Revista Colombiana de Matemáticas
Volumen 33 (1999), páginas 27–49

Non-commutative reduction rings

Klaus Madlener
Birgit Reinert[1]
Universität Kaiserslautern, Germany

Abstract. Reduction relations are means to express congruences on rings. In the special case of congruences induced by ideals in commutative polynomial rings, the powerful tool of Gröbner bases can be characterized by properties of reduction relations associated with ideal bases. Hence, reduction rings can be seen as rings with reduction relations associated to subsets of the ring such that every finitely generated ideal has a finite Gröbner basis. This paper gives an axiomatic framework for studying reduction rings including non-commutative rings and explores when and how the property of being a reduction ring is preserved by standard ring constructions such as quotients and sums of reduction rings, as well as extensions to polynomial and monoid rings over reduction rings. Moreover, it is outlined when such reduction rings are effective.

Keywords and phrases. Reduction rings, Gröbner bases, non-commutative rings, standard ring constructions.

1991 Mathematics Subject Classification. Primary 68Q40. Secondary 12Y05, 68Q42, 13P10.

1. Introduction

Reasoning and computing in finitely presented algebraic structures is widespread in many fields of mathematics, physics and computer science. Many of the resulting problems can be formulated in terms of congruences on the

[1] This author was supported by the Deutsche Forschungsgemeinschaft (DFG).

respective structures. Reduction in the sense of simplification combined with appropriate completion methods is one general technique which is often successfully applied in this context, e.g. to solve the word problem and hence to compute effectively in the structure.

One fundamental application of this technique to polynomial rings was provided by B. Buchberger [2] in his uniform effective solution of the ideal membership problem establishing the theory of Gröbner bases. Polynomials can be used as rules by giving an admissible[2] ordering on the terms and using the largest monomial according to this ordering as a left hand side of a rule. "Reduction" as defined by Buchberger then can be compared to division of one polynomial by a set of finitely many polynomials. A Gröbner basis G is a set of polynomials such that every polynomial in the polynomial ring has a unique normal form with respect to reduction using the polynomials in G as rules (the polynomials in the ideal generated by G reduce to zero using G). Buchberger developed a terminating procedure to transform a finite generating set of a polynomial ideal into a finite Gröbner basis of the same ideal. Gröbner bases can be characterized in various other manners, e.g. by properties of their head monomials or by special representations for the ideal elements with respect to a Gröbner basis (called standard representations). Since Gröbner bases can be applied to solve many problems related to ideals and varieties in polynomial rings, generalizations to other structures followed (for an overview see e.g. Becker and Weispfenning [1] or Madlener and Reinert [10]). In this context, it is interesting to find sufficient conditions allowing to define a reduction relation for a ring in such a way that every finitely generated ideal in the ring has a finite Gröbner basis with respect to that reduction relation. Such rings will be called *reduction rings*. Often additional conditions can be given to ensure effectivity for the ring operations, the reduction relation, and the computation of the Gröbner bases —the ring is then called an *effective reduction ring*. Naturally the question arises as to when and how the property of being a reduction ring is preserved under various ring constructions. This can be studied from an existential as well as from a constructive point of view. One main goal of studying abstract reduction rings is to provide universal methods for constructing new reduction rings without having to generalize the whole setting individually for each new structure: e.g. knowing that the integers $\mathbb{Z}$ form a reduction ring and that the property lifts to polynomials in one variable, we find that $\mathbb{Z}[X]$ is again a reduction ring and we can immediately conclude that also $\mathbb{Z}[X_1, \dots , X_n]$ is a reduction ring. Similarly, as sums of reduction

[2] A term ordering $\succeq$ is called admissible if for every term s, t, u, $s \succeq 1$ holds, and $s \succeq t$ implies $s \circ u \succeq t \circ u$. An ordering fulfilling the latter condition is also said to be compatible with the respective multiplication $\circ$.

rings are again reduction rings, we can directly conclude that $\mathbb{Z}^k[X_1,\dots,X_n]$ or even $(\mathbb{Z}[Y_1,\dots,Y_m])^k[X_1,\dots,X_n]$ are reduction rings. Moreover, since $\mathbb{Z}$ is an effective reduction ring it can be shown that these new reduction rings again are effective. Commutative effective reduction rings have been studied by Buchberger [3], Madlener [8] and Stifter [19]).

On the other hand, many rings of interest are non-commutative, e.g. rings of matrices, the ring of quaternions, Bezout rings and various monoid rings, and since in many cases they can be regarded as reduction rings, they are again candidates for applying ring constructions. More interesting examples of non-commutative reduction rings have been studied by Pesch [17].

A general framework for reduction rings and ring constructions including the non-commutative case was presented at the Linz conference "33 years of Gröbner Bases" in Madlener and Reinert [13]. Here we want to give an extended version of this paper including more details and proofs. Since, in a first step, we are not interested in effectivity, in Section 2 reduction rings are characterized by specifying three simple and natural axioms for the reduction relation and requiring the existence of finite Gröbner bases. In the remaining sections for different ring constructions we define natural reduction relations fulfilling the axioms and we additionally determine when the property of being a reduction ring is preserved. Moreover, in case the reduction ring is effective the resulting constructions as quotients and sums again are effective reduction rings. For the special case of monoid rings (including polynomial rings) we provide characterizations which enable to test the property of being a Gröbner basis by checking certain test sets which are finite provided the effective reduction ring fulfills additional properties. Such test sets are essential and have been used in critical-pair completion procedures as introduced by D. Knuth and P. Bendix or B. Buchberger for computing equivalent confluent reduction relations. However, while we determine when Gröbner bases exist and outline when they are additionally computable, we do not give procedures to compute them since this would go beyond the scope of this paper.

Let us close this section by summarizing some important notations and definitions of reduction relations which will be used throughout the paper (more details can be found in the book of Book and Otto [4]). Let $\mathcal{E}$ be a set of elements and $\longrightarrow$ a binary relation on $\mathcal{E}$ called *reduction*. For $a, b \in \mathcal{E}$ we will write $a \longrightarrow b$ in case $(a,b) \in \ \longrightarrow$. A pair $(\mathcal{E}, \longrightarrow)$ will be called a *reduction system*. Obviously the reflexive symmetric transitive closure $\overset{*}{\longleftrightarrow}$ is an equivalence relation on $\mathcal{E}$. The *word problem* for $(\mathcal{E}, \longrightarrow)$ is to decide for $a, b \in \mathcal{E}$, whether $a \overset{*}{\longleftrightarrow} b$ holds. An element $a \in \mathcal{E}$ is said to be *reducible* (with respect to $\longrightarrow$, also denoted by $a \longrightarrow$) if there exists an element $b \in \mathcal{E}$ such that $a \longrightarrow b$. If there is no such b, a is called *irreducible* denoted by $a \not\longrightarrow$. In case $a \overset{*}{\longrightarrow} b$ and b is irreducible, b is called a *normal form* of a. $(\mathcal{E}, \longrightarrow)$ is said to be *Noetherian* (or *terminating*) in case there are no infinitely descending reduction chains $a_0 \longrightarrow a_1 \longrightarrow \dots$, with $a_i \in \mathcal{E}$, $i \in \mathbb{N}$. It is called *confluent*, if for all $a, a_1, a_2 \in \mathcal{E}$, $a \overset{*}{\longrightarrow} a_1$ and $a \overset{*}{\longrightarrow} a_2$ implies the existence of $a_3 \in \mathcal{E}$ such that $a_1 \overset{*}{\longrightarrow} a_3$ and $a_2 \overset{*}{\longrightarrow} a_3$. We can combine these two properties to give sufficient conditions for the existence of unique normal forms: $(\mathcal{E}, \longrightarrow)$ is said to be *complete* or *convergent* in case it is both, Noetherian and confluent. In case $(\mathcal{E}, \longrightarrow)$ is Noetherian, confluence is equivalent to local confluence, i.e. for all $a, a_1, a_2 \in \mathcal{E}$, $a \longrightarrow a_1$ and $a \longrightarrow a_2$ implies the existence of $a_3 \in \mathcal{E}$ such that $a_1 \overset{*}{\longrightarrow} a_3$ and $a_2 \overset{*}{\longrightarrow} a_3$. The latter property called Newman's Lemma is often the basis of completion methods for specialized reduction systems as e.g. string rewriting systems or polynomials as rules.

2. **Reduction rings**

Let R be a ring with unit 1 and a (not necessarily effective) reduction relation $\Longrightarrow_B$ associated with subsets $B \subseteq \mathsf{R}$, satisfying the following axioms:

(A1) $\Longrightarrow_B = \bigcup_{\beta \in B} \Longrightarrow_\beta$,
$\Longrightarrow_B$ is terminating for all *finite* subsets $B \subseteq \mathsf{R}$.
(A2) $\alpha \Longrightarrow_\beta \gamma$ implies $\alpha - \gamma \in \mathsf{ideal}^{\mathsf{R}}(\beta)$.
(A3) $\alpha \Longrightarrow_\alpha 0$ for all $\alpha \in \mathsf{R} \setminus \{0\}$.

Part one of Axiom (A1) states how reduction using sets is defined and is hence applicable to arbitrary sets B. However, Axiom (A1) does *not* imply termination of reduction with respect to arbitrary sets. Consider for example the ring $\mathsf{R} = \mathbb{Q}[\{X_i \mid i \in \mathbb{N}\}]$, i.e. the polynomial ring with infinitely many indeterminates, and the reduction relation based on divisibility of head terms with respect to the length-lexicographical ordering induced by $X_1 \succ X_2 \succ \dots$. Then although reduction using a finite set of polynomials is terminating, this is no longer true for infinite sets, as e.g. the set $\{X_i - X_{i+1} \mid i \in \mathbb{N}\}$ gives rise to an infinite reduction sequence $X_1 \Longrightarrow_{X_1 - X_2} X_2 \Longrightarrow_{X_2 - X_3} X_3 \dots$.

It is possible to give a more restricted form of Axiom (A1):

(A1') $\Longrightarrow_B = \bigcup_{\beta \in B} \Longrightarrow_\beta$,
$\Longrightarrow_B$ is terminating for *all* subsets $B \subseteq \mathsf{R}$.

