form $x - y$ for reduction where x, y in $\mathcal{G}$. Then reducing a polynomial of the form $w \in \mathcal{G}$ by such a polynomial gives us either $w \longrightarrow^{s}_{x-y} y \circ (\mathsf{inv}(x) \circ w)$ in case $w = x \circ \mathsf{inv}(x) \circ w \succ y \circ \mathsf{inv}(x) \circ w$ or $w \longrightarrow^{s}_{x-y} x \circ (\mathsf{inv}(y) \circ w)$ in case $w = y \circ \mathsf{inv}(y) \circ w \succ x \circ \mathsf{inv}(y) \circ w$. Thus such a reduction step corresponds directly to a step or the form $w \Longrightarrow_{y \circ \mathsf{inv}(x)} y \circ \mathsf{inv}(x) \circ w$ respectively $w \Longrightarrow_{x \circ \mathsf{inv}(y)} x \circ \mathsf{inv}(y) \circ w$ in Wißmann's context. On the other hand, a reduction step $w \Longrightarrow_{u} u \circ w$ can be restated as strongly reducing a polynomial w by a polynomial $u - 1$ and, since we know that $w \succ u \circ w$, we get $w \longrightarrow^{s}_{u-1} u \circ w$.

More general we can show that the right ideal generated by a set of polynomials $P_U = \{u - 1 \mid u \in U\}$ has a Gröbner basis of the form $G = \{x - y \mid x, y \in \mathcal{G}\}$ and the set $B = \{x \circ \mathsf{inv}(y), y \circ \mathsf{inv}(x) \mid x - y \in G\}$ then is a confluent basis with respect to $\Longrightarrow$-reduction for the subgroup in Wißmann's sense. The proof is done using the following lemmata. The first one stresses that for a polynomial in $\mathsf{ideal}_r(P_U)$ there exist special representations in terms of polynomials containing only two monomials and involving only terms of the polynomial itself.

Lemma 7
Let g be a polynomial in the non-trivial right ideal generated by $P_U = \{u - 1 \mid u \in U\}$. Then g has a representation of the form

$$g = \sum_{i=1}^{n} \alpha_i \cdot (x_i - y_i)$$

where $\alpha_i \in \mathbf{K}$, $x_i, y_i \in \mathsf{T}(g)$, $x_i - y_i \in \mathsf{ideal}_r(P_U)$.

Proof :
Remember that $g \in \mathsf{ideal}_r(P_U) \backslash \{0\}$ implies $g = \sum_{j=1}^{m} \beta_j \cdot f_j * w_j$ where $\alpha_j \in \mathbf{K}$, $f_j \in P_U$, and $w_j \in \mathcal{G}$. Hence we show our claim by induction on m. In the base case $m = 1$ we find $g = \beta \cdot (u \circ w - w)$, and as $u \circ w \neq w$ for $u \neq \lambda$ we are done. Now let us assume $m > 1$ and

$$g = \underbrace{\sum_{j=1}^{m-1} \beta_j \cdot f_j * w_j}_{h} + \beta \cdot (u \circ w - w).$$

Then by our induction hypothesis we know $h = \sum_{i=1}^{n} \alpha_i \cdot (x_i - y_i)$ where $\alpha_i \in \mathbf{K}$, $x_i, y_i \in \mathsf{T}(h)$, $x_i - y_i \in \mathsf{ideal}_r(P_U)$. We have to distinguish the following cases: If $u \circ w, w \not\in \mathsf{T}(h)$ we are done at once. In case $u \circ w \in \mathsf{T}(h)$ and $w \not\in \mathsf{T}(h)$ (the case $u \circ w \not\in \mathsf{T}(h)$ and $w \in \mathsf{T}(h)$ is similar) without loss of generality let $x = u \circ w = x_j$ for $1 \leq j \leq s$. Then in case $\sum_{j=1}^{s} \beta_j \neq -\beta$ the representation $g = \sum_{i=1}^{n} \alpha_i \cdot (x_i - y_i) + \beta \cdot (u \circ w - w)$ already has the desired form. Else we show that such a representation can be achieved by induction on the number $s + 1$ of terms x occurring in this representation. In the base case $s = 1$ we get $\alpha_1 = -\beta$ and hence

$$\begin{aligned} g &= \sum_{i=2}^{n} \alpha_i \cdot (x_i - y_i) + \alpha_1 \cdot (x - y_1) + \beta \cdot (x - w) \\ &= \sum_{i=2}^{n} \alpha_i \cdot (x_i - y_i) - \beta \cdot (x - y_1) + \beta \cdot (x - w) \end{aligned}$$

$$= \sum_{i=2}^{n} \alpha_i \cdot (x_i - y_i) + \beta \cdot (y_1 - w)$$

and we are done. Now let $s > 1$ and

$$\begin{aligned}
g &= \sum_{i=s+1}^{n} \alpha_i \cdot (x_i - y_i) + \sum_{i=1}^{s-1} \alpha_i \cdot (x - y_i) + \alpha_s \cdot (x - y_s) + \beta \cdot (x - w) \\
&= \sum_{i=s+1}^{n} \alpha_i \cdot (x_i - y_i) + \sum_{i=1}^{s-1} \alpha_i \cdot (x - y_i) + (\alpha_s + \beta) \cdot (x - y_s) - \beta \cdot (x - y_s) + \beta \cdot (x - w) \\
&= \sum_{i=s+1}^{n} \alpha_i \cdot (x_i - y_i) + \sum_{i=1}^{s-1} \alpha_i \cdot (x - y_i) + (\alpha_s + \beta) \cdot (x - y_s) + \beta \cdot (y_s - w) \\
&= \sum_{i=s+1}^{n} \alpha_i \cdot (x_i - y_i) + \beta \cdot (y_s - w) + \sum_{i=1}^{s-1} \alpha_i \cdot (x - y_i) + (\alpha_s + \beta) \cdot (x - y_s)
\end{aligned}$$

and since x occurs at most s times in this finial representation, we can assume that g has a representation of the desired form. It remains to check the case where $u \circ w, w \in \mathsf{T}(h)$. Then we can proceed as in the previous case to first incorporate $u \circ w$ into the representation and later on do the same for w.

q.e.d.

Notice that in general for strong reduction $p \xrightarrow{\text{s}}_{q}$ and $q \xrightarrow{\text{s}}_{q_1} q_2$ need not imply $p \xrightarrow{\text{s}}_{\{q_1, q_2\}}$. Hence interreducing a strong Gröbner basis need not result in a strong Gröbner basis (see [Re95] for some examples in this context). Still in case q, q_1 and q_2 are related in a special way, we can "interreduce" a basis without losing the property of being a Gröbner basis, due to the following fact:

Lemma 8
Let p, q, q_1, q_2 be some polynomials in $\mathbf{K}[\mathcal{G}]$ such that $p \xrightarrow{\text{s}}_{q}$, $q \xrightarrow{\text{s}}_{q_1} q_2$, $q = \alpha \cdot q_1 + q_2$, $\alpha \in \mathbf{K}$ and $\mathsf{T}(q) = \mathsf{T}(q_1) \cup \mathsf{T}(q_2)$. Then we can conclude $p \xrightarrow{\text{s}}_{\{q_1, q_2\}}$.

Proof :
In case q reduces p at a term $t \in \mathsf{T}(p)$ we know that there exists an element u in $\mathcal{G}$ such that $\mathsf{HT}(q * u) = t$. Since $q = \alpha \cdot q_1 + q_2$ and $\mathsf{T}(q) = \mathsf{T}(q_1) \cup \mathsf{T}(q_2)$ only two cases are possible, namely $\mathsf{HT}(q_1 * u) = t$ or $\mathsf{HT}(q_2 * u) = t$, i.e., q_1 or q_2 can be used to strongly reduce p at t.

q.e.d.

Now remember that a set G is a strong Gröbner basis if and only if for all $g \in \mathsf{ideal}_r(G)$ we have $g \overset{*}{\longrightarrow}{}^{\text{s}}_{G} 0$, i.e., every $g \in \mathsf{ideal}_r(G) \backslash \{0\}$ is top-reducible using a polynomial in G. Suppose G contains polynomials q and q_1 as described in the lemma. Then for the set $G' = (G \backslash \{q\}) \cup \{q_2\}$ we know that $\mathsf{ideal}_r(G) = \mathsf{ideal}_r(G')$ and still every polynomial in this right ideal is top-reducible by a polynomial in G'. Hence G' is again a strong Gröbner basis.

Now it is straightforward to see that there exists a strong Gröbner basis of the right ideal generated by P_U of the desired form. Let us assume that G is an arbitrary strong Gröbner basis of $\mathsf{ideal}_r(P_U)$. Every polynomial g in G has a representation as described in lemma 7, say $g = \sum_{i=1}^{n_g} \alpha_i^{(g)} \cdot (x_i^{(g)} - y_i^{(g)})$. Then the set $G' = G \cup \{x_i^{(g)} - y_i^{(g)} \mid g = \sum_{i=1}^{n_g} \alpha_i^{(g)} \cdot (x_i^{(g)} - y_i^{(g)}), g \in G\}$ is a strong Gröbner basis which can be reduced to the set $\{x_i^{(g)} - y_i^{(g)} \mid g = \sum_{i=1}^{n_g} \alpha_i \cdot (x_i^{(g)} - y_i^{(g)}), g \in G\}$ which by our previous remark is also a strong Gröbner basis of the right ideal generated by P_U.

Hence if a group ring allows the computation of finite strong Gröbner bases for finitely generated right respectively left ideals, the subgroup problem of the corresponding group can be solved using rewriting methods. Additionally, since for strong reduction the translation lemma holds, unique representatives of the cosets then can be computed. As shown in [Re95], in special cases strong Gröbner bases can be computed using appropriate weakenings of strong reduction. For nilpotent groups presented by convergent PCNI-systems, quasi-commutative reduction as introduced in the next section is such a weakening. The following example[12] shall illustrate how in this case the subgroup problem is embedded. It shows that in this special case, due to the representation of the group elements by ordered group words and the use of the syllable ordering we can even more restrict the from of the polynomials occurring: For every letter a_i in Σ there are at most two polynomials in the reduced monic Gröbner basis and they are of the form $a_i^m \longrightarrow w$ respectively $a_i^{-1} \longrightarrow a_i^n z$ with $m, n \in \mathbf{N}$ and $w, z \in \mathsf{ORD}(\Sigma_{i+1})$.

Example 3
Let $\mathcal{G}$ be presented by the convergent reduced PCNI-system $\Sigma = \{a_1, a_1^{-1}, a_2, a_2^{-1}, a_3, a_3^{-1}, a_4, a_4^{-1}, a_5, a_5^{-1}\}$, $T = \{a_1^3 \longrightarrow a_4, a_2^3 \longrightarrow a_5, a_3^3 \longrightarrow a_4a_5, a_4^3 \longrightarrow \lambda, a_5^3 \longrightarrow \lambda, a_1^{-1} \longrightarrow a_1^2a_4^2, a_2^{-1} \longrightarrow a_2^2a_5^2, a_3^{-1} \longrightarrow a_3^2a_4^2a_5^2, a_4^{-1} \longrightarrow a_4^2, a_5^{-1} \longrightarrow a_5^2, a_2a_1 \longrightarrow a_1a_2a_4a_5^2, a_3a_1 \longrightarrow a_1a_3, a_4a_1 \longrightarrow a_1a_4, a_5a_1 \longrightarrow a_1a_5, a_3a_2 \longrightarrow a_2a_3a_4^2, a_4a_2 \longrightarrow a_2a_4, a_4a_3 \longrightarrow a_3a_4, a_5a_2 \longrightarrow a_2a_5, a_5a_3 \longrightarrow a_3a_5, a_5a_4 \longrightarrow a_4a_5\}$. Then we can compute a Gröbner basis with respect to quasi-commutative reduction of the right ideal generated by the set $\{a_1a_3a_5 - 1, a_2a_3 - 1, a_4a_5^2 - 1, a_5 - 1\}$ using the techniques which will be described in detail in the next section. We get that the set $\{a_1 - a_3^2a_4^2a_5, a_1^2 - a_3a_4a_5, a_2 - a_3^2a_4^2a_5^2, a_2^2 - a_3a_4a_5, a_4 - a_5, a_4^2 - 2, a_5 - 1, a_5^2 - 1\}$ is a Gröbner basis[13]. Interreducing this set using qc-reduction at head terms only we get the set $\{a_1 - a_3^2a_4^2a_5, a_2 - a_3^2a_4^2a_5^2, a_4 - a_5, a_5 - 1\}$ which is the set specified in example 3.3.8 in [Wi89]. Further interreduction yields a reduced Gröbner basis of the form $\{a_1 - a_3^2, a_2 - a_3^2, a_4 - 1, a_5 - 1\}$. $\diamond$

Our result for nilpotent groups presented by convergent PCNI-systems corresponds to the fact that in this case canonical bases for subgroups exist which enable confluence for Wißmann's reduction. On the other hand, if the group is presented by a convergent PCP-system for $\Longrightarrow$-reduction finite confluent bases need no longer exist (c.f. Theorem 3.6.9 in [Wi89]).

Example 4
Let $\mathcal{G}$ be presented by the convergent PCP-system $\Sigma = \{a_1, a_1^{-1}, a_2, a_2^{-1}, a_3, a_3^{-1}\}$, $T = \{a_1a_1^{-1} \longrightarrow \lambda, a_1^{-1}a_1 \longrightarrow \lambda, a_2a_2^{-1} \longrightarrow \lambda, a_2^{-1}a_2 \longrightarrow \lambda, a_3a_3^{-1} \longrightarrow \lambda, a_3^{-1}a_3 \longrightarrow \lambda, a_3a_1 \longrightarrow$

[12] The example can also be found to illustrate Wißmann's method. See example 3.3.8 in [Wi89].

[13] This set is the union of the qc-saturating sets $\textsc{Sat}_{qc}(a_1a_3a_5 - 1) = \{a_1 - a_3^2a_4^2a_5, a_1^2 - a_3a_4a_5\}$, $\textsc{Sat}_{qc}(a_2a_3 - 1) = \{a_2 - a_3^2a_4^2a_5^2, a_2^2 - a_3a_4a_5\}$, $\textsc{Sat}_{qc}(a_4a_5^2 - 1) = \{a_4 - a_5, a_4^2 - 2\}$, $\textsc{Sat}_{qc}(a_5 - 1) = \{a_5 - 1, a_5^2 - 1\}$ and it is a Gröbner basis as all s-polynomials reduce to zero.

