UNIVERSITÄT KAISERSLAUTERN
Zentrum für Computeralgebra

REPORTS ON COMPUTER ALGEBRA
NO. 14

Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings

by

K. Madlener and B. Reinert

September 1997

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/`

Relating Rewriting Techniques on Monoids and Rings: Congruences on Monoids and Ideals in Monoid Rings

Klaus Madlener and Birgit Reinert*
Fachbereich Informatik
Universität Kaiserslautern
67663 Kaiserslautern
Germany
{madlener,reinert}@informatik.uni-kl.de

September, 1997

Abstract

A first explicit connection between finitely presented commutative monoids and ideals in polynomial rings was used 1958 by Emelichev yielding a solution to the word problem in commutative monoids by deciding the ideal membership problem. The aim of this paper is to show in a similar fashion how congruences on monoids and groups can be characterized by ideals in respective monoid and group rings. These characterizations enable to transfer well known results from the theory of string rewriting systems for presenting monoids and groups to the algebraic setting of subalgebras and ideals in monoid respectively group rings. Moreover, natural one-sided congruences defined by subgroups of a group are connected to one-sided ideals in the respective group ring and hence the subgroup problem and the ideal membership problem are directly related. For several classes of finitely presented groups we show explicitly how Gröbner basis methods are related to existing solutions of the subgroup problem by rewriting methods. For the case of general monoids and submonoids weaker results are presented. In fact it becomes clear that string rewriting methods for monoids and groups can be lifted in a natural fashion to define reduction relations in monoid and group rings.

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

1 Introduction

The development of symbolic computation theory – a field related to mathematics as well as to computer science – has resulted in new constructive approaches to computational problems in algebra in particular for rings, monoids and groups. Especially reduction techniques provide concepts for representing congruences by rewriting systems, transform these systems and use them for computations in quotient structures using symbolic methods. For general varieties these techniques have been studied extensively and the general results of term rewriting are widely applied in different areas. Since monoids respectively groups, as examples of varieties, can be presented as quotients of free monoids respectively free groups, general rewriting is one technique to solve computational problems related to the respective structures. Such presentations in terms of generators and defining relations (see e.g. [Gi79, LySch77, MaKaSo76]) are closely related to so called string rewriting systems or semi-Thue systems, which can be seen as special rewriting systems. Hence knowledge and procedures from this field, especially variations of the Knuth-Bendix completion procedure [KnBe70], can be applied to solve monoid and group theoretic problems. The most basic such problem is the word problem, i.e. decide whether two representations of elements in fact describe the same element. This problem can be solved using rewriting techniques in case the Knuth-Bendix completion procedure terminates for a given string rewriting system yielding a finite convergent system. Hence the question which monoids have presentations by finite convergent (i.e. complete) semi-Thue systems and how to compute them is of special interest. Kapur and Narendran in [KaNa85] and Jantzen in [Ja81, Ja85] give examples of monoid presentations which cannot be completed although a finite convergent semi-Thue system over an other alphabet presenting the same monoid exists. Squier proved the existence of finitely presented monoids with decidable word problem which cannot be presented by any finite convergent semi-Thue system [Sq87]. Some characterizations of classes of groups with finite convergent presentations of certain syntactical type can be found in [MaOt89].

Besides the word problem, the subgroup problem or generalized word problem is another classical important well studied decision problem for groups. Kuhn and Madlener have shown how the notion of prefix rewriting – a specialization of ordinary string rewriting – can be applied to solve the subgroup problem for certain classes of groups [KuMa89]. Prefix rewriting and the corresponding completion method is a direct generalization of Nielsen's method to solve the subgroup problem in the class of free groups [Ni21]. In case of confluence it can be used to compute Schreier-representatives of the subgroup cosets. A related question is when subgroups of groups allowing certain presentations again have a presentation of the same type. For some groups such a presentation for the subgroup can be computed from a confluent prefix rewriting system for the subgroup [KuMaOt94].

The application of reduction techniques in rings for solving membership problems of ideals and subalgebras also has a long tradition and has produced multiple results beginning with Buchberger's fundamental work on Gröbner bases [Bu65].

The main purpose of this paper is to relate the reduction techniques used for monoids, groups and rings by explicitly relating decision problems in appropriate related structures. Using reductions, e.g. from the word problem for finitely presented monoids or groups to the ideal membership problem for corresponding free monoid or free group rings, the apparently different reduction techniques for solving the problems can be compared. We survey some results concerning the above mentioned decision problems. A survey on reduction techniques for rings can be found in [MaRe95].

A first connection between (finitely presented) commutative monoids and polynomial rings can be found in the work of Emelichev 1958 (see e.g. [MaMeSa93]). He gives a solution for the word problem in commutative monoids using algebraic methods. Assuming the commutative monoid $\mathcal{M}$ is presented by a set of generators $x_1, \ldots, x_n$ and a set of defining relations $l_1 = r_1, \ldots, l_m = r_m$ the following is true: A relation $u = w$ holds in $\mathcal{M}$ if and only if the polynomial $u - w$ lies in the ideal generated by the polynomials $l_1 - r_1, \ldots, l_m - r_m$ in the polynomial ring $\mathbf{Q}[x_1, \ldots, x_n]$. In his paper Emelichev uses a result of Hermann to show that the latter question is decidable. Of course the ideal membership problem is also solvable using Buchberger's method of Gröbner bases, which is based on a special reduction system associated to finite sets of polynomials which represent ideal congruences in polynomial rings. Polynomials are used 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 interpreted as division of one polynomial by a set of finitely many polynomials. A Gröbner basis now can be defined as 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 enabling to solve the membership problem for ideals).

In this paper we want to show how congruences on monoids and groups are connected to ideals in the respective monoid and group rings. These connections enable to transfer results from the former field to generalizations of Gröbner basis methods in various structures. In [Re95] we have shown that certain undecidability results for string rewriting systems carry over to monoid and group rings since the specialization of the Knuth-Bendix completion procedure for string rewriting systems is an instance of Mora's generalization [Mo85] of Buchberger's algorithm for free monoid rings. These results are summarized in section 3 after giving some basic notions in section 2. Moreover, the subalgebra respectively one-sided ideal membership problem in monoid respectively group rings are related to the submonoid respectively subgroup problem in monoids respectively groups. In section 4 and 5 we show the relations between Gröbner bases in group rings and rewriting techniques for the word and subgroup problem in groups. Section 6 outlines the more general case of subalgebras in monoid rings, and the connections to the submonoid problem in the corresponding monoid are studied. While the results presented in these sections make clear that only very restricted types of monoids or groups will allow finite Gröbner bases in the associated monoid or group rings, in the concluding remarks we collect known positive results on the existence of finite Gröbner bases in some group rings, which prove that for the groups known to have subgroup problems solvable by string rewriting methods, appropriate finite Gröbner bases can be defined in the respective group ring. These classes of finitely presented groups include the finite, the free, the plain, the context-free respectively the polycyclic groups, and the details can be found in [MaRe95].

Acknowledgments
The first author wants to thank several colleagues for fruitful discussions. In particular Bruno Buchberger who introduced him to the study of reduction rings and Deepak Kapur for sharing with him ideas all the years after the workshop held in Otzenhausen. We both thank Andrea Sattler-Klein, Teo Mora, Paliath Narendran and Friedrich Otto for valuable discussions on parts of this paper.

2 Presentations: Congruences in Monoids and Groups

The book of Lallement [La79] gives a good introduction to congruences and presentations of monoids, while the book of Johnson [Jo76] was used as a source on group presentations.

Let A be a set and $\rho \subseteq A \times A$ a binary relation on A. By ϵ we denote the special relation $\{(a,a) \mid a \in A\}$. A binary relation ρ is called an **equivalence relation** in case it is reflexive (i.e. $\epsilon \subseteq \rho$), symmetric (i.e. $\rho \subseteq \rho^{-1} = \{(b,a) \mid (a,b) \in \rho\}$) and transitive (i.e. $\rho \circ \rho = \{(a,c) \mid (a,b),(b,c) \in \rho\} \subseteq \rho$). In the following we assume that ρ is an equivalence relation. For an element $a \in A$ we call the set $[a]_\rho = \{a' \in A \mid (a,a') \in \rho\}$ the **class of** a **modulo** ρ. Then A is a disjoint union of classes modulo ρ and the set of all such classes modulo ρ is called the **quotient of** A **modulo** ρ, denoted by A/ρ.

A **congruence** on a monoid $\mathcal{M}$ is defined as an equivalence relation ρ on the set $\mathcal{M}$ which is stable under left and right multiplication with elements of $\mathcal{M}$. In particular a **right** (respectively **left**) **congruence** on $\mathcal{M}$ is stable with respect to right (respectively left) multiplication.

Given a congruence ρ on a monoid $\mathcal{M}$ and an element $m \in \mathcal{M}$, we call $[m]_\rho = \{m' \in \mathcal{M} \mid (m,m') \in \rho\}$ the **congruence class** of m. We can define a monoid structure on the set of all congruence classes M/ρ by setting $[m]_\rho \circ_{M/\rho} [m']_\rho = [m \circ_{\mathcal{M}} m']_\rho$ for $m, m' \in \mathcal{M}$. Then M/ρ is called the **quotient of** $\mathcal{M}$ **by** ρ and the homomorphism $\chi_\rho : \mathcal{M} \longrightarrow \mathcal{M}/\rho$ induced by $m \longmapsto [m]_\rho$ is in fact surjective.

Congruences now provide the means to construct presentations of monoids. A set of symbols Σ is called a set of **generators** for $\mathcal{M}$ under the mapping $\phi : \Sigma \longrightarrow \mathcal{M}$, if the extension of ϕ to the set of words Σ^* on Σ defined by $\phi(a_1 \ldots a_n) = \phi(a_1) \circ_{\mathcal{M}} \ldots \circ_{\mathcal{M}} \phi(a_n)$, is a homomorphism from Σ^* onto $\mathcal{M}$. If for two words $w, w' \in \Sigma^*$ we have $\phi(w) = \phi(w')$ we say that $\mathcal{M}$ satisfies the **relation** $w = w'$. The **word problem** for a monoid $\mathcal{M}$ now is to decide whether for two words $w, w' \in \Sigma^*$, $\mathcal{M}$ satisfies the relation $w = w'$.

Given a set of relations R we say that a word u is **directly derivable** from an other word v under the relation $(l,r) \in R$, if either $u = xly$ and $v = xry$ or $u = xry$ and $v = xly$ for words x, y. We call u **derivable** from v under R if there exist words $v_0, \ldots, v_n$ such that $v = v_0$, v_{i+1} is directly derivable from v_i for $0 \leq i \leq n-1$ and $v_n = u$. Notice that if u is derivable from v under R, then $\phi(u) = \phi(v)$ holds, i.e. $u = v$ is a relation in $\mathcal{M}$. We then call the relation a **consequence** of the relations R. In case *all and only* relations on $\mathcal{M}$ are consequences of the relations R we say that (Σ, R) is a **presentation** of $\mathcal{M}$ defined by ϕ. (Σ, R) is also called a **Thue system** in the literature.

Now the easiest way to give a presentation of a monoid $\mathcal{M}$ is to take the set $\mathcal{M}$ itself as a generating set and to use the multiplication table of $\mathcal{M}$ as the defining relations. However this presentation in general will not be finite and other presentations fulfilling additional conditions, e.g. finitely many generators of finitely many relations, are hoped for.

In order to construct a presentation of a monoid $\mathcal{M}$ one has to

1. Find a set of generators Σ for $\mathcal{M}$. Then $\phi : \Sigma \longrightarrow \mathcal{M}$ can be chosen as the natural inclusion mapping.

2. Find a set of relations R in $\mathcal{M}$ such that the smallest congruence containing these relations coincides with the kernel congruence of the extended homomorphism ϕ :

$\Sigma^* \longrightarrow \mathcal{M}$. This kernel congruence is $\{(u,v) \in \Sigma^* \times \Sigma^* \mid \phi(u) =_{\mathcal{M}} \phi(v)\}$.

In order to use reduction techniques for computations in monoids or groups, presentations are provided with an orientation of the relations and treated as string rewriting systems (for a general reference of the terms and techniques described here see [BoOt93]). For a finite alphabet Σ, again 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 **string rewriting system** or **semi-Thue system** is a pair (Σ, T) where T 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 set of rules 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 $v \equiv xry$. v is then called a proper descendant of u. The reflexive transitive symmetric closure is denoted by $\stackrel{*}{\longleftrightarrow}_T$ and is called the **Thue congruence**. If $u \stackrel{*}{\longrightarrow}_T v$ holds then one says that u reduces to v. In case for u there exists no v such that $u \stackrel{+}{\longrightarrow}_T v$ holds, i.e. at least one reduction step must take place, u is called **irreducible**. An irreducible descendant of u is called a **(T-)normal form** and is sometimes denoted by $u{\downarrow}_T$. The reduction relation induced by T is called **Noetherian** if and only if there is no infinite chain $u \longrightarrow_T v_1 \longrightarrow_T v_2 \longrightarrow_T \ldots$. It is called **confluent** if for all u,v,w in Σ^*, $u \stackrel{*}{\longrightarrow}_T v$ and $u \stackrel{*}{\longrightarrow}_T w$ imply the existence of z in Σ^* such that $v \stackrel{*}{\longrightarrow}_T z$ and $w \stackrel{*}{\longrightarrow}_T z$. A string rewriting system is called **convergent** or **complete** if it is both, Noetherian and confluent, i.e., unique normal forms exist.