Then, of course, reduction is always terminating, and many additional restrictions which we must add in later parts of the paper are no longer necessary. In this paper we prefer the more general formulation of the axiom.

Axiom (A2) states how reduction steps are related to the ideal congruence, namely, one reduction step using an element $\beta \in \mathsf{R}$ is captured by the congruence generated by $\mathsf{ideal}^{\mathsf{R}}(\beta)$. We will later on see that this extends to the reflexive transitive symmetric closure $\overset{*}{\Longleftrightarrow}_B$ of any reduction relation $\Longrightarrow_B$ for arbitrary sets $B \subseteq \mathsf{R}$.

Notice that in case R is commutative, (A2) implies $\gamma = \alpha - \beta \cdot \rho$ for some $\rho \in \mathsf{R}$. In the non-commutative case, using a single element β for reduction $\alpha - \gamma \in \mathsf{ideal}^{\mathsf{R}}(\beta)$ only implies $\gamma = \alpha - \sum_{i=1}^{k} \rho_{i1} \cdot \beta \cdot \rho_{i2}$ for some $\rho_{i1}, \rho_{i2} \in \mathsf{R}$, $1 \leq i \leq k$, involving β more than once with different multipliers. This provides a large range of possibilities for defining reduction steps, e.g. by subtracting one or more appropriate multiples of β from α. Notice further that Axiom (A2) does not provide any information on how α, $\gamma \in \mathsf{R}$ with $\alpha - \gamma \in \mathsf{ideal}^{\mathsf{R}}(\beta)$ are related with respect to the reduction relation $\Longrightarrow_{\{\beta\}}$.

We can define *one-sided right or left* reduction in rings by refining Axiom (A2) as follows:

(A2r) $\alpha \Longrightarrow_\beta \gamma$ implies $\alpha - \gamma \in \mathsf{ideal}_r^{\mathsf{R}}(\beta)$.
(A2l) $\alpha \Longrightarrow_\beta \gamma$ implies $\alpha - \gamma \in \mathsf{ideal}_l^{\mathsf{R}}(\beta)$.

In these special cases again we always get $\gamma = \alpha - \beta \cdot \rho$, respectively $\gamma = \alpha - \rho \cdot \beta$, for some $\rho \in \mathsf{R}$.

Remember that Axiom (A2) while not specific on the exact form of the reduction step ensures that reduction steps "stay" within the ideal congruence. Let us now study the situation for arbitrary sets $B \subseteq \mathsf{R}$ and let $\equiv_{\mathfrak{i}}$ denote the congruence generated by the ideal $\mathfrak{i} = \mathsf{ideal}(B)$. Then (A1)[3] and (A2) immediately imply $\overset{*}{\Longleftrightarrow}_B \subseteq \equiv_{\mathfrak{i}}$. Hence, in case the reduction relation is effective one method for deciding the membership problem for a finitely generated ideal $\mathfrak{i}$ is to transform a finite generating set B into a finite set B' such that B' still generates $\mathfrak{i}$ and $\Longrightarrow_{B'}$ is confluent on $\mathfrak{i}$. Notice that 0 has to be irreducible for all $\Longrightarrow_\alpha$, $\alpha \in \mathsf{R}$[4]. Therefore, 0 can be chosen as *the* normal form of the ideal elements. Hence the goal is to achieve $\alpha \in \mathfrak{i}$ if and only if $\alpha \overset{*}{\Longrightarrow}_{B'} 0$. In particular, $\mathfrak{i}$ is one equivalence class of $\overset{*}{\Longleftrightarrow}_{B'}$. The different definitions of reduction relations for rings existing in literature show that for deciding the membership problem of an ideal $\mathfrak{i}$ it is not necessary to enforce $\overset{*}{\Longleftrightarrow}_{B'} = \equiv_{\mathfrak{i}}$. For example the D-reduction notion given by Pan [16] does not have this property but still is sufficient to decide $\equiv_{\mathfrak{i}}$-equivalence of two elements because $\alpha \equiv_{\mathfrak{i}} \beta$ if and

[3] We only need the first part of Axiom (A1), namely how $\Longrightarrow_B$ is defined, and hence we do not have to restrict ourselves to finite sets.

[4] 0 cannot be reducible by itself since this would contradict the termination property in (A1). Similarly, $0 \Longrightarrow_\beta 0$ and $0 \Longrightarrow_\beta \gamma$, both β and γ not equal 0, give rise to infinite reduction sequences again contradicting (A1).

only if $\alpha - \beta \in \mathfrak{i}$. It may even happen that D-reduction is not only confluent on $\mathfrak{i}$ but confluent everywhere and still $\alpha \equiv_{\mathfrak{i}} \beta$ does not imply that the normal forms with respect to D-reduction are the same.

Example 2.1. Let us illustrate different ways of introducing reduction for the ring of integers $\mathbb{Z}$. For $\alpha, \beta, \gamma \in \mathbb{Z}$ we define:

- $\alpha \Longrightarrow^1_\beta \gamma$ if and only if $\alpha = \kappa \cdot |\beta| + \gamma$ where $0 \leq \gamma < |\beta|$ and $\kappa \in \mathbb{Z}$,
- $\alpha \Longrightarrow^2_\beta 0$ if and only if $\alpha = \kappa \cdot \beta$, i.e. β is a proper divisor of α.

Then for example we have $5 \Longrightarrow^1_4 1$ but $5 \not\Longrightarrow^2_4$.

It is easy to show that both reductions satisfy $(A1)$–$(A3)$. Moreover, the elements in $\mathbb{Z}$ have unique normal forms. An element belongs to $\mathsf{ideal}(4)$ if and only if it is reducible to zero using 4. For $\Longrightarrow^1$-reduction the normal forms are unique representatives of the quotient $\mathbb{Z}/\mathsf{ideal}(4)$. This is no longer true for $\Longrightarrow^2$-reduction, e.g. $3 \equiv_{\mathsf{ideal}(4)} 7$ since $7 = 3+4$, but both are $\Longrightarrow^2$-irreducible.

However, if we want unique normal forms for all elements in R so that each congruence has one representative, we need special ideal bases.

Definition 2.2. A subset B of R is called a *Gröbner basis* of the ideal $\mathfrak{i} = \mathsf{ideal}^{\mathsf{R}}(B)$, if $\overset{*}{\Longleftrightarrow}_B = \equiv_{\mathfrak{i}}$ and $\Longrightarrow_B$ is convergent[5].

Rings where finitely generated ideals have finite Gröbner bases are of particular interest.

Definition 2.3. A ring $(\mathsf{R}, \Longrightarrow)$ satisfying (A1)–(A3) is called a *reduction ring* if every finitely generated ideal in R has a finite Gröbner basis.

To simplify the notation, sometimes we will identify $(\mathsf{R}, \Longrightarrow)$ with R in case $\Longrightarrow$ is known or irrelevant. The notion of *one-sided reduction rings* is straightforward.

Effective or *computable reduction rings* can be defined similarly to Buchberger's commutative reduction rings (see Buchberger [3] or Stifter [19]), in our case by demanding that the ring operations are computable, reduction is effective, and Gröbner bases can be computed. Procedures to compute Gröbner bases are normally completion procedures, based on effective tests (e.g. testing special polynomials for reducibility to zero) to decide whether a finite set is a

[5] Notice that in the literature the definition of Gröbner bases normally require that "$\Longrightarrow_B$ is confluent". This is due to the fact that in these cases $\Longrightarrow_B$ is terminating. In our context, however, for arbitrary sets $B \subseteq \mathsf{R}$ we have seen that $\Longrightarrow_B$ need not be Noetherian. Hence we have to incorporate this additional requirement into our definition, which is done by demanding convergence. In rings where reduction using an arbitrary set of elements is always Noetherian, the weaker demand for (local) confluence is of course sufficient.

Gröbner basis and to alter that set if not. Of course, other procedures are also possible, e.g. using the Euclidean algorithm for computing Gröbner bases in $\mathbb{Z}$.

Notice that Definition 2.3 does not imply that Noetherian rings satisfying Axioms (A1), (A2) and (A3) are reduction rings. This is due to the fact that the property of being a reduction ring is, of course, strongly dependent on the reduction relation chosen for the ring. For example given a Noetherian ring R we can associate a (very simple) reduction relation to elements of R by defining $\alpha \Longrightarrow_\beta$ if and only if $\alpha = \beta$. Additionally we define $\alpha \Longrightarrow_\alpha 0$. Then the Axioms (A1), (A2) and (A3) are fulfilled but, although every ideal in the Noetherian ring R has a finite basis (in the sense of a generating set), infinite ideals will not have finite Gröbner bases[6].

Another interesting question concerns changes to ideal bases which preserve the property of being a Gröbner basis. Extensions of Gröbner bases by ideal elements are not critical.

Remark 2.4. If B is a finite Gröbner basis of $\mathfrak{i}$ and $\alpha \in \mathfrak{i}$, then $B' = B \cup \{\alpha\}$ is again a Gröbner basis of $\mathfrak{i}$. First of all we find $\overset{*}{\Longleftrightarrow}_B \subseteq \overset{*}{\Longleftrightarrow}_{B'} \subseteq \equiv_{\mathfrak{i}} = \overset{*}{\Longleftrightarrow}_B$. Moreover, since B' is again a finite set $\Longrightarrow_{B'}$ is terminating. Finally, $\Longrightarrow_{B'}$ inherits its confluence from $\Longrightarrow_B$ since $\beta \Longrightarrow_\alpha \gamma$ implies $\beta \equiv_{\mathfrak{i}} \gamma$ and so β and γ have the same normal form with respect to $\Longrightarrow_B$.

Hence, if B is a Gröbner basis of an ideal $\mathfrak{i}$ and $\beta \in B$ is reducible by $B \setminus \{\beta\}$ to α, then $B \cup \{\alpha\}$ is again a Gröbner basis of $\mathfrak{i}$. In order to remove β from $B \cup \{\alpha\}$ without losing the Gröbner basis property it is important for $\Longrightarrow$ to satisfy an additional axiom:

(A4) $\alpha \Longrightarrow_\beta$ and $\beta \Longrightarrow_\gamma \delta$ imply $\alpha \Longrightarrow_\gamma$ or $\alpha \Longrightarrow_\delta$.