$a_1a_2a_3, a_3a_1^{-1} \longrightarrow a_1^{-1}a_2^{-1}a_3, a_3^{-1}a_1 \longrightarrow a_1a_2^{-1}a_3^{-1}, a_3^{-1}a_1^{-1} \longrightarrow a_1^{-1}a_2a_3^{-1}, a_2^{\delta}a_1^{\delta'} \longrightarrow a_1^{\delta'}a_2^{\delta}, a_3^{\delta}a_2^{\delta'} \longrightarrow a_2^{\delta'}a_3^{\delta} \mid \delta, \delta' \in \{1, -1\}\}$. Then the set $U = \{a_2, a_3\}$ is a λ-confluent basis of the subgroup it generates, but while a_1 and $a_2^{-1} \circ a_3 \circ a_1$ lie in the same left coset their normal forms a_1 and a_1a_3 are not joinable with respect to $\Longrightarrow_U$. ◇

The fact that Wißmann does provide a solution for convergent PCP-systems in form of λ-confluent subgroup bases can be related to the results given in section 6 as follows: We will introduce left polycyclic reduction to treat left ideals in group rings where the group is given by a convergent PCP-system. Then the subgroup problem can be solved using a finite Gröbner basis now of the *left* ideal generated by the set P_U. Moreover, we will see how in fact the problem outlined in example 4 can be overcome when changing the presentation of the group.

5 Reduction in Nilpotent Group Rings

Let $\mathcal{G}$ be a nilpotent group given by a convergent PCNI-presentation as described in section 2. The next example illustrates that no total, well-founded admissible ordering can exist for a non-trivial group due to the existence of inverses.

Example 5
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 $\mathbf{Q}$ denote the rational numbers. Suppose we simply require divisibility of the head term to allow reduction. Then we could reduce the polynomial $a^2 + 1 \in \mathbf{Q}[\mathcal{G}]$ 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 required to allow reduction in order to prevent that a monomial is replaced by something larger. Since $\mathcal{G}$ in general is not commutative, we will at first restrict ourselves to right multiples to define reduction. How reduction using left multiples can be done is outlined in section 6 for the more general case that $\mathcal{G}$ is given as a convergent PCP-presentation.

Definition 9
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{G}]$. We say that f **quasi-commutatively (qc-) reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow_f^{\mathrm{qc}} q$, if

(a) $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$, and

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

Quasi-commutative reduction by a set $F \subseteq \mathbf{K}[\mathcal{G}]$ is denoted by $p \longrightarrow_F^{\mathrm{qc}} q$ and abbreviates $p \longrightarrow_f^{\mathrm{qc}} q$ for some $f \in F$. ◇

Notice that if f qc-reduces p at $\alpha \cdot t$ to q, then t no longer is a term in q and by lemma 5, $p > q$ holds. This reduction is effective, as it is possible to decide, whether we have $t \geq_{\text{tup}} \mathsf{HT}(f)$. Further it is Noetherian and the translation lemma holds.

Lemma 9
Let F be a set of polynomials in $\mathbf{K}[\mathcal{G}]$ and $p, q, h \in \mathbf{K}[\mathcal{G}]$ some polynomials.

1. *Let $p - q \longrightarrow_F^{\text{qc}} h$. Then there are $p', q' \in \mathbf{K}[\mathcal{G}]$ such that $p \overset{*}{\longrightarrow}{}_F^{\text{qc}} p', q \overset{*}{\longrightarrow}{}_F^{\text{qc}} q'$ and $h = p' - q'$.*
2. *Let 0 be a normal form of $p - q$ with respect to $\longrightarrow_F^{\text{qc}}$. Then there exists a polynomial $g \in \mathbf{K}[\mathcal{G}]$ such that $p \overset{*}{\longrightarrow}{}_F^{\text{qc}} g$ and $q \overset{*}{\longrightarrow}{}_F^{\text{qc}} g$.*

Proof :

1. Let $p - q \longrightarrow_F^{\text{qc}} h = p - q - \alpha \cdot f * w$, where $\alpha \in \mathbf{K}^*, f \in F, w \in \mathcal{G}$ and $\mathsf{HT}(f) \circ w = t \geq_{\text{tup}} \mathsf{HT}(f)$, 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 qc-reduction. We then get $p \longrightarrow_f^{\text{qc}} p - \alpha_1 \cdot f * w = p'$ and $q \longrightarrow_f^{\text{qc}} q - \alpha_2 \cdot f * w = q'$, 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 qc-reduction and get $p \longrightarrow_f^{\text{qc}} p - \alpha \cdot f * w = p'$ 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 qc-reduction and get $q \longrightarrow_f^{\text{qc}} q + \alpha \cdot f * w = q'$ and $p = p'$.

   In all cases we have $p' - q' = p - q - \alpha \cdot f * w = h$.

2. We show our claim by induction on k, where $p - q \overset{k}{\longrightarrow}{}_F^{\text{qc}} 0$. In the base case $k = 0$ there is nothing to show. Hence, let $p - q \longrightarrow_F^{\text{qc}} h \overset{k}{\longrightarrow}{}_F^{\text{qc}} 0$. Then by (1) there are polynomials $p', q' \in \mathbf{K}[\mathcal{G}]$ such that $p \overset{*}{\longrightarrow}{}_F^{\text{qc}} p', q \overset{*}{\longrightarrow}{}_F^{\text{qc}} q'$ and $h = p' - q'$. Now the induction hypothesis for $p' - q' \overset{k}{\longrightarrow}{}_F^{\text{qc}} 0$ yields the existence of a polynomial $g \in \mathbf{K}[\mathcal{G}]$ such that $p \overset{*}{\longrightarrow}{}_F^{\text{qc}} p' \overset{*}{\longrightarrow}{}_F^{\text{qc}} g$ and $q \overset{*}{\longrightarrow}{}_F^{\text{qc}} q' \overset{*}{\longrightarrow}{}_F^{\text{qc}} g$.

q.e.d.

In case $\mathcal{G}$ is a free Abelian group, qc-reduction coincides with Sims' reduction for Laurent polynomials, as the condition $t \geq_{\text{tup}} \mathsf{HT}(f)$ implies that $u = \mathsf{inv}(\mathsf{HT}(f)) \circ t$ is aligned with $\mathsf{HT}(f)$. Notice that in the general nilpotent case u and $\mathsf{HT}(f)$ no longer need to be aligned. Furthermore the following example shows that even if they are aligned, Sims' definition of reduction cannot be carried over to nilpotent groups.

Example 6

Let $\Sigma = \{a_1, a_1^{-1}, a_2, a_2^{-1}, a_3, a_3^{-1}\}$ and $T = \{a_2a_1 \longrightarrow a_1a_2a_3, a_2^{-1}a_1^{-1} \longrightarrow a_1^{-1}a_2^{-1}a_3, a_2^{-1}a_1 \longrightarrow a_1a_2^{-1}a_3^{-1}, a_2a_1^{-1} \longrightarrow a_1^{-1}a_2a_3^{-1}, a_3^{\delta}a_2^{\delta'} \longrightarrow a_2^{\delta'}a_3^{\delta}, a_3^{\delta}a_1^{\delta'} \longrightarrow a_1^{\delta'}a_3^{\delta} \mid \delta, \delta' \in \{1, -1\}\}$ be a convergent PCNI-presentation of the free nilpotent group on two generators. Then for a_1a_2 and a_1a_3 due to Sims' ordering we get $a_1a_3 \succ a_1a_2$, but for the aligned elements a_1 and a_1a_3 we find $a_1a_3 \circ a_1 = a_1^2a_3$, while $a_1a_2 \circ a_1 = a_1^2a_2a_3$, and hence $a_1a_3 \circ a_3 = a_1^2a_3 \prec a_1^2a_2a_3 = a_1a_2 \circ a_1$. ◇

Gröbner bases as defined by Buchberger can now be specified for right ideals in this setting as follows.

Definition 10

A set $G \subseteq \mathbf{K}[\mathcal{G}]$ is said to be a **right Gröbner basis**, if $\overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$, and $\longrightarrow^{\mathrm{qc}}_{G}$ is confluent. ◇

Since Buchberger's reduction always captures the ideal congruence, in order to characterize Gröbner bases he only has to give a confluence criteria. Now we find that in our setting we have to be more careful, as for qc-reduction $\overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$ in general will *not* hold. One reason for this phenomenon is that a reduction step is not preserved under right multiplication with elements of $\mathcal{G}$.

Example 7

Let $\mathbf{Q}[\mathcal{G}]$ be the group ring given in example 5. Then for the polynomials $p = a^2 + a$ and $f = a + \lambda$ we find that p is qc-reducible by f. This is no longer true for the multiple $p * a^{-2} = (a^2 + a) * a^{-2} = \lambda + a^{-1}$. Notice that, since $a^{-1} + \lambda \in \mathsf{ideal}_r(p)$, we have $a^{-1} + \lambda \equiv_{\mathsf{ideal}_r(p)} 0$, but $a^{-1} + \lambda \overset{*}{\longleftrightarrow}_p 0$ does not hold. ◇

We will now introduce how we can extend the expressiveness of qc-reduction. We start by enabling the reducibility of special monomial multiples of a polynomial by allowing to use not only the polynomial itself but a special set of polynomial multiples for qc-reduction. First let us take a look at what multiples are appropriate to later on enable an effective characterization of a right Gröbner basis. As our example shows, we have to pay attention to the problem that different terms of a polynomial can come to head position by right multiplication with group elements. The next lemma states how right multiples which bring other terms to head position can be constructed in case they exist.

Lemma 10

Let p be a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$. In case there exists an element $w \in \mathcal{G}$ such that $\mathsf{HT}(p*w) = t \circ w$ for some $t \in \mathsf{T}(p)$, let a_d be the distinguishing letter between t and $\mathsf{HT}(p)$. Then one can construct an element $v \in \mathsf{ORD}(\Sigma_d)$ such that $\mathsf{HT}(p * v) = t \circ v$.
In particular, given p and $t \in \mathsf{T}(p)$ it is decidable whether there exists an element $w \in \mathcal{G}$ such that $\mathsf{HT}(p * w) = t$.

Proof :

We show that for all polynomials $q \in \{p * u \mid u \in \mathcal{G}\}$ the following holds: In case $\mathsf{HT}(q*w) = t_i \circ w$ for some $w \in \mathcal{G}$, $t_i \in \mathsf{T}(q)$ then one can construct an element $v \in \mathsf{ORD}(\Sigma_d)$ where a_d is the distinguishing letter between t_i and $\mathsf{HT}(q)$, and $\mathsf{HT}(q * v) = t_i \circ v$.

This will be done by induction on k where $d = n - k$.

In the base case let $k = 0$, i.e., a_n is the distinguishing letter between $\mathsf{HT}(q) = t_1 \equiv a_1^{1_1} \dots a_n^{1_n}$ and $t_i \equiv a_1^{i_1} \dots a_n^{i_n}$. Hence $1_j = i_j$ for all $1 \leq j \leq n-1$ and $1_n >_{\mathbf{Z}} i_n$.

By our assumption there exists $w \in \mathcal{G}$ such that $\mathsf{HT}(q * w) = t_i \circ w$, with $w \equiv w' a_n^{w_n}$, $w' \in \mathsf{ORD}(\Sigma \backslash \Sigma_n)$, and there exist $k_1, \dots, k_{n-1}, x \in \mathbf{Z}$ such that $t_1 \circ w = a_1^{1_1} \dots a_n^{1_n} \circ w = a_1^{1_1} \dots a_{n-1}^{1_{n-1}} \circ w \circ a_n^{1_n} = (a_1^{1_1} \dots a_{n-1}^{1_{n-1}} \circ w') \circ a_n^{1_n + w_n} = a_1^{k_1} \dots a_{n-1}^{k_{n-1}} \circ a_n^{1_n + x}$ and $t_i \circ w = a_1^{1_1} \dots a_{n-1}^{1_{n-1}} a_n^{i_n} \circ w = a_1^{1_1} \dots a_{n-1}^{1_{n-1}} \circ w \circ a_n^{i_n} = (a_1^{1_1} \dots a_{n-1}^{1_{n-1}} \circ w') \circ a_n^{i_n + w_n} = a_1^{k_1} \dots a_{n-1}^{k_{n-1}} \circ a_n^{i_n + x}$. Thus $1_n + x <_{\mathbf{Z}} i_n + x$ or, in case a_n is bounded by $m_n \in \mathbf{N}$, $(1_n + x) \ \mathsf{mod} \ m_n <_{\mathbf{Z}} (i_n + x) \ \mathsf{mod} \ m_n$ must hold. First let us assume that the letter a_n is not bounded. Then let us set $v \equiv a_n^{-1_n}$. We show that for all $t_j \in T(q) \backslash \{t_i\}$ we have $t_i \circ v \succ t_j \circ v$. Note that for all t_j with prefix $a_1^{j_1} \dots a_{n-1}^{j_{n-1}} \prec a_1^{1_1} \dots a_{n-1}^{1_{n-1}}$ we have $t_j \circ v \prec t_i \circ v$, as right multiplication with $v \equiv a_n^{-1_n}$ only changes the exponent of a_n in the respective term. It remains to look at those terms t_j with $a_1^{j_1} \dots a_{n-1}^{j_{n-1}} \equiv a_1^{1_1} \dots a_{n-1}^{1_{n-1}}$. Then we can apply lemma 3 as we have $1_n >_{\mathbf{Z}} i_n$, $1_n >_{\mathbf{Z}} j_n$ and as seen above there exists an element x such that $1_n + x <_{\mathbf{Z}} i_n + x$ and $j_n + x <_{\mathbf{Z}} i_n + x$. Therefore $i_n - 1_n >_{\mathbf{Z}} j_n - 1_n$ and our claim must hold. In case the letter a_n is bounded by m_n, we set $v \equiv a_n^{m_n - i_n - 1}$. As before, for all t_j which have a prefix $a_1^{j_1} \dots a_{n-1}^{j_{n-1}} \prec a_1^{1_1} \dots a_{n-1}^{1_{n-1}}$ we have $t_j \circ v \prec t_i \circ v$. Tor those t_j with prefix $a_1^{1_1} \dots a_{n-1}^{1_{n-1}}$ we know that the exponent of a_n in $t_j \circ v$ cannot be $m_n - 1$ unless $t_j = t_i$, and hence $t_j \circ v \prec t_i \circ v$ must hold.