By Newman's lemma we know that under the hypothesis that a reduction relation is Noetherian, a string rewriting system is confluent if and only if it is **locally confluent**, i.e., for all u,v,w in Σ^*, $u \longrightarrow_T v$ and $u \longrightarrow_T w$ imply the existence of z in Σ^* such that $v \stackrel{*}{\longrightarrow}_T z$ and $w \stackrel{*}{\longrightarrow}_T z$. For finite string rewriting systems the global property of being locally confluent can be localized to enable a finite confluence test. Remember that presentations of monoids can be treated as string rewriting systems and notice that string rewriting systems are in fact presentations of monoids. Hence, in case they are finite, convergent and effective, we can "compute" in the monoid using the irreducible elements as representatives for the monoid elements. The process of trying to turn a Noetherian string rewriting system into a convergent one by resolving the not locally confluent situations is called completion. We will now sketch how a finite string rewriting system (Σ, T) presenting a monoid can be completed in case we have a total admissible[1] well-founded[2] ordering $\succeq$ on Σ^* such that for all $(l,r) \in T$ we have $l \succ r$. This ordering then will be called a **completion ordering** for T and the completion process transforms (Σ, T) into a (not necessarily finite) convergent string rewriting system presenting the same monoid. It is important that in order to check a finite Noetherian string rewriting system T for confluence we only have to look at a finite set of critical situations: for two not necessarily different rules $(l_1, r_1), (l_2, r_2)$ in T the set of **critical pairs** is defined as $\{\langle xr_1, r_2y\rangle \mid x,y \in \Sigma^*, xl_1 \equiv l_2y, |x| < |l_2|\} \cup \{\langle r_1, xr_2y\rangle \mid x,y \in \Sigma^*, l_1 \equiv xl_2y, |x| < |l_1|\}$. Now given a finite string rewriting system (Σ, T) with a completion ordering $\succeq$ we can specify a completion process as follows:

[1] A partial ordering $\succeq$ on Σ^* is called admissible if for all u,v,x,y in Σ^* we have $u \succeq \lambda$, and $u \succ v$ implies $xuy \succ xvy$.

[2] A partial ordering $\succeq$ on Σ^* is called well-founded if no infinite chains of the form $x_1 \succ x_2 \succ \ldots$ with $x_i \in \Sigma^*$ are possible.

Procedure: Knuth Bendix Completion

Given: A string rewriting system (Σ, T),
and a total well-founded admissible ordering $\succeq$.

$R := \{(l,r) \mid l \succ r, (l,r) \in T \text{ or } (r,l) \in T\}$;
$B := \{((l_1,r_1),(l_2,r_2)) \mid (l_1,r_1),(l_2,r_2) \in R\}$;
while $B \neq \emptyset$ **do**
  $((l_1,r_1),(l_2,r_2)) := \mathsf{remove}(B)$;
  % Remove an element using a fair strategy
  for all critical pairs $\langle z_1, z_2\rangle \in \mathsf{critical.pairs}((l_1,r_1),(l_2,r_2))$ **do**
  % $\mathsf{critical.pairs}((l_1,r_1),(l_2,r_2)) = \{\langle xr_1, r_2y\rangle \mid x,y \in \Sigma^*, xl_1 \equiv l_2y, |x| < |l_2|\} \cup$
  % $\{\langle r_1, xr_2y\rangle \mid x,y \in \Sigma^*, l_1 \equiv xl_2y, |x| < |l_1|\}$
    $z_1' := \max_{\succeq}(\mathsf{normal.form}(z_1, \longrightarrow_R), \mathsf{normal.form}(z_2, \longrightarrow_R))$;
    $z_2' := \min_{\succeq}(\mathsf{normal.form}(z_1, \longrightarrow_R), \mathsf{normal.form}(z_2, \longrightarrow_R))$;
    % $\mathsf{normal.form}(\mathrm{z}, \longrightarrow_R)$ computes an R-normal form of z
    if $z_1' \neq z_2'$
      then $B := B \cup \{((l,r),(z_1',z_2')),((z_1',z_2'),(l,r)) \mid (l,r) \in R\}$;
        $R := R \cup \{(z_1',z_2')\}$;
    endif
endwhile

Since the word problem for arbitrary string rewriting systems is undecidable, this procedure in general will not terminate. Nevertheless, using a fair[3] strategy to remove elements from the set B, it always enumerates a convergent string rewriting system based on the completion ordering $\succeq$ presenting the same monoid as the input system.

3 Relating the Word and the Ideal Membership Problems in Monoids and Free Monoid Rings

Let us start this section with some algebraic notions concerning monoid rings. For a monoid $\mathcal{M}$ with multiplication $\circ$ and a total well-founded ordering $\succeq$ on $\mathcal{M}$, the elements of the monoid ring $\mathbf{K}[\mathcal{M}]$ over a field $\mathbf{K}$ can be presented as "polynomials" $f = \sum_{t\in\mathcal{M}} \alpha_t \cdot t$ where only finitely many $\alpha_t \in \mathbf{K}$ are non-zero. The elements $\alpha_t \cdot t$ are called **monomials** consisting of a coefficient α_t and a term t. Addition and multiplication for two polynomials $f = \sum_{t\in\mathcal{M}} \alpha_t \cdot t$ and $h = \sum_{t\in\mathcal{M}} \beta_t \cdot t$ is defined as $f + h = \sum_{t\in\mathcal{M}}(\alpha_t + \beta_t) \cdot t$ and $f * h = \sum_{t\in\mathcal{M}} \gamma_t \cdot t$ with $\gamma_t = \sum_{x\circ y=t} \alpha_x \cdot \beta_y$. Given a non-zero polynomial p in $\mathbf{K}[\mathcal{M}]$, the head term $\mathsf{HT}(p)$ is the largest term in p with respect to $\succ$, which has non-zero coefficient denoted by $\mathsf{HC}(p)$, and the head monomial is $\mathsf{HM}(p) = \mathsf{HC}(p) \cdot \mathsf{HT}(p)$. $\mathsf{T}(p)$ is the set of all $t \in \mathcal{M}$ with non-zero coefficient in p. For a subset F of $\mathbf{K}[\mathcal{M}]$ we call the set $\mathsf{ideal}_r(F) = \{\sum_{i=1}^n \alpha_i \cdot f_i * w_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, w_i \in \mathcal{M}\}$[4] the **right ideal**, $\mathsf{ideal}_l(F) = \{\sum_{i=1}^n \alpha_i \cdot w_i * f_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, w_i \in \mathcal{M}\}$ the **left ideal** and $\mathsf{ideal}(F) = \{\sum_{i=1}^n \alpha_i \cdot u_i * f_i * w_i \mid n \in \mathbf{N}, \alpha_i \in \mathbf{K}, f_i \in F, u_i, w_i \in \mathcal{M}\}$ the **two-sided ideal**

[3] A fair strategy will ensure that all elements of the set B are considered at some time by the procedure.
[4] $\mathbf{N}$ denotes the natural numbers including 0.

generated by F. By $\equiv_{\mathfrak{i}}$ we will denote the (right, left respectively two-sided) congruence induced by a (right, left respectively two-sided) ideal $\mathfrak{i}$ on $\mathbf{K}[\mathcal{M}]$.

The following theorem states that the word problem for monoids is equivalent to a restricted version of the ideal membership problem in free monoid rings. This immediately implies the undecidability of the latter problem which is also stated in [Mo87, KaWe90], but the proof we give here provides a stronger result outlined below. For a string rewriting system (Σ, T) presenting a monoid, the related free monoid ring is $\mathbf{K}[\Sigma^*]$, where Σ^* is the free monoid generated by Σ with word concatenation as binary operation and λ as identity element.

Theorem 1 *Let (Σ, T) be a finite string rewriting system presenting a monoid $\mathcal{M}$ and $P_T = \{l - r \mid (l, r) \in T\}$ a set of polynomials in $\mathbf{K}[\Sigma^*]$ associated with T.*
Then for $u, v \in \Sigma^*$ the following statements are equivalent:

(1) $u \overset{*}{\longleftrightarrow}_T v$, i.e. the relation $u = v$ holds in $\mathcal{M}$.

(2) $u - v \in \mathsf{ideal}(P_T)$.

Proof :
$1 \Longrightarrow 2$: Using induction on k we show that $u \overset{k}{\longleftrightarrow}_T v$ implies $u - v \in \mathsf{ideal}(P_T)$. In the base case $k = 0$ there is nothing to show, since $u - u = 0 \in \mathsf{ideal}(P_T)$. Thus let us assume that $\tilde{u} \overset{k}{\longleftrightarrow}_T \tilde{v}$ implies $\tilde{u} - \tilde{v} \in \mathsf{ideal}(P_T)$. Then looking at $u \overset{k}{\longleftrightarrow}_T u_k \longleftrightarrow_T v$ we find $u_k \longleftrightarrow_T v$ with $(l_j, r_j) \in T$. Without loss of generality we can assume $u_k \equiv x l_j y$ for some $x, y \in \Sigma^*$ thus giving us $v \equiv x r_j y$, and since multiplication in the free monoid is concatenation, v can be expressed in terms of polynomials by $v = u_k - x * (l_j - r_j) * y$. As $u - v = u - u_k + x * (l_j - r_j) * y$ and $u - u_k \in \mathsf{ideal}(P_T)$ our induction hypothesis yields $u - v \in \mathsf{ideal}(P_T)$.

$2 \Longrightarrow 1$: It remains to show that $u - v \in \mathsf{ideal}(P_T)$ implies $u \overset{*}{\longleftrightarrow}_T v$. We know $u - v = \sum_{j=1}^{n} \beta_j \cdot x_j * (l_{i_j} - r_{i_j}) * y_j$, where $\beta_j \in \mathbf{K}^*, x_j, y_j \in \Sigma^*$. Therefore, by showing the following stronger result we are done: A representation $u - v = \sum_{j=1}^{m} p_j$ where $p_j = \alpha_j \cdot (w_j - w'_j)$, $\alpha_j \in \mathbf{K}^*$ and $w_j \overset{+}{\longleftrightarrow}_T w'_j$ implies that $u \overset{*}{\longleftrightarrow}_T v$. Thus let $u - v = \sum_{j=1}^{m} p_j$ be such a representation. Depending on this representation $\sum_{j=1}^{m} p_j$ and the ordering $\succeq$ on Σ^* we can define $t = \max_{\succeq}\{w_j, w'_j \mid j = 1, \ldots m\}$ 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 $m = 0$, then $u - v = 0$ implies $u \equiv v$ and hence $u \overset{0}{\longleftrightarrow}_T v$. Now suppose $m > 0$.
In case $K = 1$, let p_k be the polynomial containing t. Since 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 $u \equiv t$ and $p_k = t - w'_k$. Using p_k we can decrease m by subtracting p_k from $u - v$ giving us $w'_k - v = \sum_{j=1, j \neq k}^{m} p_j$. Since $u \equiv t \overset{*}{\longleftrightarrow}_T w'_k$ and our induction hypothesis yields $w'_k \overset{*}{\longleftrightarrow}_T v$ we can conclude $u \overset{*}{\longleftrightarrow}_T v$.
In case $K > 1$ there are two polynomials p_k, p_l in the corresponding representation containing the term t and without loss of generality we can assume $p_k = \alpha_k \cdot (t - w'_k)$ and $p_l = \alpha_l \cdot (t - w'_l)$, as the cases where $p_k = \alpha_k \cdot (w'_k - t)$ or $p_l = \alpha_l \cdot (w'_l - t)$ occur can be treated similarly by modifying the respective coefficient. If $w'_k \equiv w'_l$ we can immediately

decrease m by substituting the occurrence of $p_k + p_l$ by $(\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l$. Otherwise we can proceed as follows:

$$\begin{aligned}
p_k + p_l &= p_k \underbrace{-\alpha_k \cdot \alpha_l^{-1} \cdot p_l + \alpha_k \cdot \alpha_l^{-1} \cdot p_l}_{=0} + p_l \\
&= (\alpha_k \cdot (t - w'_k) - \alpha_k \cdot \alpha_l^{-1} \cdot \alpha_l \cdot (t - w'_l)) + (\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l \\
&= \underbrace{(-\alpha_k \cdot w'_k + \alpha_k \cdot w'_l)}_{=p'_k} + (\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l
\end{aligned}$$

where $p'_k = \alpha_k \cdot (w'_l - w'_k)$, $w'_k \overset{*}{\longleftrightarrow}_T t \overset{*}{\longleftrightarrow}_T w'_l$ and $w'_l \neq w'_k$. Therefore, 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., K will be decreased in any case.

q.e.d.