Lemma 2.5. *Let $(\mathsf{R}, \Longrightarrow)$ be a reduction ring satisfying (A4). Further let $B \subseteq \mathsf{R}$ be a Gröbner basis and $B' \subseteq B$ such that for all $\beta \in B$, $\beta \overset{*}{\Longrightarrow}_{B'} 0$ holds. Then B' is a Gröbner basis of $\mathsf{ideal}^{\mathsf{R}}(B)$. In particular, for all $\alpha \in \mathsf{R}$, $\alpha \overset{*}{\Longrightarrow}_B 0$ implies $\alpha \overset{*}{\Longrightarrow}_{B'} 0$.*

Proof. In this proof let $\alpha\Downarrow_B$ denote a normal form of α with respect to $\Longrightarrow_B$ and let $\mathsf{IRR}(\Longrightarrow_B)$ denote the $\Longrightarrow_B$-irreducible elements in R. Notice that by the Axioms (A1) and (A4) and our assumptions on B', all elements reducible by B are also reducible by B': We show a more general claim by induction on n: If $\alpha, \beta \in \mathsf{R}$ such that $\alpha \Longrightarrow_\beta$ and $\beta \overset{n}{\Longrightarrow}_{B'} 0$, then $\alpha \Longrightarrow_{B'}$. The base case $n = 1$ is a direct consequence of (A4), as $\alpha \Longrightarrow_\beta$ and $\beta \Longrightarrow_{\beta' \in B'} 0$ immediately imply $\alpha \Longrightarrow_{\beta' \in B'}$. In the induction step we find $\beta \Longrightarrow_{\beta' \in B'} \delta \overset{n-1}{\Longrightarrow}_{B'} 0$ and either $\alpha \Longrightarrow_{\beta' \in B'}$ or $\alpha \Longrightarrow_\delta$ and our induction hypothesis yields $\alpha \Longrightarrow_{B'}$.

[6] For any ideal $\mathfrak{i} \subseteq \mathsf{R}$, in this setting, the set $\mathfrak{i} \setminus \{0\}$ is the only possible Gröbner basis.

Hence we can conclude $\mathsf{IRR}(\Longrightarrow_{B'}) \subseteq \mathsf{IRR}(\Longrightarrow_B)$. We want to show that B' is a Gröbner basis of $\mathsf{ideal}^{\mathsf{R}}(B)$: assuming $\alpha \overset{*}{\Longrightarrow}_B \alpha\Downarrow_B$ but $\alpha \overset{*}{\Longrightarrow}_{B'} \alpha\Downarrow_{B'} \neq \alpha\Downarrow_B$, we find $\alpha \overset{*}{\Longrightarrow}_B \alpha\Downarrow_{B'}$ and $\alpha\Downarrow_{B'} \in \mathsf{IRR}(\Longrightarrow_{B'}) \subseteq \mathsf{IRR}(\Longrightarrow_B)$, contradicting the confluence of $\Longrightarrow_B$. Hence, $\alpha\Downarrow_{B'} = \alpha\Downarrow_B$, implying that $\Longrightarrow_{B'}$ is also confluent, as $\alpha\Downarrow_B$ is unique. Now it remains to show that $\overset{*}{\Longleftrightarrow}_B \subseteq \overset{*}{\Longleftrightarrow}_{B'}$ holds. This follows immediately, as for $\alpha \overset{*}{\Longleftrightarrow}_B \beta$ we have $\alpha\Downarrow_{B'} = \alpha\Downarrow_B = \beta\Downarrow_B = \beta\Downarrow_{B'}$ which implies $\alpha \overset{*}{\Longleftrightarrow}_{B'} \beta$. ☑

Remark 2.4 and Lemma 2.5 are closely related to interreduction and reduced Gröbner bases. We call a Gröbner basis $B \subseteq \mathsf{R}$ *reduced* if no element $\beta \in B$ is reducible by $\Longrightarrow_{B \setminus \{\beta\}}$.

In the remaining sections of the paper we study the question of which ring constructions, as e.g. extensions, products, sums or quotients, preserve the property of being a reduction ring.

3. Quotients of reduction rings

Let $(\mathsf{R}, \Longrightarrow)$ be a reduction ring and $\mathfrak{i}$ a finitely generated ideal in R with a (finite) Gröbner basis B. Then every element $\alpha \in \mathsf{R}$ has a unique normal form $\alpha\Downarrow_B$ with respect to $\Longrightarrow_B$. We choose the set of $\Longrightarrow_B$-irreducible elements of R as representatives for the elements in the *quotient* $\mathsf{R}/\mathfrak{i}$. Addition is defined by $\alpha + \beta := (\alpha + \beta)\Downarrow_B$ and multiplication by $\alpha \cdot \beta := (\alpha \cdot \beta)\Downarrow_B$. Then a natural reduction can be defined on the quotient $\mathsf{R}/\mathfrak{i}$ as follows:

Definition 3.1. Let $\alpha, \beta, \gamma \in \mathsf{R}/\mathfrak{i}$. We say that β *reduces* α to γ in one step, denoted by $\alpha \longrightarrow_\beta \gamma$, if there exists $\gamma' \in \mathsf{R}$ such that $\alpha \Longrightarrow_\beta \gamma'$ and $(\gamma')\Downarrow_B = \gamma$.

First we ensure that the Axioms (A1)–(A3) hold for reduction in $\mathsf{R}/\mathfrak{i}$ as defined in Definition 3.1: $\longrightarrow_S = \bigcup_{s \in S} \longrightarrow_s$ is terminating for all finite $S \subseteq \mathsf{R}/\mathfrak{i}$ since otherwise $\Longrightarrow_{B \cup S}$ would not be terminating in R, although $B \cup S$ is finite. Hence, (A1) is satisfied. If $\alpha \longrightarrow_\beta \gamma$ for some $\alpha, \beta, \gamma \in \mathsf{R}/\mathfrak{i}$, we know $\alpha \Longrightarrow_\beta \gamma' \overset{*}{\Longrightarrow}_B \gamma$, i.e. $\alpha - \gamma \in \mathsf{ideal}^{\mathsf{R}}(\{\beta\} \cup B)$, and hence $\alpha - \gamma \in \mathsf{ideal}^{\mathsf{R}/\mathfrak{i}}(\beta)$. Therefore, (A2) is also fulfilled. Finally, Axiom (A3) holds since $\alpha \Longrightarrow_\alpha 0$ for all $\alpha \in \mathsf{R} \setminus \{0\}$ implies $\alpha \longrightarrow_\alpha 0$.

Moreover, in case (A4) holds in R this is also true for $\mathsf{R}/\mathfrak{i}$: for $\alpha, \beta, \gamma, \delta \in \mathsf{R}/\mathfrak{i}$ we have that $\alpha \longrightarrow_\beta$ and $\beta \longrightarrow_\gamma \delta$ imply $\alpha \Longrightarrow_\beta$ and $\beta \Longrightarrow_\gamma \delta' \overset{*}{\Longrightarrow}_B \delta$, and since α is $\Longrightarrow_B$-irreducible this implies $\alpha \Longrightarrow_{\{\gamma, \delta\}}$, so $\alpha \longrightarrow_{\{\gamma, \delta\}}$.

Theorem 3.2. *If* $(\mathsf{R}, \Longrightarrow)$ *is a reduction ring with (A4), then for every finitely generated ideal* $\mathfrak{i}$ *the quotient* $(\mathsf{R}/\mathfrak{i}, \longrightarrow)$ *again is a reduction ring with (A4).*

Proof. Since reduction in R/i as defined above inherits (A1)–(A4) from R, it remains to show that every finitely generated ideal $\mathsf{j} \subseteq \mathsf{R}/\mathsf{i}$ has a finite Gröbner basis. Let $\mathsf{j}_{\mathsf{R}} = \{\alpha \in \mathsf{R} \mid \alpha\Downarrow_B \in \mathsf{j}\}$ be an ideal in R corresponding to j. Since j_{R} is a *finitely* generated ideal in R, it has a finite Gröbner basis, say G_{R}. Then $G = \{\alpha\Downarrow_B \mid \alpha \in G_{\mathsf{R}}\} \setminus \{0\}$ is a finite Gröbner basis of j: If $\alpha \in \mathsf{j}$ we have $\alpha \overset{*}{\longrightarrow}_G 0$ and $\mathsf{ideal}^{\mathsf{R}/\mathsf{i}}(G) = \mathsf{j}$, as every element which is reducible with an element $\beta \in G_{\mathsf{R}}$ is also reducible with an element of $G \cup B$ because (A4) holds. Since $G \cup B$ is also a Gröbner basis of j_{R} and $\longrightarrow_G \subseteq \overset{*}{\Longrightarrow}_{G\cup B}$, when restricted to elements in R/i we have $\mathsf{IRR}(\longrightarrow_G) = \mathsf{IRR}(\Longrightarrow_{G\cup B})$ and $\longrightarrow_G$ is confluent. Furthermore, because $\equiv_{\mathsf{j}} = \equiv_{\mathsf{j}_{\mathsf{R}}}$ when restricted to R/i, we get $\overset{*}{\longleftrightarrow}_G = \equiv_{\mathsf{j}}$ on R/i, implying that R/i is a reduction ring. ☑

In Example 2.1 we have seen how to associate the integers with a reduction relation $\longrightarrow^1$ and in fact $(\mathbb{Z}, \longrightarrow^1)$ is a reduction ring. Theorem 3.2 then states that for every $m \in \mathbb{Z}$ the quotient $\mathbb{Z}/\mathsf{ideal}(m)$ again is a reduction ring. In particular reduction rings with zero divisors can be constructed in this way.