In the induction step let us assume that for all polynomials $q \in \{p * u | u \in \mathcal{G}\}$ and $w \in \mathcal{G}$ with $\mathsf{HT}(q * w) = t_i \circ w$, if the distinguishing letter a_d between $\mathsf{HT}(q)$ and t_i has index $d \geq n - (k-1)$ there exists an element $v' \in \mathsf{ORD}(\Sigma_d)$ such that $\mathsf{HT}(q * v') = t_i \circ v'$. Now for $q \in \{p * u | u \in \mathcal{G}\}$, $w \in \mathcal{G}$ with $\mathsf{HT}(q * w) = t_i \circ w$ let us assume that the distinguishing letter between $\mathsf{HT}(q)$ and t_i has index $d = n - k$.

Since $\mathsf{HT}(q * w) = t_i \circ w$, for $w \equiv w' a_d^{w_d} w''$ with $w' \in \mathsf{ORD}(\Sigma \backslash \Sigma_d)$, $w'' \in \mathsf{ORD}(\Sigma_{d+1})$, we know that there exist $k_1, \dots, k_{d-1}, x \in \mathbf{Z}$ and $z_1, z_i, \tilde{z}_1 \in \mathsf{ORD}(\Sigma_{d+1})$ such that $t_1 \circ w = a_1^{1_1} \dots a_n^{1_n} \circ w = a_1^{1_1} \dots a_{d-1}^{1_{d-1}} \circ w' \circ a_d^{1_d} \circ \tilde{z}_1 = a_1^{k_1} \dots a_{d-1}^{k_{d-1}} \circ a_n^{1_d + x} \circ z_1$ and similarly $t_i \circ w = a_1^{k_1} \dots a_{d-1}^{k_{d-1}} \circ a_n^{i_d + x} \circ z_i$. As $1_d \neq i_d$ then $1_d + x <_{\mathbf{Z}} i_d + x$ or, in case a_n is bounded by $m_n \in \mathbf{N}$, $(1_n + x) \ \mathsf{mod} \ m_n <_{\mathbf{Z}} (i_n + x) \ \mathsf{mod} \ m_n$ must hold. In case a_d is not bounded we can then set $v_d \equiv a_n^{-1_d}$. We have to show that for all $t_j \in T(q) \backslash \{t_i\}$ there exists $v \in \mathsf{ORD}(\Sigma_d)$ such that we have $t_i \circ v \succ t_j \circ v$. Note that for all t_j with prefix $a_1^{j_1} \dots a_{d-1}^{j_{d-1}} \prec a_1^{1_1} \dots a_{d-1}^{1_{d-1}}$ we have $t_j \circ v_d \prec t_i \circ v_d$, as right multiplication with $v_d \equiv a_n^{-1_d}$ has no influence on the prefix in $\mathsf{ORD}(\Sigma \backslash \Sigma_d)$.

Therefore, it remains to look at those terms t_j with $a_1^{j_1} \dots a_{d-1}^{j_{d-1}} \equiv a_1^{1_1} \dots a_{d-1}^{1_{d-1}}$ and $1_d \geq_{\mathbf{Z}} j_d$. Since there further exists $x \in \mathbf{Z}$ such that $1_d + x <_{\mathbf{Z}} i_d + x$ and $j_d + x \leq_{\mathbf{Z}} i_d + x$ we can again apply lemma 3 to show our claim. In case $i_d - 1_d >_{\mathbf{Z}} j_d - 1_d$ we are done. Else we get $i_d = j_d$ and can apply the induction hypothesis since the distinguishing letter between $t_i \circ v_d$ and $t_j \circ$ will be of index greater than d, yielding an element $v' \in \mathsf{ORD}(\Sigma_{d+1})$ and we can set $v \equiv v_d v'$.

Now it remains to look at the case that a_d is bounded by m_d. Then we can set $v_d \equiv a_d^{m_d - i_d - 1}$ and proceed to construct v as above.

q.e.d.

Notice that the proof of this lemma shows that there is an algorithm which computes some $v \in \mathsf{ORD}(\Sigma_d)$ as desired in case it exists and that the element w need not be known for this computation. Hence we can enrich a polynomial by the set of those multiples which bring other terms of the polynomial to head position. But still there remain cases of multiples which are not qc-reducible by this set of polynomials due to the fact that the "divisibility" criteria 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 $p * a^{-1} = a + \lambda$ results from the head term a^2 of p, but still $a + \lambda$ is not qc-reducible by p, since a^2 is no commutative prefix of a. Therefore, let us consider some further special multiples. For a polynomial p and a term $t \in \mathsf{T}(p)$ we call a term s in a multiple $p * w$ a **t-term** if $s = t \circ w$. The following lemma states that if in two right multiples of a polynomial the head terms result from the same term t, then there is also a right 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 7 for $p * \lambda = a^2 + a$ and $p * a^{-1} = a + \lambda$, both head terms result from the same term a^2 and the head term a of $p * a^{-1}$ is a commutative prefix of the head term a^2 of $p * \lambda$.

Lemma 11

For $u, v \in \mathcal{G}$, let $p*u$ and $p*v$ be two right multiples of a non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$ such that for some term $t \in \mathsf{T}(p)$ the head terms are t-terms, i.e., $\mathsf{HT}(p * u) = t \circ u \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(p * v) = t \circ v \equiv a_1^{j_1} \dots a_n^{j_n}$. Then there exists a term $\tilde{t} \leq_{\mathrm{tup}} a_1^{\rho_1} \dots a_n^{\rho_n}$ 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 $\mathsf{HT}(p * \tilde{z}) = t \circ \tilde{z} = \tilde{t}$. In particular, we have $p * u \xrightarrow{\mathrm{qc}}_{p*\tilde{z}} 0$ and $p * v \xrightarrow{\mathrm{qc}}_{p*\tilde{z}} 0$.

Proof :

Let p, $p * u$ and $p * v$ be as described in the lemma and let the letters corresponding to our presentation be $\Sigma = \{a_1, \dots, a_n, a_1^{-1}, \dots, a_n^{-1}\}$.

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

Let us start by constructing an element $z_1 \in \mathcal{G}$ such that $\mathsf{HT}(p * z_1) = t \circ z_1 \equiv a_1^{s_1} r_1$, $r_1 \in \mathsf{ORD}(\Sigma_2)$ and $a_1^{s_1} \leq_{\mathrm{tup}} a_1^{\rho_1}$.

In case $i_1 = j_1$ or $j_1 = 0$ we can set $z_1 = v$ and $s_1 = j_1 = \rho_1$ since $\mathsf{HT}(p * v) = t \circ v \equiv a_1^{j_1} \dots a_n^{j_n}$. Similarly in case $i_1 = 0$ we can set $z_1 = u$ and $s_1 = i_1 = 0 = \rho_1$ since $\mathsf{HT}(p * u) = t \circ u \equiv a_2^{i_2} \dots a_n^{i_n} \in \mathsf{ORD}(\Sigma_2)$. 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 construction in this case 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. In case $|j_1| > |i_1|$ we set $z_1 = u$ because for $s_1 = i_1 = \rho_1$ our claim holds.

Now let us proceed with the case $\mathsf{sgn}(i_1) \neq \mathsf{sgn}(j_1)$, i.e., a_1 cannot be bounded. We construct $z_1 \in \mathcal{G}$ such that $\mathsf{HT}(p * z_1) = t \circ z_1 \in \mathsf{ORD}(\Sigma_2)$ as $\rho_1 = 0$. We claim that the letter a_1 has

the same exponent for all terms in $\mathsf{T}(p)$, say b. In case this holds, no term in the polynomial $p * a_1^{-b}$ will contain the letter a_1 and the distinguishing letter between $\mathsf{HT}(p * a_1^{-b})$ and the term $t \circ a_1^{-b}$ is at least of index 2. Furthermore we know $\mathsf{HT}((p * a_1^{-b}) * (a_1^b \circ v)) = \mathsf{HT}(p * v) = t \circ v$. Thus by lemma 14 there exists an element $r \in \mathsf{ORD}(\Sigma_2)$ such that $\mathsf{HT}((p * a_1^{-b}) * r) = t \circ a_1^{-b} \circ r \in \mathsf{ORD}(\Sigma_2)$ and thus we can set $z_1 = a_1^{-b} r$ and $s_1 = 0 = \rho_1$.
Hence it remains to prove our initial claim. Suppose we have the representatives $s' \equiv a_1^{b_{s'}} x_{s'}$, $b_{s'} \in \mathbf{Z}$, $x_{s'} \in \mathsf{ORD}(\Sigma_2)$ for the terms $s' \in \mathsf{T}(p)$ and $\mathsf{HT}(p) = s \equiv a_1^{b_s} x_s$. Then we know $b_s \geq_{\mathbf{Z}} b_t$ since $t \in \mathsf{T}(p)$.
Hence in showing that the case $b_s >_{\mathbf{Z}} b_t$ 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 $x \in \mathbf{Z}$ 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 $x \in \mathbf{Z}$ 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 $\mathsf{HT}(p * u)$ respectively $\mathsf{HT}(p * v)$ have different sign.
It remains to show that there cannot exist a term $s' \in \mathsf{T}(p)$ with $b_{s'} <_{\mathbf{Z}} b_s = b_t$. Let us assume such an s' exists. Since $\mathsf{HT}(p * u) = t \circ u \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(p * v) = t \circ v \equiv a_1^{j_1} \dots a_n^{j_n}$ there then must exist $x_1, x_2 \in \mathbf{Z}$ such that $b_{s'} + x_1 <_{\mathbf{Z}} b_t + x_1 = i_1$ and $b_{s'} + x_2 <_{\mathbf{Z}} b_t + x_2 = j_1$. Without loss of generality let us assume $i_1 > 0$ and $j_1 < 0$ (the other case is symmetric). In case $b_t < 0$ we get that $b_t + x_1 = i_1 > 0$ implies $x_1 > |b_t| > 0$. Now, as $b_{s'} <_{\mathbf{Z}} b_t$ 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 $b_{s'} + x_1 <_{\mathbf{Z}} b_t + x_1$. On the other hand, in case $b_t > 0$ 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 $b_{s'} + x_2 <_{\mathbf{Z}} b_t + x_2$.
Thus let us assume that for the letter a_{k-1} we have constructed $z_{k-1} \in \mathcal{G}$ such that $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} r_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ with $r_{k-1} \in \mathsf{ORD}(\Sigma_k)$, $r' \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} \leq_{\mathrm{tup}} a_1^{\rho_1} \dots a_{k-1}^{\rho_{k-1}}$. We now show that we can find $z_k = z_{k-1} \circ \tilde{w} \in \mathcal{G}$ such that $\mathsf{HT}(p * z_k) = t \circ z_k \equiv a_1^{s_1} \dots a_k^{s_k} r_k$ with $r_k \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \dots a_k^{s_k} \leq_{\mathrm{tup}} a_1^{\rho_1} \dots a_k^{\rho_k}$.
This will be done in two steps. First we show that for the polynomials $p * u$ and $p * z_{k-1}$ 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 $\mathsf{HT}(p * z_{k-1} * w_1) = t \circ z_{k-1} \circ w_1 \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$, $\tilde{r} \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{\tilde{s}_k} \leq_{\mathrm{tup}} a_k^{\tilde{\rho}_k}$ 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 in case $a_k^{\tilde{\rho}_k} \leq_{\mathrm{tup}} a_k^{\rho_k}$ we are done and set $z_k = z_{k-1} \circ w_1$ and $s_k = \tilde{s}_k$. Else we can similarly proceed for the polynomials $p * v$ and $p * z_{k-1} * w_1$ with head terms $a_1^{j_1} \dots a_n^{j_n}$ respectively $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$ and find an element $w_2 \in \mathcal{G}$ such that for $z_k = z_{k-1} \circ w_1 \circ w_2$ we have $\mathsf{HT}(p * z_k) = t \circ z_k \equiv a_1^{s_1} \dots a_k^{s_k} r_k$, $r_k \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{s_k} \leq_{\mathrm{tup}} a_k^{\tilde{\rho}'_k}$ 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 $a_k^{s_k} \leq_{\mathrm{tup}} a_k^{\rho_k}$ as in case $s_k = 0$ we are immediately done 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 $\mathsf{HT}(p * u) = t \circ u \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ for some $r' \in \mathsf{ORD}(\Sigma_{k+1})$. In 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 $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$. Hence let $i_k \neq l_k$ and $l_k \neq 0$.

First let us assume that $\mathsf{sgn}(i_k) = \mathsf{sgn}(l_k)$. Then in case $|i_k| \geq |l_k|$ we are done by setting $w_1 = \lambda$ as again $\mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ will do with $\tilde{s}_k = l_k = \tilde{\rho}_k$. Therefore, let us assume that $|l_k| > |i_k|$. Without loss of generality let us assume that a_k is not bounded[14]. Then we consider the multiple $p * z_{k-1} * a_k^{-l_k+i_k}$, i.e., the exponent of the letter a_k in the term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ will be i_k. If $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k}) = t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ we are done because then $t \circ z_{k-1} \circ a_k^{-l_k+i_k} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} \tilde{r}_k$ for some $\tilde{r}_k \in \mathsf{ORD}(\Sigma_{k+1})$ and we can set $w_1 = a_k^{-l_k+i_k}$ and $\tilde{s}_k = i_k = \tilde{\rho}_k$. Otherwise we show that the t-term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ in this multiple can be brought to head position using an element $r \in \mathsf{ORD}(\Sigma_{k+1})$ thus allowing to set $\tilde{s}_k = i_k = \tilde{\rho}_k$ and $w_1 = a_k^{-l_k+i_k} r$ as then we have $\mathsf{HT}(p * z_{k-1} * w_1) = t \circ z_{k-1} \circ w_1 = a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r' \circ a_k^{-l_k+i_k} r \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} \tilde{r}$ where $a_k^{l_k} r' \circ a_k^{-l_k+i_k} r \equiv a_k^{i_k} \tilde{r}$. (Note that the product of two elements in $\mathsf{ORD}(\Sigma_i)$ is again an element in $\mathsf{ORD}(\Sigma_i)$) This follows immediately if we can prove that the exponent of a_k in the term $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ is also i_k. Then we can apply lemma 14 to the polynomial $p * z_{k-1} * a_k^{-l_k+i_k}$ and the term $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$. Note that $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ and $t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ have then distinguishing letter of at least index $k+1$ and further $\mathsf{HT}((p * z_{k-1} * a_k^{-l_k+i_k}) * a_k^{-l_k+i_k}) = \mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1}$. Therefore, we show that the exponent of a_k in the term $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ 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 $p * z_{k-1}$ that became head term (note that a candidate in $\mathsf{T}(p * z_{k-1})$ for the head term in $p * z_{k-1} * a_k^{-l_k+i_k}$ must have prefix $a_1^{s_1} \dots a_{k-1}^{s_{k-1}}$ since $\mathsf{HT}(p * z_{k-1}) \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} r_{k-1}$ and multiplication with $a_k^{-l_k+i_k}$ only involves r_{k-1}), i.e., $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{b_k} r'' \circ a_k^{-l_k+i_k} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x \succ a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} y \equiv t \circ z_{k-1} \circ a_k^{-l_k+i_k}$ for some $x, y \in \mathsf{ORD}(\Sigma_{k+1})$ and therefore $c_k \geq_{\mathbf{Z}} i_k$. Then by lemma 4 there exist $z_1 \in \mathsf{ORD}(\Sigma \backslash \Sigma_{k-1})$ and $z_2 \in \mathsf{ORD}(\Sigma_k)$ such that $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{i_k} y \circ z_1 = a_1^{i_1} \dots a_{k-1}^{i_{k-1}} \circ a_k^{i_k+f_k} \circ z$ for some $z \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{i_k+f_k} \circ z \circ z_2 \equiv a_k^{i_k} a_{k+1}^{i_{k+1}} \dots a_n^{i_n}$, i.e., $z_2 = a_k^{-f_k} \circ z_2'$ for some $z_2' \in \mathsf{ORD}(\Sigma_{k+1})$. Note that the t-term is brought to head position by this multiplication. Now multiplying $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k+i_k})$ by $z_1 z_2$ we find $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x \circ z_1 z_2 \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{c_k+f_k-f_k} \tilde{x}$ for some $\tilde{x} \in \mathsf{ORD}(\Sigma_{k+1})$. This gives us $c_k \leq_{\mathbf{Z}} i_k$ and thus $i_k \leq_{\mathbf{Z}} c_k$ yields $c_k = i_k$.