In other words, the congruence generated by the relations in T on Σ^* is related to the ideal generated by P_T in $\mathbf{K}[\Sigma^*]$.

Moreover, inspecting the proof of this theorem we find that every rewriting sequence $u \overset{k}{\longleftrightarrow}_T v$ gives rise to a representation of the polynomial $u - v$ involving k multiples of the form $x * (l - r) * y$ with $x, y \in \Sigma^*$, $(l, r) \in T$. On the other hand the existence of a representation $u - v = \sum_{i=1}^{k} x_i * (l_i - r_i) * y_i$, $x_i, y_i \in \Sigma^*$, $(l_i, r_i) \in T$ implies $u \overset{*}{\longleftrightarrow}_T v$. Hence not only the word problem for finite string rewriting systems is reduced to the membership problem for finitely generated ideals in free monoid rings, but also the rewriting sequences are translated into particular polynomial representations. Especially if $\succeq$ is a total admissible well-founded ordering on Σ^* and the rules of T are ordered by $\succeq$ and we have $u \overset{k}{\longrightarrow}_T v$ then the resulting representation has the characteristics of so called standard representations, i.e. $u \succeq x_i l_i y_i$ for all $1 \leq i \leq k$. Additionally we can arrange the sum such that $u \equiv x_1 l_1 y_1 \succ x_1 r_1 y_1 \equiv x_2 l_2 y_2 \succ x_2 r_2 y_2 \ldots x_{k-1} l_{k-1} y_{k-1} \succ x_{k-1} r_{k-1} y_{k-1} \equiv x_k l_k y_k \succ x_k r_k y_k \equiv v$.

For a monoid $\mathcal{M}$ presented by a string rewriting system (Σ, T), let ρ be the smallest congruence containing the set of relations $R = \{u_i = v_i \mid u_i, v_i \in \Sigma^*\}$. Then we are interested in the quotient of $\mathcal{M}$ by ρ and similar to theorem 1 we can relate the congruence now generated by $T \cup R$ on Σ^* to the ideal generated by $P_{T \cup R} = \{l - r \mid (l, r) \in T \cup R\}$ in $\mathbf{K}[\Sigma^*]$.

Corollary 2 *Let (Σ, T) be a finite string rewriting system presenting a monoid $\mathcal{M}$. Furthermore, let R be a set of relations on $\mathcal{M}$ and let $P_{T \cup R} = \{l - r \mid (l, r) \in T \cup R\} \subseteq \mathbf{K}[\Sigma^*]$. Then for $u, v \in \Sigma^*$ the following statements are equivalent:*

(1) $u \overset{*}{\longleftrightarrow}_{T \cup R} v$.

(2) $u - v \in \mathsf{ideal}(P_{T \cup R})$.

The existence of a finite string rewriting system over an alphabet with two symbols having undecidable word problem yields that the ideal membership problem for free monoid rings with more than one generator is undecidable[5] in general. In case the free monoid is generated by one element, we have decidable ideal membership problem. In fact $\mathbf{K}[\{a\}^*]$ is the ordinary commutative polynomial ring in one variable $\mathbf{K}[a]$ and, e.g., the Euclidean algorithm determines a generating polynomial for the ideal which can be used to solve the ideal membership problem.

As in the case of commutative polynomial rings, where ideal membership can successfully be solved using reduction methods, ideal congruences in free monoid rings can be described by reduction relations. A natural definition of a reduction relation was introduced by Mora in [Mo85].

Definition 3 (Mora) *Let Σ be a finite alphabet with $\succeq$ a total admissible well-founded ordering on Σ^* and p, f be two non-zero polynomials in $\mathbf{K}[\Sigma^*]$. We say f* **reduces p to q at a monomial $\alpha \cdot t$ of p in one step**, *denoted by $p \longrightarrow_f q$, if*

(a) $x\mathsf{HT}(f)y \equiv t$ for some $x, y \in \Sigma^*$, and

(b) $q = p - (\alpha \cdot \mathsf{HC}(f)^{-1}) \cdot x * f * y$.

We write $p \longrightarrow_f$ if there is a polynomial q such that $p \longrightarrow_f q$.

Notice that for a set of polynomials F we write $p \longrightarrow_F$ in case there exists $f \in F$ such that $p \longrightarrow_f$. Then $\overset{*}{\longleftrightarrow}_F \; = \; \equiv_{\mathsf{ideal}(F)}$ holds and if additionally $\longrightarrow_F$ is confluent we call F a **Gröbner basis** of $\mathsf{ideal}(F)$ with respect to $\longrightarrow_F$.

While theorem 1 reduces the word problem for string rewriting systems to the ideal membership problem in free monoid rings, the proof of this theorem reveals that in fact for a fixed admissible ordering the existence of finite convergent string rewriting systems corresponds to the existence of finite Gröbner bases and vice versa. Since there exist finitely generated ideals in free monoid rings with unsolvable membership problem, in general finitely generated ideals will not admit finite Gröbner bases. As the ordering on $\mathcal{M}$ determines the head monomial of a polynomial, it has great influence on how a polynomial can be used for reduction. Therefore, as Gröbner bases are defined with respect to reduction, it even is possible for a finitely generated ideal to admit a finite Gröbner basis with respect to one admissible ordering and none with respect to another admissible ordering. For example in the free monoid ring over $\{a, b, c\}^*$ the ideal generated by $F = \{ac + 1, cb - bc\}$ has a finite Gröbner basis when using the length-lexicographic ordering on $\{a, b, c\}^*$ induced by the precedence $a \succ b \succ c$ and none with precedence $c \succ a \succ b$. Moreover, solvable word problem does not imply the existence of a finite Gröbner basis as the example of a finitely presented monoid $\Sigma = \{a, b\}$, $T = \{aba \longrightarrow bab\}$ with solvable word problem but no finite convergent presentation on the alphabet $\{a, b\}$ with respect to any admissible ordering shows (see [KaNa85]). Similarly, the ideal generated by the polynomial $aba - bab$ in $\mathbf{K}[\{a, b\}^*]$ has no finite Gröbner basis with respect to any admissible ordering on $\{a, b\}^*$. Notice that in this example we can apply a so called Tietze transformation to the string rewriting system, i.e. we can change the presentation without changing the monoid, giving us the isomorphic presentation $\Sigma' = \{a, b, c\}$, $T' = \{aba \longrightarrow bab, ba \longrightarrow c\}$ which can be

[5]This has also been shown by Kandri-Rody and Weispfenning in [KaWe90] for the free monoid ring $\mathbf{Q}[\{X_1, X_2\}^*]$ by reducing the halting problem for Turing machines to this problem.

successfully completed, e.g. with respect to the length-lexicographical ordering with precedence $a \succ b \succ c$ resulting in $T'' = \{ac \longrightarrow cb, ba \longrightarrow c, bcb \longrightarrow c^2, bc^2 \longrightarrow c^2a\}$. Similarly, the ideal generated by $\{aba - bab, ba - c\}$ has a finite Gröbner basis with respect to the same ordering, namely $\{ac - cb, ba - c, bcb - c^2, bc^2 - c^2a\}$[6]. Due to the result of Squire in [Sq87] there are finitely presented monoids with solvable word problem which have no finite convergent presentations at all and his examples give rise to finitely generated ideals in free monoid rings with solvable ideal membership problem which have no finite Gröbner bases. On the other hand, in [Mo85] Mora provided a completion procedure which, given an admissible ordering and a finite set of polynomials F, enumerates a Gröbner basis of $\mathsf{ideal}(F)$ with respect to reduction determined by this ordering.

Procedure: Gröbner Bases in Free Monoid Rings [Mora]

Given: A finite set $F \subseteq \mathbf{K}[\Sigma^*]$,
$\succ$ a total admissible well-founded ordering on Σ^*.

$G := F$;
$B := \{(q_1, q_2) \mid q_1, q_2 \in G\}$;
while $B \neq \emptyset$ **do**
  $(q_1, q_2) := \mathsf{remove}(B)$;
  % Remove an element using a fair strategy
  for all polynomials $h \in S(q_1, q_2)$ **do**
  % $S(q_1, q_2) = \{\mathsf{HC}(q_1)^{-1} \cdot u * q_1 * v - \mathsf{HC}(q_2)^{-1} \cdot q_2 \mid u\mathsf{HT}(q_1)v \equiv \mathsf{HT}(q_2)\} \cup$
  % $\{\mathsf{HC}(q_1)^{-1} \cdot q_1 * u - \mathsf{HC}(q_2)^{-1} * v * q_2 \mid \mathsf{HT}(q_1)u \equiv v\mathsf{HT}(q_2), |\mathsf{HT}(q_1)| < |v|\}$
    $h' := \mathsf{normal.form}(h, \longrightarrow_G)$;
    if $h' \neq 0$
      then $G := G \cup \{h'\}$;
        $B := B \cup \{(f, h'), (h', f) \mid f \in G\}$;
    endif
  endfor
endwhile

Reviewing the Knuth-Bendix completion procedure it is easy to see the connection to this Gröbner basis procedure: Let Σ be a finite alphabet, T a set of rules and $\succeq$ a total admissible well-founded ordering on Σ^*. Then there is a correspondence between rules and special polynomials in $\mathbf{K}[\Sigma^*]$ (even in $\mathbf{Z}[\Sigma^*]$) as follows:

$$T \ni (l, r) \longmapsto p(l, r) \in \mathbf{K}[\Sigma^*]$$

where

$$p(l, r) = \begin{cases} l - r & l \succ r \\ r - l & r \succ l \\ 0 & l \equiv r \end{cases}$$

[6]Notice that for $\mathfrak{i} = \mathsf{ideal}^{\mathbf{K}[\{a,b\}^*]}(\{aba - bab\})$ and $\mathfrak{j} = \mathsf{ideal}^{\mathbf{K}[\{a,b,c\}^*]}(\{aba - bab, ba - c\})$ the quotients $\mathbf{K}[\{a, b\}^*]/\mathfrak{i}$ and $\mathbf{K}[\{a, b, c\}^*]/\mathfrak{j}$ are isomorphic and for $u, v \in \{a, b\}^*$ we have $u - v \in \mathfrak{i}$ if and only if $u - v \in \mathfrak{j}$ since $\mathfrak{i} = \mathfrak{j} \cap \mathbf{K}[\{a, b\}^*]$.

[6]These polynomials are frequently called s-polynomials in the literature.

Hence we can associate to T a set of polynomials $P_T = \{p(l,r) \mid (l,r) \in T\}$. On the other hand, given a polynomial of the form $x - y$ or $-x + y$ with $x \succ y$ we can relate this to a rule (x, y) and doing so associate to a set of such polynomials G a set of rules $T_G = \{(x, y) \mid x-y \text{ or } -x+y \in G\}$. In this context it is obvious that on input T respectively P_T the initialization of both procedures gives us corresponding sets R and G and corresponding sets B. Furthermore, this is also true for the two sets $\mathsf{critical.pairs}((l_1, r_1), (l_2, r_2))$ and $S(p(l_1, r_1), p(l_2, r_2))$. It remains to show, that the treatment of a critical pair and the corresponding polynomial is in fact the "same". To see this we have to inspect the reduction process in both procedures. First let us assume a polynomial of the form $u-v$ is reduced by a polynomial f of the form $w-z$ or $-w+z$ where $w \succ z$ (the case of reducing a polynomial of the form $-u+v$ is similar). Then we either have $u \equiv xwy$ implying $u - v \longrightarrow_f xzy - v$ or $v \equiv xwy$ implying $u - v \longrightarrow_f u - xzy$. Hence in both cases the resulting polynomial will be zero or contain two monomials, one having coefficient 1 and the other having coefficient -1. Therefore we can see that for a set of polynomials G of the restricted form we can express the normal form computation in the Gröbner basis procedure using string rewriting by $\mathsf{normal.form}(u - v, \longrightarrow_G) = \mathsf{normal.form}(u, \longrightarrow_{T_G}) - \mathsf{normal.form}(v, \longrightarrow_{T_G})$ and on the other hand the normal form computed by the Gröbner basis procedure $\mathsf{normal.form}(u-v, \longrightarrow_G) = x-y$ or $-x+y$ can be used to express the pair computed in the Knuth-Bendix completion procedure since this pair is (x, y). Hence both procedures add the same information to the sets R respectively G in form of pairs or special polynomials which are essentially the same in this context. Since the only possible coefficients occurring in the Gröbner basis calculation in this special case are 1 and -1, the completion can also be done in $\mathbf{Z}_2[\Sigma^*]$.

Procedure Gröbner Bases in Free Monoid Rings terminates in case for the ideal generated by F a finite Gröbner basis exists with respect to the reduction relation determined by the chosen admissible ordering. Hence the question arises, whether it is possible to decide for a finite set of polynomials and a total admissible well-founded ordering if a finite Gröbner basis with respect to reduction determined by this ordering exists. This turns out to be undecidable.