Now if $(\mathsf{R}, \Longrightarrow)$ is an effective reduction ring, then B can be computed and addition and multiplication in R/i, as well as the reduction of Definition 3.1 are computable operations. Moreover, Theorem 3.2 can be generalized:

Corollary 3.3. *If* $(\mathsf{R}, \Longrightarrow)$ *is an effective reduction ring satisfying (A4), then for every finitely generated ideal* i *the quotient* $(\mathsf{R}/\mathsf{i}, \longrightarrow)$ *again is an effective reduction ring with (A4).*

Proof. Given R, B and a finite generating set F for an ideal j in R/i we can compute a Gröbner basis for j using the method for computing Gröbner bases in R: compute a Gröbner basis G_{R} of the ideal generated by $B \cup F$ in R. Then the set $G = \{\mathsf{normal.form}(g, \Longrightarrow_B) \mid g \in G_{\mathsf{R}}\}$, where $\mathsf{normal.form}(g, \Longrightarrow_B)$ is the normal form of g with respect to B in R and so an element of R/i, is a Gröbner basis of j in R/i. ☑

Theorem 3.2 and Corollary 3.3 extend to the case of one-sided reduction rings with (A4) provided that the two-sided ideal has a finite right respectively left Gröbner basis.

4. Sums of reduction rings

Let $(\mathsf{R}_1, \Longrightarrow^1)$, $(\mathsf{R}_2, \Longrightarrow^2)$ be reduction rings. Then $\mathsf{R} = \mathsf{R}_1 \times \mathsf{R}_2 = \{(\alpha_1, \alpha_2) \mid \alpha_1 \in \mathsf{R}_1, \alpha_2 \in \mathsf{R}_2\}$ is called the *direct sum* of R_1 and R_2. Addition and multiplication are defined componentwise, the unit is $(1_1, 1_2)$ where 1_i is the respective unit in R_i. A natural reduction can be defined on R as follows:

Definition 4.1. Let $\alpha = (\alpha_1, \alpha_2)$, $\beta = (\beta_1, \beta_2)$, $\gamma = (\gamma_1, \gamma_2) \in \mathsf{R}$. We say that β *reduces* α to γ in one step, denoted by $\alpha \longrightarrow_{\beta} \gamma$, if either ($\alpha_1 \Longrightarrow^1_{\beta_1} \gamma_1$ and $\alpha_2 = \gamma_2$) or ($\alpha_1 = \gamma_1$ and $\alpha_2 \Longrightarrow^2_{\beta_2} \gamma_2$) or ($\alpha_1 \Longrightarrow^1_{\beta_1} \gamma_1$ and $\alpha_2 \Longrightarrow^2_{\beta_2} \gamma_2$).

Again we have to prove that the Axioms (A1)–(A3) hold for reduction in R: $\longrightarrow_B = \bigcup_{\beta \in B} \longrightarrow_{\beta}$ is terminating for finite $B \subseteq \mathsf{R}$ since this property is inherited from the termination of the respective reductions in R_i. Hence, (A1) holds. (A2) is satisfied because $\alpha \longrightarrow_{\beta} \gamma$ implies $\alpha - \gamma \in \mathsf{ideal}^{\mathsf{R}}(\beta)$. (A3) is true as $\alpha \longrightarrow_{\alpha} (0_1, 0_2)$ holds for all $\alpha \in \mathsf{R} \setminus \{(0_1, 0_2)\}$. Moreover, it is easy to see that if condition (A4) holds for $\Longrightarrow^1$ and $\Longrightarrow^2$ then it is inherited by $\longrightarrow$.

Theorem 4.2. *If* $(\mathsf{R}_1, \Longrightarrow^1)$, $(\mathsf{R}_2, \Longrightarrow^2)$ *are reduction rings, then* $(\mathsf{R} = \mathsf{R}_1 \times \mathsf{R}_2, \longrightarrow)$ *is again a reduction ring.*

Proof. Since reduction in R as defined above inherits (A1)–(A3), respectively (A4), from the reductions in the R_i, it remains to show that every finitely generated ideal $\mathfrak{i} \subseteq \mathsf{R}$ has a finite Gröbner basis. To see this notice that the restrictions $\mathfrak{i}_1 = \{\alpha_1 \mid (\alpha_1, \alpha_2) \in \mathfrak{i} \text{ for some } \alpha_2 \in \mathsf{R}_2\}$ and $\mathfrak{i}_2 = \{\alpha_2 \mid (\alpha_1, \alpha_2) \in \mathfrak{i} \text{ for some } \alpha_1 \in \mathsf{R}_1\}$ are finitely generated ideals in R_1, respectively R_2, and hence have finite Gröbner bases B_1, respectively B_2. We claim that $B = \{(\beta_1, 0_2), (0_1, \beta_2) \mid \beta_1 \in B_1, \beta_2 \in B_2\}$ is a finite Gröbner basis of $\mathfrak{i}$. Notice that $\mathfrak{i} = \mathfrak{i}_1 \times \mathfrak{i}_2$ and the elements of $\mathfrak{i}_1$, $\mathfrak{i}_2$ are "included" in $\mathfrak{i}$ via multiplication with $(1_1, 0_2)$, respectively $(0_1, 1_2)$. Then $\mathsf{ideal}(B) = \mathfrak{i}$ and $\alpha \in \mathfrak{i}$ implies $\alpha \overset{*}{\longrightarrow}_B (0_1, 0_2)$ due to the fact that for $\alpha = (\alpha_1, \alpha_2)$ we have $\alpha_1 \in \mathfrak{i}_1$ and $\alpha_2 \in \mathfrak{i}_2$ implying $\alpha_1 \overset{*}{\Longrightarrow}^1_{B_1} 0_1$ and $\alpha_2 \overset{*}{\Longrightarrow}^2_{B_2} 0_2$. Similarly $\longrightarrow_B$ is confluent because $\Longrightarrow^1_{B_1}$ and $\Longrightarrow^2_{B_2}$ are confluent. Finally $\overset{*}{\longleftrightarrow}_B \; = \; \equiv_{\mathfrak{i}}$ since $(\alpha_1, \alpha_2) \equiv_{\mathfrak{i}} (\beta_1, \beta_2)$ implies $\alpha_1 \equiv_{\mathfrak{i}_1} \beta_1$, respectively $\alpha_2 \equiv_{\mathfrak{i}_2} \beta_2$, and hence $\alpha_1 \overset{*}{\Longleftrightarrow}^1_{B_1} \beta_1$, respectively $\alpha_2 \overset{*}{\Longleftrightarrow}^2_{B_2} \beta_2$. ☑

Special regular rings as introduced by Weispfenning [20] provide examples of such sums of reduction rings.

Now if $(\mathsf{R}_1, \Longrightarrow^1)$, $(\mathsf{R}_2, \Longrightarrow^2)$ are effective reduction rings, then addition and multiplication in R, as well as the reduction in Definition 4.1, are computable operations. Moreover, Theorem 4.2 can be generalized:

Corollary 4.3. *If* $(\mathsf{R}_1, \Longrightarrow^1)$, $(\mathsf{R}_2, \Longrightarrow^2)$ *are effective reduction rings, then* $(\mathsf{R} = \mathsf{R}_1 \times \mathsf{R}_2, \longrightarrow)$ *is again an effective reduction ring.*

Proof. Given a finite generating set $F = \{(f_i, g_i) \mid 1 \leq i \leq k, f_i \in \mathsf{R}_1, g_i \in \mathsf{R}_2\}$ a Gröbner basis of the ideal generated by F can be computed using the respective methods for Gröbner basis computation in R_1 and R_2. Compute a Gröbner basis B_1 of the ideal generated by $\{f_1, \ldots, f_k\}$ in R_1 and a Gröbner basis B_2 of the ideal generated by $\{g_1, \dots, g_k\}$ in R_2. Then $B = \{(\beta_1, 0_2), (0_1, \beta_2) \mid \beta_1 \in B_1, \beta_2 \in B_2\}$ is a finite Gröbner basis of the ideal generated by F in R. ☑

Due to the "simple" multiplication used when defining the structure, Theorem 4.2 and Corollary 4.3 extend directly to one-sided reduction rings. More complicated multiplications are possible and have to be treated individually.

5. **Polynomial rings over reduction rings**

For a reduction ring $(\mathsf{R}, \Longrightarrow)$ we adopt the usual notations in $\mathsf{R}[X]$, the polynomial ring in one variable X, where multiplication is denoted by $*$. Notice that for scalar multiplication by $\alpha \in \mathsf{R}$ we assume $\alpha \cdot X = X \cdot \alpha$ (see Pesch [17] for other possibilities). We specify an ordering on the set of terms $\{X^i \mid i \in \mathbb{N}\}$ in one variable by defining that if X^i divides X^j, i.e. $0 \leq i \leq j$, then $X^i \preceq X^j$. Using this ordering, the head term $\mathsf{HT}(p)$, the head monomial $\mathsf{HM}(p)$, and the head coefficient $\mathsf{HC}(p)$ of a polynomial $p \in \mathsf{R}[X]$ are defined as usual, and $\mathsf{RED}(p) = p - \mathsf{HM}(p)$. We extend the function HT to sets of polynomials $F \subseteq \mathsf{R}[X]$ by $\mathsf{HT}(F) = \{\mathsf{HT}(f) \mid f \in F\}$.

Let $\mathfrak{i} \subseteq \mathsf{R}[X]$ be a finitely generated ideal in $\mathsf{R}[X]$. It is easy to see that given a term t the set $C(t, \mathfrak{i}) = \{\mathsf{HC}(f) \mid f \in \mathfrak{i}, \mathsf{HT}(f) = t\} \cup \{0\}$ is an ideal in R. In order to guarantee that these ideals are also finitely generated we will assume that R is a Noetherian ring. Note that for any two terms t and s such that t divides s we have $C(t, \mathfrak{i}) \subseteq C(s, \mathfrak{i})$.