Finally, we have to check the case that $\mathsf{sgn}(i_k) \neq \mathsf{sgn}(l_k)$, i.e., a_k is not bounded in this case, and $l_k \neq 0$. Let us take a look at the polynomial $p * z_{k-1} * a_k^{-l_k}$, i.e., the exponent of the letter a_k in the term $t \circ z_{k-1} \circ a_k^{-l_k}$ will be 0. Suppose $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k}) \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x$, for some term $s \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{b_s} x_s \in \mathsf{T}(p * z_{k-1})$, $x, x_s \in \mathsf{ORD}(\Sigma_{k+1})$, i.e., $c_k = b_s - l_k$. In case this head term is already the corresponding t-term $t \circ z_{k-1} \circ a_k^{-l_k}$, we are done and we set $w_1 = a_k^{-l_k}$ and $\tilde{s}_k = 0 = \tilde{\rho}_k$. Now if we can show $c_k = 0$, by lemma 14 the t-term $t \circ z_{k-1} \circ a_k^{-l_k}$ can be brought to head position using an element in $\mathsf{ORD}(\Sigma_{k+1})$ since the distinguishing letter between $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k})$ and the term $t \circ z_{k-1} \circ a_k^{-l_k}$ then has

[14] In case 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. We only have to take into account that in the definition of $w_1 = a_k^{-l_k+i_k}$ the normal form looks different in case $-l_k + i_k < 0$.

at least index $k+1$ and we know $\mathsf{HT}((p * z_{k-1} * a_k^{-l_k}) * a_k^{l_k}) = \mathsf{HT}(p * z_{k-1}) = t \circ z_{k-1}$. Hence, in showing that $c_k = 0$ we are done. As before there exist $z_1 \in \mathsf{ORD}(\Sigma \backslash \Sigma_{k-1})$ and $z_2 \in \mathsf{ORD}(\Sigma_k)$ such that $t \circ z_{k-1} \circ a_k^{-l_k} \circ z_1 \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{f_k} z$ for some $z \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_k^{f_k} z \circ z_2 \equiv a_k^{i_k} \dots a_n^{i_n}$, i.e., $z_2 \equiv a_k^{-f_k + i_k} z_2'$ for some $z_2' \in \mathsf{ORD}(\Sigma_{k+1})$. Remember that this multiplication brings the t-term to head position. Hence multiplying $\mathsf{HT}(p * z_{k-1} * a_k^{-l_k})$ by $z_1 z_2$ we find $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{c_k} x \circ z_1 z_2 \equiv a_1^{i_1} \dots a_{k-1}^{i_{k-1}} a_k^{c_k + i_k} \tilde{x}$ for some $\tilde{x} \in \mathsf{ORD}(\Sigma_{k+1})$. Thus we know $c_k + i_k \leq_{\mathbf{Z}} i_k$. 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 $s \circ a_k^{-l_k}$ for some $s \in \mathsf{T}(p * z_{k-1})$ we know $b_s \leq_{\mathbf{Z}} l_k$. In case $i_k = 0$, we have $c_k \leq_{\mathbf{Z}} 0$ implying $c_k = 0$. In case $i_k > 0$ then $c_k + i_k = b_s - l_k + i_k \leq_{\mathbf{Z}} i_k$ 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 inequation can only hold in case $c_k = b_s - l_k = 0$. q.e.d.

These two lemmata now state that given a polynomial, we can construct additional polynomials, which are in fact right multiples of the original polynomial, such that every right multiple of the polynomial is qc-reducible to zero in one step by one of them. Such a property of a set of polynomials is called qc-saturation. In example 7 the multiples $p * a^{-1} = a + \lambda$ and $p * a^{-2} = a^{-1} + \lambda$ give us a qc-saturating set for $p = a^2 + a$.

Definition 11
A set $S \subseteq \{p * w \mid w \in \mathcal{G}\}$ is called a **qc-saturating set** for a non-zero polynomial p in $\mathbf{K}[\mathcal{G}]$, if for all $w \in \mathcal{G}$, $p * w \longrightarrow_S^{\mathrm{qc}} 0$. A set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$ is called **qc-saturated**, if for all $f \in F$ and for all $w \in \mathcal{G}$, $f * w \longrightarrow_F^{\mathrm{qc}} 0$. ⋄

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

Procedure Quasi-Commutative Saturation

Given: A non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$.
Find: $\textsc{Sat}_{qc}(p)$, a qc-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 $q = p * w$ with $\mathsf{HT}(p * w) = t \circ w$
             $H_t := \{s \in \mathcal{G} \mid \mathsf{HT}(q) \geq_{\mathrm{tup}} s\}$;
             % These are candidates for "smaller" polynomials with $t$-head terms
             $q := \min\{p * (\mathsf{inv}(t) \circ s) \mid s \in H_t, \mathsf{HT}(p * (\mathsf{inv}(t) \circ s)) = s\}$;
             $S_t := \{q\}$;
    endif
endfor
$\textsc{Sat}_{qc}(p) := \bigcup_{t \in \mathsf{T}(p)} S_t$    % $S$ contains at most $|\mathsf{T}(p)|$ polynomials
```

Notice that more structural information can be used to rule out unnecessary candidates from the set H_t to make this procedure more efficient.

While in the free Abelian group case symmetrized sets and qc-saturation are successfully used to repair the same deficiency such sets in general will not coincide. One reason is that Sims uses a different ordering on his elements. For example a qc-saturating set for the polynomial $g = 2 \cdot a_1^{-2}a_2^3 - 4 \cdot a_1^2a_2^3 - a_1a_2^2 + a_1a_2$ on page 14 is $\textsc{Sat}_{qc}(g) = \{g * a_1a_2^{-1} = 2 \cdot a_1^{-1}a_2^2 - 4 \cdot a_1^3a_2^2 - a_1^2a_2 + a_1^2, g * a_1^2a_2^{-1} = -4 \cdot a_1^4a_2^2 - a_1^3a_2 + a_1^3 + 2 \cdot a_2^2\}$ while the symmetrized set consisted of the polynomials $\mathcal{S}(g) = \{g * a_2^{-1}, -g * a_1a_2^{-1}, g * a_1^{-1}a_2^{-2}\}$.

Lemma 12
For a saturated set F of polynomials in $\mathbf{K}[\mathcal{G}]$, $\overset{*}{\longleftrightarrow}{}^{\text{qc}}_{F} \; = \; \equiv_{\mathsf{ideal}_r(F)}$ holds.

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

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

eliminating the occurrence of t in $q + \alpha_{m+1} \cdot f_{m+1} * u_{m+1}$.
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 $q \longrightarrow^{\text{qc}}_{f_{m+1}} q - (\beta_1 \cdot \mathsf{HC}(f_{m+1})^{-1} - \alpha_{m+1}) \cdot f_{m+1} * u_{m+1}$, i.e., q and $q + \alpha_{m+1} \cdot f_{m+1} * u_{m+1}$ are joinable.

q.e.d.

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

Definition 12
For $p_1, p_2 \in \mathbf{K}[\mathcal{G}]$ such that $\mathsf{HT}(p_1) \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(p_2) \equiv a_1^{j_1} \ldots a_n^{j_n}$ with either $i_l \cdot j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ for $1 \leq l \leq n$ we can define an **s-polynomial**, and setting

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

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

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

◇

Notice that $\mathsf{HT}(p_i) \leq_{\text{tup}} a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$ for $i \in \{1,2\}$ holds in case such an s-polynomial exists. Furthermore, if there exists a term t such that $t \geq_{\text{tup}} \mathsf{HT}(p_1) \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $t \geq_{\text{tup}} \mathsf{HT}(p_2) \equiv a_1^{j_1} \ldots a_n^{j_n}$, 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 $t \geq_{\text{tup}} a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$.

Again for the case of free Abelian groups this definition corresponds to the definition of critical pairs for Laurent polynomials and the resulting t-polynomials are a specialization of these s-polynomials for the integer group ring[15].

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

Theorem 3
For a qc-saturated set $G \subseteq \mathbf{K}[\mathcal{G}]$ the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}_r(G)$ we have $g \xrightarrow{*}{}^{\text{qc}}_{G} 0$.*
2. *For all polynomials $f_k, f_l \in G$ we have $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\text{qc}}_{G} 0$.*

Proof :
$1 \Longrightarrow 2$: By definition 12 in case for $f_k, f_l \in G$ the s-polynomial exists we get

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

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

$2 \Longrightarrow 1$: We have to show that every non-zero element $g \in \mathsf{ideal}_r(G)$ is $\longrightarrow^{\text{qc}}_{G}$-reducible to zero. Without loss of generality we assume that G contains no constant polynomials, as then we are done at once. Remember that for $h \in \mathsf{ideal}_r(G)$, $h \longrightarrow^{\text{qc}}_{G} h'$ implies $h' \in \mathsf{ideal}_r(G)$. Thus as $\longrightarrow^{\text{qc}}_{G}$ is Noetherian it suffices to show that every $g \in \mathsf{ideal}_r(G) \backslash \{0\}$ is $\longrightarrow^{\text{qc}}_{G}$-reducible. Let $g = \sum_{j=1}^{m} \alpha_j \cdot f_j * w_j$ be a representation of a non-zero polynomial g such that $\alpha_j \in \mathbf{K}^*, f_j \in F, w_j \in \mathcal{G}$. Since G is qc-saturated we can assume $g = \sum_{j=1}^{m} \alpha_j \cdot g_j * v_j$, where $\alpha_j \in \mathbf{K}^*, g_j \in G, v_j \in \mathcal{G}$ and $\mathsf{HT}(g_j * v_j) = \mathsf{HT}(g_j) \circ v_j \geq_{\text{tup}} \mathsf{HT}(g_j)$. Depending on this representation of g and our well-founded total ordering on $\mathcal{G}$ we define $t = \max\{\mathsf{HT}(g_j) \circ v_j \mid j \in \{1, \ldots m\}\}$ and K is the number of polynomials $g_j * v_j$ containing t as a term. Then $t \succeq \mathsf{HT}(g)$ and in case $\mathsf{HT}(g) = t$ this immediately implies that g is $\longrightarrow^{\text{qc}}_{G}$-reducible. Otherwise we show that g has a special representation (a standard representation corresponding to qc-reduction which is a right commutative prefix standard representation) where all terms are bounded by $\mathsf{HT}(g)$, as this implies that g is top-reducible

[15] compare page 15.

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 $\geq_{\mathrm{syll}}$ is and $K \in \mathbf{N}$. In case $t \succ \mathsf{HT}(g)$ there are two (not necessarily different) polynomials g_k, g_l in the corresponding representation such that $t = \mathsf{HT}(g_k) \circ v_k = \mathsf{HT}(g_l) \circ v_l$ and we have $t \geq_{\mathrm{tup}} \mathsf{HT}(g_k)$,$t \geq_{\mathrm{tup}} \mathsf{HT}(g_l)$. Hence by definition 12 there exists an s-polynomial $\mathsf{spol}(g_k, g_l) = \mathsf{HC}(g_k)^{-1} \cdot g_k * z_1 - \mathsf{HC}(g_l)^{-1} \cdot g_l * z_2$ and $\mathsf{HT}(g_k) \circ v_k = \mathsf{HT}(g_l) \circ v_l = \mathsf{HT}(g_k) \circ z_1 \circ w = \mathsf{HT}(g_l) \circ z_2 \circ w \geq_{\mathrm{tup}} \mathsf{HT}(g_k) \circ z_1 = \mathsf{HT}(g_l) \circ z_2$ for some $z_1, z_2, w \in \mathcal{N}$. Let us assume $\mathsf{spol}(g_k, g_l) \neq 0$ since in case $\mathsf{spol}(g_k, g_l) = 0$, we can just substitute 0 for $\sum_{i=1}^{n} \delta_i \cdot h_i * v'_i$ in the equations below. Hence, $\mathsf{spol}(g_k, g_l) \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$ implies $\mathsf{spol}(g_k, g_l) = \sum_{i=1}^{n} \delta_i \cdot h_i * v'_i, \delta_i \in \mathbf{K}^*, h_i \in G, v'_i \in \mathcal{G}$, where the h_i are due to the qc-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 5, since $t = \mathsf{HT}(g_k) \circ z_1 \circ w \geq_{\mathrm{tup}} \mathsf{HT}(g_k) \circ z_1$ and $\mathsf{HT}(g_k) \circ z_1 \succ \mathsf{HT}(\mathsf{spol}(g_k, g_l))$, we can conclude that t is a proper bound for all terms occurring in the sum $\sum_{i=1}^{n} \delta_i \cdot h_i * v'_i * w$. Since $w \in \mathcal{G}$ and G is qc-saturated, without loss of generality, we can assume that the representation has the the required form. We now have:

$$\begin{aligned}
& \alpha_k \cdot g_k * v_k + \alpha_l \cdot g_l * v_l \\
= \quad & \alpha_k \cdot g_k * v_k + \underbrace{\alpha'_l \cdot \beta_k \cdot g_k * v_k - \alpha'_l \cdot \beta_k \cdot g_k * v_k}_{=0} + \alpha'_l \cdot \beta_l \cdot g_l * v_l \\
= \quad & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot g_k * v_k - \alpha'_l \cdot \underbrace{(\beta_k \cdot g_k * v_k - \beta_l \cdot g_l * v_l)}_{= \mathsf{spol}(g_k, g_l) * w} \\
= \quad & (\alpha_k + \alpha'_l \cdot \beta_k) \cdot g_k * v_k - \alpha'_l \cdot (\sum_{i=1}^{n} \delta_i \cdot h_i * v'_i * w) \qquad (1)
\end{aligned}$$

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 (1) in our representation of g either t disappears or in case t remains maximal among the terms occurring in the new representation of g, K is decreased. q.e.d.

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

Corollary 1
For a set $G \subseteq \mathbf{K}[\mathcal{G}]$ the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}_r(G)$ we have $g \xrightarrow{*}{}^{\mathrm{qc}}_{G} 0$.*
2. *Every $g \in \mathsf{ideal}_r(G)$ has a right commutative prefix standard representation.*
3. *G is a right commutative prefix standard basis.*
4. *G is a right Gröbner basis.*

Now, using the characterization given in theorem 3 we can state a procedure which enumerates right Gröbner bases in nilpotent group rings:

Procedure Right Gröbner Bases in Nilpotent Group Rings

Given: A finite set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$.
Find: $\textsc{Gb}_r(F)$, a right Gröbner basis of $\mathsf{ideal}_r(F)$.