Theorem 4 ([Re95, MaRe95]) *Given a total admissible well-founded ordering $\succeq$, it is undecidable, whether a finitely generated ideal has a finite Gröbner basis in the free monoid ring $\mathbf{K}[\{a, b\}^*]$ with respect to reduction determined by $\succ$ as defined in definition 3.*

Proof :
Using the technique described by Ó'Dúnlaing in [OD83] Madlener and Otto have shown that the following problem is undecidable ([MaOt94]):

Let $\succeq$ be a compatible well-founded partial ordering on $\Sigma_2^* = \{a, b\}^*$ such that $a \succ \lambda$ and $b \succ \lambda$ both hold.
Given a finite string rewriting system (Σ_2, T). Is there a finite and confluent system (Σ_2, T') that is equivalent to (Σ_2, T) and based on $\succ$?

To prove our claim we show that the answer for (Σ_2, T) is "yes" if and only if the ideal generated by the set of polynomials $P_T = \{l - r \mid (l, r) \in T\}$ associated to T has a finite Gröbner basis in $\mathbf{K}[\Sigma_2^*]$ with respect to $\succ$. If there is an equivalent, finite convergent presentation (Σ_2, T') based on $\succ$, then the set $P_{T'}$ is a finite Gröbner basis of $\mathsf{ideal}(P_T)$

in $\mathbf{K}[\Sigma_2^*]$. This follows as the string rewriting reduction $\longrightarrow_{T'}$ on Σ^* can be simulated by $\longrightarrow_{P_{T'}}$ in $\mathbf{K}[\Sigma_2^*]$ (compare definition 3). Thus it remains to show that in case $\mathsf{ideal}(P_T)$ has a finite Gröbner basis in $\mathbf{K}[\Sigma_2^*]$, there exists a finite Gröbner basis G such that for all $g \in G$ we have $g = u - v$ or $g = -u + v$, where $u, v \in \Sigma_2^*$, $u \succ v$, and $u \overset{*}{\longleftrightarrow}_T v$. Then (Σ_2, T) has an equivalent, convergent, finite presentation (Σ_2, T'), namely $T' = \{(u, v) \mid u - v \in G \text{ or } -u + v \in G\}$, since reduction in $\mathbf{K}[\Sigma_2^*]$ when restricted to the usage of polynomials of the form $u - v$ or $-u + v$ can be compared to a transformation step in a string rewriting system.
First we show that for a finite set F in case $\mathsf{ideal}(F)$ has a finite Gröbner basis in $\mathbf{K}[\Sigma_2^*]$ the procedure Gröbner Bases in Free Monoid Rings also computes a finite Gröbner basis of $\mathsf{ideal}(F)$. Let $\tilde{G}$ be a finite Gröbner basis of $\mathsf{ideal}(F)$ with $\mathsf{HT}(\tilde{G}) = \{\mathsf{HT}(g) \mid g \in \tilde{G}\} = \{t_1, \ldots, t_k\}$. Let $H_{t_i} = \{xt_iy \mid x, y \in \Sigma^*\}$, then $\mathsf{HT}(\mathsf{ideal}(F)) = \bigcup_{i=1}^{k} H_{t_i}$, since all polynomials in $\mathsf{ideal}(F)$ reduce to zero by $\tilde{G}$. Further our procedure is correct and, therefore, for each t_i there has to be at least one g_i added to G such that $t_i \equiv x\mathsf{HT}(g_i)y$ for some $x, y \in \Sigma^*$, i.e., $\mathsf{HT}(g_i)$ "divides" t_i. Note that as soon as all such g_i are added to G, we have $\mathsf{HT}(\mathsf{ideal}(G)) \supseteq \bigcup_{i=1}^{k} H_{t_i}$ and all further computed s-polynomials must reduce to zero (we take the notion of s-polynomials as defined by Mora in [Mo94]). Since the procedure is correct, G then is also a Gröbner basis of $\mathsf{ideal}(F)$.
As we have seen before, procedure Gröbner Bases in Free Monoid Rings on input P_T only produces new polynomials of the form 0, $u - v$ or $-u + v$. Hence on termination the output has the desired form.

q.e.d.

This result holds even assuming decidable membership problems for the ideals [Sa96].

Corollary 5 *It is undecidable, whether for a finitely generated ideal in* $\mathbf{K}[\{a, b\}^*]$ *there exists a total admissible well-founded ordering on* $\{a, b\}^*$ *such that the ideal has a finite Gröbner basis with respect to Mora's reduction.*

Proof :
In this proof we use the following technique (described in [MaOt94]):

Let $\mathcal{P}$ be a property of string rewriting systems over the alphabet $\Sigma_2 = \{a, b\}$ satisfying the following three conditions:

(P1) Whenever (Σ_2, T_1) and (Σ_2, T_2) are two *finite equivalent* string rewriting systems, then (Σ_2, T_1) has property $\mathcal{P}$ if and only if (Σ_2, T_2) has it.

(P2) The trivial string rewriting system $(\Sigma_2, \{a \longrightarrow \lambda, b \longrightarrow \lambda\})$ has property $\mathcal{P}$.

(P3) If a finite string rewriting system (Σ_2, T) has property $\mathcal{P}$, then (Σ_2, T) has decidable word problem, i.e., the Thue congruence $\overset{*}{\longleftrightarrow}_T$ is decidable.

Then the following problem for $\mathcal{P}$ is undecidable in general:

Given: A finite string rewriting system (Σ_2, T).
Question: Does the Thue congruence $\overset{*}{\longleftrightarrow}_T$ have $\mathcal{P}$?

Now the claim follows using the correspondence between properties of string rewriting systems and ideal bases of the related ideals derived in the proof in theorem 4. Let us define a property $\mathcal{P}(T)$ for string rewriting systems (Σ_2, T) as follows: $\mathcal{P}(T)$ if and only if there exists a total, well-founded, admissible ordering $\succeq$ on Σ_2^* such that there exists an equivalent finite convergent string rewriting system (Σ_2, T') based on $\succeq$. Then $\mathcal{P}$ fulfills the conditions (P1), (P2) and (P3) mentioned above:

(P1): If $\mathcal{P}(T_1)$ holds so must $\mathcal{P}(T_2)$ as the existence of a total, well-founded, admissible ordering $\succeq$ on Σ_2^* such that there exists an equivalent finite string rewriting system (Σ_2, T') which is convergent with respect to $\succ$ for (Σ_2, T_1) at once carries over to the equivalent system (Σ_2, T_2).

(P2): The trivial system $\{a \longrightarrow \lambda, b \longrightarrow \lambda\}$ has property $\mathcal{P}$.

(P3): Having property $\mathcal{P}$ implies decidability of the Thue congruence.

Hence this property is undecidable in general and this result carries over to Gröbner bases in $\mathbf{K}[\{a, b\}^*]$ as before.

q.e.d.

This means that for two-sided ideals the case of free monoids is already hard although free monoids allow simple presentations by string rewriting systems, namely empty sets of defining relations.

For finitely generated right or left ideals the situation is much better. Using prefixes respectively suffixes of words, natural reduction relations called prefix respectively suffix reduction can be defined and finite prefix respectively suffix Gröbner bases of the right respectively left ideals exist. These bases can be in fact computed by interreducing the generating set with respect to prefix or suffix reduction (compare e.g. [Mo94] for an algorithm to compute prefix Gröbner bases for finitely generated right ideals).

As stated in the introduction, a first explicit connection between finitely presented commutative monoids and ideals in polynomial rings was used 1958 by Emelichev yielding a solution to the word problem in the monoid by deciding the ideal membership problem. In fact the word problem for finitely generated free commutative monoids can be solved using Gröbner bases in ordinary commutative polynomial rings and the word problem for arbitrary finitely generated commutative monoids can be solved using Gröbner bases in quotients of commutative polynomial rings.

4 Relating the Word and Ideal Membership Problems in Groups and Free Group Rings

In this section we want to point out how the Gröbner basis methods as introduced in [MaRe93, Re95] for general monoid rings when applied to group rings are related to the word problem. First we state that similar to theorem 1 the word problem for groups is equivalent to a restricted version of the membership problem for ideals in a free group ring. Let the group be presented by a string rewriting system $(\Sigma, T \cup T_I)$ such that there exists an involution $\imath : \Sigma \longrightarrow \Sigma$, i.e for all $a \in \Sigma$ we have $\imath(a) \neq a$, $\imath(\imath(a)) = a$, and the $T_I = \{(a\imath(a), \lambda) \mid a \in \Sigma\}$. Every group has such a presentation. Notice that the set of rules T_I is confluent with respect to any admissible ordering on Σ. By $\mathcal{F}_\Sigma$ we will denote the free group with presentation (Σ, T_I). The elements of $\mathcal{F}_\Sigma$ will be represented by **freely reduced** words, i.e. we assume that the words do not contain any subwords of the form $a\imath(a)$.

Theorem 6 ([Re95, MaRe95]) *Let $(\Sigma, T \cup T_I)$ be a finite string rewriting system presenting a group and without loss of generality for all $(l, r) \in T$ we assume that l and r are free reduced words. We associate the set of polynomials $P_T = \{l - r \mid (l, r) \in T\}$ in $\mathbf{K}[\mathcal{F}_\Sigma]$ with T.*
Then for $u, v \in \Sigma^*$ the following statements are equivalent:

(1) $u \overset{*}{\longleftrightarrow}_{T \cup T_I} v$.

(2) $u{\downarrow}_{T_I} - v{\downarrow}_{T_I} \in \mathsf{ideal}(P_T)$.

Proof :
$1 \Longrightarrow 2$: Using induction on k we show that $u \overset{k}{\longleftrightarrow}_{T \cup T_I} v$ implies $u{\downarrow}_{T_I} - v{\downarrow}_{T_I} \in \mathsf{ideal}(P_T)$. In the base case $k = 0$ we have $u \equiv v$ and, therefore, $u{\downarrow}_{T_I} - u{\downarrow}_{T_I} = 0 \in \mathsf{ideal}(P_T)$. Hence, let us assume that $\tilde{u} \overset{k}{\longleftrightarrow}_{T \cup T_I} \tilde{v}$ implies $\tilde{u}{\downarrow}_{T_I} - \tilde{v}{\downarrow}_{T_I} \in \mathsf{ideal}(P_T)$. Thus, looking at $u \overset{k}{\longleftrightarrow}_{T \cup T_I} u_k \longleftrightarrow_{T \cup T_I} v$ we can distinguish the following cases:

1. $u_k \longleftrightarrow_T v$ with $(l, r) \in T$.
   Without loss of generality we can assume $u_k \equiv xly$ and $v \equiv xry$ for some words $x, y \in \Sigma^*$. Now this gives us

   $$u{\downarrow}_{T_I} - v{\downarrow}_{T_I} = u{\downarrow}_{T_I} - \underbrace{u_k{\downarrow}_{T_I} + xly{\downarrow}_{T_I}}_{=0} - xry{\downarrow}_{T_I}$$

   and $xly{\downarrow}_{T_I} - xry{\downarrow}_{T_I} = x * (l - r) * y$, where $*$ denotes multiplication in $\mathbf{K}[\mathcal{F}_\Sigma]$. By our induction hypothesis we know $u{\downarrow}_{T_I} - u_k{\downarrow}_{T_I} \in \mathsf{ideal}(P_T)$ and, hence, we get $u{\downarrow}_{T_I} - v{\downarrow}_{T_I} \in \mathsf{ideal}(P_T)$.

2. $u_k \longleftrightarrow_{T_I} v$ with $(a\imath(a), \lambda) \in T_I$[7].
   Without loss of generality we can assume $u_k \equiv xa\imath(a)y$ for some $x, y \in \Sigma^*$ and $v \equiv xy$, i.e., $u_k{\downarrow}_{T_I} = v{\downarrow}_{T_I}$ and therefore $u{\downarrow}_{T_I} - v{\downarrow}_{T_I} \in \mathsf{ideal}(P_T)$.

$2 \Longrightarrow 1$: It remains to show that $u{\downarrow}_{T_I} - v{\downarrow}_{T_I} \in \mathsf{ideal}(P_T)$ implies $u \overset{*}{\longleftrightarrow}_{T \cup T_I} v$. We know $u{\downarrow}_{T_I} - v{\downarrow}_{T_I} = \sum_{j=1}^{n} \beta_j \cdot x_j * (l_{i_j} - r_{i_j}) * y_j$, where $\beta_j \in \mathbf{K}^*, x_j, y_j \in \mathcal{F}_\Sigma$. Therefore, by showing the following stronger result we are done: A representation $u - v = \sum_{j=1}^{m} p_j$ where $p_j = \alpha_j \cdot (w_j - w'_j)$, $\alpha_j \in \mathbf{K}^*$, $u, v, w_j, w'_j \in \mathcal{F}_\Sigma$ and $w_j \overset{+}{\longleftrightarrow}_T w'_j$ implies that $u \overset{*}{\longleftrightarrow}_T v$. Hence, let $u - v = \sum_{j=1}^{m} p_j$ be such a representation. Depending on this representation $\sum_{j=1}^{m} p_j$ and the ordering $\succeq$ on Σ^* we can define $t = \max_\succeq \{w_j, w'_j \mid j = 1, \ldots m\}$ and K is the number

[7]The case $(\imath(a)a, \lambda) \in T$ is similar.