We additionally define a (not necessarily Noetherian) partial ordering on R by setting for $\alpha, \beta \in \mathsf{R}$, $\alpha >_{\mathsf{R}} \beta$ if and only if there exists a finite set $B \subseteq \mathsf{R}$ such that $\alpha \overset{+}{\Longrightarrow}_B \beta$. Then we can define an ordering on $\mathsf{R}[X]$ as follows: For $f, g \in \mathsf{R}[X]$, $f > g$ if and only if either $\mathsf{HT}(f) \succ \mathsf{HT}(g)$ or ($\mathsf{HT}(f) = \mathsf{HT}(g)$ and $\mathsf{HC}(f) >_{\mathsf{R}} \mathsf{HC}(g)$) or ($\mathsf{HM}(f) = \mathsf{HM}(g)$ and $\mathsf{RED}(f) > \mathsf{RED}(g)$). Notice that, in general, this ordering is neither total nor Noetherian on $\mathsf{R}[X]$.

Definition 5.1. Let p, f be two non-zero polynomials in $\mathsf{R}[X]$. We say f *reduces* p to q at a monomial $\alpha \cdot X^i$ in p in one step, denoted by $p \longrightarrow_f q$, if

(a) $\mathsf{HT}(f)$ divides X^i, i.e. $\mathsf{HT}(f)X^j = X^i$ for some term X^j,

(b) $\alpha \Longrightarrow_{\mathsf{HC}(f)} \beta$, with $\alpha = \beta + \sum_{i=1}^{k} \gamma_i \cdot \mathsf{HC}(f) \cdot \delta_i$ for some $\beta, \gamma_i, \delta_i \in \mathsf{R}$, $1 \leq i \leq k$, and

(c) $q = p - \sum_{i=1}^{k} (\gamma_i \cdot f \cdot \delta_i) * X^j$.

Notice that if f reduces p to q at a monomial $\alpha \cdot t$ the term t can still occur in the resulting polynomial q. But when using a *finite* set of polynomials for the reduction we know by (A1) that reducing α in R with respect to the finite set of head coefficients of the applicable polynomials must terminate and then either the monomial containing the term t disappears or is irreducible. Hence, reduction as defined in Definition 5.1 is Noetherian when using *finite* sets of polynomials and Axiom (A1) holds. It is easy to see that (A2) and (A3) are also true, and if the reduction ring satisfies (A4) this is inherited by $\mathsf{R}[X]$.

Theorem 5.2. *If* $(\mathsf{R}, \Longrightarrow)$ *is a Noetherian reduction ring, then* $(\mathsf{R}[X], \longrightarrow)$ *is a Noetherian reduction ring.*

Proof. By Hilbert's basis theorem $\mathsf{R}[X]$ is Noetherian if R is Noetherian. We only have to prove that every (finitely generated) ideal $\mathfrak{i} \neq \{0\}$ in $\mathsf{R}[X]$ has a finite Gröbner basis.

A finite basis G of $\mathfrak{i}$ will be defined in stages according to the degree of the terms occurring as head terms among the polynomials in $\mathfrak{i}$ and then we will show that G is in fact a Gröbner basis.

Let G_0 be a finite Gröbner basis of the ideal $C(\lambda, \mathfrak{i})$ in R, which must exist since R is supposed to be Noetherian. Further, at stage $i > 0$, if for each X^j with $j < i$ we have $C(X^j, \mathfrak{i}) \subsetneqq C(X^i, \mathfrak{i})$, include in G_i for each α in $\textsc{Gb}(C(X^i, \mathfrak{i}))$ (a finite Gröbner basis of $C(X^i, \mathfrak{i})$) a polynomial p_α from $\mathfrak{i}$ such that $\mathsf{HM}(p) = \alpha \cdot X^i$. Notice that in this construction we use the axiom of choice, when choosing p_α from the infinite set $\mathfrak{i}$, and so it is non-constructive. At each stage only a finite number of polynomials can be added since the respective Gröbner bases $\textsc{Gb}(C(X^i, \mathfrak{i}))$ are always finite, and at most one polynomial from $\mathfrak{i}$ is included for each element in $\textsc{Gb}(C(X^i, \mathfrak{i}))$.

If a polynomial with head term X^i is included, then $C(X^j, \mathfrak{i}) \subsetneqq C(X^i, \mathfrak{i})$ for every $j < i$. So, if $X^i \in HT(\mathfrak{i})$ is not included as a head term of a polynomial in G_i, then there is a term X^j occurring as a head term in some set G_j, $j < i$, $C(X^i, \mathfrak{i}) = C(X^j, \mathfrak{i})$, and $C(X^j, G_j)$ is a Gröbner basis for the ideal $C(X^j, \mathfrak{i}) = C(X^i, \mathfrak{i})$ in R.

We claim that the set $G = \bigcup_{i \geq 0} G_i$ is a finite Gröbner basis of $\mathfrak{i}$.

To show that G is finite it suffices to prove that the set $\mathsf{HT}(G)$ is finite, since in every stage only finitely many polynomials, all having *new* head terms, are added. Assuming that $\mathsf{HT}(G)$ is infinite, there is a sequence X^{n_i}, $i \in \mathbb{N}$ of different terms such that $n_i < n_{i+1}$. But then by construction there is an ascending sequence of ideals in R, namely $C(X^{n_0}, \mathfrak{i}) \subsetneqq C(X^{n_1}, \mathfrak{i}) \subsetneqq \ldots$ which contradicts the fact that R is supposed to be Noetherian.

So after some step m no more polynomials p from $\mathfrak{i}$ can be found such that for $\mathsf{HT}(p) = X^i$ the set $C(X^i, \mathfrak{i})$ is different from all $C(X^j, \mathfrak{i})$, $j < i$.

Notice that for all $p \in \mathfrak{i}$ we have $p \xrightarrow{*}_G 0$ and G generates $\mathfrak{i}$. This follows immediately from the construction of G.

To see that $\longrightarrow_G$ is confluent, let p be a polynomial which has two distinct normal forms with respect to G, say p_1 and p_2. Let t be the largest term on which p_1 and p_2 differ and let α_1 and α_2 be the respective coefficients of t in p_1 and p_2. Since $p_1 - p_2 \in \mathfrak{i}$, this polynomial reduces to 0 using G and without loss of generality we can assume that these reductions always take place at the respective head terms of the polynomials in the reduction sequence. Let $s \in \mathsf{HT}(G)$ be the head term of the polynomial in G which reduces $\mathsf{HT}(p_1 - p_2)$, i.e. s divides t, $\alpha_1 - \alpha_2 \in C(s, \mathfrak{i})$, and hence $\alpha_1 \equiv_{\mathfrak{i}} \alpha_2$. Therefore, not both α_1 and α_2 can be in normal form with respect to any Gröbner basis of $C(s, \mathfrak{i})$ and so with respect to the set of head coefficients of polynomials in G with head term s. So both, $\alpha_1 \cdot t$ and $\alpha_2 \cdot t$ cannot be in normal form with respect to G, which is a contradiction to the fact that p_1 and p_2 are supposed to be in normal form with respect to G.

Finally, we have to prove $\equiv_{\mathfrak{i}} = \overset{*}{\longleftrightarrow}_G$. Let $p \equiv_{\mathfrak{i}} q$ both be in normal form with respect to G. Then, as before, $p - q \overset{*}{\longrightarrow}_G 0$ implies $p = q$. Hence, we have shown that G is in fact a finite Gröbner basis of $\mathfrak{i}$. ☑

Of course, this theorem can be applied to $\mathsf{R}[X]$ and a new variable X_2 and by iteration we immediately get the following:

Corollary 5.3. *If $(\mathsf{R}, \Longrightarrow)$ is a Noetherian reduction ring, then $\mathsf{R}[X_1, \dots, X_n]$ is a Noetherian reduction ring with the respective lifted reduction.*

Notice that other definitions of reduction in $\mathsf{R}[X_1, \dots, X_n]$ are known in the literature. These are usually based on divisibility of terms and admissible term orderings on the set of terms to distinguish the head terms. The proof of Theorem 5.2 can be generalized to these cases.

Now, if $(\mathsf{R}, \Longrightarrow)$ is an effective reduction ring, then addition and multiplication in $\mathsf{R}[X]$ as well as reduction as defined in Definition 5.1 are computable operations. Unlike in the previous sections, the proof of Theorem 5.2 does not specify how Gröbner bases for finitely generated ideals in $\mathsf{R}[X]$ can be constructed using Gröbner basis methods for R. So we cannot conclude that for effective reduction rings the polynomial ring again will be effective. A more suitable characterization of Gröbner bases requiring R to fulfill additional conditions will be provided for the more general case of monoid rings in the next section. The basic idea of that characterization will be to define Gröbner bases in terms of completion and to localize the completion test to special sets of polynomials. In order to provide effective completion procedures for computing Gröbner bases, various characterizations of Gröbner bases by finite test sets of special polynomials in certain commutative reduction rings (e.g. the integers and Euclidean domains) can be found in the literature (see e.g. Kapur and Narendran [6], Kandri-Rody and Kapur [5] and Möller [14]). A general approach to the characterization commutative reduction rings, allowing the computation of Gröbner bases via Buchberger's approach was presented by Stifter [19].

We close this section by providing similar characterizations for polynomial rings over non-commutative reduction rings and outlining the arising problems. For simplicity we restrict ourselves to the case of $\mathsf{R}[X]$, but this is no general restriction. Given a generating set $F \subseteq \mathsf{R}[X]$ the key idea is to distinguish special elements of $\mathsf{ideal}(F)$ which have representations $\sum_{i=1}^{n} g_i * f_i * h_i$, $g_i, h_i \in \mathsf{R}[X]$, $f_i \in F$, such that the head terms $\mathsf{HT}(g_i * f_i * h_i)$ are all the same within the representation. Then, on one hand the respective $\mathsf{HC}(g_i * f_i * h_i)$ can add up to zero, which means that the sum of the head coefficients is in an appropriate module generated by the $\mathsf{HC}(f_i)$; m-polynomials[7] are related to these situations. If the result is not zero the sum of the $\mathsf{HC}(g_i * f_i * h_i)$ can be described in terms of a Gröbner basis of the $\mathsf{HC}(f_i)$; g-polynomials are related to these situations. Zero divisors in the reduction ring occur as a special instance of m-polynomials where $F = \{f\}$ and $\alpha * f * \beta$, $\alpha, \beta \in \mathsf{R}$ are considered.