```
$G := \bigcup_{g \in G} \textsc{Sat}_{qc}(g)$;   % $G$ is qc-saturated and $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$
$B := \{(q_1, q_2) \mid q_1, q_2 \in G, q_1 \neq q_2\}$;
while $B \neq \emptyset$ do   % Test if statement 2 of theorem 3 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$(h, \longrightarrow^{\mathrm{qc}}_{G})$;   % Compute a normal form
            if $h' \neq 0$   % The s-polynomial does not reduce to zero
                then $G := G \cup \textsc{Sat}_{qc}(h')$; % $G$ is qc-saturated and $\mathsf{ideal}_r(F) = \mathsf{ideal}_r(G)$
                     $B := B \cup \{(f, g) \mid f \in G, g \in \textsc{Sat}_{qc}(h')\}$;
            endif
    endif
endwhile
$\textsc{Gb}_r(F) := G$
```

The set G enumerated by this procedure fulfills the requirements of theorem 3, i.e., the set G at each stage generates $\mathsf{ideal}_r(F)$ and is qc-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 in case they exist. Hence, in case the procedure terminates, it computes a right Gröbner basis. Later on we will see that every right Gröbner basis contains a finite one and hence this procedure must terminate.

To see how this procedure works let us review example 8.3. given by Sims in [Si94] (see also page 12).

Example 8
Let $\mathcal{G}$ be the free nilpotent group on two generators with a convergent PCNI-presentation $\Sigma = \{a_1, a_1^{-1}, a_2, a_2^{-1}, a_3, a_3^{-1}\}$ and $T = \{a_2a_1 \longrightarrow a_1a_2a_3, a_2^{-1}a_1^{-1} \longrightarrow a_1^{-1}a_2^{-1}a_3, a_2^{-1}a_1 \longrightarrow a_1a_2^{-1}a_3^{-1}, a_2a_1^{-1} \longrightarrow a_1^{-1}a_2a_3^{-1}, a_3^{\delta}a_2^{\delta'} \longrightarrow a_2^{\delta'}a_3^{\delta}, a_3^{\delta}a_1^{\delta'} \longrightarrow a_1^{\delta'}a_3^{\delta} \mid \delta, \delta' \in \{1, -1\}\}$.
We want to compute a right Gröbner basis of the ideal generated by the polynomials $a_1 + a_2$ and $a_1 + a_3$. We get $\textsc{Sat}_{qc}(a_1 + a_2) = \{a_1 + a_2, a_1^{-1} + a_2^{-1}\}$ and $\textsc{Sat}_{qc}(a_1 + a_3) = \{a_1 + a_3, a_1^{-1} + a_3^{-1}\}$. From the pairs of polynomials in B only $(a_1 + a_2, a_1 + a_3)$ and $(a_1^{-1} + a_2^{-1}, a_1^{-1} + a_2a_3^{-1})$ result in two s-polynomials, namely $\mathsf{spol}(a_1 + a_2, a_1 + a_3) = a_2 - a_3$ adding the set $\textsc{Sat}_{qc}(a_2 - a_3) = \{a_2 - a_3, a_2^{-1} - a_3^{-1}\}$ to G and $\mathsf{spol}(a_1^{-1} + a_2^{-1}, a_1^{-1} + a_2a_3^{-1}) = a_2^{-1} - a_2a_3^{-1} \longrightarrow^{\mathrm{qc}}_{a_2^{-1} - a_3^{-1}} - a_2a_3^{-1} + a_3^{-1} \longrightarrow^{\mathrm{qc}}_{a_2 - a_3} a_3^{-1} - 1$ adding the set $\textsc{Sat}_{qc}(a_3^{-1} - 1) = \{a_3^{-1} - 1, a_3 - 1\}$ to G. Then for $G = \{a_1 + a_2, a_1^{-1} + a_2^{-1}, a_1 + a_3, a_1^{-1} + a_3^{-1}, a_2 - a_3, a_2^{-1} - a_3^{-1}, a_3^{-1} - 1, a_3 - 1\}$ there are no more critical pairs left and this is in fact a right Gröbner basis. Notice that in reducing the set G we get the set $\{a_1 + 1, a_1^{-1} + 1, a_2 - 1, a_2^{-1} - 1, a_3 - 1, a_3^{-1} - 1\}$ which is again an interreduced right Gröbner basis[16] of the right ideal generated by $\{a_1 + a_2, a_1 + a_3\}$ and this set contains one polynomial more than the result given by Sims (see again page 12) due

[16] While interreduction in group rings can destroy the property of being a Gröbner basis for certain reductions, qc-reduction allows to incorporate this idea into Gröbner basis computations and produces unique monic reduced Gröbner bases.

to the fact that his basis is only sufficient to prove ideal membership of polynomials with positive exponents of the letter a_1, which in his context can be achieved my multiplication by an appropriate potency of a_1. $\diamond$

For free Abelian groups the procedure of course computes Gröbner bases of ideals and is a similar generalization of Buchberger's algorithm as Sims' function GRÖBNER on page 15. The resemblance of the ideas used in Sims' approach to Laurent polynomials and our approach restricted to free Abelian groups suggests that this is a natural way to treat these classes of group rings. The possible generalizations of our reduction to nilpotent and later on polycyclic groups stress this impression.

Let us now continue to show how similar to the case of solvable polynomial rings or skew polynomial rings ([Kr93, We92]), Gröbner bases of two-sided ideals in nilpotent group rings can be characterized by right 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 fulfills one of the equivalent statements in the next theorem.

Theorem 4
For a set of polynomials $G \subseteq \mathbf{K}[\mathcal{G}]$, assuming that $\mathcal{G}$ is presented by (Σ, T) as described above, the following properties are equivalent:

1. *G is a right Gröbner basis and $\mathsf{ideal}_r(G) = \mathsf{ideal}(G)$.*
2. *For all $g \in \mathsf{ideal}(G)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$.*
3. *G is a right Gröbner basis and for all $w \in \mathcal{G}$, $g \in G$ we have $w * g \in \mathsf{ideal}_r(G)$.*
4. *G is a right Gröbner basis and for all $a \in \Sigma$, $g \in G$ we have $a * g \in \mathsf{ideal}_r(G)$.*

Proof :
$1 \Longrightarrow 2$: Since $g \in \mathsf{ideal}(G) = \mathsf{ideal}_r(G)$ and G is a right Gröbner basis, we are done.

$2 \Longrightarrow 3$: To show that G is a right Gröbner basis we have to prove $\overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$ and for all $g \in \mathsf{ideal}_r(G)$, $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$. The latter follows immediately since $\mathsf{ideal}_r(G) \subseteq \mathsf{ideal}(G)$ and hence for all $g \in \mathsf{ideal}_r(G)$ we have $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$. The inclusion $\overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} \subseteq \equiv_{\mathsf{ideal}_r(G)}$ is obvious. Hence let $f \equiv_{\mathsf{ideal}_r(G)} g$, i.e., $f - g \in \mathsf{ideal}_r(G)$. But then we have $f - g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$ and hence by lemma 9 there exists a polynomial $h \in \mathbf{K}[\mathcal{G}]$ such that $f \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} h$ and $g \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} h$, yielding $f \overset{*}{\longleftrightarrow}{}^{\mathrm{qc}}_{G} g$. Finally, $w * f \in \mathsf{ideal}(G)$ and $w * f \overset{*}{\longrightarrow}{}^{\mathrm{qc}}_{G} 0$ implies $w * f \in \mathsf{ideal}_r(G)$.

$3 \Longrightarrow 4$: This follows immediately.

$4 \Longrightarrow 1$: Since it is obvious that $\mathsf{ideal}_r(G) \subseteq \mathsf{ideal}(G)$ it remains to show that $\mathsf{ideal}(G) \subseteq \mathsf{ideal}_r(G)$ 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 $\alpha_i \in \mathbf{K}$, $g_i \in G$ and $u_i, w_i \in \mathcal{G}$. We will show by induction on $|u_i|$ that for $u_i \in \mathcal{G}$, $g_i \in G$, $u_i * g_i \in \mathsf{ideal}_r(G)$ holds. Then g also has a representation in terms of right multiples and hence lies in the right ideal generated by G as well. In case $|u_i| = 0$ we are immediately done. Hence let us assume $u_i \equiv ua$ for some $a \in \Sigma$ and by our assumption we know $a * g_i \in \mathsf{ideal}_r(G)$. Let $a * g_i = \sum_{j=1}^{m} \beta_j \cdot g'_j * v_j$ for some $\beta_j \in \mathbf{K}$, $g'_j \in G$ and $v_j \in \mathcal{G}$. Then we get $u_i * g_i = ua * g_i = u * (a * g_i) = u * (\sum_{j=1}^{m} \beta_j \cdot g'_j * v_j) = \sum_{j=1}^{m} \beta_j \cdot (u * g'_i) * v_j$ and by our induction hypothesis

$u * g_j' \in \mathsf{ideal}_r(G)$ holds for every $1 \leq j \leq m$. Therefore, we can conclude $u_i * g_i \in \mathsf{ideal}_r(G)$.

q.e.d.

Statement 4 enables a constructive approach to use procedure Right Gröbner Bases in Nilpotent Group Rings in order to compute Gröbner bases of two-sided ideals and item 2 states that such bases can be used to decide the membership problem for the two-sided ideal by using qc-reduction. The following corollary of the previous two theorems can then be the foundation of a procedure to compute two-sided Gröbner bases.

Corollary 2

For a qc-saturated set $G \subseteq \mathbf{K}[\mathcal{G}]$ the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}(F)$ we have $g \xrightarrow{*}{}^{\text{qc}}_{G} 0$.*
2. *(a) For all polynomials $f_k, f_l \in G$ we have $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\text{qc}}_{G} 0$.*

   (b) For all $a \in \Sigma$, $g \in G$ we have $a * g \xrightarrow{*}{}^{\text{qc}}_{G} 0$.

The termination of enumerating procedures for right respectively two-sided ideals is ensured by the following result.

Theorem 5

Every (right) Gröbner basis contains a finite one.

Proof :

Let F be a subset of $\mathbf{K}[\mathcal{G}]$ and G a Gröbner basis (the proof for the existence of a finite right Gröbner basis for $\mathsf{ideal}_r(F)$ is similar) of $\mathsf{ideal}(F)$, i.e., $\mathsf{ideal}(F) = \mathsf{ideal}(G) = \mathsf{ideal}_r(G)$ and for all $g \in \mathsf{ideal}(F)$ we have $g \xrightarrow{*}{}^{\text{qc}}_{G} 0$. We can assume that G is infinite as otherwise we are done. Further 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 $\mathsf{HT}(f) \geq_{\text{tup}} t$.

Each element $u \in H$ then can be viewed as an n-tuple over $\mathbf{Z}$ as it is presented by an ordered group word. But we can also view it as a 2n-tuple over $\mathbf{N}$ by representing each element $u \in \mathcal{G}$ 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 $i_l, j_l \in \mathbf{N}$ and the representing 2n-tuple is $(i_1, j_1, \ldots, i_n, j_n)$. Notice that at most one of the two exponents i_l and j_l is non-zero. Now only considering the ordered group word parts of the terms, each set 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 $w \geq_{\text{tup}} b$. 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 $\mathsf{HT}(f) \geq_{\text{tup}} \mathsf{HT}(g_t) = t$. Hence all polynomials in $\mathsf{ideal}(F)$ are qc-reducible to zero using G_B.

q.e.d.

Notice that so far our theorems only characterize special Gröbner bases which are additionally qc-saturated[17]. Of course there also exist Gröbner bases which are not qc-saturated. It is even possible to introduce interreduction for qc-reduction and to compute reduced Gröbner bases which are unique in case we demand that the polynomials are monic, i.e., they have head coefficient 1.

Definition 13
We call a set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$ **interreduced** or **reduced** with respect to $\longrightarrow^{\text{qc}}$, if no polynomial f in F is qc-reducible by the other polynomials in $F \backslash \{f\}$. $\diamond$

Theorem 6
Every (right) ideal in $\mathbf{K}[\mathcal{G}]$ contains a unique monic finite reduced right Gröbner basis.

Proof :
The proof can be done as for the ordinary polynomial ring. Let G be a finite Gröbner basis of the ideal $\imath$ which must exist by theorem 5 (the proof for the existence of a unique reduced right Gröbner basis for $\mathsf{ideal}_r(F)$ is similar). Then similar to a characterization of Buchberger's Gröbner bases by head terms the following equation holds:

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

The sets $\mathsf{HT}(G)$ and $\mathsf{HT}(\imath\backslash\{0\})$ of course depend on the presentation of $\mathcal{M}$ chosen, 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 $m \geq_{\text{tup}} m'$,

(b) for all $m \in H$ there exists no element $m' \in H\backslash\{m\}$ such that $m' <_{\text{tup}} m$, and

(c) $\{t \in \mathcal{G} \mid t \geq_{\text{tup}} \mathsf{HT}(g), g \in H\} = \{t \in \mathcal{G} \mid t \geq_{\text{tup}} \mathsf{HT}(g), g \in G\} = \mathsf{HT}(\imath\backslash\{0\})$.

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 $g \in \imath$, $g \overset{*}{\longrightarrow}{}^{\text{lpc}}_{G'} 0$ holds. Further 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-interreduce G' giving us another set of polynomials G'', we know $\mathsf{HT}(G') = \mathsf{HT}(G'')$ and this set is a Gröbner basis of $\imath$ as well since still for every $g \in \imath$, $g \overset{*}{\longrightarrow}{}^{\text{lpc}}_{G''} 0$ 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 $\imath$. Further let $f \in S \bigtriangleup G'' = (S\backslash G'') \cup (G''\backslash S)$ be a polynomial such that $\mathsf{HT}(f)$ is minimal in the set of terms $\mathsf{HT}(S \triangle G'')$. Without loss of generality we can assume that $f \in S\backslash G''$. As G'' is a Gröbner basis and $f \in \imath$ there exists a polynomial $g \in G''$ such that $\mathsf{HT}(f) \geq_{\text{tup}} \mathsf{HT}(g)$. We can even state

[17] In Sims' approach he also computes Gröbner bases which are additionally symmetrized (see page 15).

that $g \in G''\backslash S$ as otherwise S would not be lpc-interreduced. Since f was chosen such that $\mathsf{HT}(f)$ was minimal in $\mathsf{HT}(S \triangle G'')$, 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.

q.e.d.

Such reduced Gröbner bases can be computed by incorporating interreduction in to procedure Right Gröbner Bases in Nilpotent Group Rings. For more details on the subject of incorporating interreduction see [Re95], where reduced Gröbner bases are constructed with respect to prefix respectively commutative reduction.

6 Reduction in Polycyclic Group Rings

Let $\mathcal{G}$ be a polycyclic group given by a convergent PCP-presentation. As we have seen in section 2, due to the more general form of the commutation rules, lemma 5 no longer holds for right multiples. But using lemma 6 , we can define a reduction based on commutative prefixes now using left multiples which enables us to study left ideal congruences, and later on even ideal congruences.

Definition 14
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{G}]$. We say that f **left polycyclic (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 $F \subseteq \mathbf{K}[\mathcal{G}]$ is denoted by $p \longrightarrow_{F}^{\mathrm{lpc}} q$ and abbreviates $p \longrightarrow_{f}^{\mathrm{lpc}} q$ for some $f \in F$. ⋄

Notice that if f lpc-reduces p at $\alpha \cdot t$ to q, then t no longer is a term in q and by lemma 6, $p > q$ holds. This reduction is effective, as it is possible to decide, whether we have $t \geq_{\mathrm{tup}} \mathsf{HT}(f)$. Further it is Noetherian and the translation lemma holds.

Lemma 13
Let F be a set of polynomials in $\mathbf{K}[\mathcal{G}]$ and $p, q, h \in \mathbf{K}[\mathcal{G}]$ some polynomials.