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 $m = 0$, then $u - v = 0$ implies $u = v$ and hence $u \overset{0}{\longleftrightarrow}_T v$[8]. Now suppose $m > 0$.
In case $K = 1$, let p_k be the polynomial containing t. Since 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 $u = t$ and $p_k = t - w_k'$. Using p_k we can decrease m by subtracting p_k from $u - v$ giving us $w_k' - v = \sum_{j=1, j \neq k}^{m} p_j$. Since $u = t \overset{*}{\longleftrightarrow}_T w_k'$ and our induction hypothesis yields $w_k' \overset{*}{\longleftrightarrow}_T v$ we get $u \overset{*}{\longleftrightarrow}_T v$.
In case $K > 1$ there are two polynomials p_k, p_l in the corresponding representation containing the term t and without loss of generality we can assume $p_k = \alpha_k \cdot (t - w_k')$ and $p_l = \alpha_l \cdot (t - w_l')$, as the cases where $p_k = \alpha_k \cdot (w_k' - t)$ or $p_l = \alpha_l \cdot (w_l' - t)$ occur can be treated similarly by modifying the respective coefficient. If $w_k' = w_l'$ we can immediately decrease m by substituting the occurrence of $p_k + p_l$ by $(\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l$. Otherwise we can proceed as follows:

$$
\begin{aligned}
p_k + p_l &= p_k \underbrace{- \alpha_k \cdot \alpha_l^{-1} \cdot p_l + \alpha_k \cdot \alpha_l^{-1} \cdot p_l}_{=0} + p_l \\
&= \underbrace{(-\alpha_k \cdot w_k' + \alpha_k \cdot w_l')}_{=p_k'} + (\alpha_k \cdot \alpha_l^{-1} + 1) \cdot p_l
\end{aligned}
$$

where $p_k' = \alpha_k \cdot (w_l' - w_k')$, $w_k' \overset{*}{\longleftrightarrow}_T t \overset{*}{\longleftrightarrow}_T w_l'$ and $w_l' \neq w_k'$. Hence, 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., K will be decreased in any case.

q.e.d.

The existence of a finite group presentation over four letters (resulting from two generators as a group) with unsolvable word problem implies that the ideal membership problem for free group rings with more than one generator is undecidable in general. Groups with one generator are known to have decidable word problem. The ideal membership problem for free group rings with one generator is solvable as this ring corresponds to the ring of Laurent polynomials for the (commutative) free group with one generator (see e.g. [Si94]).

In theorem 6 we have shown how the congruence generated by the relations in T on $\mathcal{F}_\Sigma$ is related to the ideal generated by P_T in $\mathbf{K}[\mathcal{F}_\Sigma]$. As in the monoid case in fact we can use additional relations R and investigate the quotient of $\mathcal{F}_\Sigma$ by the congruence generated by R.

Corollary 7 *Let $(\Sigma, T \cup T_I)$ be a finite string rewriting system as specified in theorem 6. Furthermore, let R be a set of relations and let $P_{T \cup R} = \{l - r \mid (l, r) \in T \cup R\}$. Then for $u, v \in \mathcal{F}_\Sigma$ the following statements are equivalent:*

(1) $u \overset{*}{\longleftrightarrow}_{T \cup R} v$.

[8] Remember that $u, v \in \mathcal{F}_\Sigma$, i.e., they are in normal form with respect to T_I.

(2) $u\downarrow_{T_I} - v\downarrow_{T_I} \in \mathsf{ideal}(P_{T \cup R})$.

As in the monoid case (compare definition 3) we can define a natural reduction relation on $\mathbf{K}[\mathcal{F}_\Sigma]$ and we then can link the existence of finite convergent string rewriting systems for groups to the existence of finite Gröbner bases for the respective ideals and vice versa. Moreover, the situations described for presentations of monoids (following definition 3) can be generalized to groups hence extending the whole scenario to free group rings. Negative results on the question of the decidability of the existence of a finite Gröbner basis with respect to a given ordering similar to theorem 4 or the question of the decidability of the existence of an ordering such that a finite Gröbner basis exists as in corollary 5 can be derived.

5 Relating the Generalized Word and One-Sided Ideal Membership Problems in Groups and Group Rings

This section is concerned with another fundamental decision problem introduced by Dehn in 1911 for groups.

Definition 8 *Given a subgroup $\mathcal{U}$ of a group $\mathcal{G}$ the* **generalized word problem for $\mathcal{U}$** *or the* **subgroup problem for $\mathcal{U}$** *is to determine, given $w \in \mathcal{G}$, whether $w \in \mathcal{U}$.*

Given a finite subset S of a group $\mathcal{G}$, we let $\langle S \rangle = \{s_1 \circ \ldots \circ s_n \mid n \in \mathbf{N}, s_i \in S \cup S^{-1}\}$ denote the subgroup generated by S. A subgroup $\mathcal{U}$ of a group $\mathcal{G}$ is called **finitely generated** if there exists a finite subset S of $\mathcal{G}$ such that $\mathcal{U} = \langle S \rangle$.

The word problem for a group $\mathcal{G}$ is just the generalized word problem for the trivial subgroup in $\mathcal{G}$ since $u = v$ holds in $\mathcal{G}$ if and only if $u \circ v^{-1} = \lambda$ holds in $\mathcal{G}$, i.e. $u \circ v^{-1} \in \langle \lambda \rangle$. Thus the existence of a group with undecidable word problem yields undecidability for the generalized word problem for this group as well. On the other hand, decidable word problem for a group does not imply decidable generalized word problem (for an overview on various decision problems for groups see e.g. [Mi91]).

Now due to the existence of inverses, the word problem for congruences on free groups can also be formulated as a special type of subgroup problem. Let T be a set of relations on a free group $\mathcal{F}_\Sigma$. Then we can associate a set $T_1 \subseteq \mathcal{F}_\Sigma$ to T by setting $T_1 = \{l \circ_{\mathcal{F}_\Sigma} r^{-1} \mid (l,r) \in T\}$. Let $\mathcal{N}$ be the normal closure[9] of T_1 in $\mathcal{F}_\Sigma$. Then in fact the word problem for the group $\mathcal{F}_\Sigma / \mathcal{N}$ can be reduced to the subgroup problem for $\mathcal{N}$ since a relation $u = v$ holds in $\mathcal{F}_\Sigma/\mathcal{N}$ if and only if $u \circ v^{-1} = \lambda$ holds in $\mathcal{F}_\Sigma/\mathcal{N}$, i.e. $u \circ v^{-1} \in \mathcal{N}$. Notice that in general $\mathcal{N}$ is not a finitely generated subgroup.

Subgroups of groups can be characterized by one-sided congruences on the group. In the following we restrict ourselves to the case of right congruences (left congruences can be introduced in a similar fashion). Let $\mathcal{U}$ be a subgroup of a group $\mathcal{G}$. Then for $u, v \in \mathcal{G}$ we can define

$$u \sim_{\mathcal{U}} v \text{ if and only if } \mathcal{U}u = \mathcal{U}v$$

[9] The normal closure of a set T in $\mathcal{F}_\Sigma$ is the smallest normal subgroup containing T.

where $\mathcal{U}u = \{g \circ u \mid g \in \mathcal{U}\}$. It is easy to prove that $\sim_{\mathcal{U}}$ is a right congruence induced by $\mathcal{U}$ on $\mathcal{G}$. The subgroup $\mathcal{U}$ itself is a congruence class, namely the one generated by λ. This right congruence is a congruence if and only if $\mathcal{U}$ is a normal subgroup.

The fact that $\mathcal{U}u = \mathcal{U}v$ holds if and only if $v \circ u^{-1} \in \mathcal{U}$, is used in the proof of the next theorem, which states that the subgroup problem for a group is equivalent to a special instance of the right respectively left ideal membership problem in the corresponding group ring.

Theorem 9 ([Re95, MaRe93]) *Let S be a finite subset of $\mathcal{G}$ and $\mathbf{K}[\mathcal{G}]$ the group ring over $\mathcal{G}$. Further let $P_S = \{s - 1 \mid s \in S\} \subseteq \mathbf{K}[\mathcal{G}]$ be the set of polynomials associated to S. Then the following statements are equivalent:*

(1) $w \in \langle S \rangle$.

(2) $w - 1 \in \mathsf{ideal}_r(P_S)$.

(3) $w - 1 \in \mathsf{ideal}_l(P_S)$.

Proof :
$1 \Longrightarrow 2$: Let $w = s_1 \circ \ldots \circ s_k \in \langle S \rangle$, i.e., $s_1, \ldots, s_k \in S \cup \{\mathsf{inv}(s) | s \in S\}$. We show $w - 1 \in \mathsf{ideal}_r(P_S)$ by induction on k. In the base case $k = 0$ there is nothing to show, as $w = \lambda \in \langle S \rangle$ and $0 \in \mathsf{ideal}_r(P_S)$. Hence, suppose $w = s_1 \circ \ldots \circ s_{k+1}$ and $s_1 \circ \ldots \circ s_k - 1 \in \mathsf{ideal}_r(P_S)$. Then $(s_1 \circ \ldots \circ s_k - 1) * s_{k+1} \in \mathsf{ideal}_r(P_S)$ and, since $s_{k+1} - 1 \in \mathsf{ideal}_r(P_S)$[10], we get $(s_1 \circ \ldots \circ s_k - 1) * s_{k+1} + (s_{k+1} - 1) = w - 1 \in \mathsf{ideal}_r(P_S)$.

$2 \Longrightarrow 1$: We have to show that $w - 1 \in \mathsf{ideal}_r(P_T)$ implies $w \in \langle S \rangle$. We know $w - 1 = \sum_{j=1}^{n} \alpha_j \cdot (s_j - 1) * x_j$, where $\alpha_j \in \mathbf{K}^*$, $s_j \in S \cup \{\mathsf{inv}(s) | s \in S\}$, $x_j \in \mathcal{G}$. 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 $w_j \circ \mathsf{inv}(w'_j) \in \langle S \rangle$ implies $w \in \langle S \rangle$. 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 $t = \max_{\succeq}\{w_j, w'_j \mid j = 1, \ldots m\}$ 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 $w = 1 = 1 \circ \lambda = \lambda$ and hence $w \in \langle S \rangle$. Thus let us assume $m > 0$.
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 $t \circ \mathsf{inv}(w'_k) \in \langle S \rangle$ and our induction hypothesis yields $w'_k \in \langle S \rangle$, we can conclude $w = t = t \circ (\mathsf{inv}(w'_k) \circ w'_k) = (t \circ \mathsf{inv}(w'_k)) \circ w'_k \in \langle S \rangle$.
In case $K > 1$ there are at least 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

[10] We either have $s_{k+1} - 1 \in P_S$ or $\mathsf{inv}(s_{k+1}) \in S$, i.e., $(\mathsf{inv}(s_{k+1}) - 1) * s_{k+1} = 1 - s_{k+1} \in \mathsf{ideal}(P_S)$.

$(\alpha_k + \alpha_l) \cdot p_l$. Otherwise we can proceed as follows:

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

where $p'_k = \alpha_k \cdot (w'_l - w'_k)$, $w'_k \neq w'_l$ and $w'_k \circ \mathsf{inv}(w'_l) \in \langle S \rangle$, since $w'_k \circ \mathsf{inv}(t), t \circ \mathsf{inv}(w'_l) \in \langle S \rangle$ 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.
The equivalence for the left ideal can be shown analogously.

q.e.d.

Remember that in the free monoid ring the one-sided ideal membership problem is decidable by special string rewriting techniques (prefix or suffix rewriting) for the finitely generated case. For group rings the existence of a group, while presented by a finite convergent string rewriting system, having undecidable subgroup problem immediately implies that the one-sided ideal membership problem in group rings is undecidable in general. Hence we can only expect group rings where the group has solvable generalized word problem to allow solvable membership problem for right or left ideals. So appropriate candidates are e.g. finite, free, plain, context-free, Abelian, nilpotent and polycyclic groups [KuMaOt94]. The proof of theorem 9 again reveals how representations of products in subgroups are related to representations of sums of products of special polynomials in group rings and vice versa (compare the monoid case in theorem 1). We will again link rewriting techniques used to solve the subgroup problems to the respective ideal membership problems in analogy to the study of the word problem for monoids in the previous section.