In case R is a commutative or one-sided reduction ring the first problem is related to solving linear homogeneous equations in R and to the existence of finite bases of the respective modules. In case we want effectiveness, we have to require that these bases are computable. This becomes more complicated for non-commutative two-sided reduction rings, as the equations are no longer linear and we have to distinguish right and left multipliers simultaneously. In some cases the problem for two-sided ideals can be translated into the one-sided case and hence solved via one-sided reduction techniques (Kandri-Rody and Weispfenning [7]).

The g-polynomials can be finitely described whenever finite Gröbner bases exist. Here, if we want effectiveness, we have to require that a Gröbner basis as well as representations for its elements in terms of the generating set are computable.

Then using m- and g-polynomials, Gröbner bases can be characterized similarly to the characterizations in terms of syzygies (a direct generalization of the approaches by Kapur and Narendran [6] respectively Möller [14]). In case the respective terms $\mathsf{HT}(g_i * f_i * h_i)$ give rise only to finitely many m- and g-polynomials, these situations can be localized to finitely many terms —to the least common multiples of the $\mathsf{HT}(f_i)$, i.e. the maximal term when $f_i \in \mathsf{R}[X]$— and we can provide a completion procedure based on this characterization which will indeed compute a finite Gröbner basis if R is Noetherian. In principal ideal

[7] Explicit definitions of m- and g-polynomials will be provided in the next section.

rings, where the function gcd (greatest common divisor) is defined, it is sufficient to consider sets F of size 2.

We will give the details of this approach for right reduction rings and the more general case of monoid rings in the next section.

6. Monoid rings over reduction rings

While polynomial rings over Noetherian reduction rings are again reduction rings, this cannot be achieved for the more general case of monoid rings. Already "non-commutative polynomial rings" over fields as presented by Mora [15], which are in fact free monoid rings, give us negative results concerning the existence of finite Gröbner bases for finitely generated two-sided ideals due to the fact that they are closely related to the word problem for monoids (Kandri-Rody and Weispfenning [7], Reinert [18] and Madlener and Reinert [11]). However, when restricting the focus to one-sided ideals in this special setting, the existence of finite one-sided Gröbner bases can be shown (Mora [15]).

Hence, we will restrict our attention to monoid rings over a right reduction ring $(\mathsf{R}, \Longrightarrow)$ satisfying (A4) and provide a characterization of right Gröbner bases for finitely generated right ideals in this setting —the case of left ideals in monoid rings over left reduction rings with (A4) being similar.

Given a cancellative[8] monoid $\mathcal{M}$ with multiplication $\circ$, we call $\mathsf{R}[\mathcal{M}]$ the monoid ring over R with elements presented as "polynomials" $f = \sum_{t \in \mathcal{M}} \alpha_t \cdot t$ where only finitely many coefficients are non-zero. The elements $\alpha_t \cdot t$ are called monomials, consisting of a coefficient $\alpha_t \in \mathsf{R}$ and a term $t \in \mathcal{M}$. 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 $\gamma_t = \sum_{x \circ y = t} \alpha_x \cdot \beta_y$. Assuming a total well-founded ordering $\succ$ on $\mathcal{M}$, the usual notions as $\mathsf{HT}(p)$, $\mathsf{HC}(p)$, and $\mathsf{HM}(p)$ are defined for $p \in \mathsf{R}[\mathcal{M}] \setminus \{0\}$. For a subset F of $\mathsf{R}[\mathcal{M}]$ we call the set $\mathsf{ideal}_r(F) = \{\sum_{i=1}^{n} f_i * (\alpha_i \cdot w_i) \mid n \in \mathbb{N}, \alpha_i \in \mathsf{R}, f_i \in F, w_i \in \mathcal{M}\}$ the *right ideal* generated by F in $\mathsf{R}[\mathcal{M}]$.

As before, we define a partial ordering on R by setting for $\alpha, \beta \in \mathsf{R}$, $\alpha >_{\mathsf{R}} \beta$ if and only if there exists a finite set $B \subseteq \mathsf{R}$ such that $\alpha \overset{+}{\Longrightarrow}_B \beta$. This ordering can be extended to an ordering on $\mathsf{R}[\mathcal{M}]$ as follows. For $f, g \in \mathsf{R}[\mathcal{M}]$, $f > g$ if and only if either $\mathsf{HT}(f) \succ \mathsf{HT}(g)$ or $(\mathsf{HT}(f) = \mathsf{HT}(g)$ and $\mathsf{HC}(f) >_{\mathsf{R}} \mathsf{HC}(g))$ or $(\mathsf{HM}(f) = \mathsf{HM}(g)$ and $\mathsf{RED}(f) > \mathsf{RED}(g))$. Notice that the ordering in general is neither total nor Noetherian on $\mathsf{R}[\mathcal{M}]$.

[8] In case we allow arbitrary monoids we have to be more careful in defining right reduction and critical situations corresponding to it.

Definition 6.1. Let p, f be two non-zero polynomials in $\mathsf{R}[\mathcal{M}]$. We say that f *right reduces* p to q at a monomial $\alpha \cdot t$ in p in one step, denoted by $p \longrightarrow^{\mathrm{r}}_{f} q$, if

(a) $\mathsf{HT}(f * w) = \mathsf{HT}(f) \circ w = t$ for some $w \in \mathcal{M}$,
(b) $\alpha \Longrightarrow_{\mathsf{HC}(f)} \beta$, i.e. $\alpha = \beta + \mathsf{HC}(f) \cdot \gamma$, $\gamma \in \mathsf{R}$ and
(c) $q = p - f * (\gamma \cdot w)$.

While reduction needs no longer eliminate the occurrence of a term, it is Noetherian when using a fixed *finite* set of polynomials due to Axiom (A1) for $\Longrightarrow$ (compare Section 5). It is easy to see that (A2)–(A4) also hold and we can define Gröbner bases as before:

Definition 6.2. A set $G \subseteq \mathsf{R}[\mathcal{M}]$ is called a *right Gröbner basis* of $\mathfrak{i} = \mathsf{ideal}_r(G)$, if $\overset{*}{\longleftrightarrow}^{\mathrm{r}}_{G} = \equiv_{\mathfrak{i}}$, and $\longrightarrow^{\mathrm{r}}_{G}$ is convergent.

Notice that, contrary to the polynomial ring cases, $p * (\alpha \cdot w) \longrightarrow^{\mathrm{r}}_{p} 0$ will not hold in general since the ordering on $\mathcal{M}$ will not be necessarily compatible with the multiplication in $\mathcal{M}$, i.e., in general $\mathsf{HT}(p * w) \neq \mathsf{HT}(p) \circ w$. In fact, for groups it cannot be admissible and well-founded at the same time unless the group is trivial. To repair this phenomenon which leads to $\overset{*}{\longleftrightarrow}^{\mathrm{r}}_{G} \neq \equiv_{\mathsf{ideal}_r(G)}$ in general we introduce the concept of saturation.

Definition 6.3. A set of polynomials $F \subseteq \{p * (\alpha \cdot w) \mid \alpha \in \mathsf{R}^*, w \in \mathcal{M}\}$ is called a (right) *saturating set* for a polynomial $p \in \mathsf{R}[\mathcal{M}]$, if for all $\alpha \in \mathsf{R}$, $w \in \mathcal{M}$, $p*(\alpha \cdot w) \longrightarrow^{\mathrm{r}}_{F} 0$ holds in case $p*(\alpha\cdot w) \neq 0$. A set F of polynomials in $\mathsf{R}[\mathcal{M}]$ is called (right) *saturated*, if $f * (\alpha \cdot w) \longrightarrow^{\mathrm{r}}_{F} 0$ holds for all $f \in F$, $\alpha \in \mathsf{R}$, $w \in \mathcal{M}$ in case $f * (\alpha \cdot w) \neq 0$.

We do not go into the details of when finite saturated sets exist and how they can be computed (see e.g. in Reinert [18] or Madlener and Reinert [10]). In order to characterize right Gröbner bases we now introduce special polynomials.

Definition 6.4. Let $P = \{p_1, \ldots, p_k\}$ be a set of polynomials in $\mathsf{R}[\mathcal{M}]$ and t an element in $\mathcal{M}$ such that there are $w_1, \ldots, w_k \in \mathcal{M}$ with $\mathsf{HT}(p_i * w_i) = \mathsf{HT}(p_i) \circ w_i = t$, for all $1 \leq i \leq k$. Further, let $\gamma_i = \mathsf{HC}(p_i)$ for $1 \leq i \leq k$[9]. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a right Gröbner basis of $\{\gamma_1, \ldots, \gamma_k\}$ and

$$\alpha_i = \gamma_1 \cdot \beta_{i,1} + \ldots + \gamma_k \cdot \beta_{i,k}$$

for $\beta_{i,j} \in \mathsf{R}$, $1 \leq i \leq n$, and $1 \leq j \leq k$. Notice that the α_i respectively the $\beta_{i,j}$ do not depend on t. Then we define the *g-polynomials (Gröbner polynomials)*

[9] Note that this definition has to be modified for non-cancellative monoids, as then $\mathsf{HT}(p * w) = \mathsf{HT}(p) \circ w$ no longer implies $\mathsf{HC}(p * w) = \mathsf{HC}(p)$.

corresponding to P and t by setting

$$g_i = \sum_{j=1}^{k} p_j * (\beta_{i,j} \cdot w_j) \text{ for each } 1 \leq i \leq k.$$

Notice that $\mathsf{HM}(g_i) = \alpha_i \cdot t$.

For the right module $M = \{(\delta_1, \dots, \delta_k) \mid \sum_{i=1}^{k} \gamma_i \cdot \delta_i = 0\}$, let the set $\{A_i \mid i \in I \subseteq \mathbb{N}\}$ be a basis with $A_i = (\alpha_{i,1}, \dots, \alpha_{i,k})$ for $\alpha_{i,j} \in \mathsf{R}$, $i \in I$, and $1 \leq j \leq k$. Notice that the A_i do not depend on t. Then we define the *m-polynomials (module polynomials) corresponding to P and t* by setting

$$m_i = \sum_{j=1}^{k} p_j * (\alpha_{i,j} \cdot w_j) \text{ for each } i \in I.$$

Notice that $\mathsf{HT}(m_i) \prec t$.