1. *Let $p - q \longrightarrow_{F}^{\mathrm{lpc}} h$. Then there are polynomials $p', q' \in \mathbf{K}[\mathcal{G}]$ 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 $g \in \mathbf{K}[\mathcal{G}]$ such that $p \overset{*}{\longrightarrow}_{F}^{\mathrm{lpc}} g$ and $q \overset{*}{\longrightarrow}_{F}^{\mathrm{lpc}} g$.*

Proof :
This can be shown as lemma 9.

q.e.d.

Gröbner bases as defined by Buchberger can now be specified for left ideals in this setting as before.

Definition 15
A set $G \subseteq \mathbf{K}[\mathcal{G}]$ is said to be a **left Gröbner basis**, if $\overset{*}{\longleftrightarrow}{}^{\mathrm{lpc}}_{G} = \equiv_{\mathsf{ideal}_l(G)}$, and $\longrightarrow^{\mathrm{lpc}}_{G}$ is confluent. $\diamond$

Again we find that in our setting we have to be more careful, as for lpc-reduction $\overset{*}{\longleftrightarrow}{}^{\mathrm{lpc}}_{G} = \equiv_{\mathsf{ideal}_l(G)}$ in general does not hold. One reason for this phenomenon is that a reduction step is not preserved under left multiplication with elements of $\mathcal{G}$.

Example 9
Let $\mathbf{Q}[\mathcal{G}]$ be the group ring given in example 5. Then similar to example 7 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 $a^{-1} + \lambda \overset{*}{\longleftrightarrow}{}^{\mathrm{lpc}}_{p} 0$ does not hold. $\diamond$

We will now introduce how we can extend the expressiveness of lpc-reduction. We start by enabling the reducibility of special monomial multiples of a polynomial by allowing to use not only the polynomial itself but a special set of polynomial multiples for lpc-reduction. First let us take a look at what multiples are appropriate to later on enable an effective characterization of a left Gröbner basis. We proceed similar to the case of qc-reduction for nilpotent groups rings.

Lemma 14
Let p be a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$. Then it is decidable for $t \in \mathsf{T}(p)$ whether there exists an element $w \in \mathcal{G}$ such that $\mathsf{HT}(w * p) = w \circ t$.

Proof :
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: In case there exists $w \in \mathcal{G}$ such that for some $t_i \in T \backslash \{t_1\}$ we have $w \circ t_i \succ w \circ t_j$ for all $t_j \in T \backslash \{t_i\}$, then we can effectively construct $v \in \mathcal{G}$ such that $v \circ t_i \succ v \circ t_j$ for all $t_j \in T \backslash \{t_i\}$ 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 $1_n >_{\mathbf{Z}} i_n$. By our assumption there exists $w \in \mathcal{G}$ with $w \equiv w' a_n^{w_n}$, $w' \in \mathsf{ORD}(\Sigma \backslash \Sigma_n)$ such that $w \circ t_i \succ w \circ t_j$ must hold for all $t_j \in T \backslash \{t_i\}$. 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 $t_j \in T \backslash \{t_i\}$ we have $-1_n + i_n >_{\mathbf{Z}} -1_n + j_n$. The case $t_j = t_1$ is trivial and for each $t_j \in T \backslash \{t_1, t_i\}$ the equation is a consequence of lemma 3 as we have $1_n >_{\mathbf{Z}} i_n$, $1_n >_{\mathbf{Z}} j_n$ and as seen above there exists an element x, namely w_n, such that $1_n + x <_{\mathbf{Z}} i_n + x$ and $j_n + x <_{\mathbf{Z}} i_n + x$. Now in case a_n is bounded by $m_n \in \mathbf{N}$ we can set $v \equiv a_n^{m_n - i_n - 1}$. We find that since for

all $t_j \in T \backslash \{t_i\}$, 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 $t_j \in T \backslash \{t_i\}$. 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 $w' \in \mathsf{ORD}(\Sigma \backslash \Sigma_{n-k})$, $w'' \in \mathsf{ORD}(\{a_{n-k+1}, \ldots, a_{d-1}\})$, $w''' \in \mathsf{ORD}(\Sigma_{d+1})$. As before let us first consider the case that the letter a_d is not bounded. Then there exist $l_{n-k}, \ldots, l_{d-1}, x \in \mathbf{Z}$, $z_1, z_i \in \mathsf{ORD}(\Sigma_{d+1})$ 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 $t_j \in T \backslash \{t_1, t_i\}$. In case 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 $j_s <_{\mathbf{Z}} i_s = 1_s$ respectively $j_d <_{\mathbf{Z}} i_d <_{\mathbf{Z}} 1_d$ 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 $x_i \in \mathsf{ORD}(\Sigma \backslash \Sigma_s)$, $y_i, y_j \in \mathsf{ORD}(\Sigma_{s+1})$ 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 $y_j \in T' \backslash \{y_i\}$. 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 $t_j \in T \backslash \{t_i\}$ 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 $t_j \in T \backslash \{t_i\}$.

q.e.d.

Notice that the proof of this lemma shows that there is an algorithm which computes some $v \in \mathcal{G}$ as desired in case it exists and that the element w need not be known for this computation. Hence we can enrich a polynomial by the set of those multiples which bring other terms of the polynomial to head position. But still there remain cases of multiples which are not lpc-reducible. 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, as a^2 is no commutative prefix of a. Therefore, let us consider some further special multiples. For a polynomial p and a term $t \in \mathsf{T}(p)$ we call a term s in a multiple $w * p$ a **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 9 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 15
For $u, v \in \mathcal{G}$, let $u * p$ and $v * p$ be two left multiples of a non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$ such that for some term $t \in \mathsf{T}(p)$ the head terms are t-terms, i.e., $\mathsf{HT}(u * p) = u \circ t \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(v * p) = v \circ t \equiv a_1^{j_1} \dots a_n^{j_n}$. Then there exists a term $\tilde{t} \leq_{\mathrm{tup}} a_1^{\rho_1} \dots a_n^{\rho_n}$ 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 $u * p \xrightarrow{\mathrm{lpc}}_{\tilde{z} * p} 0$ and $v * p \xrightarrow{\mathrm{lpc}}_{\tilde{z} * p} 0$.

Proof :
Let p, $p * u$ and $p * v$ be as described in the lemma and let the letters corresponding to our presentation be $\Sigma = \{a_1, \dots, a_n, a_1^{-1}, \dots, a_n^{-1}\}$.

We show the existence of $\tilde{z}$ by constructing a sequence $z_1, \dots, z_n \in \mathcal{G}$, such that for $1 \leq l \leq n$ we have $\mathsf{HT}(z_l * p) = z_l \circ t \equiv a_1^{s_1} \dots a_l^{s_l} r_l$ with $r_l \in \mathsf{ORD}(\Sigma_{l+1})$ and $a_1^{s_1} \dots a_l^{s_l} \leq_{\mathrm{tup}} a_1^{\rho_1} \dots a_l^{\rho_l}$. 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 $a_1^{s_1} \leq_{\mathrm{tup}} a_1^{\rho_1}$.
In case $i_1 = j_1$ or $j_1 = 0$ we can set $z_1 = v$ and $s_1 = j_1 = \rho_1$ since $\mathsf{HT}(v * p) = v \circ t \equiv a_1^{j_1} \dots a_n^{j_n}$. Similarly in case $i_1 = 0$ we can set $z_1 = u$ and $s_1 = i_1 = 0 = \rho_1$ since $\mathsf{HT}(u * p) = u \circ t \equiv a_2^{i_2} \dots a_n^{i_n} \in \mathsf{ORD}(\Sigma_2)$. 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. In case $|j_1| > |i_1|$ 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. In case 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 14 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 $s' \equiv a_1^{b_{s'}} x_{s'}$, $b_{s'} \in \mathbf{Z}$, $x_{s'} \in \mathsf{ORD}(\Sigma_2)$ for the terms $s' \in \mathsf{T}(p)$ and $\mathsf{HT}(p) = s \equiv a_1^{b_s} x_s$. Then we know $b_s \geq_{\mathbf{Z}} b_t$ since $t \in \mathsf{T}(p)$.
Hence in showing that the case $b_s >_{\mathbf{Z}} b_t$ 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 $x \in \mathbf{Z}$ 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 $x \in \mathbf{Z}$ 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 sign.
It remains to show that there cannot exist a term $s' \in \mathsf{T}(p)$ with $b_{s'} <_{\mathbf{Z}} b_s = b_t$. Let us assume such an s' exists. Since $\mathsf{HT}(u*p) = u \circ t \equiv a_1^{i_1} \dots a_n^{i_n}$ and $\mathsf{HT}(v*p) = v \circ t \equiv a_1^{j_1} \dots a_n^{j_n}$ there then must exist $x_1, x_2 \in \mathbf{Z}$ such that $b_{s'} + x_1 <_{\mathbf{Z}} b_t + x_1 = i_1$ and $b_{s'} + x_2 <_{\mathbf{Z}} b_t + x_2 = j_1$. Without loss of generality let us assume $i_1 > 0$ and $j_1 < 0$ (the other case is symmetric). In case $b_t < 0$ we get that $b_t + x_1 = i_1 > 0$ implies $x_1 > |b_t| > 0$. Now, as $b_{s'} <_{\mathbf{Z}} b_t$ 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 $b_{s'} + x_1 <_{\mathbf{Z}} b_t + x_1$. On the other hand, in case $b_t > 0$ 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 $b_{s'} + x_2 <_{\mathbf{Z}} b_t + x_2$.
Thus let us assume that for the letter a_{k-1} we have constructed $z_{k-1} \in \mathcal{G}$ such that $\mathsf{HT}(z_{k-1} * p) = z_{k-1} \circ t \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} r_{k-1} \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ with $r_{k-1} \in \mathsf{ORD}(\Sigma_k)$, $r' \in \mathsf{ORD}(\Sigma_{k+1})$ and $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} \leq_{\text{tup}} a_1^{\rho_1} \dots a_{k-1}^{\rho_{k-1}}$. 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 in case $a_k^{\tilde{\rho}_k} \leq_{\text{tup}} a_k^{\rho_k}$ we are done and set $z_k = w_1 \circ z_{k-1}$ and $s_k = \tilde{s}_k$. Else we can similarly proceed for the polynomials $v * p$ and $w_1 * z_{k-1} * p$ with head terms $a_1^{j_1} \dots a_n^{j_n}$ respectively $a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{\tilde{s}_k} \tilde{r}$ 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 case $s_k = 0$ we are immediately done 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 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[18]. Then in case $|i_k| \geq |l_k|$ we are done by setting $w_1 = \lambda$ as again

[18] In case 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.

$\mathsf{HT}(z_{k-1} * p) = z_{k-1} \circ t \equiv a_1^{s_1} \dots a_{k-1}^{s_{k-1}} a_k^{l_k} r'$ 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 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 14 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 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 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 $c_k \geq_{\mathbf{Z}} i_k$. 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 $c_k \leq_{\mathbf{Z}} i_k$ and thus $i_k \leq_{\mathbf{Z}} c_k$ 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., $c_k = b_s - l_k$. In case this head term is already the corresponding t-term $y \circ z_{k-1} \circ t$, we are done and we set $w_1 = y$ and $\tilde{s}_k = 0 = \tilde{\rho}_k$. Now if we can show $c_k = 0$, by lemma 14 the t-term $y \circ z_{k-1} \circ t$ can be brought to head position using an element as constructed in lemma 14 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 $c_k = 0$ we are done. 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 $c_k + i_k \leq_{\mathbf{Z}} i_k$. 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 $b_s \leq_{\mathbf{Z}} l_k$. In case $i_k = 0$, we have $c_k \leq_{\mathbf{Z}} 0$ implying $c_k = 0$. In case $i_k > 0$ then $c_k + i_k = b_s - l_k + i_k \leq_{\mathbf{Z}} i_k$ 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 inequation can only hold in case $c_k = b_s - l_k = 0$.

q.e.d.

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 (lpc-) saturation. In example 9 the multiples $a^{-1} * p = a + \lambda$ and $a^{-2} * p = a^{-1} + \lambda$ give us a lpc-saturating set for $p = a^2 + a$.

Definition 16
A set $S \subseteq \{w * p \mid w \in \mathcal{G}\}$ is called a **(lpc-) saturating set** for a non-zero polynomial p in $\mathbf{K}[\mathcal{G}]$, if for all $w \in \mathcal{G}$, $w * p \longrightarrow^{\text{lpc}}_{S} 0$. A set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$ is called **(lpc-) saturated**, if for all $f \in F$ and for all $w \in \mathcal{G}$, $w * f \longrightarrow^{\text{lpc}}_{F} 0$. ◇

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

Procedure Left-Polycyclic Saturation

Given: A non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$.
Find: Sat(p), a lpc-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 $\mathsf{HT}(w * p) = w \circ t$
             $H_t := \{s \in \mathcal{G} \mid \mathsf{HT}(q) \geq_{\text{tup}} s\}$;
             % 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
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 more structural information should be used, e.g. to rule out unnecessary candidates from the sets H_t.

Lemma 16
For a lpc-saturated set F of polynomials in $\mathbf{K}[\mathcal{G}]$, $\overset{*}{\longleftrightarrow}^{\text{lpc}}_{F} \; = \; \equiv_{\mathsf{ideal}_l(F)}$ holds.

Proof :
This can be shown as in the proof of lemma 12.

q.e.d.

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

Definition 17
For $p_1, p_2 \in \mathbf{K}[\mathcal{G}]$ such that $\mathsf{HT}(p_1) \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $\mathsf{HT}(p_2) \equiv a_1^{j_1} \ldots a_n^{j_n}$ with either $i_l \cdot j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ for $1 \leq l \leq n$ we can define an **s-polynomial**, and setting

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

the situation $a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}} = w_1 \circ \mathsf{HT}(p_1) = w_2 \circ \mathsf{HT}(p_2)$ 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 $\mathsf{HT}(p_i) \leq_{\text{tup}} a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$ for $i \in \{1, 2\}$ holds in case such an s-polynomial exists. Furthermore, if there exists a term t such that $t \geq_{\text{tup}} \mathsf{HT}(p_1) \equiv a_1^{i_1} \ldots a_n^{i_n}$ and $t \geq_{\text{tup}} \mathsf{HT}(p_2) \equiv a_1^{j_1} \ldots a_n^{j_n}$, an s-polynomial always exists since then the condition for its existence 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 $t \geq_{\text{tup}} a_1^{\rho_1 \cdot \max\{|i_1|,|j_1|\}} \ldots a_n^{\rho_n \cdot \max\{|i_n|,|j_n|\}}$.

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

Theorem 7
For a lpc-saturated set $G \subseteq \mathbf{K}[\mathcal{G}]$ the following statements are equivalent:

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

Proof :
Again we can follow the lines of the proof given for the similar theorem 3 for nilpotent groups and qc-reduction.

q.e.d.

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

Corollary 3
For a set $G \subseteq \mathbf{K}[\mathcal{G}]$ the following statements are equivalent:

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

Now, using the characterization given in theorem 7 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 $F \subseteq \mathbf{K}[\mathcal{G}]$.
Find: $\textsc{Gb}_l(F)$, a left Gröbner basis of $\mathsf{ideal}_l(F)$.