As we have discussed before, a subgroup of a group induces a right congruence on the group. Hence it is important to find means of describing one-sided congruences by rewriting techniques. For groups presented by string rewriting systems this has been done using prefix rewriting by Kuhn and Madlener (see [KuMa89, Ku91]) and for polycyclic groups by Wißmann (see [AvWi89, Wi89, KuMaOt94]). More details on these approaches will be given later on.

First we review how the subgroup problem can be treated by rewriting techniques. Let $\mathcal{G}$ be a group presented by a finite convergent string rewriting system (Σ, T) and S be a finite generating set of a subgroup of $\mathcal{G}$. We assume that S is closed under inverses, i.e., if $s \in S$ so is $\mathsf{inv}(s)$. Then we can define a right congruence on Σ^* by $w \sim_S v$ if and only if there exists $x \in \langle S \rangle$ such that $w \overset{*}{\longleftrightarrow}_T xv$. Now the key idea is to express this right congruence by a rewriting relation. This can for example be done by introducing a reduction relation $\Longrightarrow_S$ depending on the generators S such that $w \Longrightarrow_S v$ for $w, v \in \mathcal{G}$ if and only if there exists $s \in S \cup S^{-1}$ such that $v = s \circ w$ and $w \succ v$ where $\succ$ is the ordering on $\mathcal{G}$ induced by the completion ordering of the string rewriting system (Σ, T) presenting $\mathcal{G}$. Moreover, since $\langle S \rangle$ is the coset of the empty word λ presenting the unit, a **λ-confluent generating set** B of $\langle S \rangle$ for this reduction relation, i.e. we have $\langle B \rangle = \langle S \rangle$ and for all $w \in \langle S \rangle$ we have $w \overset{*}{\Longrightarrow}_B \lambda$, then is sufficient to decide the subgroup problem.

We now want to demonstrate how **strong reduction**[11] in group rings is related to solutions of the subgroup problem by rewriting techniques. This is a specialization of our techniques developed for right ideals in general monoid rings. A similar definition for left ideals is possible.

Strong reduction $\longrightarrow^{\mathsf{s}}$ 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 $p \longrightarrow^{\mathsf{s}}_{f} p - \alpha \cdot f * w = q$, where $\alpha \in \mathbf{K}$ such that $t \notin \mathsf{T}(q)$. Notice that for a set of polynomials F we write $p \longrightarrow^{\mathsf{s}}_{F}$ in case there exists $f \in F$ such that $p \longrightarrow^{\mathsf{s}}_{f}$. Then $\stackrel{*}{\longleftrightarrow}^{\mathsf{s}}_{F} = \equiv_{\mathsf{ideal}_r(F)}$ holds and if additionally $\longrightarrow^{\mathsf{s}}_{F}$ is confluent we call F a **strong Gröbner basis** of $\mathsf{ideal}_r(F)$.

First we take a closer look at the outcome of using only restricted polynomials f of the form $x - y$ or $-x + y$ for reduction where $x \succ y$ are in $\mathcal{G}$. Then reducing a polynomial of the form $w \in \mathcal{G}$ by such a polynomial gives us either $w \longrightarrow^{\mathsf{s}}_{f} y \circ (\mathsf{inv}(x) \circ w)$ in case $w = (x \circ \mathsf{inv}(x)) \circ w \succ (y \circ \mathsf{inv}(x)) \circ w$ or $w \longrightarrow^{\mathsf{s}}_{f} x \circ (\mathsf{inv}(y) \circ w)$ in case $w = (y \circ \mathsf{inv}(y)) \circ w \succ (x \circ \mathsf{inv}(y)) \circ w$. Thus such a reduction step in the group ring corresponds directly to a reduction step of 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 the group. On the other hand, for $s \in \mathcal{G}$ a reduction step $w \Longrightarrow_{s} s \circ w$ can be restated as strongly reducing a polynomial w by a polynomial $s - 1$ and, since we know that $w \succ s \circ w$, we get $w \longrightarrow^{\mathsf{s}}_{s-1} s \circ w$.

Moreover we can show that the right ideal generated by a set of polynomials $P_S = \{s - 1 \mid s \in S\}$ has a (not necessarily finite) Gröbner basis with respect to strong reduction 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 generating set of the subgroup $\langle S \rangle$ such that $\Longrightarrow_B$ is confluent. The proof is done using two lemmata. The first one shows that for a polynomial in $\mathsf{ideal}_r(P_S)$ there exist special representations in terms of polynomials containing only two monomials and involving only terms of the polynomial itself.

Lemma 10 ([Re96]) *Let g be a polynomial in the non-trivial right ideal generated by $P_S = \{s - 1 \mid s \in S\} \subseteq \mathbf{K}[\mathcal{G}]$. Then g has a representation of the form*

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

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

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

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

[11] A thorough study of the properties of strong reduction as well as other possible definitions of reduction applicable in this context can be found in [Re95].

Then by our induction hypothesis we know $h = \sum_{i=1}^{n} \alpha_i \cdot (x_i - y_i)$ where $\alpha_i \in \mathbf{K}$, $x_i, y_i \in \mathsf{T}(h)$, $x_i - y_i \in \mathsf{ideal}_r(P_S)$. Notice that $\mathsf{T}(h) \subseteq \mathsf{T}(g) \cup \{s \circ w, w\}$. We have to distinguish the following cases: If $s \circ w, w \notin \mathsf{T}(h)$ we are done at once since this either implies $s \circ w, w \in \mathsf{T}(g)$ or $\beta \cdot (s \circ w - w) = 0$. In case $s \circ w \in \mathsf{T}(h)$ and $w \notin \mathsf{T}(h)$ (the case $s \circ w \notin \mathsf{T}(h)$ and $w \in \mathsf{T}(h)$ is similar) without loss of generality let $s \circ w = x_j$ for $1 \leq j \leq k$. Then in case $\sum_{j=1}^{k} \beta_j \neq -\beta$ we find $s \circ w \in \mathsf{T}(g)$ and the representation $g = \sum_{i=1}^{n} \alpha_i \cdot (x_i - y_i) + \beta \cdot (s \circ w - w)$ already has the desired form. Else we show that such a representation can be achieved by induction on the number k of terms $s \circ w$ occurring in this representation. In the base case $k = 1$ we get $\alpha_1 = -\beta$ and hence

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

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

$$\begin{aligned} g &= \sum_{i=k+1}^{n} \alpha_i \cdot (x_i - y_i) + \sum_{i=1}^{k-1} \alpha_i \cdot (s \circ w - y_i) + \alpha_k \cdot (s \circ w - y_k) + \beta \cdot (s \circ w - w) \\ &= \sum_{i=k+1}^{n} \alpha_i \cdot (x_i - y_i) + \sum_{i=1}^{k-1} \alpha_i \cdot (s \circ w - y_i) + (\alpha_k + \beta) \cdot (s \circ w - y_k) \\ &\qquad - \beta \cdot (s \circ w - y_k) + \beta \cdot (s \circ w - w) \\ &= \sum_{i=k+1}^{n} \alpha_i \cdot (x_i - y_i) + \sum_{i=1}^{k-1} \alpha_i \cdot (s \circ w - y_i) + (\alpha_k + \beta) \cdot (s \circ w - y_k) + \beta \cdot (y_k - w) \\ &= \sum_{i=k+1}^{n} \alpha_i \cdot (x_i - y_i) + \beta \cdot (y_k - w) + \sum_{i=1}^{k-1} \alpha_i \cdot (s \circ w - y_i) + (\alpha_k + \beta) \cdot (s \circ w - y_k) \end{aligned}$$

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

q.e.d.

Notice that in general for polynomials p, q, q_1, q_2, $p \longrightarrow_{q}^{s}$ and $q \longrightarrow_{q_1}^{s} q_2$ need not imply $p \longrightarrow_{\{q_1, q_2\}}^{s}$. This property is closely related to interreduction and hence interreducing a basis might destroy properties of the basis and there are examples where the property of being a Gröbner basis with respect to strong reduction is lost. Still in case q, q_1 and q_2 are related in a special way, this will not happen due to the following fact:

Lemma 11 ([Re96]) *Let p, q, q_1, q_2 be some polynomials in* $\mathbf{K}[\mathcal{G}]$ *such that* $p \longrightarrow^{s}_{q}$, $q \longrightarrow^{s}_{q_1} q_2$, $q = \alpha \cdot q_1 + q_2$, $\alpha \in \mathbf{K}$ *and* $\mathsf{T}(q) = \mathsf{T}(q_1) \cup \mathsf{T}(q_2)$. *Then we can conclude* $p \longrightarrow^{s}_{\{q_1,q_2\}}$.

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.

It holds that a (not necessarily finite) set G is a strong Gröbner basis if and only if for all $g \in \mathsf{ideal}_r(G)$ we have $g \overset{*}{\longrightarrow}^{s}_{G} 0$, i.e., every $g \in \mathsf{ideal}_r(G) \backslash \{0\}$ is strongly reducible using a polynomial in G. Suppose G contains polynomials q, q_1 as described in lemma 11. Then in case we have $q \longrightarrow^{s}_{q_1} q_2$, 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 strongly 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 (not necessarily finite) Gröbner basis of the right ideal generated by P_S which contains only polynomials of the form $u - v$. Let G be an arbitrary strong Gröbner basis of $\mathsf{ideal}_r(P_S)$. Every polynomial g in G has a representation as described in lemma 10, say $g = \sum_{i=1}^{n_g} \alpha_i^{(g)} \cdot (x_i^{(g)} - y_i^{(g)})$. Then the set $G' = G \cup \{x_i^{(g)} - y_i^{(g)} \mid g = \sum_{i=1}^{n_g} \alpha_i^{(g)} \cdot (x_i^{(g)} - y_i^{(g)}), g \in G, i = 1, \ldots, n_g\}$ is again a strong Gröbner basis which can be transformed into a (interreduced) generating set $\{x_i^{(g)} - y_i^{(g)} \mid g = \sum_{i=1}^{n_g} \alpha_i \cdot (x_i^{(g)} - y_i^{(g)}), g \in G, i = 1, \ldots, n_g\}$ which by our previous remark remains a strong Gröbner basis of the right ideal generated by P_S.

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 $f - g \overset{*}{\longrightarrow}^{s}_{G} 0$ implies the existence of a polynomial h such that $f \overset{*}{\longrightarrow}^{s}_{G} h$ and $g \overset{*}{\longrightarrow}^{s}_{G} h$, i.e. unique representatives can be computed by reduction and this can be used to compute unique representatives for the cosets in the group case. As shown in [Re95], in special cases finite strong Gröbner bases can be computed using appropriate weakenings of strong reduction. We now want to illustrate how such weakenings are related to known rewriting solutions of the subgroup problem.

In [KuMa89] Kuhn and Madlener have shown how the notion of prefix rewriting – a specialization of ordinary string rewriting – can be applied to solve the subgroup problem for certain classes of groups, namely finite, free and plain groups. Prefix rewriting and its completion procedure is a direct generalization of Nielsen's method to solve the subgroup problem in the class of free groups [Ni21]. Finite confluent prefix rewriting systems then can be used to compute Schreier-representatives of the subgroup cosets. An extension of the prefix rewriting approach has been given by Cremanns and Otto for the case of context-free groups [CrOt94], and a thorough study of such systems and their limits can be found in [Cr95]. In order to show the connection to Gröbner bases in group rings, we consider the following weakening of strong reduction – **prefix reduction**. For $p, f \in \mathbf{K}[\mathcal{G}]$, let $\mathsf{HT}(f)w \equiv t$ for some $t \in \mathsf{T}(p)$, $w \in \mathcal{G}$, then $p \longrightarrow^{p}_{f} p - \alpha \cdot f * w = q$, where $\alpha \in \mathbf{K}$ such that $t \notin \mathsf{T}(q)$. Then a finite prefix Gröbner basis for the right ideal generated by a set $P_S = \{s - 1 \mid s \in S\}$ implies the existence of a finite prefix Gröbner basis of the form $\{x - y \mid x, y \in \mathcal{G}\}$, which can be interpreted as a finite convergent prefix rewriting system for the subgroup problem. In [MaRe93, MaRe95] it is shown that finite convergent prefix Gröbner bases exist for finitely generated ideals in group rings over finite, free, plain and context-free groups. And the proof of theorem 9 reveals an even closer connection, namely that the rewriting solutions to the subgroup problem provided by convergent prefix rewriting systems are directly correspond to those provided using prefix Gröbner bases of the respective right ideals.