Since R is a right reduction ring the number of g-polynomials related to P and t is finite. If in R every right module of solutions to linear homogeneous equations is finitely generated, the number of m-polynomials related to P and t is finite.

Definition 6.5. Given $F \subseteq \mathsf{R}[\mathcal{M}]$, the *set of g- and m-polynomials corresponding to F* contains for each finite subset $P \subseteq F$ and each term $t \in \mathcal{M}$ the g- and m-polynomials as specified in Definition 6.4.

For a set consisting of one polynomial the corresponding m-polynomials reflect the multiplication of the polynomial with zero-divisors of the head coefficient, i.e., by a basis of the annihilator of the head coefficient.

We can use g- and m-polynomials to characterize special bases in monoid rings over a reduction ring in case they are additionally saturated.

Theorem 6.6. *For a finite saturated subset F of $\mathsf{R}[\mathcal{M}]$ the following statements are equivalent:*

1. *For all polynomials $g \in \mathsf{ideal}_r(F)$ we have $g \xrightarrow{*}{}^{\mathrm{r}}_{F} 0$.*
2. *F is a right Gröbner basis of $\mathsf{ideal}_r(F)$.*
3. *All g-polynomials and all m-polynomials corresponding to F right reduce to zero using F.*

Proof.

$1 \Longrightarrow 2$: The inclusion $\xleftrightarrow{*}{}^{\mathrm{r}}_{F} \subseteq \equiv_{\mathsf{ideal}_r(F)}$ is obvious. Hence, let us assume $f \equiv_{\mathsf{ideal}_r(F)} g$, i.e., $f - g \in \mathsf{ideal}_r(F)$ and, therefore, $f - g \xrightarrow{*}{}^{\mathrm{r}}_{F} 0$. We show that this implies $f \xleftrightarrow{*}{}^{\mathrm{r}}_{F} g$. In case $f - g = 0$ we are immediately done. Hence, let us assume $f - g \neq 0$ and, as any polynomial in $\mathsf{ideal}_r(F)$ is right reducible to zero using F, without loss of generality we can assume that the reduction sequence $f - g \xrightarrow{*}{}^{\mathrm{r}}_{F} 0$ uses top-reduction, i.e., all reductions take place at the respective head monomial. Further, let $t = \mathsf{HT}(f - g)$ and let γ_1, respectively γ_2, be the coefficients of t in f, respectively g. We will now show that $f \xleftrightarrow{*}{}^{\mathrm{r}}_{F} g$ holds by induction on the term $t = \mathsf{HT}(f-g)$. In case $t = \lambda$ we find $f-g = \gamma_1 - \gamma_2 \xrightarrow{*}{}^{\mathrm{r}}_{F} 0$ and by lemma 2.5 the finite set $C_F(\lambda) = \{\mathsf{HC}(f) \mid f \in F, \lambda = \mathsf{HT}(f * z) = \mathsf{HT}(f) \circ z$ for some $z \in \mathcal{M}\} \subseteq \mathsf{R}$ is a Gröbner basis of $\mathsf{ideal}^{\mathsf{R}}_r(C_F(\lambda))$. Hence, as $\gamma_1 - \gamma_2 \in \mathsf{ideal}^{\mathsf{R}}_r(C_F(\lambda))$, $\gamma_1 \equiv_{\mathsf{ideal}^{\mathsf{R}}_r(C_F(\lambda))} \gamma_2$ implies $\gamma_1 \overset{*}{\Longleftrightarrow}_{C_F(\lambda)} \gamma_2$. Using the respective polynomials belonging to the elements in $C_F(\lambda)$, we get $f \xleftrightarrow{*}{}^{\mathrm{r}}_{F} g$. Now let us assume $t \succ \lambda$ and $f - g \xrightarrow{k}{}^{\mathrm{r}}_{F} h$ where $k \in \mathbb{N}^+$ is minimal such that $\mathsf{HT}(h) \neq t$. Further, let $f_1, \ldots, f_k$ be the polynomials used in the respective reduction steps, i.e., $\gamma_1 - \gamma_2 \overset{*}{\Longrightarrow}_{\{\mathsf{HC}(f_i) \mid 1 \leq i \leq k\}} 0$. Again, since

$$\begin{aligned} &C_F(t) = \\ &\quad \{\mathsf{HC}(f) \mid f \in F,\ t = \mathsf{HT}(f) \circ z \text{ for some } z \in \mathcal{M}, \mathsf{HT}(f * z) = \mathsf{HT}(f) \circ z\} \end{aligned}$$

is a finite right Gröbner basis of $\mathsf{ideal}^{\mathsf{R}}_r(C_F(t))$ and $\{\mathsf{HC}(f_i) \mid 1 \leq i \leq k\} \subseteq C_F(t)$, we find $\gamma_1 \overset{*}{\Longleftrightarrow}_{C_F(t)} \gamma_2$. Now applying the polynomial multiples belonging to the elements of $C_F(t)$ used in this last sequence to the monomial with term t in f, we find an element $\tilde{f} \in \mathsf{R}[\mathcal{M}]$ such that $f \xleftrightarrow{*}{}^{\mathrm{r}}_{F} \tilde{f}$, $\mathsf{HM}(\tilde{f}) = \gamma_2 \cdot t$, $\tilde{f} - g \in \mathsf{ideal}_r(F)$, and $t \succ \mathsf{HT}(\tilde{f} - g)$. Hence, our induction hypothesis yields $g \xleftrightarrow{*}{}^{\mathrm{r}}_{F} \tilde{f} \xleftrightarrow{*}{}^{\mathrm{r}}_{F} f$ and we are done.

It remains to show that right reduction using F is confluent. Suppose there is a polynomial g having two distinct normal forms with respect to F, say p_1 and p_2. Let t be the largest term on which p_1 and p_2 differ and let α_1 respectively α_2 be the coefficients of t in p_1 respectively p_2. Since $p_1 - p_2 \in \mathsf{ideal}_r(F)$ we know $p_1 - p_2 \xrightarrow{*}{}^{\mathrm{r}}_{F} 0$ and $\alpha_1 - \alpha_2 \in \mathsf{ideal}^{\mathsf{R}}_r(C_F(t))$, and $C_F(t)$ is a right Gröbner basis. Hence, $\alpha_1 \overset{*}{\Longleftrightarrow}_{C_F(t)} \alpha_2$, and either α_1 or α_2 must be reducible using $C_F(t)$, i.e., not both p_1 and p_2 can be in normal form with respect to F, contradicting our assumption.

$2 \Longrightarrow 3:$ This follows from the fact that all g- and m-polynomials belong to the right ideal generated by F.

$3 \Longrightarrow 1:$ We have to show that every element $g \in \mathsf{ideal}_r(F) \setminus \{0\}$ is right reducible to zero using F. Remember that for $h \in \mathsf{ideal}_r(F)$, $h \longrightarrow^{\mathrm{r}}_{F} h'$ implies $h' \in \mathsf{ideal}_r(F)$. Thus, as $\longrightarrow^{\mathrm{r}}_{F}$ is Noetherian since F is finite, it suffices to show that every $g \in \mathsf{ideal}_r(F) \setminus \{0\}$ is right reducible using F. This will be done by assuming the contrary. Let $g = \sum_{j=1}^{m} f_j * (\gamma_j \cdot w_j)$ with $\gamma_j \in \mathsf{R}^*, f_j \in F, w_j \in \mathcal{M}$

be a representation of a polynomial $g \in \mathsf{ideal}_r(F) \setminus \{0\}$. As F is saturated, we can always assume $\mathsf{HT}(f_i * (\gamma_i \cdot w_i)) = \mathsf{HT}(f_i) \circ w_i$. Depending on this representation of g and the well-founded total ordering $\succeq$ on $\mathcal{M}$ we define the *critical term* of g to be $t = \max\{\mathsf{HT}(f_j) \circ w_j \mid j \in \{1, \dots m\}\}$. We call another representation of g "smaller" if for the corresponding critical term $\tilde{t}$ we have $\tilde{t} \prec t$. Let us assume that our polynomial g is not right reducible by F and that our representation of g is a minimal one with respect to t. We have to distinguish two cases. In case $t \neq \mathsf{HT}(g)$, without loss of generality assume that t occurs in the first k products of our representation. Hence, we have $\mathsf{HT}(f_i) \circ w_i = t$ for each $1 \leq i \leq k$ and $\sum_{i=1}^{k} \mathsf{HC}(f_i) \cdot \gamma_i = 0$, i.e., the vector $(\gamma_1, \dots, \gamma_k)$ is in the right module $M = \{(\alpha_1, \dots, \alpha_k) \mid \sum_{i=1}^{k} \mathsf{HC}(f_i) \cdot \alpha_i = 0\}$. By our assumption this module has been considered when generating the m-polynomials for $\{f_1, \dots, f_k\}$ and t. Let the set $B = \{A_i = (\alpha_{i,1}, \dots, \alpha_{i,k}) \mid i \in I\}$ be a basis of M. Without loss of generality, we assume that there are $A_1, \dots, A_n \in B$ such that for $1 \leq i \leq k$ we have $\gamma_i = \sum_{j=1}^{n} \alpha_{j,i} \cdot \delta_j$ for some $\delta_j \in R$. Thus, we get

$$\begin{aligned}\sum_{i=1}^{k} f_i * (\gamma_i \cdot w_i) &= \sum_{i=1}^{k} f_i * ((\sum_{j=1}^{n} \alpha_{j,i} \cdot \delta_j) \cdot w_i) \\ &= \sum_{j=1}^{n} (\sum_{i=1}^{k} f_i * (\alpha_{j,i} \cdot w_i)) \cdot \delta_j\end{aligned} \tag{1}$$

Taking a closer look at the last sum of these transformations in (1), we see that we can express the sum of the first k elements of our representation of g by a sum of m-polynomials. Since these m-polynomials belonging to $\{f_1, \dots, f_k\}$ and t all have head terms smaller than t and are right reducible to zero using F, we get a new representation of g with a critical term smaller than t, contradicting our assumption that our chosen representation was minimal.