```
$G := \bigcup_{g \in G} \textsc{Sat}(g)$;   % $G$ is lpc-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 7 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$(h, \xrightarrow{\text{lpc}}_G)$;   % Compute a normal form
             if $h' \neq 0$   % The s-polynomial does not reduce to zero
                 then $G := G \cup \textsc{Sat}(h')$; % $G$ is lpc-saturated and $\mathsf{ideal}_l(F) = \mathsf{ideal}_l(G)$
                      $B := B \cup \{(f, g) \mid f \in G, g \in \textsc{Sat}(h')\}$;
             endif
    endif
endwhile
$\textsc{Gb}_l(F) := G$
```

The set G enumerated by this naive procedure fulfills the requirements of theorem 7, i.e., the set G at each stage generates $\mathsf{ideal}_l(F)$ and is lpc-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 in case they exist. Hence, in case 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.

Theorem 8
Every left Gröbner basis contains a finite one.

Proof :
Since lpc-reduction is based on commutative prefixes this can be shown using Dickson's lemma as in the proof of theorem 5.

q.e.d.

Let us now continue to show how again 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 fulfills one of the equivalent statements in the next theorem.

Theorem 9
For a set of polynomials $G \subseteq \mathbf{K}[\mathcal{G}]$, 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 $g \xrightarrow{*}{}^{\mathrm{lpc}}_{G} 0$.*

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 $g * a \in \mathsf{ideal}_l(G)$.*

Proof :
This can be shown as in the proof of theorem 4.

q.e.d.

Statement 4 enables a constructive approach to use procedure Left Gröbner Bases in Polycyclic Group Rings in order to compute Gröbner bases of two-sided ideals and item 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 7 can be used as the foundation of a procedure to compute two-sided Gröbner bases.

Corollary 4
For a lpc-saturated set $G \subseteq \mathbf{K}[\mathcal{G}]$ the following statements are equivalent:

1. *For all polynomials $g \in \mathsf{ideal}(G)$ we have $g \xrightarrow{*}{}^{\mathrm{lpc}}_{G} 0$.*

2. (a) *For all polynomials $f_k, f_l \in G$ we have $\mathsf{spol}(f_k, f_l) \xrightarrow{*}{}^{\mathrm{lpc}}_{G} 0$.*

   (b) *For all $a \in \Sigma$, $g \in G$ we have $g * a \xrightarrow{*}{}^{\mathrm{lpc}}_{G} 0$.*

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

Corollary 5
Every Gröbner basis contains a finite one.

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

Definition 18
We call a set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$ **interreduced** or **reduced** with respect to $\longrightarrow^{\mathrm{lpc}}$, if no polynomial f in F is lpc-reducible by the other polynomials in $F \backslash \{f\}$. $\diamond$

Theorem 10
Every (left) ideal in $\mathbf{K}[\mathcal{G}]$ contains a unique monic finite reduced (left) Gröbner basis.

Proof :
The proof again can be done using standard techniques as in the case of ordinary polynomial rings.

q.e.d.

Such reduced Gröbner bases can be computed by incorporating interreduction into the respective procedures.

Let us close this section by sketching a possible approach to treat right ideals in polycyclic group rings. As seen in section 2 a stability property for right multiples need not hold when using the idea of commutative prefixes for reduction if $\mathcal{G}$ is given by a convergent PCP-presentation. Furthermore, Wißmann's result given in section 4 for the existence of only λ-confluent bases in case the group is given by a convergent PCP-system, states that in general no finite Gröbner bases will exist when using weakenings of strong reduction and every reduction based on commutative prefixes and using right multiples is such a weakening. Anyhow, a similar approach is possible in case we change the presentation of our polycyclic group. Let (Σ, T) be a convergent PCP-presentation of a polycyclic group. Then the presentation $(\Sigma, \rho(T))$, where $\rho(T) = \{\rho(l) \longrightarrow \rho(r) \mid l \longrightarrow r \in T\}$ and $\rho(\lambda) = \lambda$, $\rho(wa) = a\rho(w)$, is again a polycyclic power presentation which is convergent[19] with respect to the syllable ordering now with status right, i.e., the syllables are compared from the right to the left. Such a presentation will be called a **reversed polycyclic power commutation presentation** (with status right). The irreducible elements now are reversed ordered words of the form $a_n^{i_n} \dots a_1^{i_1}$, i.e., $\mathsf{REVORD}(\Sigma) = \mathsf{REVORD}(\Sigma_1)$, where we define $\mathsf{REVORD}(\Sigma_i)$ recursively by $\mathsf{REVORD}(\Sigma_{n+1}) = \{\lambda\}$, and $\mathsf{REVORD}(\Sigma_i) = \{w \in \Sigma_i^* \mid w \equiv vu$ for some $u \in \{a_i\}^* \cup \{a_i^{-1}\}^*, v \in \mathsf{REVORD}(\Sigma_{i+1})\}$. We can show similar properties as in the case of Wißmann's PCP-presentations.

Lemma 17
Let $\mathcal{G}$ be a polycyclic group with (Σ, T) a convergent reversed polycyclic power commutation presentation with status right. Further for some $1 \leq i < n$ let $w \in \mathsf{REVORD}(\Sigma_{i+1})$. Then we have $a_i \circ w \equiv z a_i$ for some $z \in \mathsf{REVORD}(\Sigma_{i+1})$.

Based on the form of the rules occurring in the presentation of $\mathcal{G}$ we can again prove stability for certain right multiples. From now on we will always assume that $\mathcal{G}$ is presented by a convergent reversed polycyclic power commutation system with status right.

Lemma 18
Let $\mathcal{G}$ be a group presented by a convergent reversed polycyclic power commutation system with status right and $w, v, \tilde{v} \in \mathcal{G}$ with $w \geq_{\text{tup}} v$ 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 $u = \mathsf{inv}(v) \circ w$.

The proof of this lemma and the ones follwing in the remaining part of this section follow the lines of the proofs given for the comparable facts for lpc-reduction due to the symmetrical situation provided by the form of the reversed presentation of $\mathcal{G}$. We now proceed to study an appropriate reduction based on commutative prefixes for this setting.

Definition 19
Let p, f be two non-zero polynomials in $\mathbf{K}[\mathcal{G}]$. We say that f **right polycyclic (rpc-) reduces** p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow_f^{\text{rpc}} q$, if

(a) $t \geq_{\text{tup}} \mathsf{HT}(f)$, and

[19] For a proof of this see section 8.

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

Rpc-reduction by a set $F \subseteq \mathbf{K}[\mathcal{G}]$ is denoted by $p \longrightarrow^{\text{rpc}}_{F} q$ and abbreviates $p \longrightarrow^{\text{rpc}}_{f} q$ for some $f \in F$. ⋄

Notice that if f rpc-reduces p at $\alpha \cdot t$ to q, then t no longer is a term in q and by lemma 18, $p > q$ holds. This reduction is effective, as it is possible to decide, whether we have $t \geq_{\text{tup}} \mathsf{HT}(f)$. Further it is Noetherian and the translation lemma holds.

Lemma 19
Let F be a set of polynomials in $\mathbf{K}[\mathcal{G}]$ and $p, q, h \in \mathbf{K}[\mathcal{G}]$ some polynomials.

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

Gröbner bases as defined by Buchberger can now be specified for right ideals in this setting as follows.

Definition 20
A set $G \subseteq \mathbf{K}[\mathcal{G}]$ is said to be a **Gröbner basis with respect to rpc-reduction**, if $\overset{*}{\longleftrightarrow}^{\text{rpc}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$, and $\longrightarrow^{\text{rpc}}_{G}$ is confluent. ⋄

As before, in general we do not have the property $\overset{*}{\longleftrightarrow}^{\text{rpc}}_{G} = \equiv_{\mathsf{ideal}_r(G)}$, but it can be restored by saturation due to the following lemmata:

Lemma 20
Let p be a non-zero polynomial in $\mathbf{K}[\mathcal{G}]$. Then it is decidable whether for $t \in \mathsf{T}(p)$ there exists an element $w \in \mathcal{G}$ such that $\mathsf{HT}(p * w) = t \circ w$.

Lemma 21
For $u, v \in \mathcal{G}$, let $p*u$ and $p*v$ be two right multiples of a non-zero polynomial $p \in \mathbf{K}[\mathcal{G}]$ such that for some term $t \in \mathsf{T}(p)$ the head terms are t-terms, i.e., $\mathsf{HT}(p * u) = t \circ u \equiv a_n^{i_n} \dots a_1^{i_1}$ and $\mathsf{HT}(p * v) = t \circ v \equiv a_n^{j_n} \dots a_1^{j_1}$. Then there exists a term $\tilde{t} \leq_{\text{tup}} a_n^{\rho_n} \dots a_1^{\rho_1}$ 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 $\mathsf{HT}(p * \tilde{z}) = t \circ \tilde{z} = \tilde{t}$. In particular, we have $p * u \longrightarrow^{\text{rpc}}_{p*\tilde{z}} 0$ and $p * v \longrightarrow^{\text{rpc}}_{p*\tilde{z}} 0$.

Definition 21
A set $S \subseteq \{p * w \mid w \in \mathcal{G}\}$ is called an **(rpc-) saturating set** for a non-zero polynomial p in $\mathbf{K}[\mathcal{G}]$, if for all $w \in \mathcal{G}$, $p * w \longrightarrow^{\text{rpc}}_{S} 0$. A set of polynomials $F \subseteq \mathbf{K}[\mathcal{G}]$ is called **(rpc-) saturated**, if for all $f \in F$ and for all $w \in \mathcal{G}$, $f * w \longrightarrow^{\text{rpc}}_{F} 0$. ⋄

Lemma 22
For a rpc-saturated set F of polynomials in $\mathbf{K}[\mathcal{G}]$, $\overset{*}{\longleftrightarrow}{}^{\text{rpc}}_{F} = \equiv_{\mathsf{ideal}_r(F)}$ holds.

Now it remains to give a confluence criteria which can be done using s-polynomials a usual.

Definition 22
For $p_1, p_2 \in \mathbf{K}[\mathcal{G}]$ such that $\mathsf{HT}(p_1) \equiv a_n^{i_n} \dots a_1^{i_1}$ and $\mathsf{HT}(p_2) \equiv a_n^{j_n} \dots a_1^{j_1}$ with either $i_l \cdot j_l = 0$ or $\mathsf{sgn}(i_l) = \mathsf{sgn}(j_l)$ for $1 \leq l \leq n$, we can define an **s-polynomial**, and setting

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

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

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

◇

Theorem 11
For a saturated set $G \subseteq \mathbf{K}[\mathcal{G}]$ the following statements are equivalent:

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

Procedures to compute rpc-saturating sets and Gröbner bases with respect to rpc-reduction can be given as in the case of lpc-reduction before. Again the concept of interreduction can be supplied to yield unique monic reduced Gröbner bases, and it is possible to characterize two-sided ideals by right ideals using the same ideas as cited before.

Let us close this section by showing how in fact reversed polycyclic power commutation presentations and rpc-reduction yield a solution to the subgroup problem in polycylic groups giving rise to confluent bases of the subgroup.

Example 10
Let $\mathcal{G}$ be the group specified on page 20 now presented by a convergent *reversed* polycyclic power commutation presentation assuming a syllable ordering with precedence $a_1^{-1} \succ a_1 \succ a_2^{-1} \succ a_2 \succ a_3^{-1} \succ a_3$ and status right, $\Sigma = \{a_1, a_1^{-1}, a_2, a_2^{-1}, a_3, a_3^{-1}\}$, $T = \{a_1 a_1^{-1} \longrightarrow \lambda, a_1^{-1} a_1 \longrightarrow \lambda, a_2 a_2^{-1} \longrightarrow \lambda, a_2^{-1} a_2 \longrightarrow \lambda, a_3 a_3^{-1} \longrightarrow \lambda, a_3^{-1} a_3 \longrightarrow \lambda, a_1 a_3 \longrightarrow a_3 a_2 a_1, a_1^{-1} a_3 \longrightarrow a_3 a_2^{-1} a_1^{-1}, a_1 a_3^{-1} \longrightarrow a_3^{-1} a_2^{-1} a_1, a_1^{-1} a_3^{-1} \longrightarrow a_3^{-1} a_2 a_1^{-1}, a_1^{\delta} a_2^{\delta'} \longrightarrow a_2^{\delta'} a_1^{\delta}, a_2^{\delta} a_3^{\delta'} \longrightarrow a_3^{\delta'} a_2^{\delta} \mid \delta, \delta' \in \{1, -1\}\}$. Then for the right ideal generated by $P_U = \{a_2 - 1, a_3 - 1\}$ the set $G = \{a_2 - 1, a_2^{-1} - 1, a_3 - 1, a_3^{-1} - 1\}$ is a Gröbner basis corresponding to the subgroup generated by U. While in the setting of example 4 the elements $a_2^{-1} \circ a_3 \circ a_1$ and a_1 have no common descendant with respect to $\Longrightarrow_U$, now we find that the normal form $a_3 a_2^{-1} a_1$ of the element $a_2^{-1} \circ a_3 \circ a_1$ is reducible by G as follows: $a_3 a_2^{-1} a_1 \longrightarrow^{\text{rpc}}_{a_3 - 1} a_2^{-1} a_1 \longrightarrow^{\text{rpc}}_{a_2^{-1} - 1} a_1$. Hence now $a_3 a_2^{-1} a_1$ and a_1 are clearly joinable. ◇