Another class of groups where rewriting techniques have been successfully applied to solve the subgroup problem are the polycyclic groups. Using the consequences of theorem 9 in this case we are able to strengthen the results known from literature. In [AvWi89, Wi89] Wißmann gives a completion based approach to the subgroup problem for polycyclic groups using prefix rewriting for nilpotent groups presented by convergent so called PCNI-systems and $\Longrightarrow$-reduction for polycyclic groups presented by convergent so called PCP-systems. In the latter case he gives a completion procedure which computes a finite λ-confluent basis B of $\langle S \rangle = [\lambda]_{\sim_{\langle S \rangle}}$, i.e., for all $g \in \langle S \rangle$ we have $g \stackrel{*}{\Longrightarrow}_B \lambda$. Furthermore, Wißmann states for $\Longrightarrow$-reduction that while for PCNI-systems finite confluent bases always exist, this need not be the case for PCP-systems (c.f. Theorem 3.6.9 in [Wi89]). Wißmann's rewriting solution for the subgroup problem in nilpotent groups can be directly related to Gröbner bases with respect to so called quasi-commutative reduction, a weakening of strong reduction which is appropriate for groups presented by convergent PCNI-systems. In choosing different presentations for polycyclic groups, which we named reversed PCP-systems, we have succeeded to give terminating completion algorithms for Gröbner bases with respect to another weakening of strong reduction appropriate for those presentations of the groups. This result now implies that when using the appropriate presentation for the polycyclic groups it is indeed possible to give a rewriting solution for the subgroup problem even by a *convergent* system, i.e. providing unique representatives for the quotient. Left ideals can also be studied using PCNI- respectively PCP-systems. The respective reductions are based on the concept of commutative prefixes due to the fact that the normal forms representing the group elements are ordered group words of the form $a_1^{i_1} \ldots a_n^{i_n}$. However, due to the different collection properties associated with the respective commutation rules in the string rewriting systems presenting the groups, one has to be much more careful in defining a Noetherian reduction than in the commutative case. For more details the reader is referred to [Re95, MaRe95, MaRe97, Re96, MaRe96].

6 Relating the Submonoid and Subalgebra Membership Problems in Monoids and Monoid Rings

While the subgroup problem is thoroughly studied in the literature, the submonoid problem is less investigated except for some special cases like the free monoid case. Submonoids in free monoids are used in the theory of codes, but codes (as regular languages) are usually studied using techniques from formal language theory. Since rewriting techniques are seldom used in this context, in this section we want to introduce appropriate notions for describing submonoids of monoids to give an analogon to the approach presented for subgroups of groups..

Definition 12 *Given a submonoid $\mathcal{U}$ of a monoid $\mathcal{M}$, the* **submonoid problem** *is to* *determine, given $w \in \mathcal{M}$, whether $w \in \mathcal{U}$.*

Given a finite subset S of a monoid $\mathcal{M}$, we let $\langle S \rangle = \{s_1 \circ \ldots \circ s_n \mid n \in \mathbf{N}, s_i \in S\}$ denote the submonoid generated by S. A submonoid $\mathcal{U}$ of a monoid $\mathcal{M}$ is called **finitely generated** if there exists a finite subset S of $\mathcal{M}$ such that $\mathcal{U} = \langle S \rangle$.

In the previous section we have seen how the subgroup problem is related to the membership problem for right respectively left ideals in group rings. Unfortunately, theorem 9 cannot be generalized for the submonoid problem as the following example shows:

Example 13 *Let $\Sigma = \{a, b\}, T = \{ab \longrightarrow \lambda\}$ be a string rewriting system presenting of a monoid $\mathcal{M}$, the bicyclic monoid. Let $\mathcal{U} = \{a^n \mid n \in \mathbf{N}\}$ be the submonoid of $\mathcal{M}$ generated by $S = \{a\}$. Then we have $b - 1 \in \mathsf{ideal}_r(P_S)$ since $b - 1 = -1 \cdot (a - 1) * b$ but $b \notin \mathcal{U}$. Theorem 9 would lead to $b \in \mathcal{U}$.*

The problem shown in this example is due to the following observation: As in the subgroup case, a submonoid $\mathcal{U}$ of a monoid $\mathcal{M}$ induces a right congruence on $\mathcal{M}$ by setting

$$u \sim_{\mathcal{U}} v \text{ if and only if } \mathcal{U}u = \mathcal{U}v$$

for $u, v \in \mathcal{M}$. But the submonoid itself in general is no longer the right congruence class $[\lambda]_{\sim_{\mathcal{U}}}$. In our example we find that $b \in [\lambda]_{\sim_{\mathcal{U}}}$ while $b \notin \mathcal{U} = \{a^n \mid n \in \mathbf{N}\}$. Hence the submonoid cannot be described adequately in the monoid ring using the right ideal congruence as in the subgroup case studied before. But there is another algebraic substructure of monoid rings which is appropriate to restate the submonoid problem in algebraic terms - the subalgebra.

Definition 14 *A nonempty subset S of $\mathbf{K}[\mathcal{M}]$ is called a* **subalgebra** *of $\mathbf{K}[\mathcal{M}]$, if the following hold:*

1. *$\mathbf{K} \subseteq S$,*
2. *for all $f, g \in S$ we have $f - g \in S$, and*
3. *for all $f, g \in S$ we have $f * g \in S$.*

Notice how the third condition differs from the definition of ideals. For a subset $P \subset \mathbf{K}[\mathcal{M}]$ let $\mathsf{subalgebra}(P)$ denote the minimal subalgebra of $\mathbf{K}[\mathcal{M}]$ containing P. The next theorem states that the submonoid problem for a monoid is equivalent to a special instance of the subalgebra membership problem in the corresponding monoid ring.

Theorem 15 *Let S be a subset of $\mathcal{M}$ and $P_S = \{s - 1 \mid s \in S\}$ a subset of $\mathbf{K}[\mathcal{M}]$ associated to S. Then the following statements are equivalent:*

(1) $w \in \langle S \rangle$.

(2) $w - 1 \in \mathsf{subalgebra}(P_S)$.

Proof :
$1 \Longrightarrow 2$: Let $w = s_1 \circ \ldots \circ s_k \in \langle S \rangle$, i.e., $s_1, \ldots, s_k \in S$. We show $w - 1 \in \mathsf{subalgebra}(P_S)$ by induction on k. In the base case $k = 0$ there is nothing to show, as $w = 1 \in \langle S \rangle$ and $1 - 1 = 0 \in \mathsf{subalgebra}(P_S)$. Hence, suppose $k > 1$, i.e. $w = s_1 \circ \ldots \circ s_k$ and $s_1 \circ \ldots \circ s_{k-1} - 1, s_k - 1 \in \mathsf{subalgebra}(P_S)$. We can write

$$w - 1 = \underbrace{(s_1 \circ \ldots \circ s_{k-1} - 1) * (s_k - 1)}_{\in\, \mathsf{subalgebra}(P_S)} + \underbrace{(s_1 \circ \ldots \circ s_{k-1} - 1)}_{\in\, \mathsf{subalgebra}(P_S)} + \underbrace{(s_k - 1)}_{\in\, \mathsf{subalgebra}(P_S)}$$

implying that $w - 1 \in \mathsf{subalgebra}(P_S)$.
$2 \Longrightarrow 1$: To see that $w-1 \in \mathsf{subalgebra}(P_S)$ implies $w \in \langle S \rangle$ we show a more general result: For every $f \in \mathsf{subalgebra}(P_S)$ we have that every term $t \in \mathsf{T}(f)$ is an element of $\langle S \rangle$. By the definition of a subalgebra, $f \in \mathsf{subalgebra}(P_S)$ has a representation of the form $f = \sum_{i=1}^{n} \alpha_i \cdot \prod_{j=1}^{k_n} p_{i_j}$ with $p_{i_j} \in P_S$ and $\alpha_i \in \mathbf{K}$. We show that every term occurring in such a product $\prod_{j=1}^{k_n} p_{i_j}$ lies in $\langle S \rangle$ by induction on k_n. In the base case $k_n = 1$ we find $\prod_{j=1}^{1} p_{i_j} = s - 1$ and since $s, 1 \in \langle S \rangle$ we are done. Hence, suppose $k_n > 1$, i.e. $\prod_{j=1}^{k_n} p_{i_j} = (\prod_{j=1}^{k_n - 1} p_{i_j}) * (s - 1)$, and by our induction hypothesis we know that $\prod_{j=1}^{k_n-1} p_{i_j} = \sum_{l=1}^{m} \beta_i \cdot t_i$ where every term t_i belongs to $\langle S \rangle$. Then every term occurring in $\sum_{l=1}^{m} \beta_i \cdot t_i * (s-1) = \sum_{l=1}^{m} \beta_i \cdot t_i \circ s - \sum_{l=1}^{m} \beta_i \cdot t_i$ again must lie in $\langle S \rangle$.

q.e.d.

Two basic approaches to solve the subalgebra problem in the commutative case using rewriting techniques can be found in the literature. In [KaMa89] Kapur and Madlener introduce a special rewriting relation which describes subalgebras in polynomial rings and provide a completion procedure. Their procedure in fact computes "Gröbner bases" of subalgebras but in general need not terminate, even in case the subalgebra is finitely generated. The termination problem can be overcome for finitely generated subalgebras when transforming the subalgebra membership problem into a special ideal membership problem in an extended polynomial ring. This is done in [ShSw88] by Shannon and Sweedler by introducing tag variables and computing ordinary Gröbner bases of the transformed ideals in the "enlarged" polynomial ring. Other approaches can be found in [RoSw90, Mi96].

Here we want to generalize the approach given in [ShSw88]: Let S be a finite subset of a monoid $\mathcal{M}$. For each $s \in S$ let z_s be a new letter not occurring among the generators of $\mathcal{M}$ and let Z_S denote the set of all such tag variables. With $\mathcal{M} \times Z_S^*$ we denote the free product of the monoid $\mathcal{M}$ and the free monoid Z_S^*. We associate a set of polynomials to S in the monoid ring $\mathbf{K}[\mathcal{M} \times Z_S^*]$ by setting $P_S = \{s - z_s \mid s \in S\}$. In this context the following holds:

Theorem 16 *Let S be a subset of $\mathcal{M}$ and $P_S = \{s - z_s \mid s \in S\}$ a subset of $\mathbf{K}[\mathcal{M} \times Z_S^*]$ associated to S. Then the following statements are equivalent:*

(1) $w \in \langle S \rangle$.

(2) $w - t_w \in \mathsf{ideal}^{\mathbf{K}[\mathcal{M} \times Z_S^*]}(P_S)$ *for some* $t_w \in Z_S^*$.

Proof :
Within this proof we will abbreviate $\mathsf{ideal}^{\mathbf{K}[\mathcal{M} \times Z_S^*]}(P_S)$ by $\mathsf{ideal}(P_S)$.

$1 \Longrightarrow 2$: Let $w = s_1 \circ \ldots \circ s_k \in \langle S \rangle$, i.e., $s_1, \ldots, s_k \in S$. We show the existence of some $t_w \in Z_S^*$ such that $w - t_w \in \mathsf{ideal}(P_S)$ by induction on k. In the base case $k = 0$ there is nothing to show, as $w = 1$, $t_w = 1 \in Z_S^*$ and $1 - 1 = 0 \in \mathsf{ideal}(P_S)$. Hence, suppose $k > 1$, i.e. $w = s_1 \circ \ldots \circ s_k$ and there exists $t \in Z_S^*$ such that $s_1 \circ \ldots \circ s_{k-1} - t, s_k - z_{s_k} \in \mathsf{ideal}(P_S)$. Then we find that

$$\underbrace{(s_1 \circ \ldots \circ s_{k-1} - t) * (s_k - z_{s_k})}_{\in \mathsf{ideal}(P_S)} + \underbrace{(s_1 \circ \ldots \circ s_{k-1} - t) * z_{s_k}}_{\in \mathsf{ideal}(P_S)} + \underbrace{t * (s_k - 1)}_{\in \mathsf{ideal}(P_S)}$$

lies in $\mathsf{ideal}(P_S)$ and this sum equals $s_1 \circ \ldots \circ s_k - t * z_{s_k}$, i.e. we can choose $t_w = t * z_{s_k} \in Z_S^*$ and we are done.
$2 \Longrightarrow 1$: Let us introduce the following homomorphisms:

$$\begin{array}{rcl} \phi_1 : Z_S^* & \longrightarrow & \mathcal{M} \\ \lambda & \longmapsto & \lambda \\ z_s & \longmapsto & s \end{array}$$

which is lifted to elements of Z_S^* and then to

$$\begin{array}{lrcl} \phi_2 : & \mathcal{M} \times Z_S^* & \longrightarrow & \mathcal{M} \\ & w_1 v_1 \ldots w_l v_l & \longmapsto & \phi_1(w_1) \circ \phi_1(v_1) \circ \ldots \phi_1(w_l) \circ \phi_1(v_l) \end{array}$$

where $l \in \mathbf{N}$, $w_i \in \mathcal{M}$ and $v_l \in Z_S^*$ and again lifted to

$$\begin{array}{rcl} \phi : \mathbf{K}[\mathcal{M} \times Z_S^*] & \longrightarrow & \mathbf{K}[\mathcal{M}] \\ \sum_{i=1}^{m} \alpha_i \cdot t_i & \longmapsto & \sum_{i=1}^{m} \alpha_i \cdot \phi_2(t_i) \end{array}$$

Then $\mathsf{ideal}(P_S) \subseteq \mathsf{kernel}(\phi)$, as $f \in \mathsf{ideal}(P_S)$ implies $f = \sum_{i=1}^m p_i * (s_i - z_{s_i}) * q_i$ for some $s_i \in S$, $p_i, q_i \in \mathbf{K}[\mathcal{M} \times Z_S^*]$. Hence $w - t_w \in \mathsf{ideal}(P_S)$ yields $\phi(w - t_w) = 0$ and therefore $w = \phi(t_w) = \phi_1(t_w)$. As $t_w \in Z_S^*$ this gives us $w \in \langle S \rangle$.

q.e.d.