In case $t = \mathsf{HT}(g)$, we know that there exists a finite subset $P \subseteq F$ such that $\mathsf{HC}(g) \in \mathsf{ideal}^{\mathsf{R}}(\{\mathsf{HC}(p) \mid p \in P\})$, and as this ideal is finitely generated it has a right Gröbner basis, say G_P. Then $\mathsf{HC}(g)$ is reducible by an element $\alpha \in G_P$. By our assumption, now $\alpha \cdot t$ is head monomial of a g-polynomial corresponding to P and t and since this g-polynomial is right reducible to zero using F, in particular there exist polynomials $f_1, \dots, f_k \in F$ involved in the reduction of $\alpha \cdot t$ such that $\alpha \Longrightarrow_{\mathsf{HC}(f_1)} \alpha_1 \Longrightarrow_{\mathsf{HC}(f_2)} \dots \Longrightarrow_{\mathsf{HC}(f_k)} 0$. We will now show that this implies that $\mathsf{HM}(g)$ is right reducible using F, by induction on k. For $k = 1$ we find $\mathsf{HC}(g) \Longrightarrow_{\alpha}$ and $\alpha \Longrightarrow_{\mathsf{HC}(f_1)} 0$, and hence Axiom (A4) implies $\mathsf{HC}(g) \Longrightarrow_{\mathsf{HC}(f_1)}$, i.e., g is right reducible at $\mathsf{HM}(g)$ using $f_1 \in F$. Now let $k > 1$. Then by Axiom (A4), $\mathsf{HC}(g)$ is either reducible by $\mathsf{HC}(f_1)$ or by α_1. This again gives us a contradiction, as either g is right reducible at $\mathsf{HM}(g)$

using $f_1 \in F$ or the induction hypothesis can be applied to α_1 and $f_2, \dots, f_k$. ☑

We have already determined when for a finite set of polynomials P and a term t the respective sets of g- and m-polynomials described in Definition 6.4 are finite. However, these conditions do not imply that the set of polynomials to be tested in Theorem 6.6 (3) will be finite due to the fact that in general infinitely many terms t have to be considered (compare Definition 6.5). Hence it is important to find a localization to crucial term overlaps, similar to the case of s-polynomials in commutative polynomial rings where only the least common multiple of the head terms has to be considered. In our setting, the key idea are suitable weakenings of the reduction relation: recall that for two reductions $\longrightarrow^1 \subseteq \longrightarrow^2$ with $\overset{*}{\longleftrightarrow}^1 = \overset{*}{\longleftrightarrow}^2$ the confluence of $\longrightarrow^1$ will imply the confluence of $\longrightarrow^2$. To identify such weaker reduction relations we have to take a closer look at the representations of the monoid elements. Remember that monoids can be presented by string rewriting systems (see the book of Book and Otto [4] for more details on string rewriting systems). Henceforth, we will assume that $\mathcal{M}$ is presented by a finite convergent string rewriting system such that the ordering on $\mathcal{M}$ is compatible with the completion ordering of the string rewriting system. This implies that the monoid elements are the irreducible words, the ordering on $\mathcal{M}$ is compatible with concatenation, and multiplication can be done by normal form computation. We can give the following syntactical weakening of right reduction.

Definition 6.7. Let p, f be two non-zero polynomials in $\mathsf{R}[\mathcal{M}]$. We say f *prefix reduces* p to q at a monomial $\alpha \cdot t$ of p in one step, denoted by $p \longrightarrow^{\mathrm{p}}_{f} q$, if

(a) $\mathsf{HT}(f)w \equiv t$ for some $w \in \mathcal{M}$, i.e., $\mathsf{HT}(f)$ is a prefix of t as a word in the generators,
(b) $\alpha \Longrightarrow_{\mathsf{HC}(f)} \beta$, i.e. $\alpha = \beta + \mathsf{HC}(f) \cdot \gamma$, $\gamma \in \mathsf{R}$, and
(c) $q = p - f * (\gamma \cdot w)$.

Then term overlaps correspond to common prefixes of words and in defining g- and m-polynomials we can restrict the attention to minimal such situations giving rise only to finitely many such candidates for a set F. This localization is possible because for prefixes and concatenation our ordering on $\mathcal{M}$ behaves admissible, i.e. $t \succ u$ and $t \circ w \equiv tw$ implies $tw \succ u \circ w$ for $t, u, w \in \mathcal{M}$. For more details see Reinert [18] and Madlener and Reinert [9, 12]. In substituting prefix saturation for saturation and prefix reduction for right reduction, Theorem 6.6 can be specialized to characterize prefix Gröbner bases, which are of course right Gröbner bases of the same right ideal.

Now, if $(\mathsf{R}, \Longrightarrow)$ is an effective reduction ring then addition and multiplication in $\mathsf{R}[\mathcal{M}]$ as well as reduction as defined in Definition 6.7 are computable operations.

The existence of finite prefix Gröbner bases can be shown for the classes of finite, respectively free, monoids and the classes of finite, free, plain, respectively context-free, groups. Using different syntactical weakenings of right reduction also finitary results are gained for the class of polycyclic groups (which includes the Abelian and nilpotent groups). The details on these approaches are presented in Reinert [18] and Madlener and Reinert [9, 12]. Hence, all these monoid rings are indeed reduction rings.

It remains to determine when in fact these monoid and group rings are effective right reduction rings: We need that right Gröbner bases and representations of their elements in terms of the elements of the generating set are computable, and that it is possible to compute finite bases for right modules of solutions to linear homogeneous equations over R. With these assumptions the bases are computable in the special cases of monoids and groups mentioned above. In fact they can be computed using completion procedures based on resolving non-trivial g- and m-polynomials.

7. Conclusions

The aim of this paper was to show how, starting with a reduction ring, new reduction rings can be constructed using standard ring constructions such as quotients and sums and extensions to polynomial and monoid rings. This enables us to present many results known from the literature in a uniform setting. Other ring constructions such as skew-polynomial rings, solvable polynomial rings or Ore extensions could be studied in a similar fashion.

On the other hand, reduction relations in arbitrary rings fulfilling the Axioms (A1)–(A3) and (A4) will inherit similar properties resulting directly from the axioms. E.g., when applying the ring constructions of this paper they will yield similar natural reduction relations for the resulting rings. A well-known example is the free monoid ring (also called the non-commutative polynomial ring) where many properties of the reduction relation for commutative polynomial rings carry over, although of course finite Gröbner bases in general will no longer exist.

References

[1] T. Becker & V. Weispfenning, *Gröbner Bases —A Computational Approach to Commutative Algebra,* Springer Verlag, 1992.

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

[3] B. Buchberger, *A Critical-Pair/Completion Algorithm for Finitely Generated Ideals in Rings*, in: Symposium "Rekursive Kombinatorik", Münster (FRG), May 1983. Springer LNCS 171 (1984), 137–161.

[4] R. Book, and F. Otto, *String-Rewriting Systems*, Springer Verlag, 1993.

[5] A. Kandri-Rody and D. Kapur, *Computing a Gröbner Basis of a Polynomial Ideal over a Euclidean Domain*, Journal of Symbolic Computation **6** (1988), 37–57.

[6] D. Kapur and P. Narendran, *Constructing a Gröbner Basis for a Polynomial Ring*, in: J. Avenhaus, K. Madlener (eds): Summary in Proceedings of Combinatorial Algorithms in Algebraic Structures, Otzenhausen. Universität Kaiserslautern, 1985.

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

[8] K. Madlener, *Existence and Construction of Gröbner Bases for Ideals in Reduction Rings*, Working paper, Universität Kaiserslautern, 1986.

[9] K. Madlener and B. Reinert, *Computing Gröbner Bases in Monoid and Group Rings*, in: Proc. ISSAC'93, 1993, 254–263.

[10] K. Madlener and B. Reinert, *String Rewriting and Gröbner Bases —A General Approach to Monoid and Group Rings*, in: Proceedings of the Workshop on Symbolic Rewriting Techniques, Monte Verita, 1995, 127–180.

[11] K. Madlener and B. Reinert. *Relating rewriting techniques on monoids and rings: Congruences on monoids and ideals in monoid rings*, Theoretical Computer Science, **208** (1998), 3–31.

[12] K. Madlener and B. Reinert. *A generalization of Gröbner basis algorithms to polycyclic group rings,* Journal of Symbolic Computation, **25** (1998) 23–43.

[13] K. Madlener and B. Reinert. *Gröbner bases in non-commutative reduction rings*, in B. Buchberger and F. Winkler, editors, *Gröbner Bases and Applications (Proc. of the Conference 33 Years of Gröbner Bases)*, volume 251 of London Mathematical Society Lecture Notes Series, 408–420, Cambridge University Press, 1998.

[14] H. M. Möller, H. M., *On the Construction of Gröbner Bases Using Syzygies*, Journal of Symbolic Computation **6** (1998), 345–359.

[15] F. Mora, *Gröbner Bases for Non-Commutative Polynomial Rings*, in: Proc. AAECC-3, Springer LNCS 229 (1985), 353–362.

[16] L. Pan, *On the Gröbner Bases of Ideals in Polynomial Rings over a Principal Ideal Domain*, University of California, Santa Barbara, Department of Mathematics, Internal Manuscript, 1985.

[17] M. Pesch, *Gröbner Bases in Skew Polynomial Rings*, Doctoral Dissertation, Universität Passau, 1997.

[18] B. Reinert, *On Gröbner Bases in Monoid and Group Rings*, Doctoral Dissertation, Universität Kaiserslautern, 1995.

[19] S. Stifter, *A Generalization of Reduction Rings*, Journal of Symbolic Computation **4** (1987), 351–364.

[20] V. Weispfenning, *Gröbner Basis for Polynomial Ideals over Commutative Regular Rings*, in: Proc. EUROCAL'87, Springer LNCS 378 (1987), 336–347.

(Recibido en octubre de 1998)

Fachbereich Informatik
Universität Kaiserslautern
67663 Kaiserslautern, Germany
madlener@informatik.uni-kl.de
reinert@informatik.uni-kl.de