7 Concluding Remarks

In this paper we have shown how Gröbner basis methods can be successfully introduced to nilpotent respectively polycyclic group rings. We have illustrated how depending on the respective group presentations commutative divisors can be used to define Noetherian reductions. Left ideals can be handled by so called lpc-reduction using convergent PCNI- as well as PCP-systems for presenting the group. For right ideals we have to be more careful. While the collecting process induced by convergent PCNI-presentations allows to define a Noetherian reduction using right multiples, this cannot be generalized for convergent PCP-systems. Hence we have introduced reversed PCP-systems with status right and in this setting again reduction can be specified. The results can be summarized as follws:

Group presentation	*left GBs*	*right GBs*	*two-sided GBs*
PCNI-system	$\longrightarrow^{\mathrm{lpc}}$	$\longrightarrow^{\mathrm{qc}}$	$\longrightarrow^{\mathrm{qc}}$ $\longrightarrow^{\mathrm{lpc}}$
PCP-system	$\longrightarrow^{\mathrm{lpc}}$	none[20]	$\longrightarrow^{\mathrm{lpc}}$
reversed PCP-system	none	$\longrightarrow^{\mathrm{rpc}}$	$\longrightarrow^{\mathrm{rpc}}$

In [Re95] we have shown how the theory of Gröbner bases in monoid and group rings over fields can be lifted to monoid and group rings over reduction rings fulfilling special axioms, e.g., allowing to compute finite Gröbner bases for ideals in the coefficient domain. Hence the results of this paper also hold for nilpotent respectively polycyclic group rings over reduction rings, e.g., the integers $\mathbf{Z}$.

Finally we want to sketch how the results of this report can be lifted to group rings over nilpotent-by-finite respectively polycyclic-by-finite groups. Essential in this approach is the use of semi-Thue systems related to extensions of groups as introduced for context-free groups by Cremanns and Otto in [CrOt94]. Details of the lifting process for respective group rings can be found in [Re95] and [MaRe96]. The key idea is to combine a convergent presentation $(\Sigma_{\mathcal{E}}, T_{\mathcal{E}})$ of a finite group $\mathcal{E}$ with a convergent PCNI-presentation respecitively PCP-presentation of a nilpotent respectively polycyclic group $\mathcal{N}$ presented by $(\Sigma_{\mathcal{N}}, T_{\mathcal{N}})$. Assuming $\Sigma_{\mathcal{E}} \cap \Sigma_{\mathcal{N}} = \emptyset$, let $\Sigma = \Sigma_{\mathcal{E}} \cup \Sigma_{\mathcal{N}}$ and let T consist of the set of rules $T_{\mathcal{N}}$, and the following additional rules:

$$\begin{array}{lcll} l & \longrightarrow & rw_r & \text{for all } l \longrightarrow r \in T_{\mathcal{E}}, \text{ where } w_r \in \Sigma_{\mathcal{N}}^* \cap \mathrm{IRR}(T_{\mathcal{N}}), \\ xa & \longrightarrow & aw_x & \text{for all } a \in \Sigma_{\mathcal{E}}, \text{ for all } x \in \Sigma_{\mathcal{N}}, \text{ where } w_a \in \Sigma_{\mathcal{N}}^* \cap \mathrm{IRR}(T_{\mathcal{N}}). \end{array}$$

Then in case (Σ, T) is convergent it is called the extension presentation of $\mathcal{G}$ as an extension of $\mathcal{N}$ by $\mathcal{E}$ (see e.g. [Cr95]). Every element in $\mathcal{G}$ has a representative of the form eu where $e \in \mathcal{E}$ and $u \in \mathcal{N}$. We can specify a total well-founded ordering $\succ$ on our group by combining a total well-founded ordering $\succeq_{\mathcal{E}}$ on $\mathcal{E}$ and the syllable ordering $\geq_{\mathrm{syll}}$ on $\mathcal{N}$: For $e_1u_1, e_2u_2 \in \mathcal{G}$ we define $e_1u_1 \succ e_2u_2$ if and only if $e_1 \succ_{\mathcal{E}} e_2$ or ($e_1 = e_2$ and $u_1 >_{\mathrm{syll}} u_2$). Furthermore, we can lift the tuple ordering to $\mathcal{G}$ as follows: For two elements eu, ev, we

[20] "none" in this context means that no reduction based on commutative divisors and using right multiples exists.

define $eu \geq_{\text{tup}} ev$ if $u >_{\text{tup}} v$ and we define $eu >_{\text{tup}} \lambda$. According to this ordering we call ev a (commutative) **prefix** of eu if $v \leq_{\text{tup}} u$ and introducing the concept of $\mathcal{E}$-closure as in [Re95] or [MaRe96] we can proceed to prove lemmata and theorems similar to those in section 5 and 6.

References

[ApLa88] J. Apel and W. Lassner. *An Extension of Buchberger's Algorithm and Calculations in Enveloping Fields of Lie Algebras.* Journal of Symbolic Computation(1988) 6. pp 361-370.

[BaCaMi81] G. Baumslag, F. Cannonito and C. Miller, III. *Computable Algebra and Group Embeddings.* Journal of Algebra 69(1981). pp 186-212.

[BeWe92] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra.* Springer Verlag(1992).

[Bu65] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal.* Dissertation. Universität Innsbruck. 1965.

[BoOt93] R. Book and F. Otto. *String-Rewriting Systems.* Springer Verlag(1993).

[Cr95] R. Cremanns. *Finiteness Conditions for Rewriting Systems.* PhD Thesis. Kassel. 1995.

[CrOt94] R. Cremanns and F. Otto. *Constructing Canonical Presentations for Subgroups of Context-Free Groups in Polynomial Time.* Proc. ISSAC'94.

[KaMe79] M.I. Kargapolov and Ju.I. Merzljakov. *Fundamentals of the Theory of Groups.* Springer Verlag(1979).

[KaWe90] A. Kandri-Rody and V. Weispfenning. *Non-Commutative Gröbner Bases in Algebras of Solvable Type.* Journal of Symbolic Computation 9(1990). pp 1-26.

[Kr93] H. Kredel. *Solvable Polynomial Rings.* Verlag Shaker, Aachen. 1993.

[La85] W. Lassner. *Symbol Representations of Noncommutative Algebras.* EUROCAL'85. Springer LNCS 204, pp. 99-115.

[MaOt89] K. Madlener and F. Otto. *About the Descriptive Power of Certain Classes of Finite String-Rewriting Systems.* Theoretical Computer Science 67(1989). pp 143-172.

[MaRe93a] K. Madlener and B. Reinert. *On Gröbner Bases in Monoid and Group Rings.* SEKI Report SR-93-08. Universität Kaiserslautern.

[MaRe93b] K. Madlener and B. Reinert. *Computing Gröbner Bases in Monoid and Group Rings.* Proc. ISSAC'93. pp 254-263.

[MaRe96] K. Madlener and B. Reinert. *A Generalization of Gröbner Bases Algorithms to Nilpotent Group Rings.* to appear in AAECC.

[Mo85] F. Mora. *Gröbner Bases for Non-Commutative Polynomial Rings.* Proc. AAECC-3(1985). Springer LNCS 229. pp 353-362

[Mo94] T. Mora. *An Introduction to Commutative and Non-Commutative Gröbner Bases.* Theoretical Computer Science 134(1994). pp 131-173.

[Re95] B. Reinert. *Gröbner Bases in Monoid and Group Rings* PhD Thesis. Universität Kaiserslautern. 1995

[Ro93] A. Rosenmann. *An Algorithm for Constructing Gröbner and Free Schreier Bases in Free Group Algebras.* Journal of Symbolic Computation 16(1993). pp 523-549.

[Si94] C. Sims. *Computation with finitely presented groups.* Cambridge University Press 1994.

[We87] V. Weispfenning. *Gröbner Basis for Polynomial Ideals over Commutative Regular Rings.* Proc. EUROCAL'87. Springer LNCS 378. pp 336-347.

[We92] V. Weispfenning. *Finite Gröbner Bases in Non-Noetherian Skew Polynomial Rings.* Proc. ISSAC'92. pp 329-334.

[Wi89] D. Wißmann. *Anwendung von Rewriting-Techniken in polyzyklischen Gruppen.* Dissertation. Universität Kaiserslautern. 1989.

8 Appendix

In this section we show that polycyclic groups have reversed polycyclic power commutation presentations which are convergent with respect to a syllable ordering with status right.

Let $\mathcal{G}$ be a polycyclic group with (Σ, T) a convergent PCP-system as described in section 2. For the set of rules T we define $\rho(T) = \{\rho(l) \longrightarrow \rho(r) \mid l \longrightarrow r \in T\}$ and $\rho(\lambda) = \lambda$, $\rho(wa) = a\rho(w)$, $a \in \Sigma$, $w \in \Sigma^*$. It is easily seen that this rewriting system is terminating with respect to the syllable ordering with status right induced by the precedence $a_1^{-1} \succ a_1 \succ \ldots \succ a_n^{-1} \succ a_n$. In order to show (local) confluence we will need the following fact:

> *If $a_1^{i_1} \ldots a_n^{i_n}$ is the normal form of x with respect to T, then $a_n^{i_n} \ldots a_1^{i_1}$ is a normal form of $\rho(x)$ with respect to $\rho(T)$.*

This is due to the fact that in case $x \longrightarrow_{(l,r)\in T} y$ then there exists a rule $(\rho(l), \rho(r))$ in $\rho(T)$ such that $\rho(x) \longrightarrow_{(\rho(l),\rho(r))} \rho(y)$.

Now to see that our system $(\Sigma, \rho(T))$ is confluent we take a closer look at possible critical pairs. Such pairs are due to the following two possible overlaps of rules $(\rho(l_1), \rho(r_1))$ and $(\rho(l_2), \rho(r_2))$: In case we have x, y in Σ^* such that $x\rho(l_1) \equiv \rho(l_2)y$ this corresponds to an overlap $l_1\rho(x) \equiv \rho(y)l_2$ respectively if we have $x\rho(l_1)y \equiv \rho(l_2)$ this corresponds to an overlap $\rho(y)l_1\rho(x) \equiv l_2$ of the rules (l_1, r_1) and (l_2, r_2) in T. Now since the critical pairs for T are confluent and the overlaps for $\rho(T)$ are just reversed instances of these systems, we know that they reduce to the same common descendant which is a reverse instance of the common descendant in the T-case. Hence the rewriting system is confluent and obviously it has similar properties as the original system and gives us normal forms of the desired form.

List of papers published in the Reports on Computer Algebra series

[1] H. Grassmann, G.-M. Greuel, B. Martin, W. Neumann, G. Pfister, W. Pohl, H. Schönemann, and T. Siebert. Standard bases, syzygies and their implementation in singular. 1996.

[2] H. Schönemann. Algorithms in singular. 1996.

[3] R. Stobbe. Factory: a C++ class library for multivariate polynomial arithmetic. 1996.

[4] O. Bachmann and H. Schönemann. A Manual for the MPP Dictionary and MPP Library. 1996.

[5] O. Bachmann, S. Gray, and H. Schönemann. MPP: A Framework for Distributed Polynomial Computations. 1996.

[6] G.M. Greuel and G. Pfister. Advances and improvements in the theory of standard bases and szyzygies. 1996.

[7] G.M. Greuel. Description of singular: A computer algebra system for singularity theory, algebraic geometry, and commutative algebra. 1996.

[8] T. Siebert. On strategies and implementations for computations of free resolutions. September 1996.

[9] B. Reinert. Introducing reduction to polycyclic group rings – a comparison of methods. October 1996.

[10] O. Bachmann, S. Gray, and H. Schönemann. A proposal for syntactic data integration for math protocols. January 1997.

[11] O. Bachmann. Effective simplification of cr expressions. January 1997.

[12] O. Bachmann, S. Gray, and H. Schönemann. MP Prototype Specification. January 1997.

[13] O. Bachmann. MPT – a library for parsing and Manipulating MP Trees. January 1997.

[14] K. Madlener and B. Reinert. Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings. September 1997.

[15] B. Martin and T. Siebert. Splitting Algorithm for vector bundles. September 1997.

[16] K. Madlener and B. Reinert. String Rewriting and Gröbner Bases – A General Approach to Monoid and Group Rings. October 1997.

[17] Thomas Siebert. An algorithm for constructing isomorphisms of modules. January 1998.

[18] O. Bachmann and H. Schönemann. Monomial Representations for Gröbner Bases Computations. January 1998.

[19] B. Reinert, K. Madlener, and T. Mora. A note on nielsen reduction and coset enumeration. February 1998.