The proof of this theorem also provides a technique which can be used to give a more precise characterization of the subalgebra generated by S. Let us study the following homomorphism:

$$\begin{array}{lrcl} \psi : & \mathbf{K}[Z_S^*] & \longrightarrow & \mathbf{K}[\mathcal{M}] \\ & \sum_{i=1}^{m} \alpha_i \cdot t_i & \longmapsto & \sum_{i=1}^{m} \alpha_i \cdot \phi_1(t_i) \end{array}$$

Then we can show that the kernel of this homomorphism is in fact $\mathsf{ideal}^{\mathbf{K}[\mathcal{M} \times Z_S^*]}(P_S) \cap \mathbf{K}[Z_S^*]$. The inclusion $\mathsf{ideal}^{\mathbf{K}[\mathcal{M} \times Z_S^*]}(P_S) \cap \mathbf{K}[Z_S^*] \subseteq \mathsf{kernel}(\psi)$ follows at once as in the previous proof. Hence let us assume $f \in \mathsf{kernel}(\psi)$, i.e. $f = \sum_{i=1}^m \alpha_i \cdot t_i$ with $\alpha_i \in \mathbf{K}$, $t_i \in Z_S^*$ and $\psi(f) = 0$.

Then we can represent f as

$$\begin{aligned} f &= f - \psi(f) \\ &= \sum_{i=1}^{m} \alpha_i \cdot t_i - \sum_{i=1}^{m} \alpha_i \cdot \phi_1(t_i) \\ &= \sum_{i=1}^{m} \alpha_i \cdot (t_i - \phi_1(t_i)). \end{aligned}$$

In showing $t_i - \phi_1(t_i) \in \mathsf{ideal}(P_S)$ we are done. Since $\phi_1(t_i) \in \langle S \rangle$ this can be shown straightforward as in the proof of theorem 16 by induction on k where t_i contains k variables, i.e. $\phi_1(t_i) = s_1 \circ \ldots \circ s_k$, $s_1, \ldots, s_k \in S$.

In commutative polynomial rings *elimination orderings* are used to compute Gröbner bases of the kernel of ψ. We can proceed in a similar fashion and introduce elimination orderings for Σ^*. Then in case a finite Gröbner basis G_e can be computed for $\mathsf{ideal}^{\mathbf{K}[\Sigma^* \times Z_S^*]}(P_S)$ in $\mathbf{K}[\Sigma^* \times Z_S^*]$ with respect to an elimination ordering the submonoid problem for $\langle S \rangle$ can be solved using rewriting techniques since for $w \in \Sigma^*$ we have $w \in \langle S \rangle$ if and only if the normal form of w with respect to $\longrightarrow_{G_e}$ is a word in Z_S^*. Notice that since the existence of finite such Gröbner bases in $\mathbf{K}[\Sigma^* \times Z_S^*]$ due to theorem 1 is very restricted, this reduction is mainly of theoretical interest.

The results of this section differ from the ones in the previous sections in the following way: While the word problems in monoids and groups and the generalized word problem for groups have been studied first and reduction techniques for the respective rings have been introduced later, here the well-studied subalgebra membership problem is generalized for monoid rings providing new techniques to treat submonoid problems. How useful these techniques are remains to be seen.

7 Concluding Remarks

The class of finitely presented groups contains subclasses which – using appropriate presentations – allow to solve the subgroup problem using string rewriting techniques. In this paper we have pointed out how these results are related to the existence (and in fact even the construction) of Gröbner bases in the respective group rings. This shall now be summarized in the following table, which lists the reductions which – again using appropriate presentations for the groups – ensure the construction of the respective finite Gröbner basis of ideals. Note that $\longrightarrow^{\mathrm{su}}$ stands for suffix, $\longrightarrow^{\mathrm{p}}$ for prefix, $\longrightarrow^{\mathrm{qc}}$ for quasi-commutative, $\longrightarrow^{\mathrm{lpc}}$ for left-polycyclic reduction and $\longrightarrow^{\mathrm{rpc}}$ for right-polycyclic reduction (for more information on the reductions and the computation of Gröbner bases related to them see [MaRe93, Re95, MaRe95, MaRe97, Re96, MaRe96]).

Group	*left ideals*	*right ideals*	*two-sided ideals*
free	$\longrightarrow^{\mathrm{su}}$	$\longrightarrow^{\mathrm{p}}$	none[12]
plain	$\longrightarrow^{\mathrm{su}}$	$\longrightarrow^{\mathrm{p}}$	none
context-free	$\longrightarrow^{\mathrm{su}}$	$\longrightarrow^{\mathrm{p}}$	none
nilpotent	$\longrightarrow^{\mathrm{lpc}}$	$\longrightarrow^{\mathrm{qc}}$	$\longrightarrow^{\mathrm{qc}}$ $\longrightarrow^{\mathrm{lpc}}$
polycyclic	$\longrightarrow^{\mathrm{lpc}}$	$\longrightarrow^{\mathrm{rpc}}$	$\longrightarrow^{\mathrm{lpc}}$ $\longrightarrow^{\mathrm{rpc}}$

As mentioned above, the different reductions require special forms of presentations for the respective groups. Free groups need free presentations with length-lexicographical completion ordering for prefix and suffix reduction. Plain groups require canonical 2-monadic presentations with inverses of length 1 and again length-lexicographical completion ordering for prefix as well as suffix reduction. Context-free groups demand virtually free presentations (see [CrOt94]) for prefix and a modified version of these presentations for suffix reduction. All these special forms of the presentations are similarly required when solving the subgroup problem using prefix rewriting techniques. For nilpotent groups we need convergent PCNI-systems for quasi-commutative and left-polycyclic reduction. In the case of polycyclic groups we need PCP-systems for left-polycyclic and reversed PCP-systems for right-polycyclic reduction.

References

[AvWi89] J. Avenhaus and D. Wißmann. *Using Rewriting Techniques to Solve the Generalized Word Problem in Polycyclic Groups.* Proc. ISSAC'89. pp 322-337.

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

[Bu83] B. Buchberger. *A Critical-Pair Completion Algorithm for Finitely Generated Ideals in Rings.* Proc. Logic and Machines: Decision Problems and Complexity. Springer LNCS 171(1983). pp 137-161.

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

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

[12] By theorem 6 the existence of such finite bases would solve the word problem for groups presented by finite string rewriting systems.

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

[Gi79] R. Gilman. *Presentations of Groups and Monoids.* Journal of Algebra 57(1979). pp 544-554.

[Hu80] G. Huet. *Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems.* Journal of the ACM 27(4)(1980). pp 797-821.

[Hu81] G. Huet. *A Complete Proof of Correctness of the Knuth-Bendix Completion Algorithm.* Journal of Computer and System Science 23(1)(1981). pp 11-21.

[Ja81] M. Jantzen. *On a Special Monoid with Single Defining Relation.* Theoretical Computer Science 16(1981). pp 61-73.

[Ja85] M. Jantzen. *A Note on a Special One-rule Semi-Thue System.* Information Processing Letters 21(1985). pp 135-140.

[Jo76] D.L. Johnson. *Presentation of Groups.* London Mathematical Society Lecture Note Series 22. Cambridge University Press. 1976.

[KaKaWi89] A. Kandri-Rody, D. Kapur and F. Winkler. *Knuth-Bendix Procedure and Buchberger Algorithm – a Synthesis.* Proc. ISSAC'89. pp 55-67.

[KaMa89] D. Kapur and K. Madlener. *A Completion Procedure for Computing a Canonical Basis for a k-Subalgebra.* Computers and Mathematics. Springer Verlag. 1989. pp 1-11.

[KaNa85] D. Kapur and P. Narendran. *A Finite Thue System with Decidable Word Problem and Without Equivalent Finite Canonical System.* Theoretical Computer Science 35(1985). pp 337-344.

[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.

[KnBe70] D. Knuth and P. Bendix. *Simple Word Problems in Universal Algebras.* J. Leech (editor). Computaional Problems in Abstract Algebra. Pergamon Press. Oxford. 1970. pp 263-297.

[Ku91] N. Kuhn. *Zur Entscheidbarkeit des Untergruppenproblems für Gruppen mit kanonischen Darstellungen.* Dissertation. Universität Kaiserslautern. 1991.

[KuMa89] N. Kuhn and K. Madlener. *A Method for Enumerating Cosets of a Group Presented by a Canonical System.* Proc. ISSAC'89. pp 338-350.

[KuMaOt94] N. Kuhn, K. Madlener and F. Otto. *Computing Presentations for Subgroups of Polycyclic Groups and of Context-Free Groups.* Applicable Algebra in Engineering, Communication and Computing 5(1994). pp 287-316.

[La79] G. Lallement. *Semigroups and Combinatorial Applications.* John Wiley & Sons. New York. 1979.

[LySch77] R. C. Lyndon and P. E. Schupp. *Combinatorial Group Theory.* Springer Verlag(1977).

[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.

[MaOt94] K. Madlener and F. Otto. *Some Undecidability Results for Finitely Generated Thue Congruences on a Two-Letter Alphabet.* E. Schock (ed.). Beiträge zur Angewandten Analysis und Informatik, Helmut Brakhage zu Ehren. Verlag Shaker. Aachen. 1994. pp 248-261.

[MaRe93] K. Madlener and B. Reinert. *Computing Gröbner Bases in Monoid and Group Rings.* Proc. ISSAC'93. pp 254-263.

[MaRe95] K. Madlener and B. Reinert. *String Rewriting and Gröbner Bases – A General Approach to Monoid and Group Rings.* Proceedings of the Workshop on Symbolic Rewriting Techniques. Monte Verita. 1995. (to appear)

[MaRe96] K. Madlener and B. Reinert. *A Generalization of Gröbner Basis Algorithms to Polycyclic Group Rings.* Journal of Symbolic Computation. (to appear)

[MaRe97] K. Madlener and B. Reinert. *A Generalization of Gröbner Bases Algorithms to Nilpotent Group Rings.* Applicable Algebra in Engineering, Communication and Computing Vol. 8 No. 2(1997). pp 103-123.

[MaKaSo76] W. Magnus, A. Karrass and D. Solitar. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations.* Dover Publications. New York. 1976.

[MaMeSa93] S. Margolis, J. Meakin and M. Sapir. *Algorithmic Problems in Groups, Semigroups and Inverse Monoids.* Semigroups, Formal Languages and Groups. J. Fountain (ed). Kluwer Academic Press. 1993. pp 147-214.

[Mi91] C.F. Miller. *Decision Problems for Groups – Survey and Reflections.* Algorithms and Classification in Combinatorial Group Theory. G. Baumslag, C.F. Miller (eds.). Springer Verlag. 1991. pp 1-60.

[Mi96] J.L. Miller. *Analogs of Gröbner Bases in Polynomial Rings over a Ring.* Journal of Symbolic Computation 21(1996). pp 139-153.

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

[Mo87] T. Mora. *Gröbner Bases and the Word Problem.* Working Paper. 1987.

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

[Ni21] J. Nielsen. *Om Regning med ikke kommutative Faktoren og dens Anvendelse i Gruppeteorien.* Mat. Tidsskr. B.(1921). pp 77-94.

[OD83] C. Ó'Dúnlaing. *Undecidable Questions Related to Church-Rosser Thue Systems.* Theoretical Computer Science 23(1983). pp 339-345.

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

[Re96] B. Reinert. *Introducing Reduction to Polycyclic Group Rings - A Comparison of Methods.* Reports on Computer Algebra No 9. Centre of Computer Algebra. Universität Kaiserslautern. 1996.

[RoSw90] L. Robbiano and M. Sweedler. *Subalgebra Bases.* Proc. Commutative Algebra Salavador. W. Burns, A. Simis (eds.). Springer LNM 1430. 1990. pp 61-87.

[Sa96] A. Sattler-Klein. *A Systematic Study of Infinite Canonical Systems generated by Knuth-Bendix Completion and Related Problems.* Dissertation. Universität Kaiserslautern. 1996.

[ShSw88] D. Shannon and M. Sweedler. *Using Gröbner Bases to Determine Algebra Membership, Split Surjective Algebra Homomorphisms Determine Birational Equivalence.* Journal of Symbolic Computation 6(1988). pp 267-273.

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

[Sq87] C. Squier. *Word Problems and a Homological Finiteness Condition for Monoids.* Journal of Pure Applied Algebra 49(1987). pp 201-217.

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

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.